OWASP SUMMIT 2011
LISBON PORTUGAL
FEB 8-11

Post-Summit Report & Working Session Outcomes

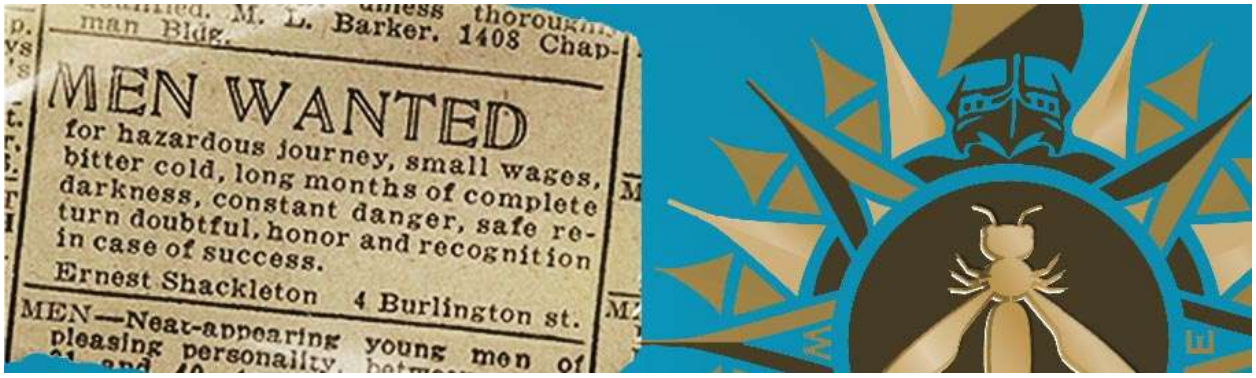
Post-Summit Report and Working Session Outcomes

Documents compiled and report written by Sarah Baso.
Summit design identity, marketing materials, and artwork created by Sarah Cruz.

Last revised July 27, 2011

Send any corrections, comments, or questions to sarah.baso@owasp.org

Table of Contents



Section I: Acknowledgments

While I spent much time planning for the 2011 OWASP Global Summit, as well as compiling this post-summit report and summary of outcomes, the 2011 Summit would not have been possible without the time, energy, and great ideas of many other individuals. On behalf of the all the Summit attendees and those who will benefit from the Summit outcomes and lessons learned in the years to come, I would like to extend my sincere thanks and appreciation to the Summit volunteers and paid support team**.**

Volunteers:

Lorna Alamri	Dinis Cruz	Anastasios Stasinopoulos
Marco Batista	Julio Cesar Fort	John Wilander
Mark Bristow	Martin Knobloch	Doug Wilson
Brad Causey	Jason Li	Stefan Wuensch
Justin Clarke	Linda Potjes	

Paid support team:

Deb Brewer	Sarah Cruz	Sandra Paiva
Paulo Coimbra	Kate Hartmann	Marta Pegorelli

Prior to the Summit, there are a few key individuals who were involved in making the magic happen. I am fortunate to have had such great people to work with: Lorna Alamri, Brad Causey, Justin Clarke, Dinis Cruz, Martin Knobloch, Jason Li, and John Wilander. A special thanks to Jason Li for the uncountable number of sleepless nights he stayed awake with me working on wiki pages, drafting make-shift contracts, and rehashing the budget.

Furthermore, I would like to express my gratitude to all the people that were involved in Summit working sessions – planning the sessions, running the sessions, taking notes during the sessions, and putting together the session outcomes. I am indebted to Paulo Coimbra and Sandra Paiva for all their hard work in the vetting and organization of these sessions into a consumable format for Summit attendees.

I would also like to recognize Mark Bristow and Doug Wilson who stepped up in the days before and during the Summit to coordinate recording the working sessions and setting up the audio visual equipment needed to stream these sessions live to hundreds of remote participants around the world. Without the help of these two stellar guys, the remote participation would probably not have gotten off the ground.

The Summit would not have been possible without the support of the 2010 OWASP Board Members: Tom Brennan, Dinis Cruz, Seba Deleersnyder, Eoin Keary, Matt Tesauro, Dave Wichers, and Jeff Williams who not only voted to allocate a large amount of OWASP Foundation funds to the Summit, but also demonstrated their enthusiasm for the event by all taking time out of their schedules to attend and participate in the working sessions.

Recognition is also due to Dinis Cruz for his guidance and seemingly limitless supply of energy in preparing for and running the Summit. In 2008, Dinis had the idea for an OWASP Summit[1] that would bring together OWASP leaders and application security experts from around the world to engage in working sessions. He spearheaded the OWASP EU Summit in 2008 and then built and improved upon his model in 2011 with the OWASP Global Summit. While many of his ideas and lofty aspirations for the event seemed crazy at times, Dinis's enthusiasm and faith in the summit concept brought about the great sentiments and outcomes we have today surrounding the event.

Last but not least I would like to give a HUGE thank you to Alison Shrader, OWASP's accountant, for her infinite patience in reconciling the Summit budget. Alison not only kept track of all the budget reallocations between various OWASP accounts, but also made sure that the various Summit bills and venues were paid in a timely fashion. Most significantly for me, Alison was calm and tolerant in dealing with my complicated and colorful spreadsheets that often times were based on shorthand that only I understood.

Thank you to everyone that made this great event possible!

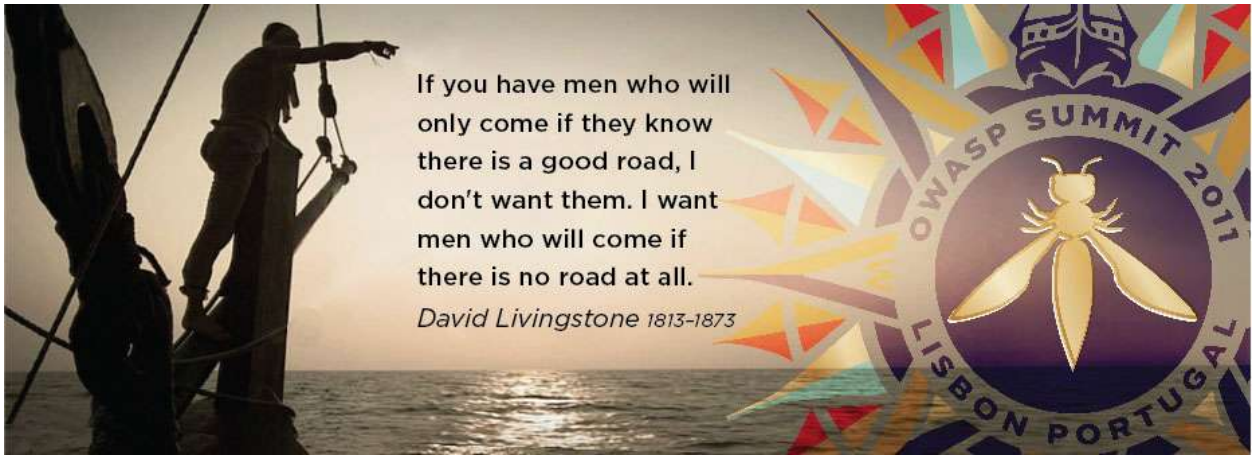
Sarah Baso
OWASP 2011 Global Summit Support Team

[1] For details on the OWASP Summer of Code 2008 initiative: https://www.owasp.org/index.php/OWASP_Summer_of_Code_2008

Section II: About OWASP

The Open Web Application Security Project (OWASP) is a worldwide free and open community dedicated to improving the security of application software worldwide. OWASP's mission is to make application security visible so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. Find out more at www.owasp.org.

Reader Contact Information:
OWASP Foundation, 9175 Guilford Road, Suite #300; Columbia, MD 21046, Tel: (301) 275-9403, Fax: (301) 604-8033, www.owasp.org, kate.hartmann@owasp.org



Section III: About OWASP Summits

OWASP Summits are where application security experts can meet in a neutral, non-commercial setting to discuss plans, projects and solutions for the future of application security.

OWASP Summits are NOT conferences - there are no talks or training seminars. An OWASP Summit is an opportunity to do actual work to further the field of application security. Participants stay in shared accommodations and collaborate to produce tangible progress towards influencing standards, establishing roadmaps, and setting the tone for OWASP and application security for the coming years.

Anyone can attend an OWASP Summit! OWASP community members, application security experts, industry players, and developers are all welcome at OWASP Summits. Attendees come ready to work and produce deliverables that advance the state-of-the-art in application security.

Section IV: Summary of 2011 Summit Outcomes

The 2011 OWASP Global Summit took place February 8-11 at Campo Real Resort outside of Lisbon, Portugal. Over 180 application security experts from over 120 companies, 30 different countries[2], and representing 44 local OWASP chapters[3], joined forces to plan, build, and execute initiatives aimed at improving the security of the world's software applications. The Summit was a significant step towards OWASP's mission to ensure all types of organizations are empowered to build, select, and use software applications securely.

As a result of this event, OWASP launched and advanced dozens of concrete initiatives to bring application security to governments, educational institutions, browser vendors, standards bodies, software development teams, and mobile platform vendors.

Some highlights from the 2011 OWASP Summit include:

- **OWASP-Portugal Partnership** – OWASP has been working to establish relationships with various governments around the world, particularly the United States, Brazil, Portugal, and Greece. At the Summit, OWASP representatives worked directly with senior Portuguese IT officials to establish a protocol for working with Portugal to improve their application security capabilities.

- **OWASP Outreach to Educational Institutions** – Reaching students is a unique opportunity to reach developers early in their development. At the Summit, delegates drafted an OWASP Code of Conduct for Educational Institutions, created a detailed plan for OWASP Student Chapters and continued development of the OWASP "Academies" Portal with extensive education and training materials.

- **OWASP Industry Outreach** – OWASP resolved to develop industry working sessions to be held at major OWASP conferences starting with OWASP EU 2011 in Dublin, Ireland. The objective of these sessions will be to solicit feedback from industry players to help better focus OWASP efforts and make sure OWASP deliverables are relevant to industry concerns.

[2] List of countries appears in the Appendix.

[3] List of local OWASP chapters appears in the Appendix.

- **OWASP Browser Security Project** – The Summit brought representatives from browser vendors Mozilla, Google, and Microsoft together with leading security researchers to discuss, and strategize about browser security issues. Several new OWASP initiatives were launched, including a browser security scorecard project based on OWASP's recently created browser testing framework. There were extensive discussions on browser initiatives such as Mozilla's Content Security Policy (CSP) and browser sandboxes.

- **OWASP-Apache Partnership** – OWASP forged a relationship with the Apache Software Foundation (ASF) to start the process of sharing OWASP software projects with the ASF with the intention of including OWASP-provided code in Apache projects. The intention of this collaboration is to improve the security of the widely-used ASF Open Source software, as well to improve visibility for OWASP efforts.

- **OWASP Mobile Security Initiative** – OWASP made progress on their upcoming Top 10 Mobile Vulnerabilities and Top 10 Mobile Defenses lists. In addition, OWASP resolved to reach out to mobile platform vendors to work with them on integrating better security into their environments.

- **OWASP Governance Expansion** – OWASP updated its Charter and worked out procedures for the upcoming Board elections. These governance updates will help best support the dynamic and growing OWASP community.

- **International Focus** – OWASP reaffirmed a commitment to be a truly international organization. Delegations from several countries and regions around the world including Asia-Pacific and South America participated in outreach workshops. Addition focus has been given to expanding international representation on OWASP's Board and Global Committees.

- **Application Security Programs** – To help organizations actually implement application security programs, we are mapping OWASP projects to all major approaches, including OWASP OpenSAMM, Microsoft's SDL, and BSIMM.

- **Application Security Certification** – OWASP reaffirmed its commitment to avoid becoming a certification body. Instead, it created the OWASP Code of Conduct for Certification Bodies that defines what application security certification program should entail.

Section V: OWASP Summit Background

The OWASP Summit EU 2008

At the OWASP Summit EU 2008[4] over 80 OWASP leaders and key industry players from 20 countries gathered to present and discuss the latest OWASP tools and documentation projects. In addition to the 40+ presentations from the OWASP Leaders, the Summit hosted multiple working sessions designed to improve collaboration, achieve specific objectives and decide roadmaps for OWASP projects, chapters, and the OWASP community itself.

The key results from the 2008 Summit included:

- Updated OWASP Principles
- Updated Code of Ethics
- New Outreach Programs
- New Global Committee Structure
- New Free Tools and Guidance

2008 Summit Finances

The total amount spent by the OWASP Foundation on the 2008 Summit was **$135,978.93**.[5] This amount covered the flights, accommodation, food, and conference ticket for 71 people; the accommodation, food and conference ticket for three more people; and the food and conference ticket for two more. In total, the OWASP Foundation paid for some (if not all) of the expenses for 76 people to attend the Summit.

Category	**Cost**
Summit Travel Costs	$66,889.56
Venue & Accommodations Costs	$58,018.12
Summit Equipment & Services	$9,564.48
Summit Support Staff	$960.00
Miscellaneous	$6,337.91
Banking & Currency Corrections	$ 498.90
SUBTOTAL	$142,268.97
Income - Reimbursements/Donations	- $6,290.04
TOTAL	**$135,978.93**

[4] The OWASP Summit EU 2008 took place November 3rd-7th and was hosted at the Grande Real Santa Eulalia resort in Algarve Portugal. For more details on the 2008 Summit:
https://www.owasp.org/index.php/OWASP_EU_Summit_2008

[5] A chart with a general breakdown of Summit expenses appears below, details appear in the Appendix.

Lessons Learned from the 2008 Summit

Location:

- The 2008 Summit in Portugal was held in Albufeira/Faro/Algarve which required a lot of attendees to catch at least two flights (and in some case have to extend the trip by one or two days). One of the chief complaints by attendees was location - it did not take place in/near a hub city

Scheduling of Working Sessions:

- There are a number of critical pieces of information required to create a really effective schedule that are only known (or finalized) in the last couple days/week before the Summit.
- It is possible to create a dynamic working schedule a couple of days before the start of the Summit. This is not to say that the goal is to wait until last minute to start working on the schedule, only that last minute changes will likely be necessary and so the final schedule should only be published a couple day(s) before.
- New ideas for working sessions will appear when attendees focus on the Summit (which in 2008 only happened after the attendees arrived). Try to encourage/facilitate/reward attention to the Summit working sessions before the start of the Summit, but also find a way to facilitate those sessions that spring up during the course of the event.
- In order to counter the perception of a chaotic schedule and event that is associated with schedule changes, it is important to have no schedule changes after 1pm Monday (the day before the Summit starts).
- Creating a personalized schedule for each attendee is critical; it makes a big difference for attendees and it keeps the schedule team focused.
- Don't start the main sessions and keynotes at 9:00am. At the 2008 Summit, the planning team had to push the schedule 30m forward since it would had not been fair to the OWASP leaders that worked so hard on their projects and only had 50% of the Summit attendees there. (In the future, possibly put smaller working sessions starting at 9:00am so that if people miss that session they are shooting themselves in the foot).

Food and Beverages:

- “Working” lunches worked quite well. (This is not to say that the planning team should put that as part of the schedule, but if the attendees are so passionate on the working sessions they are involved in, that they still want to continue the conversation over lunch the planning team should be prepared to accommodate.)
- Beer/wine delivery at 4pm was a massive success. In 2008, the hotel crew (plus the Summit Staff) would appear in the main working session rooms around 4 pm with a massive bucket of cold beers and wines, which was then distributed to the attendees.
- We need to provide dinner and beverages/beer to all attendees. This was something that the planning team was not counting on doing in 2008, but it proved completely impractical (and expensive for the attendees) NOT to do it. It ended up working great to use the villas for serving/eating dinner, especially since the working session conversations continued over dinner and into the night.

- Make sure to provide enough food and drinks. Most of the attendees not only showed up on time for the morning sessions, but also stayed up talking about OWASP on the villas until 1am (if not later).

OWASP Mini Summit at AppSec DC 2009

On November 11th 2009, as part of OWASP AppSec DC 2009 November 10-13th, OWASP chapter leaders, committee members, project leaders and OWASP members gathered in Washington DC to discuss the latest OWASP tools, documentation projects and set the application security agenda for 2010. This was a one track, one day event in which each of the Global Committees gave a report of their progress since the 2008 Summit. Additionally, the 2009 Board of Directors Election was officially launched and each of the candidates was time to say a few words about themselves. The day concluded with a recap on what the OWASP Foundation as a whole accomplished in the one year since the previous summit and what the organizations goals were for the upcoming year.

2009 Summit Finances

The total amount spent on the 2009 Mini Summit was **$19,048.11**, of which the primary expenses were $2,000 for the meeting space and $13,369 for catering/food costs. Additional costs included a videographer ($632) and approximately $3000 to cover the hotel costs of one attendee and the flight and hotel of another.

Lessons Learned from the 2009 Summit

The primary goal of this Mini Summit was to communicate about OWASP internal governance and provide those that attended with an OWASP "State of the Union." While having the Mini Summit alongside the OWASP AppSec DC conference worked ok for committees to present on their progress, the format would not have worked well for a summit with working sessions similar to that which took place in 2008. First, the conference provides too many distractions for people attending the working session to get actual work done. Also, part of the "chemistry" of the Summit is the bonding that just the Summit attendees have outside of the working sessions themselves. A conference atmosphere does not lend itself to this process.

Section VI: OWASP Global Summit 2011 Operational Details

Summit Preparation

** Author's Note: The goal of this section was not to narrate every detail of the planning process, recap the reasoning behind every decision that was made, or even to serve as a handbook for planning future Summits. Instead, the purpose was to provide an overview of the critical stages of planning for the event and a historical record of hurdles that were encountered along the way. Also, almost all of the information contained in this section can be found on the Global Summit mailing list, of which the archives are publicly available.*[6]

Gathering a Team

The 2011 Summit Planning Committee started to come together in early August, 2010. Dinis Cruz led the Committee, which also included Justin Clarke, Martin Knobloch, and John Wilander. A couple of weeks later Brad Causey joined, then after learning about the Summit at AppSec USA in Irvine, Lorna Alamri decided to help out. Jason Li joined mid-September and in late October Dinis solicited the help of Sarah Baso and Tara Causey (who withdrew from the Committee December 1 due to personal time constraints).

Initial Planning Steps

One of the first stages of the Summit planning process was to discuss who would be invited, where and when the event would be located, what the initial and projected budgets would be, and what defined a "successful" summit:

- Target attendees: Board Members and Global Committee Members.
- Summit timing: 3-4 days sometime between mid-January and mid-February.
- Summit location: No exact location, but a number of criteria were established
    - Someone to serve as a local liaison and stay in close contact with the venue
    - Ability to host 30-100 people
    - Cost per attendee not to exceed $2,000 USD (flight/accommodation/meals)
    - Conference facilities – multiple small meeting rooms and one big meeting room
    - Apartments or villas if possible (to share living space and save money)
    - 4 to 5 star hotel (with conference facilities in hotel or within walking distance)
    - Maximum 50 km from International Airport (Hub)
    - Ability to provide sufficient internet access
- Budget projections : $150,000 ($50,000 from OWASP and $100,000 from outside sponsors)
- Summit "success" factors:
    - Break even financially
    - Establish that Summits are the place to go to discuss web application security and do actual work
    - Review of OWASP's last year
    - Conduct working sessions on committees, projects, education, and industry sectors such as the browsers and frameworks
    - Setup/Conduct a Board election
    - Address strategic OWASP issues
    - Create a roadmap and action plans for the next 12 months

[6] https://lists.owasp.org/pipermail/owasp-summit-2011

On 30-Aug-2010 the Board approved $50,000 as initial funding for the Summit. The money had been set aside for a possible 2010 Summit to occur again at AppSec DC; when plans changed the Board reallocated the funds to the 2011 Summit initiative. Dave Wichers, one of the Board Members, supported the allocation of $50,000 but noted that if the planning committee was not able to get the additional $100,000 necessary to pay for the summit (projection based on 2008) through sponsorship, they should consider scaling back or delaying the summit to make it more cost affordable to OWASP and valuable to the participants.

Picking a Location

Lorna Alamri, on behalf of the Summit Planning Committee, sent a Summit venue request for proposals to the OWASP-Leaders on 21-Sept-2010.[7] A local chapter leader from France expressed initial interest but proximity (within 50km) to an International Airport was too large of a hurdle for them to overcome. When the RFP closed on 4-Oct-2010, only two submissions – Brazil and Portugal – had been received. Jason Li put together a form for the people submitting from Brazil and Portugal to complete,[8] which would also provide the planning committee a more objective format to compare the venue proposals. The Planning Committee ultimately decided hold the Summit in Portugal for a number of reasons including likelihood that the total cost for all attendees would stay under $2,000 USD, the local vendor relationships which had already been established since this was also the location of the 2008 Summit, proximity of the venue to a major international airport (Lisbon), the pleasant regional weather during mid-January to mid-February, the availability of both a Board Member (Dinis Cruz) and an OWASP employee (Paulo Coimbra) to assist with local decisions and needs during the planning process.

.

Choosing a Date

At the same time that the Planning Committee was deciding on a venue, Jason Li sent a doodle to the Board and Global Committee Members looking for the date that work best for the most people from 15-Jan-2011 to 15-Feb-2011. Based on the results (25 responses), the planning committee chose the week of 7-Feb-2011 for the Summit.

Location Selection, Take 2

In early November, as the Planning Committee worked with representatives from Diplomata Tours as well as staff from the Quinta da Marinha venue to flesh out some of the venue details, Dinis learned that for the dates that the summit was planned, the hotel was not able to provide sufficient availability in terms of both villas and meeting rooms because of concurrent events at that location. The concern was that if the attendance at the Summit grew above 100 (which was anticipated), they would not have room to host the event. Therefore, Dinis asked Nuno Fernandes from Diplomata Tours to look for another venue option in the Lisbon area. After about a week of looking, Nuno found Campo Real Resort, which was actually cheaper than the first venue (Quinta de Marinha) and had much more availability in terms of both meeting rooms and accommodations. After several weeks of negotiation with Campo Real (also Sandra Paiva, Paulo Coimbra, and Nuno Fernandes went to visit the venue 15-Nov-2010) the Planning Committee decided to move forward with this second venue. On 30-Nov-2010 Dinis authorized Kate Hartmann to proceed with transferring an initial 30% payment as a down payment to secure the venue.

Vetting of Committee Members

The initial budget allocated by the Board was $50,000 and the idea was that this initial funding would cover the travel and accommodation costs of the Board members, OWASP employees, and *active* Global Committee Members to attend the Summit. The problem was in determining who was an *active*

[7] https://lists.owasp.org/pipermail/owasp-leaders/2010-September/003695.html

[8] http://sl.owasp.org/summit2011_proposal

Committee Member. Since the Planning Committee did not think it was appropriate for them to make this decision, they tasked board with determining who was active. Each Board Member was to go to his committee and nominate the active members. While in theory this seemed to be a reasonable plan, in practice it did not go so smoothly.

Part of the problem was that even some of the Board Members were unprepared to make the decision on what constitutes *active* in a committee. Additionally, the standard for *active* was different depending on the Board Member and the overall committee initiatives. One technique was for the Board Member just make a decision himself, and another was to ask the committee members themselves whether they were active or not. After a somewhat arduous process in early December, the Global Committee Members were each designated with one of the following categories: active committee members ("A"), new committee members ("N," joined in the last month or so), committee members that were inactive but upon contact from a Board member they recommitted to the committee ("R"), committee members stepping down ("S"), and inactive committee members with no response "I"). Committee members that stepped down were those identified as inactive and also chose not to recommit themselves to activity in the future. Those receiving the "I" categorization were those committee members determined to be inactive by virtue of no response to inquiries on their activity.

After receiving the results of the status of each committee member, the Planning Committee decided that the priority funding (i.e. first $50,000 that had already been solidified) would go to the committee members with the "A" categorization. Second priority was given to both new committee members and recommitted members. So the primary funding was allocated to the Summit Planning Committee (7), OWASP Staff (4), Board Members (7) and active Global Committee Members (9). Incidentally, there were 17 global committee members categorized as active, but 6 of them part of the Planning Committee and thus had their trip covered by OWASP already. Additionally, 2 active committee members had their trips sponsored by their companies. This meant 27 people were on the priority funding list. Estimating an average of $2,000 per person, the cost to send these 27 people to the summit was estimated to be $54,000 ($4,000 more than the budget allocation).

Request to "Re-structure" Summit Financials

Based on the estimated cost to just those on the priority funding list, as well as the anticipated venue costs, operational expenses and an estimated 50 more people who were either new or recommitted committee member or OWASP chapter leaders and participants who expressed an interest in attending the summit via the initial survey sent out by the planning committee (sent out to the OWASP-Leaders 1-Nov-2011[9]), Dinis made a request to the Board to "re-structure" the summit financials.[10] This proposal included using the original $50,000 allocated by the Board for Summit operational expenses and using any of the existing $150,000 from the OWASP investment budget (not scheduled to be spent) to cover travel expenses for the summit attendees. This funding request was approved by the Board on 20-Dec-2011.

OWASP Summit Travel Fund

At the same time as Dinis's request to the Board to "re-structure" the Summit Financials, Tom Brennan, determined that there was $80,677.00 USD of unused local chapter funds in the OWASP account. Tom sent an email out to the OWASP-Leaders requesting that they look at their available funds and determine what operational requirements (supplies, promotional merchandise, and related program/speaker funding)

[9] http://sl.owasp.org/summit2011_attendeesurvey

[10] Proposal with request for comments from the board: https://lists.owasp.org/pipermail/owasp-board/2010-December/004114.html , Request for vote: https://lists.owasp.org/pipermail/owasp-board/2010-December/004122.html

would be needed in the upcoming year. Then the leaders were to complete an online form[11] specifying some chapter details (Name, location, chapter leader contact information, number of leaders/board members) as well as whether their chapter was sending a representative to the Summit and what percentage of their available chapter funds they were willing to transfer to the OWASP Summit Travel Fund (OSTF). It was clearly noted in Tom's email that "it [was] OK not to transfer any funds to the OSTF"; however, should the chapter *not* respond to the survey by 15-Jan-2010 at 12:00 EST, the chapter would be tagged as inactive and the OWASP Foundation would proceed in automatically transferring any available funds to the Summit Travel Fund.

When the response period for the OSTF closed on 15-Jan-2010, the preliminary calculations were: Total donated (via response) $14,215.25 and total forfeited (via no response) $13,707.00, for a total of $27,922.25. After Alison checked the numbers and some clarifications were made with Chapters who "earmarked" their funds to pay for a specific attendee (and some chapters who responded that they were donating 0% but then agreed separately to sponsor an attendee), the total amount donated by OWASP Chapters for the Summit was $44, 095.65.

Hashing out the travel policy

It was initially decided that Diplomata Tours would be the local Portuguese Travel agent used to coordinate all flights by Summit attendees, reserving accommodations, and liaising with the venue (Campo Real Resort). Our main point of contact at Diplomata was Maria Jose. On many occasions in late November and early December, signing a "contract" with the venue and another with Diplomata was mentioned, but nothing more than a proposal of costs was provided. Although both Sarah Baso and Jason Li expressed concerns to Dinis and the Summit Planning Committee, no contract was ever obtained from either service provider.

As more and more questions and confusion seemed to arise between Maria Jose, summit attendees contacting Maria to book their summit trip, and the Summit Planning Committee, Sarah and Jason decided to draft their own "contract" that established the "Rules of Engagement" between OWASP and Diplomata Tours.[12] This document evolved from mid-December to mid-January and each time Maria or a possible Summit attendee had a question about cost or the policy on what would be covered by a summit sponsorship (i.e. what airline fares would be covered?, what if a flight that covered a 7 day stay was cheaper than a 4 day stay just for the time of the summit events?), either Jason or Sarah would add the decision/guideline to the "Rules of Engagement" in order to have a central repository of the terms of agreement between the parties, but also maintain consistency in decision making. Additionally, Sarah and Jason put together a second document that outlined all the quoted prices of Diplomata Tours and Campo Real Resort.[13] Both documents were shared with Maria Jose at Diplomata Tours, who did not articulate any disagreement with the terms stated.

After a conference call between Kate Hartmann, Lorna Alamri, Jason Li, and Sarah Baso on 8-Jan-2011, it was decided that instead of having the rest of the Summit attendees (i.e. those who had not booked their flight or accommodation) register through Maria at Diplomata Tours, all booking would go directly through OWASP. More specifically, Kate Hartmann set up the RegOnline system to process not only corporate sponsorships[14], but also individual attendee registration. Additionally, it was decided that Sarah Baso would take over booking all Summit flights. An Orbitz account was set up to bill OWASP, and

[11] http://tinyurl.com/owaspleaderOSTF
[12] http://sl.owasp.org/diplomataroe
[13] http://sl.owasp.org/diplomataprices
[14] http://www.regonline.com/owasp_global_summit_2011_sponsorship_registration
Additionally, the corporate sponsorship link was integrated into the Summit wiki page:
https://www.owasp.org/index.php/Summit_2011_Corporate_Sponsorship

Sarah would work directly with the attendees to determine the appropriate flight and promptly schedule it. The main reasons for this change in responsibilities were: the necessity for expedited booking and a having central point of contact in booking reservations in the final month before the Summit. Based on the lag time may attendees who booked through Diplomata Tours had experienced (and shared their dissatisfaction with us), concern arose over the ability of Diplomata Tours to handle an even larger influx of conference registrants.

Dinis's Point system

Once the Summit Planning Committee secured additional funding via Board vote on 20-Dec-2011, concerns regarding how the Planning Committee would allocate the remaining travel budget to those who wanted to attend the summit but did not have the funds to do so. Initially, the Planning Committee intended for any OWASP Leaders who sought OWASP funds to pay for their trip, to go directly through their Chapters.[15] While this worked with some chapters (whose funds were captured in the OSTF explained above), not all OWASP participants followed these directions.

For those attendees who did not ask for or receive funds directly from a local chapter, Dinis created a point system which recognized OWASP participation.[16] The point system involved many stages of disagreement and decisions for the Planning Committee. Aside from Dinis, most of the Planning Committee determined that the point system was a good idea *in theory*, but there wasn't the necessary time or resources to put such a system in place (the Summit was less than 2 months away and the members of the Planning Committee were all stretched to the max in terms of their time commitment to the event). Despite the consensus among the rest of the committee to move forward with a different system for deciding who would get what amount of funding in which order, Dinis moved forward on his own (and with the assistance of Paulo Coimbra) in creating this point system: setting criteria on which to base the allocation of points, create a formula to use in mapping the total points for each attendee, conduct a "first-pass" or initial assessment of the mappings to each of the attendees requesting funding, and allowing the attendees an opportunity to rebut the points they were determined to have.

The Summit Planning Team was concerned about the timeline for approving sponsorships for Summit attendees and additionally was not keen on relying on the completion and implementation of Dinis's point system in a timely manner. Thus, they pushed the decision regarding how the remaining Summit Travel Funds would be allocated (via Dinis's point system or not) to the Board. The Board seemed to be in support of Dinis's plan and not as concerned about the impending time crunch.

Dinis finished the first two stages of the point mapping during the first week of January – setting criteria on which to base the allocation of points and create a formula to use in mapping the total points for each attendee. He also created a UI and scripts using O2 which would automatically run the attendee point mappings once their OWASP areas of participation were entered into their attendee templates (which were used on the Summit Attendee page to keep information relating to their sponsorship and attendance status[17]) The categories for determining participation (and points) were:

| Project Leadership (less than 6 months old) =
| Project Leadership (more than 6 months old) =
| Release Leadership (less than 6 months old) =
| Release Leadership (more than 6 months old) =
| Project Contribution (less than 6 months old) =

[15] Application for chapter/project sponsorship: http://sl.owasp.org/summit2011_rff

[16] Along the same lines as the OWASP Points System being developed by Mark Bristow: https://www.owasp.org/index.php/OWASP_Points

[17] https://www.owasp.org/index.php/Summit_2011_Attendee (To view an attendee's details, click on the "edit" link to the left of the Attendee's name)

| Project Contribution (more than 6 months old) =
| Release Contribution (less than 6 months old) =
| Release Contribution (more than 6 months old) =
| Committee Membership =
| Chapter Co-Leadership =
| Conference Co-Leadership =
| Projected Funding Cost =

Dinis emailed the attendees who had requested funds the mapping details on 5-Jan-2011.[18] A follow up reminder was also sent by Sarah Baso on 6-Jan-2011, asking the sponsorship applicants to complete/check their mappings no later than 7-Jan-2011. The first round of sponsorships using the ranking system was decided and awarded on 10-Jan-2011[19] and the second round on 18-Jan-2011.[20] A summary of the process for obtaining sponsorship funds, the rules for using such funds, and the decisions surrounding who would get the limited sponsorship funds were all posted to the Summit Wiki page to provide as much transparency and information to attendees as possible.[21]

One Last Funding Hurdle

After the second round of sponsorships was awarded on 18-Jan-2011, there were still a handful of summit hopefuls seeking funds for their attendance. Sarah Baso estimated the cost of all sponsorships that had been awarded up to this point as well as the cost to sponsor the remaining individuals requesting funds and determined that an additional $25k USD would be more than enough to cover the expenses for the remaining applicants. Based on this information as well as a request from Dinis for a bit more money to cover Summit Operational expenses, Jeff Williams requested an additional $15k for operational expenses and $25k for summit travel expenses from the Board.[22] The Board approved Jeff's request on 23-Jan-2011 and Sarah promptly contacted the remaining individuals to let them know that their sponsorship had been approved.

Creating Working Sessions

From the initial planning stages of the Summit in Aug-2010, there were a few main ideas for what would later make up the tracks (and working sessions) for the event:

- Browser Day – One of the great challenges of application security is browser security. The idea behind this track was to spend a full day working together with the leading browser vendors to penetrate current problems, new ideas, and determine how security fits in alongside other requirements for developers and end-users.
- XSS – Facilitate a half day working session on cross site scripting, specifically how OWASP can make 2011 the year of XSS…going away. Topics covered: Outreach to frameworks/other constituent parties and OWASP XSS awareness – making OWASP and other freely available resources more accessible to the wider community.
- OWASP Projects – How should OWASP support, grow, and manage projects? This discussion should in include: assessment criteria, orphaned projects, funding, marketing, commercial services.
- OWASP Around the World – OWASP is a fast growing global community. How should we support and manage this growth? During this session we'll look into the issues of

[18] https://lists.owasp.org/pipermail/owasp-summit-2011/2011-January/000518.html
[19] http://sl.owasp.org/summit2011_ranking1
[20] http://sl.owasp.org/summit2011_ranking2
[21] https://www.owasp.org/index.php/Summit_2011_Attendee_Funding
[22] https://lists.owasp.org/pipermail/owasp-board/2011-January/004256.html

internationalization, the global job board, and facilitating the growth of new OWASP chapters in parts of the world where we have not spread much.

These initially proposed topics were posted to the Summit wiki page with a note encouraging community members to add subtopics, or even new topics they wanted to be covered during the Summit. Only a couple more topics were added –University Outreach and Enterprise Web Defense Roundtable – before early December (about 2 months before the Summit). Throughout December, more working session ideas trickled in and in late December in order to facilitate both a format that was easy to view and easy to update, Sarah created a template for the working sessions[23], which were organized under the following categories/tracks:

- Browser Security
- Cross-Site Scripting Eradication
- Metrics
- Mitigation
- University Outreach, Education, and Training
- OWASP Secure Coding Workshop
- Individual OWASP Projects
- OWASP Governance
- OWASP/"Birds of a Feather"

Once the templates for the working sessions were created, it was easier for anyone who wanted to set up their own working session to just go on the wiki page and fill in the template. Nevertheless, maintaining the working session page, answering questions about the template as well as the working sessions, and following up with individuals who entered only minimal information about their session was a large task. So, when the task of booking flights and coordinating travel moved from Diplomata Tours to Sarah Baso, she needed help managing the working sessions (which instead of becoming *less* work, would only become *more* work as the Summit approached). Dinis solicited the help of Paulo Coimbra (already working full time for OWASP) and Sandra Paiva (hired as a "Working Session Editor"[24]) to take over the task of managing the working sessions and then developing a schedule for the Summit.

One of Paulo and Sandra's first steps was establishing a timeline for managing the working sessions in the final month before the Summit:

- 12-Jan to 16-Jan – Paulo and Sandra review new and existing working sessions, requesting more information where necessary.
  The following information was requested for each working session:
  - A detailed description of the working session,
  - Well defined, concise and clear objectives,
  - A set of working session outcomes (deliverables) that should be feasible and concrete,
  - A list of working session participants.

- 17-Jan to 23-Jan - No additional input (session details) considered by Sandra and Paulo during this week, which is to be spent working directly on the consolidation, cleaning up and systematization of the contents received, produced and imported from the existing layouts on the Summit page.
- 24-Jan to 25-Jan - On the 24th, the 1st proposal of Tracks and Working Sessions to go live and presented to the community, requesting feedback, comments and suggestions.

[23] Listing of all working sessions: https://www.owasp.org/index.php/Summit_2011_Working_Sessions
[24] https://www.owasp.org/index.php/Summit_2011/External_Contractors

- 26-Jan to 29-Jan - Feedback and suggestions analyzed by Paulo and Sandra and, whenever possible, incorporated.
- 30-Jan – Paulo and Sandra deliver a final proposal for the Working Sessions and Tracks to the Summit'11 team (in preparation for the final Summit schedule)

Fixed and Dynamic Schedules

Early in the Summit planning process, we had determined that most (if not all) of the Summit's schedule would be structured as working sessions, which we intended to be both a time and place for groups to meet and produce tangible results. Each working session would meet in a room where participants could discuss, argue, collaborate, and most importantly produce a deliverable. Up until this point in the planning process, however, it had not been determined how all the proposed sessions would be organized over the 4-day Summit.

Given the total number of working sessions proposed, trying to include them all into a fixed agenda would have meant that each session would have a 15 minute slot. In order to make the Summit a hub of productive and meaningful discussions Paulo, Sandra, and Dinis (with input from some of the key working session leaders) decided that the fixed schedule would only include the working sessions with a higher number of attendees and focused on matters of interest to the wider community. Also, working session leaders and other interested parties were encouraged to have one or more informal or dynamic working sessions *prior* to their spot on the fixed schedule if they thought more than 85 minutes (the time period for each session on the schedule) would not be enough time to sit down and produce results.

Many of the sessions included on the final fixed schedule were those that started as ideas early on in the Summit planning process: XSS and the Frameworks; XSS-Awareness, Resources, and Partnerships; Enterprise Web Defense Roundtable; OWASP Board and Committee Governance; OWASP Projects; University Outreach; and multiple sessions related to browser security. [25]

All of the working sessions that were not placed on the fixed schedule were placed in the "Dynamic Working Sessions" category.[26] Dynamic working sessions were defined as fluid, informal, and spontaneous working sessions that could happen throughout the day in different locations and at different times. Before the start of the Summit, the Dynamic Schedule was completely empty. The idea was that attendees that wanted to schedule a dynamic working session (whether it was listed on the working session wiki page prior to the Summit or not) would look at the available time slots and available locations and then schedule the session at the time and location that would work best for the anticipated attendees. Once that information (time and location) was decided, the working session leader would email the Schedule Team or contact Sarah Baso to make their request. Sarah would work with Paulo and Sandra who did the final confirmation of availability and placed the working session on the dynamic schedule. Once the session was on the schedule, Sarah would follow up with the working session leader to confirm the date and time.

While the process appears complicated, it worked quite efficiently – with Sarah Baso being the "scheduler" that interfaced with attendees and Paulo and Sandra working behind the scenes to check availability and update the wiki. The format also seemed to work well for the attendees/session leaders who had a single point of contact for scheduling their session and directing questions. This minimized confusion or mixed messages about whether the space and time they requested was still available.

[25] The full list of fixed working sessions is available here:
https://www.owasp.org/index.php/Summit_2011_Schedule_Fixed

[26] More information on the Dynamic Working Sessions as well as the final dynamic schedules is available at:
https://www.owasp.org/index.php/Summit_2011_Schedule_Dynamic

In order to provide some sort of mechanism for "advertising" or communicating which dynamic sessions would be happening when, there was a cut-off time for submissions to each day's dynamic schedule.[27] After the cut off (and even outside the dynamic schedule format), attendees were encouraged to meet and do work, but the working session would not be "supported" by the Summit Team. This support included communicating the time and date of the session via daily schedule distribution, as well as providing any supplies or equipment needed for the session.

Fixed Working Sessions

Tuesday, February 8	Wednesday, February 9	Thursday, February 10
XSS and the Frameworks	Protecting Information Stored Client-Side	Contextual Output Encoding
XSS -Awareness, Resources, & Partnerships	Common structure & numbering	ESAPI-CORE
OWASP Training	OWASP Common vulnerability list	OWASP Board/Committee Governance
OWASP Academies	Providing Access to Persisted Data	Board Structure
WAF Mitigations for XSS	OWASP Testing Guide	ESAPI for Ruby
Virtual Patching Best Practices	Site Security Policy	Applying ESAPI Input Validation
OWASP Exams	OWASP Industry Outreach	Professionalize OWASP
University Outreach	Microsoft's SDL in 16 steps	OWASP funding and CEO discussion
Risk Metrics	OWASP Projects	EcmaScript 5 Security
Metrics and Labeling	DOM Sandboxing	OWASP Certification
Government Outreach	Overhauling the OWASP Website	HTML5 Security
Counting & Scoring AppSec Defects		What is an OWASP Leader?
OWASP Secure Coding Practices Project		Tracking OWASP Participation
Enterprise Web Defense Roundtable		Mobile Security
Threat Modeling		OWASP Licensing

Dynamic Working Sessions

Tuesday, February 8	Wednesday, February 9	Thursday, February 10
OWASP vs Government vs Universities	Formal Risk Assessment Methods	How can OWASP engage with auditors?
Building the Brazilian Leaders Group	TOP 10 Online Training in Hacking-Lab	Hackademic Challenges
Common structure & numbering	Defining AppSensor Detection Points	OWASP Java Project
Board/Committee Governance, pt. 1	OWASP Asia/Pacific Working Group	OWASP Exams
XSS and the Frameworks	Development Guide	Industry Outreach
OWASP Academy Portal	Defining an AppSec Program for Universities, Govts, & Standards Bodies	Scaling Web Application Security Testing
Browser Security Meet-Up	OWASP Portuguese Language Project	OWASP CEO & Funding Opportunities
	ASVS Project	Improving Conference Planner Support
	Secure Dev. Guidelines for Smartphone Devs.	OWASP College Chapter Program
	Privacy-Personal Data, Legislation & OWASP	Vulnerability Disclosure Policies
	Mobile Security	Global Conferences Committee Meeting
	Should OWASP work with PCI-DSS?	Planning AppSec South America
	OpenSAMM	Global Chapters Committee Meeting
	Threat Modeling	O2 Platform
	Board/Committee Governance, pt. 2	ESAPI framework integration
		Global Education Committee Meeting

Remote Participation

In late January, a few weeks before the Summit, an increasing number of questions and requests for the Summit to be broadcasted online prompted the Planning Committee coordinate remote participation. A

[27] For working sessions to appear on the Tuesday (first day of the Summit) afternoon schedule, they had to be received by the Scheduling Team by Tuesday morning at 10:00. For working sessions to appear on the Wednesday schedule, they had to be received by Tuesday at 18:00. Likewise, for the Thursday schedule, they had to be received by Wednesday at 18:00.

poll[28] was created and sent out to the OWASP-All asking those with initial interest to let the team know the approximate number of remote participants to plan for, the prevailing type of remote participants (attendees or active participants), and the working sessions that those participants considered most attractive. Within a day more than 65 people had already expressed an interest in remote participation.

Dinis found a Portuguese sponsor for the video broadcast of the Summit – SAPO. As part of their sponsorship, SAPO agreed to provide:

- Temporary ADSL link for 1 video stream
- Equipment to convert the video signal
- Broadcast up to 1000 concurrent users
- Simple personalization of the broadcast video page (i.e. logo)
- Setup and Support during the Summit

The estimated cost of the sponsorship (if OWASP had paid for it) would have been 4,350€ or approximately $6,000 USD. This provided 1 high quality 24h video stream of the Summit with the backing of a professional team who had experience providing this service for other events.

Based on the responses to the remote participation poll (343 people expressed interest in at least part of the Summit), video streaming was set up for 4 rooms (2 for the fixed schedule and 2 for the dynamic schedule) and accounts were set up for live blogging during each of these sessions using: http://www.coveritlive.com/

Mark Bristow and Doug Wilson setup all of the streaming systems, cameras and audio. Although SAPO's infrastructure was used to do the streaming, Mark and Doug planned to use Justin.tv as backup if there were any issues. Each room had its own published link to view the streaming video[29] Campo Real 1, the large ballroom where the keynotes and sessions expected to have the largest number of attendees were scheduled, had its own dedicated line. The Aletejo (small boardroom) and Lusitano (large meeting room) shared a second line. The Gameroom (small meeting room) shared the Summit Attendee network upstream.

Video Streaming for Remote Participants – number of views per day

Date	**CampoReal 1** (Large Ballroom)	**Aletejo** (Small Boardroom)	**Lusitano** (Large meeting room)	**Gameroom** (Small meeting room)
Schedule	Fixed	Fixed	Dynamic	Dynamic
8-Feb	289	73	162	35
9-Feb	171	78	80	26
10-Feb	120	44	51	24
11-Feb	15	4	3	2

Although there were some initial complaints concerning audio quality the two smaller rooms, as a whole, the remote participation/streaming went off without a hitch once it was set up. Mark and Doug did periodic checks of the equipment, and Stefan Wuench along with one of the student volunteers, Marco Batista, provided much of the constant maintenance that was necessary to make sure the audio levels and other environmental issues were just right in each room for each session. The above chart shows the number of remote participants in each room on each day.

[28] http://bit.ly/gTchDB
[29] http://www.owasp.org/index.php/Summit_2011/Remote_Participants

Summit-Related Activities & Social Events
In mid January, John Wilander, Martin Holst Swende, and Mario Heiderich (with help from gaz, sirdarckcat, and thornmaker) organized a "makeXORbreak" Summit Challenge. – A JavaScript fighting arena where your script should show its name more prominently than its competitors. The Challenge, consisting of four generations, was launched 23-Jan and by 26-Jan, **http://makexorbreak.com** had 4,600 page requests from over 1,000 hosts.

During the Summit itself, a number of social events provided an opportunity to get out from behind the computer screen and spend time getting to know other attendees. One of the most anticipated of these events, was the Brazilian BBQ and OWASP Band performance that took place at one of the large villas on the last evening of the Summit. During the first few days of the Summit, any musically inclined attendees were encouraged to add their name to a list, along with their instrument/talent. Dinis was able to rent some instruments and equipment locally (since most people did not have instruments with them). Then, on Wednesday night the band had a practice, before their big performance on Thursday. First some of the Brazilian attendees volunteered their services in serving up some freshly barbequed meat. Then, the band hit the stage, belting out some hits of the 80's and 90's as well as a newly composed song called the "SQL Injection Blues." They also entertained the audience by taking some requests before they lost their voices and were forced to call it a night.

The second most anticipated social event of the Summit was the football (soccer) match that took place on Friday morning. While there was a clear rivalry motivating the Portuguese and Brazilians, the camaraderie gained by everyone far exceeded the national pride of any one team.

The Summit Support Team[30]

The Summit Planning Team was initially composed of a group of volunteers that provided most of the planning up until the first day of the Summit; some new volunteers came on board to fill in during the Summit itself so the Summit pre-planners could be involved with the working Sessions.

Lorna Alamri, Brad Causey, Dinis Cruz, Martin Knobloch, Jason Li, and John Wilander were the volunteers involved in the pre-planning of the Summit**. Lorna Alamri** coordinated most of the planning meeting – coordinating people's schedules, compiling agendas, recording minutes, and tracking the assigned tasks. She made sure we stayed on task and sent out many emails to the Summit team as well as the OWASP community soliciting RFPs for the venue and coordinating attendance.

Jason Li also did a huge amount of behind the scenes work – crunching numbers to make sure the budget was on track and costs associated with the venue and travel were properly assessed. Additionally, he spent many long nights working on the Summit wiki page, creating and modifying templates, tracking frequently asked questions and providing answers, and ensuring that information was communicated to attendees in a clear and concise manner.

John Wilander, Justin Clarke, Martin Knobloch, and Brad Causey were all involved in the strategic planning – coming up with targeted industry personnel to invite to the event and then sending out initial inquiries to find out whether there was interest in the event. **John** was primarily organized in coordinating the browser security track, which was a tremendous success based on the amount of positive feedback received and "big names" he was able to solicit to attend. **Justin** reached out to individuals who he thought should be involved in the cross-site scripting eradication track, which was also a highlight of the

[30] A list of the external contractors and details surrounding their role is available at: https://www.owasp.org/index.php/Summit_2011/External_Contractors

Summit. **Martin** focused his energy on inviting members of the education community – university professors and students, as well as those involved with the OWASP Training and Academies initiatives.

Brad provide feedback on also put together a couple of surveys that were necessary in determining the dates of the summit, projected board and committee attendees, as well as the gathering information on the recent activity of global committee members.

Each of these five volunteers, along with Dinis and some of the paid Summit support, also went to the Summit venue several days before the beginning of the Summit to make sure everything was ready to go when attendees arrived.

In addition to the volunteer efforts that made up most of the summit pre-planning, **Sarah Baso** was brought on as paid support staff[31] to assist with much of the behind the scenes work. Sarah's various duties included creating Summit invitations and sponsorship letters for attendees and their employers, creating and maintaining wiki content, responding to questions from attendees, the travel agency, and venue, tracking allocation of summit sponsorship funds, assisting with travel and accommodations for both sponsored and non-sponsored attendees, and facilitating the creation of working sessions and posting them to the wiki page.

Sarah Cruz, Dinis's wife, was brought on at the beginning of January to work on graphic design for all the Summit-related material. She created a Summit identity through logos, PowerPoint templates, and signage for the various tracks. She also created a variety of Summit marketing materials. During the Summit itself, Sarah assisted with general event management and also did graphic design work "on-the-fly" creating signage, schedules, and forms whenever needed. Sarah had assisted with the 2008 Summit and already had a good handle on the events and what to expect, which proved very helpful as many of the other support team members during the summit itself had not been a part of the previous event.

Paulo Coimbra, Sandra Paiva, and Kate Hartmann were all somewhat involved in the Summit planning from the initial stages, being paid staff of the OWASP Foundation. **Paulo** and **Sandra** served as local Portuguese points of contact for the venue and travel agency and also looked at many different venues in the area during the venue selection process. In January, Paulo and Sandra were solicited to assist with sorting out and organizing the Summit Working Sessions into a consumable format for session leaders and attendees. They also worked tirelessly during the week of the summit to continuously update the schedule with the dynamic working session information.

Kate Hartmann provided many different levels of support to the Summit Planning Committee. Just a few of these items include: providing oversight of the Summit budget and availability of OWASP Foundation funds, constructing and maintaining the RegOnline sight that was used to automate the registration process and determine the level of interest in the various working sessions, collecting information and liaising with vendors in order to provide giveaways to the attendees and set up an OWASP store with Summit branded attire at the event. Additionally, on-site the week of the event, Kate worked to ensure that all the operational details were taken care of – printing materials, compiling folders,

[31] Initially, Dinis solicited Sarah's help in exchange for paid expenses to attend the Summit. Then due to a scheduling conflict, Sarah was unable to attend the Summit. The Summit Planning Committee agreed to pay Sarah the $2,000, which was the approximate amount that would have been spent on her Summit travel. Sarah planned to continue helping the Summit Committee until 1-Jan-2011. Near the end of December, Dinis realized that there was an *increasing* need for help in planning the final Summit details and arranging the travel for attendees so he offered Sarah another $2,000 to continue working with the Planning Committee up to the Summit. Sarah found out at the end of January that she *would* be able to attend the Summit and so the Planning Committee agreed to pay for her expenses in exchange for her assistance during the course of the Summit event.

printing nametags, greeting and checking in attendees, answering questions about all areas of OWASP, and participating in the OWASP "internal" working sessions including Global Committee meetings and OWASP Governance.

When Dinis Cruz attended OWASP AppSec Brazil in Nov-2010, he met **Marta Pegorelli** who provided event management services for the conference through her company, Anggulo Eventos. Dinis (and many others who attended the Brazilian conference) was amazed at Marta's impressive work. In early December Dinis solicited Marta's help and services to organize and OWASP Summit Brazilian Delegation.[32] The agreement provided that Marta would help promote the Summit in Brazil amongst many industry verticals including Government and Academia. Maria hoped to help OWASP put together a Brazilian delegation which would include OWASP Brazilian chapter leaders as well as key people from the Brazilian Government and Educational Institutions. Although it was not part of her original contract, in exchange for OWASP covering her travel costs, Marta also agreed to attend the Summit to assist with event coordination. She was helpful in bridging the English-Portuguese Language barrier, as she fluent in her native Portuguese and reasonably proficient in English.

One additional member of the paid Summit support Team was **Deb Brewer** from LX Studios who was asked to get involved as the primary event coordinator. Deb's responsibilities were to coordinate the events and the timeline for each room as well as general problem solving and crisis management. Deb also ensured that each working session had the necessary equipment and supplies and then the room was re-set appropriately for the next session. Deb interacted with all the various summit team members – paid and volunteer – as well as SAPO telecom, which was on site providing video streaming of the sessions to remote participants, and the hotel staff.
The final piece of the puzzle was the additional summit attendees who volunteered their time during the summit event to help out with operational tasks in exchange for having their travel expenses covered by OWASP. **Linda Potjes**, a friend of Martin Knobloch, agreed to help out with a number of miscellaneous tasks – putting together Summit participant folders, printing name tags, distributing cell phones and sim cars, posting updated schedules, and ensuring that someone was present at the "table" where attendees could request dynamic working sessions (along with Sarah Baso). **Stefan Wuensch** from Hacker News Network, was solicited by Kuai Hinojosa, to assist with some interviews at the Summit, but also to provide general networking help. Stefan worked around the clock to set up and reset wireless networks, do A/V checks on the cameras in each of the working session rooms, and generally make sure that the other members of the Summit Team had what they needed at all times. Three students also assisted with networking and connectivity issues: **Marco Batista**, **Anastasios Stasinopoulos**, and **Julio Cesar Fort**.

Although they did not attend the Summit with the intent of assisting with operational tasks (they attended as OWASP contributors), **Mark Bristow** and **Doug Wilson** played a large role in setting up the cameras and other A/V equipment, and along with Brad Causey, spent many hours testing connectivity and "viewability" for the remote participants to watch and "virtually attend" the working sessions. Mark and Doug also were diligent in checking the cameras (and back-up drives) throughout the course of the Summit to make sure everything was working – both broadcasting and recording – as planned.

Finally, **Dinis Cruz** served as the leader of the Summit Team both before and during the event as well as the Team's liaison with the Board of Directors. Dinis created much of the initial energy that motivated the planning committee and continued with his drive throughout the process, creating a means to the end that we all hoped for – a successful summit.

[32] https://lists.owasp.org/pipermail/owasp-board/2010-December/004055.html

2011 Summit Finances

The OWASP Foundation spent a total of **$226,606.29** on the 2011 Summit. This covered the flights for 85 people and the food and accommodations for 96 people. In total, the OWASP Foundation paid for some (if not all) of the expenses for 103 people to attend the Summit. An additional 50+ attendees were sponsored by their companies or paid for their own travel/accommodations to attend the event.[33]

Category	Cost	Notes
Summit Venue Expenses	$51,572.34	Meeting rooms, A/V equipment rental, catered meals, venue staff
Summit Giveaways	$7,054.17	Podcast CDs, Stickers, Passports, Compasses
Summit Equipment and Services	$14,138.18	Marketing, PR, SAPO (internet connectivity), Apparel, Band Equipment Rental, Misc.
Summit Support Staff	$17,015.77	Sarah Baso (Logistical Support), Marta Pergorelli (Brazilian Delegation), Sarah Cruz (Logo & Design Work), Sandra Paiva (Working Sessions Editor), Deb Brewer (Event Coordinator)
Summit Travel & Accommodations	$152,855.58	Flights, room, and board for sponsored attendees
COST SUBTOTAL	$242,636.04	
Income - Non OWASP funds used to pay for Summit expenses	$16,029.75	Non-OWASP funds (less transactional fees): wiki donations, lunch sponsorship ($(ISC)^2$), wireless sponsorship (Trustwave), corporate membership (Praetorian, Security Innovation), accommodation credit
Total Cost to OWASP	**$226,606.29**	

Lessons Learned from the 2011 Summit

Summit planning:

- Start planning earlier. The 2011 Summit planning began 6 months before the Summit. In order to do a proper "call for venues" (giving more than 2 weeks to submit) as well as compiling the materials to get corporate sponsors, such an event should be planned a year in advance (similar to what is done in preparation for successful Global AppSec Conferences).
- Require contracts with Venue, Travel Agency and other service providers. Additionally, think through the terms of engagement that the Summit Planning Team would like to set with the vendor before finalizing the contract. This can help prevent hidden costs and miscommunication.
- Let Americans handle the customer service. Americans like customer service and know how it's done, whereas the rest of the world is behind to various extents. Many of the guests and leaders that attend OWASP events expect American customer service so we need to proxy those services (travel agency etc) for events outside the US.

[33] More details on the Summit finances as well as the sponsored attendees appear in the Appendix.

- Plan for more internet bandwidth. Don't rely on anything but a paid, major ISP to set things up. A countryside hotel will never understand what it takes to serve 170 geeks.
- Planning the sessions further ahead of the actual summit. This was a bit messy and people missed some sessions. So, having a "call for sessions" early previous to the Summit.
- Involve the conference committee in all stages of the planning and execution of the Summit. They have much combined experience with event planning and potential “problem” areas that can and should be avoided.
- Coordinate office supplies and other equipment needs before arriving on site.

Summit Operations:

- Get more "OWASP external Stuffing", local students would be great, to have someone taking notes at each session (not getting distracted by involvement).
- Have a 'serious' operational desk (again, e.g. using students) that is continually manned.
- Hire video support staff (instead of relying on volunteers or whoever is in the room)

Working sessions/scheduling:

- Set clear expectations (with examples) before attendees arrive about what kinds of outcomes should come out of the Summit.
- Sessions are about people. Get-the-Right-People-There. Invite early. With the right people you can fix session content in a week.
- Set small goals. A session is 45 minutes to 1.5 hours. That's not a lot. Set goals that can be achieved in that time.
- Make time for preparation of and collect Summit outcomes BEFORE attendees leave the Summit. Gathering results for months after the fact is difficult and wastes a lot of time and resources.
- Prepare for less productivity on the 4th/final day of the Summit. This should be a day for presenting what was done over the first 3 days and regrouping after breakout sessions.

The OWASP Summit is in the Right Direction

(From blog post[34] of John Wilander, Summit Planning Team)

I was on the organizing team for the OWASP Summit 2011. Not as deeply involved as Sarah, Dinis, Lorna, Jason, Deb, Sandra, and Paulo ... but I did organize the four Browser Security sessions.

I truly believe that the Summit format is the way OWASP conferences should go. We should not try to compete with Black Hat, Defcon, BSides or whatever conference out there. We should do something different, geared towards productivity.

Below is how I setup the browser security track and my humble suggestion for making a difference:

1. Prioritize People when Planning

The success of your session boils down to people. If you're at a workshop and "the guy who has all the answers" is not there the workshop is not going to be productive. So my overall goal was to get the right people there. However, you cannot start by inviting people, you only need to start with it as your top priority.

2. Build a Draft Agenda

To be able to successfully invite the right people I had to have a relevant draft agenda. So I spent a weekend watching various webcasts of talks from the people I wanted to invite. From that I built my draft agenda. I basically adopted their agenda and tweaked it with some personal stuff.

3. Reach Out to Key Players

Now that you have a draft agenda you can reach out to key players you already know and that are likely to say yes. Ask them what they think of the draft agenda and more importantly, ask if they would consider co-chairing a topic or two. Get their names up there.

4. Market Your Heroes

When you have a first couple of key players onboard it's time to get the buzz started. Tweet about it. Blog about it. Talk about it. And make use of the heroes who are already booked.

5. Reach Out in Waves

Now you need to get key players onboard that you did not previously know. It's time consuming so I do it in waves. A good weekend with the right inspiration you can hunt down a few more of the people you need to get there, explain the agenda and who else is going. Make use of your network and CC people who might be able to vouch for your workshop. As soon as you get people hooked ask if they want to be involved.

[34] http://appsandsecurity.blogspot.com/2011/02/owasp-summit-is-right-direction.html

6. Have Faith

A lot of the so called key players are very busy. You may have gotten a confirmation four weeks ago but not heard anything since. Just make sure you send them updates every other week anyway. They'll come. Have faith.

7. Work Onsite

At the workshop you need to tend to practical stuff. I think I was the only session chair who cleaned all the tables up on stage before my sessions. Fresh blocks of paper, new water glasses, no garbage. Also make sure you have an announcement up on the big screen and walk around reminding people that it's only 10 minutes to you session. Do not underestimate what this kind of lightweight service can do for your session.

Links to other Summit-related blog posts can be found at:
https://www.owasp.org/index.php/Summit_2011_Outcomes

Section VII: Working Session Outcomes

Browser Security

(John Wilander)

Five of the Summit sessions were subtopics of Browser Security Track:

- Site Security Policy
- DOM Sandboxing
- HTML5 Security
- EcmaScript 5 Security
- Enduser Warnings

Outcome Summary: Browser Security Report[35]

Apart from achieving the goal of getting browser security key players together, the sessions reached the following outcome:

- The HTTP header *X-Frame-Options* will be adopted by IETF and proposed as a standard HTTP header.
- A combined Site Security Policy header consisting of *Content Security Policy* (CSP), *X-Frame-Options* (XFO), and *HTTP Strict Transport Security* (HSTS) was discussed by the authors (all present at the summit). Core differences identified were cached (HSTS) versus non-cached (CSP & XFO) policies and applicability to third party resources (CSP but not HSTS & XFO).
- DOM Sandboxing as a built-in browser feature was discussed and encouraged. Both Mozilla and Google will consider it. Maybe built from the HTML5 sandbox or via selective CSP for iframes.
- New attack surfaces as well as new ways of protection in HTML5 and EcmaScript 5 were brought to light.

XSS Eradication

- **DOM based XSS Prevention Cheat Sheet**[36]
  (Jim Manico & Abraham Kang)

  Created DOM based Prevention Cheat Sheet: When looking at XSS (Cross-Site Scripting), there are three generally recognized forms of XSS. Reflected, Stored, and DOM Based XSS. The XSS Prevention Cheat Sheet does an excellent job of addressing Reflected and Stored XSS. This Cheat

[35] The full Browser Security Report appears in the next section. It is also available at: http://sl.owasp.org/browsersecurityreport

[36] The DOM based XSS Prevention Cheat Sheet appears in full in the next section. It is also available at: https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet

Sheet addresses DOM (Document Object Model) based XSS and is an extension (and assumes comprehension of) the XSS Prevention Cheat Sheet.

- **XSS and the Frameworks: XSS – Awareness, Resources, and Partnerships**[37]
  (Justin Clarke)

    - Discussed ways for OWASP (and the larger web appsec community) to influence browser vendors and framework producers in order to combat/mitigate/eradicate this vulnerability.
    - Concluded that a multi-layered approach was needed, using techniques like auto-escaping templates, server policies, browser sandboxing and the use of something like Content Security Policy (CSP).
    - Concluded that both developer outreach and training is needed, but additionally developers need help from the technologies, vendors, browsers, OWASP, etc.
    - Determined that OWASP can start addressing this vulnerability by creating a list of the technologies, the barriers of entry, pros and cons.
    - Action item: update the wiki to improve cross-referencing and have all resources in one place... e.g. a XSS landing page with links to both internal and external resources.
    - Action item: create and distribute an open letter to browsers, vendors, and anyone else in the community asking about open source resources to help solve this issue.

- **WAF Mitigation for XSS**
  (Ryan Barnett)

    - Discussed Dynamic Taint Propagation Detection – where the WAF can track user-supplied data and see if it is echoed back to the client without unescaping (either in current response or later).
    - Discussed Application Response Profiling – where a WAF can monitor the number of expected script/iframe tags on a page and then alert when there are deviations.
    - Discussed JavaScript Sandbox Injection – where a WAF can add links to JS sandboxing code to the top of response bodies.
    - Action item – research if it possible to use Anti-Samy type functionality in a WAF.

- **Virtual Patching Best Practices**[38]
  (Ryan Barnett)

    - Agreed upon a standard definition for Virtual Patching – A security policy enforcement layer which prevents the exploitation of a known vulnerability.
    - Agreed upon the main benefits of virtual patching – Reducing both the time-to-fix interval and attack surface for exploiting a known vulnerability.
    - Agreed upon potential drawbacks of virtual patching – accuracy and coverage is variable depending on the vulnerability type, virtual patching tool deployment mode (3rd party

[37]Working session notes available: http://sl.owasp.org/summit2011_xss
[38]Working Session Notes: http://sl.owasp.org/summit2011_virtualpatching

device, embedded web server plugin or app filter hook), policy flexibility (rule engine capabilities) and virtual patching rule writer's skill.
    - Discussed who should be involved with virtual patching creation – Virtual Patching Tech Lead (WAF admin) and Application-specific Dev POC.
    - Action item – Create a table that lists virtual patching effectiveness for various attacks/vulnerabilities (OWASP Top 10, etc….).
    - Action item – Create an Incident Response type of process flow (Preparation, Identification, Analysis, Patch Creation, Testing, Deployment and Follow-Up).

Metrics

- **Counting and Scoring Application Security Defects**[39]
  (Chris Eng & Chris Wysopal)

    - Discussed existing methods for counting and scoring application security defects by vendors and practitioners willing to share their methodologies, including OWASP's Risk Rating Methodology[40] (Part of the OWASP Testing Guide v3), which is used by the OWASP Top 10 to provide generic information about likelihood and technical impact for each of the "Top 10" risks.
    - Discuss advantages and disadvantages of a standardized approach.
    - Discuss the CWSS 0.1 draft and how it might be incorporated into a standard. Steve Christey outlined the Common Weakness Scoring System (CWSS), part of the Common Weakness Enumeration (CWE) project, co-sponsored by the Software Assurance program in the National Cyber Security Division (NCSD) of the US Department of Homeland Security (DHS).

- **Risk Metrics: Metrics and Measuring**[41]
  (Chris Eng & Chris Wysopal)

    - Discussed the US federal OMB M-04-04 risk classification **(**guidance reflects outcomes of the E-Authentication E-Government Initiative and standards issued by the National Institute of Standards and Technology (NIST)) - e-authentication guidance for federal agencies - and other methods for risk assessment used in other sectors.
    - Debated the appropriateness of using any form of risk determination in a cross-industry approach.
    - Examined possibility of more factual labeling, aimed at the supply chain rather than end-users. OWASP is an organization that can help define the labels, not enforce. Then, government can choose whether to enforce.

[39] Brief Introduction to Common Weakness Scoring System ppt created by Steve Christey: http://sl.owasp.org/summit2011_cwss
[40] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
[41] Working Session Transcripts: http://sl.owasp.org/summit2011_metricsnotes

OWASP Projects: New or Updated Tools, Documents or Resources

- **Application Security Verification Standard (ASVS)**
  (Dave Wichers)

  - Received feedback from users of the ASVS that they are seeing some demand for it in certain circles, particularly Germany.
  - Heard that a number of consultants are using ASVS because it contains one of the best set of requirements publically available.
  - Received feedback in the following areas:
    - Specific requirements that could be improved;
    - The ability to tailor out or tailor in requirements based on the needs of the application being assessed;
    - Adjusting ASVS Level 1 to not be so tool focused, but rather simply represent a light level of assessment vs. a more detailed level of assessment as currently expressed at Level 2.
  - Updating ASVS to align with the Common Numbering Scheme.
  - Action item: Update ASVS before the end of 2011.

- **Development Guide**
  (Vishal Garg)

  Developed "to do" list for new version of the Development Guide:
  - Review existing content and identify areas that need further improvements (additions/deletions).
  - Recruit more volunteers to contribute to the project. The goal is to release the new version of the guide before the end of 2011.
  - Identify and review copyright and licensing issues.

- **Common Structure and Numbering for All Guides**
  (Merged with the **Common Vulnerability List**[42])
  (Keith Turpin, Matteo Meucci, Vishal Garg, & Dave Wichers)

  - Develop a set of common application security requirements with an associated numbering scheme.
  - Use this numbering scheme to align the following projects initially: OWASP Security Requirements Doc (Currently the Secure Coding Checklist, ASVS, Development Guide, Testing Guide, Code Review Guide).
  - Develop a maintenance plan to handle an evolving set of requirements.
  - These 'common' requirements are not intended to dictate to any project what they need to address or how they should be organized, but we would hope that at least the projects listed above would generally be organized in a similar way and use the numbers to help cross reference their material with related materials in other OWASP projects.

[42]Common Vulnerability List ppt presentation created by Matteo Meucci for the Summit available at: http://sl.owasp.org/summit2011_commonvulnerabilitylist

- Action items: two short-term milestones (in the next 4-6 weeks):
  - Create a draft of the numbering scheme within 2 weeks of the summit (this is the numbering system and the security areas, not a completely populated list);
  - Create a draft of the scheme filled out for 1 security area, along with matching completion in both the OWASP security requirements document and the ASVS so we can see how the scheme works across a set of related document.
- Action item: Update all of these documents by the end of 2011 to include updates to their content, plus reorganization or realignment relative to the common numbering scheme.

- **Open SAMM**
  (Pravir Chandra)

  - BSIMM activities mapped to SAMM[43]

- **OWASP Java Project**
  (Lucas Ferreira)

  - Created an action plan for the Java Project:
    - Compile a list of OWASP projects related to Java (parallel to other activities).
    - Define criteria so we can compare frameworks:
      - Use known vulnerabilities,
      - Use ASVS.
    - Reach frameworks to gather information on how they address the criteria items.
    - Compile results.
    - Re-Plan based on the results.
  - Decided to keep the Java project and the .Net project aligned as much as possible.
  - Chose Matthias Rohr as new project leader.

- **OWASP Mobile Security Project**[44]
  (Mike Zusman)

  - Gathered from working session participants a list of 37 mobile risks. Risks will be further classified and used to survey pen-testing / app-assessment companies in creating a data driven OWASP Top 10 Mobile Risks document.
  - Established working relationships, resulting in people assuming responsibilities for key project initiatives/deliverables (Top 10 Survey - Jerry Hoff; Secure Mobile Development Guidelines - Mike Zusman/Giles Hogben from ENISA).
  - Engaged in sometimes-heated discussion, leading to a general consensus on the mission, target audience, and key deliverables of the Mobile Security project.
  - Created additional wiki content.

[43] http://www.opensamm.org/2011/03/bsimm-activities-mapped-to-samm/
[44] Working Session Notes: http://sl.owasp.org/summit2011_mobilesecuritynotes

- **OWASP Portuguese Language Project**[45]
  (Lucas Ferreira)

    - Defined priorities for the project (translation and revision).
    - Defined strategy for coordination – to be detailed and posted to wiki.
    - Defined a process to be used for translation.
    - Action item: Build common language rules to be used by all translators, regardless of their home country.

- **OWASP Project Disclosure Policy**
  (Chris Schmidt)

    - Defined a Disclosure Policy for OWASP Projects[46] - This policy describes the official OWASP Policies on reporting security vulnerabilities, project staff responsibilities, how users are protected, and the lifecycle of reported vulnerabilities in OWASP branded projects.
    - Developed and refined a template to be used for disclosing.[47]

- **OWASP Secure Coding Practices Project**[48]
  (Keith Turpin)

    - Gained broader exposure of the Secure Coding Practices Guide, including to other document project leaders.
    - Clarified the purpose of the Secure Coding Practices Guide.
    - Identified some areas for improvement for the next release:
        - Rename the guide - proposed new title: "Secure Software Requirements 2011,"
        - Update project references,
        - Incorporate contributions from new contributors,
        - Implement number system based on common numbering schema, to be defined.
    - Identified additional volunteers to contribute to the next release of the Guide.

- **OWASP Testing Guide**[49]
  (Matteo Meucci)

  Identified plan for future of project:
    - Collaborate with other guide leaders and come up with common numbering scheme and
    - Restructure the guide to adhere to common numbering scheme to enable cross-referencing with other guides. (First draft of the common numbering scheme is anticipated before the end of February 2011.)

[45] https://www.owasp.org/index.php/Summit_2011_Working_Sessions/Session048/Deliverable_1
[46] Full Policy details available at: http://sl.owasp.org/projectdisclosurepolicy
[47] Template available at: http://sl.owasp.org/projectdisclosuretemplate
[48] Working Session notes: http://sl.owasp.org/summit2011_securecodingnotes
[49] Planning the OWASP Testing Guide 4.0 ppt presentation: http://sl.owasp.org/testingguide4ppt
Complete Working Session Notes: http://sl.owasp.org/summit2011_testingguidenotes

- Review existing content and identify areas that need further improvements (additions/deletions).
- Recruit more volunteers to contribute to the project. The goal is to release the new version of guide before the end of 2011.
- Identify and review copyright and licensing issues.

- **Threat Modeling**[50]
  (Anurag Agarwal)

  - Voted unanimously to have an OWASP threat modeling project.
  - Discussed need to promote project not only to security consultants, but also obtaining contributors from an end user organization to provide feedback on challenges and such.
  - Set goal of having OWASP promote the methodology with the hope of establishing it as a standard in the industry.
  - Gained insight on how people have been doing threat modeling individually - There is no set standard used by people but everyone has their own.
  - Discussed starting an OWASP threat modeling project and letting OWASP build and drive a standard which can be adopted by the industry.
  - Discussed various components of threat modeling and how they fit into the process.

Secure Coding Workshop

- **Applying ESAPI Input Validation**
  (Chris Schmidt)

  - Reviewed and explained entire validation codebase.
  - Action item: Attendees to add Google code issues for improvements to functions.

- **Contextual Output Encoding**
  (Chris Schmidt)

  - Ensure that existing codecs are working to specification for their context and cover all escaping and encoding rules for that context
    - Are there any new escaping rules for HTML5, ES5, or CSS3 that are not addressed by the current codecs?
    - Can we improve the MySQL Codec to account for additional modes of operation?
    - Is documentation on these codecs and when/where they should be used sufficient?
  - Create a new set of Codecs to address additional popular encoding contexts
    - Database Codecs
      - Sybase
      - Postgres

[50]Working Session discussion points and notes: http://sl.owasp.org/summit2011_threatmodelingnotes

        - Client Side
            - Flash
            - Applet
            - JavaFX
            - ECMA
        - Data-Grid and DA
            - Gigaspaces
            - Hibernate Query Language
            - SparQL
    - Implementation Guide for Framework Developers to integrate Output Encoding – Notes: What we need from framework developers
        - Contextual Output Encoding that is easy for developers to use
        - Text Box: Special Case
        - Output Encoding must happen at the view layer
        - Granular Output Tags

- **ESAPI-Core**
  (Jim Manico)

    - Worked with Apache to strengthen Apache Commons-Validator functions.
    - Worked with Apache to start a common-security project in Apache Commons.

- **Defining AppSensor Detection Point**
  (Michael Coates)

    - Built the future roadmap of the AppSensor project that included 6 specific actionable items. This roadmap is a result of the brainstorming session conducted with the 50+ attendees at this session[51]
    - Identified what additional documentation is needed and desired by potential adopters in order to explain the project and drive adoption.
    - Identified methods of integrating AppSensor into existing framework code in order to drive adoption through a grass roots style approach.

- **Providing Access to Persisted Data**[52]
  (Dan Cornell)

[51] https://lists.owasp.org/pipermail/owasp-appsensor-project/2011-February/000208.html
[52] Working Session notes: http://sl.owasp.org/summit2011_persisteddatanotes

University Outreach, Education and Training

- **OWASP Certification Working Session**[53]
  (Jason Taylor & Jason Li)

  During the working session, the OWASP community reaffirmed that OWASP **does not** and **will not** do certification. However, we recognize that outside organizations overwhelmingly want such certifications to exist and as a result, companies *will* arise to offer these certifications. While OWASP will **never** endorse any certification, we are also uniquely positioned to provide some guiding principles so that organizations can navigate the certification space confidently. These principles will be encapsulated as part of the OWASP Code of Conduct series, which also includes codes of conduct for educational institutions, government organizations, and standards bodies. An initial draft was produced as an outcome for the working session and will be submitted to the Board for approval along with the other Codes of Conduct.

- **OWASP Exams**
  (Jason Taylor)

  - Received validation that OWASP Exams have value.
  - Received feedback that the existing exam can be improved by the following:
    - Clearer questions, especially if they are scenario based
    - Careful review of distractors to ensure they are not in a ray-area that could be argued if they are correct or incorrect answers
    - Careful with terminology to ensure it aligns with OWASP and is consistent throughout
  - Some tests for an exam:
    - Can an expert in the subject area pass with a 90% or greater score?
    - Will a non-expert fail the exam?
    - Is it tied too tightly to a training course, in which the training is required in order to do well on the exam?

- **OWASP Hackademic Challenge**
  (Kostas Papapanagiotou & Vasileros Vlachos)

  - Received positive feedback on the initiative and decided to turn the Hackademic Challenges into an OWASP project.
  - Determined Project Leaders: Kostas Papapanagiotou and Anastasios Stasinopoulos

- **OWASP Training**[54]
  (Sandra Paiva)

  - Presented the OWASP Training Model and the initiatives undertaken to operationalize it.
  - Promoted the consolidation of this model as a base for Chapter-lead training initiatives.

[53] A draft of the Codes of Conduct for Certifying Bodies appears in full in the next section. It is also available at: http://sl.owasp.org/summit2011_redbook
[54] More information: http://sl.owasp.org/summit2011_owasptraining

- Defined what would be the next steps to take in order to maintain and keep this model alive and active.

- **University Outreach - OWASP Academies**[55]
  (Sandra Paiva)

  - Presented proceedings and outcomes from OWASP Academies event held in Lisbon, Portugal on 5-6 January, 2011.
  - Explained the OWASP Academies Portal Project[56] including advantages, contributors, and roadmap for moving forward.
    - The Academy Portal was created to enable teachers and to supply a single point of access to OWASP Educational Material.
    - The Academy Portal has 4 major areas: teacher area (where teachers can create and use predefined events), a student learning area, a forum for teachers, and a forum for students.
  - Discussed alternative ways of working with Universities when possible, including Summer School proposal (ISCTE).
  - Presented the OWASP AppSec Tutorial Series[57] and discussed how to best disseminate and use it.

- **University Outreach - OWASP College Chapter Program**[58]
  (Renamed to **OWASP Student Chapters Program)**
  (Martin Knobloch)

  This is one piece of the University Outreach program and aims at connecting students within the application security community. During the Summit three key points were discussed for moving this initiative forward (with the assistance of the Global Education, Membership, and Chapters Committees):
  - Student chapters should not be competing with regular (local) OWASP chapters;
  - Student chapters are encouraged to visit and contribute to chapter meetings in their area;
  - Regular chapters in an area near a college or university are encouraged to assist in starting or supporting student chapters.

[55]More information: http://sl.owasp.org/summit2011_owaspacademies
[56] https://www.owasp.org/index.php/OWASP_Academy_Portal_Project
[57] More info on the tutorial series can be found at:
https://www.owasp.org/index.php/OWASP_Appsec_Tutorial_Series
[58]https://www.owasp.org/index.php/OWASP_Student_Chapters_Program

OWASP Internal Governance and Global Committees

- **Global Chapters Committee**[59]
  (Seba Deleersnyder)

  Held two working sessions with 20+ local chapter leaders to facilitate Q & A regarding the logistics of running a local chapter. The second working session was more strategic, discussing ideas for growing local chapters, facilitating involvement in the local chapters, and ways in which the Global Chapters Committee can better assist the local chapters.

- **Global Industry Committee**[60]
  (Eoin Keary & Colin Watson)

  - Discussed 2011 Global Industry Committee initiative to undertake greater efforts to listen to industry. In order to solicit information in a suitable environment, the concept of face-to-face industry forums will be progressed. One such event will be a meeting with a small group of influential leaders from the financial services sector, possibly arranged for during AppSec EU 2011 (Dublin) in June. Other sectors to be targeted are healthcare, and government.
  - Introduced Industry Outreach Survey[61]: The Industry Committee will proceed with its efforts to seek feedback from industry more widely (but not security consultants or vendors) using a questionnaire in association with ISC2. The survey needs final review, building into an online system, testing and then promotion to target groups. It may be useful to have some incentive for completion of the survey.
  - Immediately after the Summit: the committee received pledges from at least four leaders outside the US/EU to become new members of the Industry Committee

- **Global Membership Committee**[62]
  (Dan Cornell)

  - Decided to explore better ways to attract international members by adjusting costs and positioning of benefits.
  - Decided to explore an NPR/EFF-like model to allow people to contribute more and get OWASP materials
  - Decided to target more non-vendor Organizational Supporters in 2011

- **Global Projects Committee**
  (Jason Li & Brad Causey)

  During the working session, the GPC solicited feedback on two GPC initiatives: OWASP Projects Hosting and the OWASP Project Lifecycle.

[59]Meeting minutes from 2 working sessions: https://www.owasp.org/index.php/Summit_2011_Working_Sessions/Session018/Deliverable_1
[60] Working Session Notes: http://sl.owasp.org/summit2011_industrynotes
[61] Survey is available at: https://www.surveymonkey.com/s/SCJBX7R
[62]Working Session Notes: http://sl.owasp.org/summit2011_membershipnotes

- The Project Hosting initiative is an effort to provide a consistent, centralized infrastructure for OWASP projects so we better manage, support and promote projects.
- The Project Lifecycle initiative is an effort to help clarify the maturity of an OWASP project in order to better serve users and help facilitate allocation our resources to properly support our projects.
- These outcomes are encapsulated in a draft project hosting Request For Proposals[63] and draft lifecycle diagrams[64]
- As a direct result of the Summit, the GPC also welcomed two new members: Chris Schmidt and Justin Searle. Both of them made contributions to the GPC during the Summit.

Since the Summit:
The GPC has welcomed two additional members: Larry Casey and Keith Turpin. With the Board's approval of the GPC 2011 Budget, the GPC is now actively pursuing proposals for project hosting services. Our current plan is to pilot the hosting services by migrating select projects to the hosting infrastructure before announcing general availability of the service by the end of the year. Project hosting services will be used to directly support the OWASP Project Lifecycle and will help the GPC determine maturity of projects. In addition, the Project Lifecycle has been augmented to include the OWASP Enterprise category of projects, which are projects specifically geared and supported to be used in enterprise companies. Projects in this category will be required to conform to the strictest project requirements and pursue "product" or "production-ready" levels of maturity.

- **OWASP Board and Global Committee Governance**
  (Mark Bristow)

  - Conducted a 3-part working session to discuss problems with Global Board and Committee Governance, and then came up with solutions in the form of draft governance documents: revised OWASP Foundation Bylaws,[65] drafted OWASP Foundation operational policies, and discussed a universal committee governance policy.[66]
  - Discussed OWASP Foundation mission, core purpose, and values [67]
  - Revised election process for OWASP Foundation Global Board of Directors,[68] including:
    - Recommended change of the total number of Global Board Members from 7 to 6,
    - Recommended that Global Board Elections should be held annually, with have of the Board seats up for election each year.
    - Recommended that Board Members serve 2 year terms with a 3 term-limit.

[63] http://sl.owasp.org/projecthostingrfp
[64] http://sl.owasp.org/projectlifecyclediagram1, http://sl.owasp.org/projectlifecyclediagram2
[65] The new OWASP Foundation Bylaws are included in the next session of this document. They are also available at: http://sl.owasp.org/2012bylaws
[66] Global Conference Committee Governance document: https://www.owasp.org/index.php/Global_Conferences_Committee_Governance
[67] Current OWASP mission, core purpose, and values: https://www.owasp.org/index.php/About_OWASP
Notes and draft core purpose and values: http://sl.owasp.org/corepurpose_values
[68] New election policy: http://sl.owasp.org/2011electionpolicy
2011 Election details: www.https://www.owasp.org/index.php/Membership/2011Election

        - Recommended that the 3 Board Members that have been on the Board for the longest time put their seats up for election in 2011 (Jeff Williams, Dave Wichers, Seba Deleersnyder) and the other 3 put their seats up for election in 2011 (Tom Brennan, Eoin Keary, and Matt Tesauro). [69]
    - Came up with strategies to facilitate better communication between Global Board and Committee Members:
        - Committee Chairs should start calling in and giving monthly committee reports at the Board's monthly meetings.
        - Committee Chairs should hold their own monthly call in order to facilitate better cross-committee communication and discuss issues that may be affecting more than one committee.

- **OWASP Chapters: Asia/Pacific Working Group**
  (Helen Gao)

    - Created an APAC mailing list.
    - Discussed problems and possible solutions to low regional membership – Currently there are very few paying members in APAC. The reasons are both economical and cultural. Ofer Maor volunteered to create a model that is easy to implement and administer. He will propose the model to the membership committee.
    - Discussed ideas for conferences in APAC – Annual conferences in China as well as additional conferences in other APAC area. Conference organizers should summit their schedule to Global Conference Committee as early as possible, preferably one year in advance. This will help GCC allocating funds and recommending vendor sponsors to support the conference. Offer CPE or participation certificate. This will not only provide conference/workshop participants something to show, it will also create awareness among his colleagues and employers. Please note the certificate will be similar to CPE credits, Continual Professional Education, and will not be a general OWASP certificate.
    - Membership Perks/Discounted Training – We need to show people more in APAC what's in the membership for them. Proposed to provide paid members free or discounted in-person training during or outside of conferences.
    - Online itinerary, tripit.com - The goal is attract members by improving communication and corporation among chapters. This will be especially beneficial to chapters outside of US and Europe. Cecil will use tripit or another method for entering itineraries. Local chapters can invite the traveler to their meeting, training or just for a drink.

- **OWASP Chapters: Building the OWASP Brazilian Leaders Group**
  (Lucas Ferreira)

  Defined objectives and created action plan to improve OWASP presence in Brazil:
    - A new local chapter has been created in the city of Recife, which will be lead by Felipe Ferraz and Rodrigo Assad.
    - The Brazilian Chapters must be empowered through periodic meetings.

[69] Jeff and Dave became Board Members in 2004, Tom in 2008, and Seba in 2007. Most recently, Eoin and Matt became Board Members in 2009. 2009 Election details: https://www.owasp.org/index.php/Board_member

        - Periodicity must be defined.
        - The meetings must be promoted to the Brazilian AppSec Community.
        - The Chapter leaders must leverage the OWASP wiki and the specific mailing list to make the meetings happen.
    - The Brazilian groups and individuals that develop activities related to Application Security must be identified and contacted. Three categories have been defined:
        - Government,
        - Industry,
        - Academia.
    - The Summit synergies must be leveraged to increase the collaboration with other Latin American Countries.
    - Boost the 3rd AppSec Brasil (1st AppSec LA) by the creation of a Latin-American organization committee focused in the local efforts to seek resources and event promotion. This committee should contribute to the success of the event.
    - Organize a working session at AppSec Brasil to assess the outcomes of the item 3 above.
    - Seek OWASP financial support to start the project.
    - Keep the efforts to approach industry, government and academia to promote and empower OWASP.

- **OWASP Funding and CEO Discussion**[70]
  (Keith Turpin)

    - Gained broader exposure of the current OWASP funding model and operating expenses.
    - Agreed to next steps for gathering, reviewing and implementing new funding ideas.
    - Came to no clear resolution on the CEO topic; however, it was clear that a CEO would not be feasible without new funding sources to support the additional expenses.

- **OWASP Licensing**[71]
  (Abraham Kang)

    - Discussed licensing requirements for OWASP Documentation and existing licenses used by OWASP Projects.
    - Identified problem(s) corporations face with adopting and utilizing OWASP materials and code: It was determined that the major issue with enterprise adoption of OWASP documents was the requirement to open source/share back any derivative documents upon use (older licenses) or utilize the same or similar open source license upon distribution (Creative Commons 3.0 SA Attribution). Can we clarify the meaning of "distribution" such that the passing of derived works to partners or affiliates does not constitute public "distribution" under Creative Commons 3.0 SA Attribution)?
    - Made recommendations for changes in the OWASP License: Clarify the term "distribution" so that it does not include affiliates and partners of enterprises. This would

[70] Session notes are available at: http://sl.owasp.org/summit2011_ceo&funding
Additional notes: http://sl.owasp.org/summit2011_ceo&funding2
[71] Detailed notes on Licensing: http://sl.owasp.org/summit2011_licensing

help enterprises who modify OWASP documents to use them for internal operations with occasional distribution to affiliates and partners.
    - Created "OWASP: Licensing FAQ"

- **Overhauling the OWASP Website**
  (Jason Li & Larry Casey)

  During the working session, the OWASP community overwhelming asserted a preference to support message forums as a means of communicating. Additionally, suggestions were made to explore community servers and alternative home page layouts.

  Since the Summit: Matt Tesauro has been working with RackSpace to finalize their donation of five enterprise virtual machines to act as OWASP servers. Larry Casey has several virtual machines configured for OWASP services ready to be loaded pending finalization of the arrangement. With these virtual machines in place, we will be able to experiment with various services such as community servers and message forums.

- **OWASP Points**[72]
  (Mark Bristow)

  Discussion of initial "points system" detail and point values:
    - OWASP Points are a system that allows us to recognize an individual's achievement and accomplishments in OWASP. The system is designed to self-monitored.
    - Each Global Committee will establish its own criteria for assigning points for participation in the committee's area of responsibility. Also, each Global Committee will be responsible for providing oversight of points claimed under their areas.
    - The OWASP Board will establish points for areas outside committee areas of responsibility.
    - The Global Committee Chairs and a Board Member will meet as needed (at least quarterly) to normalize the point values.
    - OWASP Members will have the ability to self nominate for points.

[72] More details available at: https://www.owasp.org/index.php/OWASP_Points

Other OWASP Initiatives

- **Defining a Minimal AppSec Program for Universities, Governments, and Standards Bodies: OWASP Codes of Conduct**[73]
  (Jeff Williams & Dinis Cruz)

  Created the OWASP Codes of Conduct for Educational Institutions, Government Institutions, and Standards Bodies

  "In order to achieve our mission, OWASP needs to take advantage of every opportunity to affect software development everywhere. At the OWASP Summit 2011 in Portugal, the idea was created to try to influence Educational Institutions, government agencies, and standards bodies. We set out to define a set of minimal requirements for these organizations specifying what we believe to be the most effective ways to support our mission. We call these requirements a "code of conduct" to imply that these are normative standards, they represent a minimal baseline, and that they are not difficult to achieve."

- **Enterprise Web Defense Roundtable**[74]
  (Michael Coates & Chris Lyon)

  - Successfully engaged eight security experts and the session attendees to frankly discuss security approaches that work or fail within an enterprise environment.
  - Shared feedback and lessons learned from the Mozilla bounty program for websites and identified barriers to entry for a bounty program in other companies.
  - The developer training discussion revealed large gaps in the overall training approaches used within organizations. The specific details from this session will all be captured in the white paper deliverable.

- **Government Outreach**
  (Doug Wilson)

  Created a list of suggestions to pass along to the Global Connections Committee of the best ways to engage government. The initial recommendations of the working group are as follows:
  - OWASP should establish entities outside of the US that other governments will respect and be comfortable interacting with. Being a "US Only" entity legally is hurting the organization in terms of being able to really interact with governments outside the US.
  - OWASP should present simple, accessible, digestible and actionable programs and frameworks for the consumption of governments worldwide.
  - OWASP should look into partnering with other coalitions with similar goals and small standards bodies that already interact with government, and/or drawing best practices from these bodies.
  - OWASP should research the viability of liaisons to/from various government agencies that have an interest in working with OWASP.

[73] These Codes of Conduct are included in the next section of this document. They can also be found at: http://sl.owasp.org/summit2011_draftcodesofconduct
[74] Etherpad Notes Page w/Agenda & Background Reading: http://etherpad.mozilla.org:9000/OWASP-EWDR

- **How can OWASP reach/talk/engage with auditors?**[75]
  (Matthew Chalmers)

    - Decided that it would be useful to set up a mailing list (or forum) to discuss this issue more widely and get more ideas, and possibly start a project to explore different ideas.
    - Would like to get an auditor to look at some of the existing release projects and do a gap analysis from an audit perspective to see what might be missing.

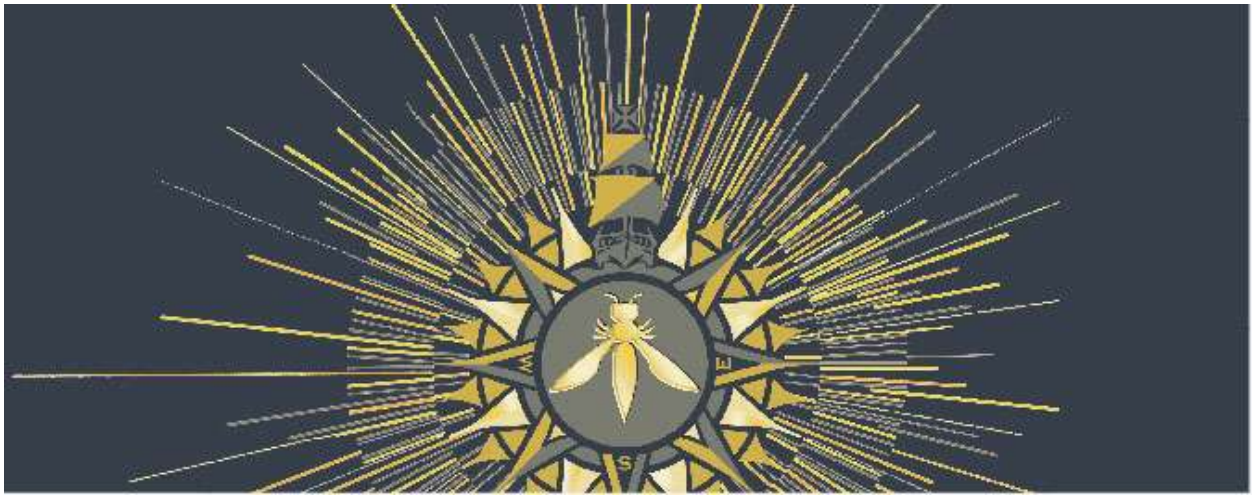
- **Privacy - Personal Data/PII, Legislation and OWASP**[76]
  (Colin Watson)

    - Discussed the importance of privacy protection:
        - OWASP must involve itself with the security aspects of software applications which have an effect on privacy protection.
        - There is a lack of guidance for building privacy into software development lifecycle.
    - Session attendees agreed to pool their knowledge of Government legislation & policies relating to privacy, privacy enhancing technologies, and ideas for what OWASP could help with.
    - Immediately after the working session:
        - Drafted OWASP response to "FTC Protecting Consumer Privacy in an Era of Rapid Change - A Framework for Businesses and Policymakers" was submitted to the FTC on 17th February 2011
        - Conducted a mini survey: A quick straw poll was carried out with a small number of OWASP leaders, to ascertain other perceptions about privacy and its relevance to OWASP. Survey results showed a range of views, with a general feeling that privacy is a relevant area, but that some aspects are not security-related, and therefore not fully within OWASP's mission.

- **Should OWASP work directly with PCI-DSS?**[77]
  (Matthew Chalmers)

    - Decided OWASP *should* work directly with PCI-DSS
    - Decided to look into re-chartering the inactive "PCI" Project and find a contact within the Council to start a dialogue about working together (part of the re-chartered project).

[75] Working Session Notes: http://sl.owasp.org/summit2011_engageauditors
[76] Complete Working Session Notes available: http://sl.owasp.org/summit2011_privacy
[77] Working Session Notes: http://sl.owasp.org/summit2011_owasp&pci



Section VIII: Working Session Artifacts

Browser Security Report

Compiled and Written by: John Wilander

Five of the Summit sessions were subtopics of Browser Security Track:

- Site Security Policy
- DOM Sandboxing
- HTML5 Security
- EcmaScript 5 Security
- Enduser Warnings

Outcome Summary

Apart from the goal of getting browser security key players together, the sessions reached the following outcome:

- The HTTP header *X-Frame-Options* will be adopted by IETF and proposed as a standard HTTP header.
- A combined Site Security Policy header consisting of *Content Security Policy* (CSP), *X-Frame-Options* (XFO), and *HTTP Strict Transport Security* (HSTS) was discussed by the authors (all present at the summit). Core differences identified were cached (HSTS) versus non-cached (CSP & XFO) policies and applicability to third party resources (CSP but not HSTS & XFO).
- DOM Sandboxing as a built-in browser feature was discussed and encouraged. Both Mozilla and Google will consider it. Maybe built from the HTML5 sandbox or via selective CSP for iframes.
- New attack surfaces as well as new ways of protection in HTML5 and EcmaScript 5 were brought to light.

Session Participants

Key players in browser security such as major browser vendors discussed current state of affairs and future challenges and collaboration opportunities. Invited panelists were:

- Ian Fette, Jasvir Nagra, Mike Samuel, Justin Schuh, and Eduardo Vela Nava from Google
- Lucas Adamski and Brandon Sterne from Mozilla
- David Ross from Microsoft
- Jeff Hodges from PayPal
- Peleus Uhley, Adobe
- Tobias Gondrum, IETF
- Mario Heiderich, Ruhr-Universität Bochum
- David Lindsay, Cigital
- Stefano Di Paola, Minded Security
- Gareth Heyes, independent researcher
- John Wilander, OWASP (chair)

Others who took active part in the sessions were Robert Hansen (SecTheory), John Steven (Cigital), Giles Hogben (Enisa), and Chris Hofmann (Mozilla).

All browser security sessions are presented further below.

Browser Security Session 1 – New Site Security Policies

As attacks against web applications increase, so does the need for proactive countermeasures that can be deployed by the application host and executed in the enduser's browser. Security critical web applications should be able to use whitelisting and feature blocking. During the OWASP Summit three such browser enhancements were discussed during the Site Security Policy session.

These important security features come in the form of three new HTTP response headers, namely:

- *Content Security Policy* – Whitelisting of domains from which the page may load resources such as JavaScript and images. Main benefit is to provide a countermeasure for cross-site scripting (XSS).
- *X-Frame-Options* – Policy for disallowing other pages from framing webpages from your domain. Countermeasure for clickjacking.
- *HTTP Strict Transport Security* – Opt-in policy that allows a website to indicate to the browser that only requests over HTTPS are allowed to be sent to the website. HSTS also eliminates the ability for users to override warnings when an invalid certificate is accepted. Countermeasure for man in the middle attacks such as *SSLStrip*[78].

Content Security Policy (CSP)

The content security policy header is still an unofficial W3C draft spec[79] but it's already supported by Firefox 4+ and will be shortly for WebKit browsers, announced for Chrome 13[80]. Besides Brandon Sterne from Mozilla and Adam Barth from Google, Robert Hansen, Jeremiah Grossman, and Gervase Markham have contributed to CSP. The development of CSP is very much alive as of June 2011 and anyone interested is encouraged to join the `public-web-security@w3.org` mailing list.

By including a CSP header in an HTTP response the server specifies permitted sources of content in the page and restricts the capabilities of that content. The header effectively whitelists resource domains - for script sources. Any inline script is disallowed when using CSP.

Example Use Cases[81]

- Site wants all content to come from its own domain:
  ```
  X-Content-Security-Policy: allow 'self'
  ```
- Auction site wants to allow images from anywhere, plugin content from a list of trusted media providers, and scripts only from its server hosting sanitized JavaScript:
  ```
  X-Content-Security-Policy: allow 'self'; img-src *; object-src
  media1.com media2.com; script-src userscripts.example.com
  ```
- Online payments site wants to ensure that all of the content in its pages is loaded over SSL to prevent attackers from eavesdropping on requests for insecure content
  ```
  X-Content-Security-Policy: allow https://payments.example.com
  ```

[78] http://www.thoughtcrime.org/software/sslstrip/
[79] https://dvcs.w3.org/hg/content-security-policy/raw-file/tip/csp-specification.dev.html
[80] http://blog.chromium.org/2011/06/new-chromium-security-features-june.html
[81] From http://people.mozilla.com/~bsterne/content-security-policy/details.html#examples

X-Frame-Options (XFO)

The x-frame-options header[82] is a *de facto* standard supported by Internet Explorer 8+, Firefox 3.6+, Chrome 4.1+, Safari 4+, and Opera 10.50+. At the summit Tobias Gondrom from IETF took on the responsibility to write a spec together with David Ross from Microsoft. It has since been published as a draft[83].

By including an XFO header in an HTTP response the server restricts framing of the page, i.e. loading the page in a `<frame>` or `<iframe>` element. Unintended framing is used in clickjacking attacks.

Examples

- Deny all framing
  `X-Frame-Options: DENY`
- Allow framing only from same domain
  `X-Frame-Options: SAMEORIGIN`
- Allow framing only from whitelisted domains (proposed enhancement in the draft spec)
  `Frame-Options: DENY; ALLOW-FROM https://www.example.com`

HTTP Strict Transport Security (HSTS)

The strict transport header is an IETF Internet-draft[84] supported by Chrome 4+ and Firefox 4+ (also earlier Firefox versions via the plugin NoScript).

By including an HSTS header in an HTTP response the server instructs the browser to enforce HTTPS for the current domain and, if specified, for its subdomains too. The policy directive is cached by the browser for the number of seconds specified in max-age.

Examples:

- Enforce HTTPS for this domain for the coming ten minutes
  `Strict-Transport-Security: max-age=600`
- Enforce HTTPS for this domain and all subdomains for the coming 24 hours
  `Strict-Transport-Security: max-age=86400; includeSubdomains`
- Enforce HTTPS for this domain, only accept extended validation certificates, and pin the signing root CA for the coming 24 hours (additions discussed by IETF[85], Chrome 12 already allows manual CA pinning[86])
  `Strict-Transport-Security: max-age=86400; includeSubdomains; EVOnly; lockCA`

Summit Discussion

David Ross introduced XFO and told about the ideas to add an option in which your page can specify domains that are allowed to frame it. Tobias Gondrom brought up the problem with all these custom headers starting with `X-` and promised to get standardization of XFO started together with David. XFO will become just `Frame-Options`. Content security policy will most probably likewise drop its X from

[82] https://developer.mozilla.org/en/the_x-frame-options_response_header
[83] https://datatracker.ietf.org/doc/draft-gondrom-frame-options/
[84] http://tools.ietf.org/html/draft-ietf-websec-strict-transport-sec-01
[85] Personal communication with Jeff Hodges, April 13, 2011
[86] Enter chrome://net-internals/#hsts in Chrome's omnibar (address bar)

today's `X-Content-Security-Policy` (experimental `X-WebKit-CSP` in Chrome 13) as soon as it becomes an IETF standard.

CSP and several of its challenges was discussed. Notably how to propagate policy directives to framed content (injected meta tags?), granularity of media sources, and CSP's applicability for plugins such as Flash.

Jeff Hodges brought up the idea of a joint site security policy along the lines of:
`SiteSec: allow 'self'; img-src example.org; STS max-age 1200;`
Having one policy header would be beneficial for adoption, future additions and bytes-on-the-wire. However, there are fundamental differences between the policy mechanisms that would make the semantics of a joint policy complex;

- HSTS is a cached policy whereas CSP and XFO are not.
- CSP regulates third party domains, XFO might do with the whitelisting addition, whereas HSTS only applies to the source domain.

A full transcript of the site security policy discussion can be found on the OWASP wiki[87].

Browser Security Session 2 – DOM Sandboxing

Not only mashups but also almost any website or web application uses third party content. This content can be markup, styling, and scripts. To be able to load and execute/render this content safely in the browser's DOM, the browsers need to provide some kind of sandboxing or virtualizing functionality. Traditionally iframes are used for this purpose but they are crude since they obey the same-origin policy meaning content from different domains may not communicate. Content from different *subdomains* may communicate by changing to the same `document.domain` but for content from truly different domains not even that trick will work. Here developers typically resort to proxy solutions, JSONP or the like. It becomes a choice of all-or-nothing, where all means full access to you DOM.

The WHATWG spec for HTML5 contains s new `sandbox` attribute for iframes[88] where the following directives can be set `allow-same-origin`, `allow-top-navigation`, `allow-forms`, and `allow-scripts`. This is a good start but in a properly sandboxed environment the developer can decide what authority or information to give third party content.

Two such projects were represented on the summit panel – Google Caja[89] represented by Jasvir Nagra and Mike Samuel, and the OWASP tools JSReg/HTMLReg/CSSReg[90] authored by Gareth Heyes.

With Caja the developer can for instance allow an embedded application to use a particular web service, but not to send arbitrary network requests, by giving the application an object that interacts with that web service, but deny access to `XMLHttpRequest`.

JSReg *et al* are all sandboxes based on regular expressions. For instance third party scripts are denied global variables and access to the `window` object.

[87] https://www.owasp.org/images/6/6d/OWASPSummit2011SiteSecurityPolicyBrowserSecurityTrack.pdf
[88] http://www.whatwg.org/specs/web-apps/current-work/multipage/the-iframe-element.html#attr-iframe-sandbox
[89] http://code.google.com/p/google-caja/
[90] https://code.google.com/p/jsreg/

Summit Discussion

Gareth argued for built-in sandboxing features that execute while rendering. This would ensure sandbox execution whereas executing the sandbox in the same environment as the web application itself can never guarantee anything (ordering, what objects are actually operated on etc.). The Chrome team argued against saying browsers do things differently which would lead to debugging problems for developers (Why does this work here but not here? Oh, it's the sandbox in browser X …). Mozilla mentioned the potential performance cost of adding sandboxing in the core rendering engine.

A suggestion that browser vendors liked better was enhancing the iframe sandbox in place in HTML5. Perhaps applying CSP specifically for an iframe? Both Mozilla and Google were in favor of such an approach. "A good starting point is always to ask 'Is it possible now?' Extend existing APIs where feasible. Always start by comparing with existing solutions."

Then there's the challenge of deciding what to whitelist. For your own code it might be easy but third party script suppliers will have to supply their own whitelists since they know what their code needs. That pushes the trust boundary back to the third party.

There's a need for concrete use cases to motivate browsers to implement more sandboxing features. The application security community could help out here.

A full transcript of the DOM sandboxing discussion can be found on the OWASP wiki[91].

Browser Security Session 3 – HTML5 Security

The two following sections are written by Mario Heiderich, co-chair of the HTML5 Security session and the host of the HTML5 Security Cheat Sheet[92].

HTML5 Introduction

HTML5 is an often misused umbrella term for a lot of novel ways how modern websites and browsers interact with their users. While HTML4, specified by the World Wide Web Consortium (W3C) was used to describe a precise and static language specification for rich multi-purpose hypertext documents, HTML5 primarily aims for being the language the world wide web is being fueled and driven with. HTML5 attempts to be as open, dynamic and fast as the communication medium, which changed our modern times so significantly: The world wide web. Two major cooks are stirring the soup in the giant HTML5 pot, the W3C and the WHATWG - a group of experts who once split and then reunited with the W3C to form a better web.

Behind HTML5 a lot of novelties and changes hide and wait to be discovered by developers to be used in mainstream and high traffic websites. These include possibilities to enrich web forms with more interactive elements, gadgets and native dialogs, novel ways to retrieve and use a user's location data as well as countless ways to ease the creation of rich and highly interactive content - not only for experienced developers, but also for regular users willing to share and publish information.

It's become easier to embed video and audio into websites than with HTML4 and older versions - many compatibility problems have been aligned and removed to make room for slick and easy to implement ways of generating multimedia centric web content. New elements specifically designed for rich and well structured websites help developers to avoid time and resource hungry workarounds to present their data and information. HTML5 also stands for openness and accessibility - and thrives towards an open web

[91] https://www.owasp.org/images/0/06/OWASPSummit2011DOMSandboxingBrowserSecurityTrack.pdf
[92] http://html5sec.org/

without much more necessity for closed source data such as Flash content, Java and other soon to be deprecated technologies. HTML5 aims for renovating the WWW without losing compatibility to HTML4 and rendering older websites and applications useless

Many new features HTML5 provides can be found under the hood - allowing smaller and faster websites, increasing user friendliness and better surfing experience. Most modern browsers such as Internet Explorer 9, Firefox and Chrome support a wide range of HTML5 features - sometimes partly, sometime fully. Since HTML5 has just recently been renamed into "HTML - The Living Standard", one can never be sure where the HTML will be tomorrow or even in a month or a year. HTML aims towards being as dynamic as the medium it has been created for - the world wide web. A static specification would - according to many of the minds behind HTML5 - just stand in the way of evolution and deprecate itself the same way as HTML4 did. Technically interested users can follow the constant and daily development of HTML5 on many ways, the specification daft is being updated frequently and contains dozens to hundreds of new features to be implemented by browser vendors very soon.

HTML5 and Security

The goals behind HTML5 are driven by ambitions spirit and engagement. The "language the web is written in" has to scale immensely to keep pace with the quick and agile development the web has - and will experience in the coming months and years. But this dynamic nature and ever evolving specification comes with a price tag attached. Browser vendors will air for quick and selective implementations - leaving developers and users uncertain, which subsets of the HTML5 feature set are supported - and which aren't. Imagine a car - having a technician changes single party every single night, to see how the whole things performs the next day. This constantly moving glacier of features generates confusion for developers, and adds new pressure for browser vendors. While HTML4 was a static standard, leaving few questions unanswered "what" should be implemented "how", HTML5 constantly morphs and forces vendors to quickly implement features, even risking them to be deprecated a day later. Some browsers actually fell for that trap by implementing a former beta version of HTML5 called Web Forms 2.0 - until they had to realize that this draft was abandoned by the editors behind it.

Furthermore many of the HTML5 features have not been designed with security in mind. New form features can be used to steal the focus of a user's keyboard activity and redirect his typed characters to different areas of a website - maybe a hidden frame sniffing for passwords or credit card numbers. New attributes to validate form data in the browser can cause trouble when combined with specially crafted styles and background images - a different and hard to fix source for data leakage problems. Even worse - an attacker can override the target URL of a form submit from outside the actual form - and again steal sensitive data by redirecting the information flow to his domain. Several real life attacks based on form data stealing with HTML5 features have already been reported - most times shortly after being unearthed and discussed by the security scene.

The HTML5 specification draft contains many surprises for technically sophisticated people. Many of the described features may never find their way into modern browsers - or in slightly or heavily modified form. Some browsers already started to add own features - based on older HTML5 specification versions and abandoned designs. Among these are notifications, allowing the browser to display small info windows containing HTML outside the browser window, drag and drop up- and downloads and many more useful but off road functionality. This increases the lack of a homogeneous set of browser features a developer can rely on and might bear the risk of introducing a new browser war like once in the nineties between two major vendors. One of the few winners of such a browser war are attackers, profiting from a wide range of half-baked feature implementations, insecure design and quick strategic decision backfiring years later thanks to a lack of reflection and planning.

A dynamic HTML5 standard is not a bad thing per-se - but should be handled with enormous care. Browser vendors as well as the specifying editors from the W3C and the WHATWG should listen closely to the security community and collaborate before features are implemented - not after having them help leverage attacks against users. Usability and open standards are a feature the modern web can only benefit from, but hasty development, arms races between browser vendors and focus on features over security will cause increasing harm for the user base. HTML5 is meant to attract more users to create and share on the world wide web. Making browsers and websites be a larger attack target by specification neither helps vendors, not developers or the most important part in the equation for a better web - the users.

Summit Discussion

The HTML5 security discussion at the summit came to the following conclusions:

- Security documentation is scattered throughout the HTML5 spec and therefore not easily found or digestible. However, the European Network and Information Security Agency Enisa is working on an HTML5 threat model.
- HTML5 is adding a lot of new functionality including completely new tags. This will inevitably mean an increased attack surface. Browser vendors' take: We want the new functionality so we'll have to live with (some) increased risks. It's a tradeoff.
- There will be security bugs both in the spec and in the implementations of the spec. Bugs in the spec have to be reported to WHATWG whereas bugs in implementations/assumptions should be reported to each vendor, sometimes with a bounty in return.

A full transcript of the HTML5 security discussion can be found on the OWASP wiki[93].

Browser Security Session 4 – EcmaScript 5 Security

EcmaScript, the formal name of JavaScript, reached version 5 in December 2009. Not counting the so called *strict mode* the ES5 support in browsers is good – Firefox 4+, Chrome 7+, and Internet Explorer 9+. So far only Firefox 4+ supports strict mode[94] but Internet Explorer 10 will support it[95] and WebKit already does so soon Chrome and Safari will too.

EcmaScript 5 enables several security enhancements such as:

- `Object.preventExtensions()` which prevents adding new properties to an object.
- `Object.seal()` which prevents adding new properties as well as re-configurating or deleting any of the existing ones.
- `Object.freeze()` which prevents adding new properties, deletion, re-configuration, and alteration. Frozen objects become non-writable.
- `Object.defineProperty()` and its descriptor `configurable` which can be set to `false`. This means the developer can add property features or even disable setters and getters for sensitive DOM properties such as cookies and those altered functions are then *final*, i.e. cannot be changed again by an attacker.

Add to that EcmaScript 5 strict mode that solves common pitfalls (accidental global variable declarations), potential security holes (leaking the `window` object via `this`) and allows for better static analysis.

[93] https://www.owasp.org/images/c/cd/OWASPSummit2011HTML5SecurityBrowserSecurityTrack.pdf
[94] http://kangax.github.com/es5-compat-table/
[95] http://msdn.microsoft.com/en-us/ie/gg192966#_ECMAScript5

Summit Discussion

The panel mostly agreed that ES5 and strict mode are good for browser security. However there are concerns on the ES5 spec not defining how getters and setters for global properties should behave. They can effectively ignore `freeze()` and `defineProperty()` and still standards compliant. Hopefully, ES.next (ES6) will fix this and all current browsers "do the right thing" and accept sealed and frozen global properties.
As always there's a risk that the burden on developers is too big. If they have to have a blacklist of all properties to manually freeze chances are slim for broad adoption.

Also, popular JavaScript frameworks have to be strict mode compliant and work properly with frozen globals. As of June 2011 for instance jQuery 1.6.1 and ExtJS 4 are strict mode compliant.

A full transcript of the EcmaScript 5 security discussion can be found on the OWASP wiki[96].

Browser Security Session 5 – Enduser Warnings

The final browser security session dealt with enduser warnings such as HTTPS warnings.

Browser vendors have a tough time finding effective, non-disruptive warnings. Google tried skull & bones for bad SSL certificates but had to back out. At the same time a New Zealand online bank accidently had an expired SSL certificate for 12 months. During that time 299 out of 300 customers clicked through the warning[97].

PayPal would like to see browsers preloaded with HSTS lists for security sensitive sites. Browser vendors responded by saying they can't ship with nor maintain a whitelist of million sites.

Robert Hansen brought up the issue of how to signal DNSSEC. Google responded that if you're under DNSSEC, a signed top level domain, and you include a file with a cert fingerprint. Chrome will treat your cert as if signed by a recognized root CA.

A full transcript of the enduser warnings discussion can be found on the OWASP wiki[98].

[96] https://www.owasp.org/images/f/f7/OWASPSummit2011EcmaScript5SecurityBrowserSecurityTrack.pdf
[97] As told by Jeff Hodges, PayPal.
[98] https://www.owasp.org/images/f/f7/OWASPSummit2011EnduserWarningsBrowserSecurityTrack.pdf

The OWASP Application Security Code of Conduct for Educational Institutions

(The OWASP "Blue Book")

Special thanks to Jeff Williams for creating this document, and to Dinis Cruz, Colin Watson, Dave Wichers, and all the participants in the Working Session at the OWASP Summit 2011 in Portugal for their ideas and contributions to this effort.

The OWASP Application Security Code of Conduct for Educational Institutions (The OWASP "Blue Book")

Introduction

Educational Institutions have an unparalleled opportunity to help improve application security worldwide. For many software developers and others studying information technology, their core thought patterns, ethics, and values are defined during their educational experience. We believe that all developers need to be exposed to application security during these critical formative years. While we recognize that not all developers will become application security experts, some level of awareness and experience is critical. We also believe that there is critical demand for application security experts, and that Educational Institutions are uniquely positioned to provide students with the proper foundation and awareness to develop these skills.

Code of Conduct

1. **The Educational Institution MUST include application security content somewhere in the standard computer science curriculum.**

   This requirement is intended to expose all students studying computer science and other information technology degrees to some level of application security. At a minimum, they should be exposed to the most critical application security risks. This should not imply that they are experts in the problem, but at least that they might recognize the problem in their work and know to get additional assistance or perform additional research.

2. **The Educational Institution MUST offer at least one course dedicated to application security annually.**

   To support the critical demand for application security experts, we believe that Educational Institutions should offer an opportunity for interested students to become experts in the field. This is not a topic that is necessarily suitable for all students. We do not attempt to specify the exact coverage for this application security course, other than that the general content of the most popular OWASP projects would be very good starting points.

3. **The Educational Institution MUST ensure that an OWASP Chapter is available to their students and support it.**

   We believe that an important part of application security is staying on top of the latest threats and technologies. This exposes students to a different kind of learning experience from great speakers and real-world practitioner experiences in application security as well as creating social connections. So we would like to see Educational Institutions ensure that their students have access to an OWASP Chapter available. If there is already a local OWASP Chapter, then the institution simply needs to help students find it. If no local Chapter is available, the process to set up a student-run Chapter is very simple and OWASP will help get it started.

Recommendations

4. The Educational Institution SHOULD be an OWASP Supporter.

There is no charge for an educational institution to become an OWASP Supporter, and it promotes your institution on our website. The main benefit of becoming an OWASP Supporter is to demonstrate your belief that application security is important and that you are working to prepare your students to understand security and write secure code.

5. The Educational Institution SHOULD assign a liaison to the OWASP Educational Institution Executive Council.

The OWASP Educational Institution Executive Council is a group that focuses on improving application security in educational institutions. The group collaborates via email and at OWASP events worldwide. We expect the liaison to monitor the list and participate as much as they care to. The institution can define their level of participation. The Liaison will be considered an OWASP Leader and eligible for free attendance at our worldwide events.

6. The Educational Institution SHOULD leverage OWASP by attending our events, using our materials, and asking our experts for help.

OWASP has a lot to offer educators. We have freely available tools, documents, guidelines, and standards. We have worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in classrooms. We even have packaged curricula, eLearning, and educational materials that are available for educators to use and modify free of charge. Educators are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.

7. The Educational Institution SHOULD encourage interested students to participate in OWASP.

Participation in OWASP projects is a fantastic way for students to build their skills, enhance their resume, and learn from real-world practitioners. All OWASP projects are open to student participation simply by joining a mailing list, asking what needs to be done, and volunteering. Motivated students can start new OWASP projects and get advice and guidance from the world's leading experts. Given the early state of application security, there are many opportunities for groundbreaking research in our field. Consider working on OWASP projects as classroom assignments, such as contributing new lessons to WebGoat, or developing or improving articles at OWASP on application security subjects. Imagine the enthusiasm of your students when their homework will live on as a contribution to the world, rather than simply being graded and discarded.

The OWASP Application Security Code of Conduct for Government Institutions

(The OWASP "Green Book")

Special thanks to Jeff Williams for creating this document, and to Dinis Cruz, Colin Watson, Dave Wichers, and all the participants in the Working Session at the OWASP Summit 2011 in Portugal for their ideas and contributions to this effort.

The OWASP Application Security Code of Conduct for Government Agencies (The OWASP "Green Book")

Introduction

Government Institutions are massive consumers of application technology, and also have influence over the operation of many industries and the behavior of individuals. We believe that Government Institutions should use this power to ensure that software applications are secure enough for their intended purposes. We offer this code of conduct to help guide Government Institutions to improve the state of application security in their own applications and all those under their jurisdiction.

Code of Conduct

1. **The Government Institution MUST establish and enforce a standard that requires application security for organizations and applications under their jurisdiction.**

   Given the rapid influence of application technology over all aspects of modern life, virtually every government institution is now responsible for some aspect of application security. We ask you to establish a standard that captures your requirements for protecting data, ensuring safety, defending citizens, etc… We do not specify the exact form or substance of this standard, only that it represent your desire for applications that affect your jurisdiction to be secure.

2. **The Government Institution MUST build application security into software acquisition guidelines.**

   One of the most powerful forces in the information technology industry is the buying power of governments worldwide. As a massive consumer of application technology, we believe that including appropriate language in acquisition guidelines will strongly encourage the software industry to do a better job with application security. We do not suggest what this language should contain, but point to our Software Security Contract Annex as a possible starting point.

3. **The Government Institution MUST provide OWASP a "notice and comment" period when releasing laws and regulations that are relevant to application security.**

   OWASP wants to help government institutions create laws and regulations that will result in improvements in application security. Ideally, we would be involved from the beginning in the creating of the laws and regulations, but we believe it is critical that we have an opportunity to provide comments and guidance to help shape the final result.

4. **The Government Institution MUST define or adopt a definition of application security.**

   Without a definition of application security, government institutions may struggle with whether a particular issue should be covered or not. We do not try to mandate a single definition of application security for all institutions. Rather, we simply suggest that government institutions must have such a definition in place. We recommend using OWASP materials as a way to help figure out what that definition should encompass.

5. **The Government Institution <u>MUST</u> create and promote public service messages focused on application security.**

   By creating and promoting a public service message that focuses on application security, government institutions demonstrate the importance of this issue in a simple and direct way. We do not attempt to specify the exact form or substance of the message, simply that it should encourage all organizations and individuals to understand the risks and take appropriate action.

Recommendations

6. **The Government Institution <u>SHOULD</u> be an OWASP Supporter.**

   There is no charge for a government institution to become an OWASP Supporter, and it promotes your institution on our website. The main benefit of becoming an OWASP Supporter is to demonstrate your belief that application security is important and that you are working to prepare your students to understand security and write secure code.

7. **The Government Institution <u>SHOULD</u> assign a liaison to the OWASP Government Institution Executive Council.**

   The OWASP Government Institution Executive Council is a group that focuses on improving application security in government institutions. The group collaborates via email and at OWASP events worldwide. We expect the liaison to monitor the list and participate as much as they care to. The institution can define their level of participation. The Liaison will be considered an OWASP Leader and eligible for free attendance at our worldwide events.

8. **The Government Institution <u>SHOULD</u> encourage educational institutions to focus on application security.**

   We believe that educational institutions represent a unique opportunity to influence software developers and other information technology students while they are still forming their ideas, ethics, and values. Government institutions can influence these organizations to focus on application security and hopefully get their institution in line with the OWASP Code of Conduct for Educational Institutions ("The OWASP Blue Book"). Government institutions might take the opportunity to sponsor training in application security for educational institutions.

9. **The Government Institution <u>SHOULD</u> leverage OWASP by attending our events, using our materials, and asking our experts for help.**

   OWASP has a lot to offer government institutions. We have freely available tools, documents, guidelines, and standards. We have worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in classrooms. We even have packaged curricula, eLearning, and educational materials that are available for government institutions to use and modify free of charge. Government institutions are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.

The OWASP Application Security Code of Conduct for Standards Bodies

(The OWASP "Yellow Book")

Special thanks to Jeff Williams for creating this document, and to Dinis Cruz, Colin Watson, Dave Wichers, and all the participants in the Working Session at the OWASP Summit 2011 in Portugal for their ideas and contributions to this effort.

The OWASP Application Security Code of Conduct for Standards Bodies (The OWASP "Yellow Book")

Introduction

The world of information technology is driven largely by standards bodies such as the IETF, ENISA, PCI, ISO, W3C, OASIS, and many more. We believe that every technical standard that involves software in any way should take the time to consider possible application security risks and, if necessary, address them in the standard. OWASP is ready to work with standards bodies and has considerable resources to help standards bodies make good decisions and get application security right.

Code of Conduct

1. **The Standards Body MUST include an "Application Security" section in each software related technical standard.**

   We believe that the most important way to ensure that application security is considered during the development of any technical standard related to software is to require a section focusing on that topic. Even for standards that do not have any need for specific application security requirements, the process of considering possible application security implications and documenting the outcome is a critical part of the standards creation process.

2. **The Standards Body MUST provide OWASP a "notice and comment" period when releasing standards that include an application security aspect.**

   OWASP wants to help standards bodies create strong standards that will secure technologies. Ideally, we would be involved from the beginning in the creating of the standard, but we believe it is critical that we have an opportunity to provide comments and guidance to help shape the final result.

Recommendations

3. **The Standards Body SHOULD be an OWASP Supporter.**

   There is no charge for a standards body to become an OWASP Supporter, and it promotes your organization on our website. The main benefit of becoming an OWASP Supporter is to demonstrate your belief that application security is important and that you are working to help your constituents properly address application security in the projects affected by the standards you develop.

4. **The Standards Body SHOULD assign a liaison to the OWASP Standards Body Executive Council.**

   The OWASP Standards Body Institution Executive Council is a group that focuses on improving application security in standards bodies. The group collaborates via email and at OWASP events worldwide. We expect the liaison to monitor the list and participate as much as they care to. The

standards body can define their level of participation. The Liaison will be considered an OWASP Leader and eligible for free attendance at our worldwide events.

5. **The Standards Body <u>SHOULD</u> define or adopt a definition of Application Security**

   Without a definition of application security, standards bodies may struggle with whether a particular issue should be covered or not. We do not try to mandate a single definition of application security for all standards bodies. Rather, we simply suggest that standards bodies must have such a definition in place. We recommend using OWASP as a way to help figure out what that definition should encompass.

6. **The Standards Body <u>SHOULD</u> leverage OWASP by attending our events, using our materials, and asking our experts for help.**

   OWASP has a lot to offer standards bodies. We have freely available tools, documents, guidelines, and standards. We have worldwide events that are open to everyone and all the presentations are recorded. Participants are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects.

7. **The Standards Body <u>SHOULD</u> involve a security expert early in their standard definition process.**

   Organizations creating standards may want to include a security expert to assist throughout the process of creating a standard. While OWASP does have experts with a very broad array of expertise, we may not understand your domain fully. However, we believe there is huge value in having a security expert available to assist with threat modeling, vulnerability analysis, risk assessment, and other security activities that should be applied during the creation of any technical standard.

The OWASP Application Security Code of Conduct for Certifying Bodies

(The OWASP "Red Book")

Primary Contributors: Jason Li and Jason Taylor

Special thanks to all the participants in the Working Session at the OWASP Summit 2011 in Portugal for their ideas and contributions to this effort.

The OWASP Application Security Code of Conduct for Certifying Bodies (The OWASP "Red Book")

Introduction

As understanding of application security becomes a critical part of an individual's skill set, organizations are eagerly seeking guidance in identifying knowledgeable individuals in application security. We believe that Certifying Bodies can play a role to empower organizations to identify security-minded individuals. While OWASP will ***never*** endorse or support any particular certification, we offer this code of conduct to help guide Certifying Bodies to better serve organizations that are ready to embrace an application security certification.

Code of Conduct

1. **The Certifying Body <u>MUST NOT</u> misrepresent the Certifying Body's certification as endorsed or supported by OWASP.**

   *While OWASP recognizes the need of organizations to identify individuals with an understanding of application security, OWASP will **not** endorse any certifying body or their certification. One of the bedrock principles of OWASP is to maintain a vendor-neutral position and any endorsement of a certifying body or their certification is in direct contradiction of this core value. We respect your desire to fill a void in the application security space and expect that you will in turn respect our core values and brand name.*

2. **The Certifying Body <u>MUST</u> include a visible disclaimer if the Certifying Body's certification is "based on OWASP materials".**

   *OWASP will **not** allow our brand name to be used in the certification title. However, we welcome a Certifying Body to leverage tools, documents, guidelines, and standards that are freely available from OWASP. We recognize that in such cases, a Certifying Body may wish to inform their audience that their certification is "based on OWASP materials". We are honored by your desire to leverage OWASP materials, but we ask that you honor the OWASP name and clearly disclaim that your use of OWASP materials does **not** represent an endorsement or association with OWASP.*

3. **The Certifying Body <u>SHOULD</u> collect and publish feedback from certification applicants, recipients, and organizations recognizing the certification.**

   Certifications represent the Certifying Body's assertion that the recipient meets some minimal criteria, as defined by the Certifying Body. Organizations depend on that assertion when recognizing a Certifying Body's certification. We believe that organizations need feedback to effectively determine the value of a certification. We do not suggest what feedback should be solicited, nor the exact form or method for this publication; only that it represents your desire to honestly communicate the value and esteem or your certification.

4. **The Certifying Body <u>SHOULD</u> utilize questions, answers, evaluation material and processes that are open and freely available to the general public.**

   Organizations around the world are depending on certifying bodies to help identify individuals that understand application security. Supplying open questions and answers allows organizations to evaluate for themselves whether or not a certification adequately satisfies their need. We ask you publish the bank of all questions and answers for any examination-based certification. We do not specify the exact form or method for administering the exam nor for publishing the questions and answers; only that it represents your desire to enable organizations to understand and evaluate the substance of your examination as it pertains to their organizational needs. OWASP suggests that the certifying body uses questions and answers developed by the OWASP community.

5. **The Certifying Body <u>SHOULD</u> be an OWASP Supporter.**

   The main benefit of becoming an OWASP Supporter is to demonstrate your belief that application security is important and that you are working to help improve the state of application security in the world.

6. **The Certifying Body <u>SHOULD</u> leverage OWASP by attending our events, using our materials, and asking our experts for help.**

   OWASP has a lot to offer certifying bodies. We have freely available tools, documents, guidelines, and standards. We have worldwide events that are open to everyone and all the presentations are recorded and downloadable for use in classrooms. We even have packaged curricula, eLearning, and educational materials that are available for potential applicants to use and modify free of charge. Certifying bodies are strongly encouraged to reach out to our experts with their questions, ideas, and even participate in projects

DOM based XSS Prevention Cheat Sheet

Introduction

When looking at XSS (Cross-Site Scripting), there are three generally recognized forms of XSS. Reflected, Stored, and DOM Based XSS. The XSS Prevention Cheat Sheet does an excellent job of addressing Reflected and Stored XSS. This cheat sheet addresses DOM (Document Object Model) based XSS and is an extension (and assumes comprehension of) the XSS Prevention Cheat Sheet.

In order to understand DOM based XSS, one needs to see the fundamental difference between reflected and stored XSS when compared to DOM based XSS. Reflected and Stored XSS exist in a higher level rendering context and DOM based XSS is primarily found in a lower level execution context. A rendering context is associated with the parsing of HTML tags and their attributes. The HTML parser of the rendering context dictates how data is presented and laid out on the page and can be further broken down into the standard contexts of HTML, HTML attribute, URL, and CSS. The JavaScript or VBScript parser of an execution context is associated with the parsing and execution of script code. Each parser has distinct and separate semantics in the way they can possibly execute script code (XSS) which make creating consistent rules for mitigating both rendering and execution based contexts difficult. The complication is compounded by the differing meanings and treatment of encoded values within each subcontext (HTML, HTML attribute, URL, and CSS) within the execution context.

This paper refers to the HTML, HTML attribute, URL, and CSS Cheat Sheet contexts as subcontexts because each of these contexts can be reached and set within a JavaScript execution context. In JavaScript code, the main context is JavaScript but since an attacker can try to attack the other 4 contexts using equivalent JavaScript DOM methods, we refer to the other contexts besides the JavaScript context as subcontexts.

The following is an example of an attack which occurs in the JavaScript context and HTML subcontext:

```
<script>
var x = '<%= htmlAndJavaScriptEncodedVar %>';
var d = document.createElement('div');
d.innerHTML = x;
document.body.appendChild(d);
</script>
```

One consistency, however, is the need to JavaScript encode in addition to the encoding required for the subcontext in the execution context. Let's look at the individual subcontexts of the execution context in turn.

HTML Subcontext within the Execution Context

There are several methods and attributes which can be used to directly render HTML content within JavaScript. These methods constitute the HTML Subcontext within the Execution Context.

Attributes

```
element.innerHTML = "<HTML> Tags and markup";
element.outerHTML = "<HTML> Tags and markup";
```

Methods

```
document.write("<HTML> Tags and markup");
document.writeln("<HTML> Tags and markup");
```

Guideline

In a pure HTML execution context (not HTML Attribute) use HTML and JavaScript encoding to mitigate against attacks.

```
element.innerHTML =
"<%=Encoder.encodeForJS(Encoder.encodeForHTML(untrustedData))%>";
element.outerHTML =
"<%=Encoder.encodeForJS(Encoder.encodeForHTML(untrustedData))%>";
```

Methods

```
document.write("<%=Encoder.encodeForJS(Encoder.encodeForHTML(untrusted
Data))%>");
document.writeln("<%=Encoder.encodeForJS(Encoder.encodeForHTML(untrust
edData))%>");
```

HTML Attribute Subcontext within the Execution Context

The HTML attribute Subcontext within the Execution context is divergent from the standard encoding rules. This is because the rule to HTML attribute encode in an HTML attribute rendering context is mitigating attacks which try to exit out of the attribute to add additional attributes and/or tags which could have executable code. When you are in a DOM execution context you only need to JavaScript encode HTML attributes which do not execute code (attributes other than event handler, CSS, and URL attributes).

For example, the general rule is to HTML Attribute encode untrusted data (data from the database, http request, user, backend system, etc.) placed in an HTML Attribute. This is the appropriate step to take when outputting data in a rendering context, however using HTML Attribute encoding in an execution context will break the application display of data.

```
var x = document.createElement("input");
x.setAttribute("name", "company_name");
x.setAttribute("value",
'<%=Encoder.encodeForJS(Encoder.encodeForHTMLAttr(companyName))%>');
var form1 = document.forms[0];
form1.appendChild(x);
```

The problem is that if companyName had the value "Johnson & Johnson". What would be displayed in the input text field would be "Johnson & Johnson". The appropriate encoding to use in the above case would be only JavaScript encoding to disallow an attacker from closing out the single quotes and in-lining code, or escaping to HTML and opening a new script tag.

```
var x = document.createElement("input");
x.setAttribute("name", "company_name");
```

```
x.setAttribute("value", '<%=Encoder.encodeForJS(companyName)%>');
var form1 = document.forms[0];
form1.appendChild(x);
```

It is important to note that when setting an HTML attribute which does not execute code the value is set directly within the object attribute of the HTML element so there is no concerns with injecting up.

URL Attribute Subcontext within the Execution Context

The logic which parses URLs in both execution and rendering contexts looks to be the same. Therefore there is little change in the encoding rules for URL attributes in an execution (DOM) context.

```
var x = document.createElement("a");
x.setAttribute("href",
'<%=Encoder.encodeForJS(Encoder.encodeForURL(userRelativePath))%>');
var y = document.createTextElement("Click Me To Test");
x.appendChild(y);
document.body.appendChild(x);
```

If you utilize fully qualified URLs then this will break the links as the colon in the protocol identifier ("http:" or "javascript:") will be URL encoded preventing the "http" and "javascript" protocols from being invoked.

CSS Attribute Subcontext within the Execution Context

Normally executing JavaScript from a CSS context required either passing `javascript:attackCode()` to the CSS url() method or invoking the CSS expression() method passing JavaScript code to be directly executed. From my experience, calling the expression() function from an execution context (JavaScript) has been disabled. In order to mitigate against the CSS url() method ensure that you are URL encoding the data passed to the CSS url() method.

```
document.body.style.backgroundImage =
"url(<%=Encoder.encodeForJS(Encoder.encodeForURL(companyName))%>)";
```

TODO: We have not been able to get the expression() function working from DOM JavaScript code. Need some help.

Event Handler and JavaScript code Subcontexts within an Execution Context

Putting dynamic data within JavaScript code is especially dangerous because JavaScript encoding has different semantics for JavaScript encoded data when compared to other encodings. In many cases, JavaScript encoding does not stop attacks within an execution context. For example, a JavaScript encoded string will execute even though it is JavaScript encoded.

```
var x = document.createElement("a");
x.href="#";
x.setAttribute("onclick",
"\u0061\u006c\u0065\u0072\u0074\u0028\u0032\u0032\u0029");
var y = document.createTextNode("Click To Test");
```

```
x.appendChild(y);
document.body.appendChild(x);
```

The setAttribute(*name_string*,*value_string*) method is dangerous because it implicitly coerces the *string_value* into the DOM attribute datatype of *name_string*. In the case above, the attribute name is a JavaScript event handler, so the attribute value is implicitly converted to JavaScript code and evaluated. In the case above, JavaScript encoding does not mitigate against DOM based XSS. Other JavaScript methods which take code as a string types will have a similar problem as outline above (setTimeout, setInterval, new Function, etc.). This is in stark contrast to JavaScript encoding in the event handler attribute of a HTML tag (HTML parser) where JavaScript encoding mitigates against XSS.

```
<a id="bb" href="#"
onclick="\u0061\u006c\u0065\u0072\u0074\u0028\u0031\u0029"> Test
Me</a>
```

An alternative to using Element.setAttribute(...) to set DOM attributes is to set the attribute directly. Directly setting event handler attributes will allow JavaScript encoding to mitigate against DOM based XSS.

```
   <a id="bb" href="#"> Test Me</a>
          //The following does NOT work because the event handler is
being set to a string.  "alert(7)" is JavaScript encoded.
          document.getElementById("bb").onclick =
"\u0061\u006c\u0065\u0072\u0074\u0028\u0037\u0029";

          //The following does NOT work because the event handler is
being set to a string.
          document.getElementById("bb").onmouseover = "testIt";
          //The following does NOT work because of the encoded "("
and ")". "alert(77)" is JavaScript encoded.
          document.getElementById("bb").onmouseover =
\u0061\u006c\u0065\u0072\u0074\u0028\u0037\u0037\u0029;
          //The following does NOT work because of the encoded ";".
"testIt;testIt" is JavaScript encoded.
          document.getElementById("bb").onmouseover =
\u0074\u0065\u0073\u0074\u0049\u0074\u003b\u0074\u0065\u0073\u0074\u00
49\u0074;

          //The following DOES WORK because the encoded value is a
valid variable name or function reference.  "testIt" is JavaScript
encoded
          document.getElementById("bb").onmouseover =
\u0074\u0065\u0073\u0074\u0049\u0074;
          function testIt() {

              alert("I was called.");
          }
```

There are other places in JavaScript where JavaScript encoding is accepted as valid executable code.

```
for ( var \u0062=0; \u0062 < 10; \u0062++){
```

```
    \u0064\u006f\u0063\u0075\u006d\u0065\u006e\u0074
    .\u0077\u0072\u0069\u0074\u0065\u006c\u006e

("\u0048\u0065\u006c\u006c\u006f\u0020\u0057\u006f\u0072\u006c\u0064")
;
}
\u0077\u0069\u006e\u0064\u006f\u0077
.\u0065\u0076\u0061\u006c
\u0064\u006f\u0063\u0075\u006d\u0065\u006e\u0074
.\u0077\u0072\u0069\u0074\u0065(111111111));
```

or

```
var s = "\u0065\u0076\u0061\u006c";
var t = "\u0061\u006c\u0065\u0072\u0074\u0028\u0031\u0031\u0029";
window[s](t);
```

Because JavaScript is based on an international standard (ECMAScript), JavaScript encoding enables the support of international characters in programming constructs and variables in addition to alternate string representations (string escapes).

However the opposite is the case with HTML encoding. HTML tag elements are well defined and do not support alternate representations of the same tag. So HTML encoding cannot be used to allow the developer to have alternate representations of the <a> tag for example.

HTML Encoding's Disarming Nature
In general, HTML encoding serves to castrate HTML tags which are placed in HTML and HTML attribute contexts. Working example (no HTML encoding):
`<a href="…" >`

Normally encoded example (Does Not Work – DNW):

```
&#x3c;a href=… &#x3e;
```

HTML encoded example to highlight a fundamental difference with JavaScript encoded values (DNW):

```
<&#x61; href=…>
```

If HTML encoding followed the same semantics as JavaScript encoding. The line above could have possibly worked to render a link. This difference makes JavaScript encoding a less viable weapon in our fight against XSS.

Guidelines for Developing Secure Applications Utilizing JavaScript

DOM based XSS is extremely difficult to mitigate against because of its large attack surface and lack of standardization across browsers. The guidelines below are an attempt to provide guidelines for developers when developing Web based JavaScript applications (Web 2.0) such that they can avoid XSS.

1. Untrusted data should only be treated as displayable text. Never treat untrusted data as code or markup within JavaScript code.
2. Always JavaScript encode and delimit untrusted data as quoted strings when entering the application (Jim Manico and Robert Hansen)

```
var x = "<%=encodedJavaScriptData%>";
```

3. Use `document.createElement("…"), element.setAttribute("…","value"), element.appendChild(…)`, etc. to build dynamic interfaces. Avoid use of HTML rendering methods:

1. `element.innerHTML = "…";`
2. `element.outerHTML = "…";`
3. `document.write(…);`
4. `document.writeln(…);`

4. Understand the dataflow of untrusted data through your JavaScript code. If you do have to use the methods above remember to HTML and them JavaScript encode the untrusted data (Stefano Di Paola).
5. There are numerous methods which implicitly eval() data passed to it. Make sure that any untrusted data passed to these methods is delimited with string delimiters and enclosed within a closure or JavaScript encoded to N-levels based on usage, and wrapped in a custom function. Ensure to follow step 4 above to make sure that the untrusted data is not sent to dangerous methods within the custom function or handle it by adding an extra layer of encoding.

Utilizing an Enclosure (as suggested by Gaz)

The example that follows illustrates using closures to avoid double JavaScript encoding.

```
setTimeout((function(param) { return function() {
         customFunction(param);
         }
})("<%=Encoder.encodeForJS(untrustedData)%>"), y);
```

The other alternative is using N-levels of encoding.

N-Levels of Encoding

If your code looked like the following, you would need to only double JavaScript encode input data.

```
setTimeout("customFunction('<%=doubleJavaScriptEncodedData%>', y)");
function customFunction (firstName, lastName)
      alert("Hello" + firstName + " " + lastNam);
}
```

The `doubleJavaScriptEncodedData` has its first layer of JavaScript encoding reversed in the single quotes. Then the implicit `eval()` of `setTimeout()` reverses another layer of JavaScript encoding to pass the correct value to `customFunction`. The reason why you only need to double JavaScript encode is that the `customFunction` function did not itself pass the input to another method which implicitly or explicitly called `eval()`. If "firstName" was passed to another JavaScript method

which implicitly or explicitly called eval() then `<%=doubleJavaScriptEncodedData%>` above would need to be changed to `<%=tripleJavaScriptEncodedData%>`.

An important implementation note is that if the JavaScript code tries to utilize the double or triple encoded data in string comparisons, the value may be interpreted as different values based on the number of evals() the data has passed through before being passed to the if comparison and the number of times the value was JavaScript encoded.

If "A" is double JavaScript encoded then the following if check will return false.

```
var x = "doubleJavaScriptEncodedA";
//\u005c\u0075\u0030\u0030\u0034\u0031
if (x == "A") {
   alert("x is A");
} else if (x == "\u0041") {
   alert("This is what pops");
}
```

This brings up an interesting design point. Ideally, the correct way to apply encoding and avoid the problem stated above is to server-side encode for the output context where data is introduced into the application. Then client-side encode (using a JavaScript encoding library such as ESAPI4JS) for the individual subcontext (DOM methods) which untrusted data is passed to. ESAPI4JS (located at http://bit.ly/9hRTLH) and jQuery Encoder (located at https://github.com/chrisisbeef/jquery-encoder/blob/master/src/main/javascript/org/owasp/esapi/jquery/encoder.js) are two client side encoding libraries developed by Chris Schmidt.
Here are some examples of how they are used:

```
var input = "<%=Encoder.encodeForJS(untrustedData)%>";  //server-side
encoding
window.location = ESAPI4JS.encodeForURL(input);  //URL encoding is
happening in JavaScript
document.writeln(ESAPI4JS.encodeForHTML(input));  //HTML encoding is
happening in JavaScript
```

It has been well noted by the group that any kind of reliance on a JavaScript library for encoding would be problematic as the JavaScript library could be subverted by attackers. One option is to wait till ECMAScript 5 so the JavaScript library could support immutable properties.
Another option provided by Gaz (Gareth) was to use a specific code construct to limit mutability with anonymous clousures.

An example follows:

```
function escapeHTML(str) {
     str = str + "";
     var out = "";
     for(var i=0; i<str.length; i++) {
         if(str[i] === '<') {
             out += '&lt;';
         } else if(str[i] === '>') {
             out += '&gt;';
```

```
            } else if(str[i] === "'") {
                out += '&#39;';
            } else if(str[i] === '"') {
                out += '&quot;';
            } else {
                out += str[i];
            }
        }
        return out;
}
```

Chris Schmidt has put together another implementation of a JavaScript encoder at http://yet-another-dev.blogspot.com/2011/02/client-side-contextual-encoding-for.html.

6. Limit the usage of dynamic untrusted data to right side operations. And be aware of data which may be passed to the application which look like code (e.g. `location`, `eval()`). (Achim)

```
var x = "<%=properly encoded data for flow%>";
```

If you want to change different object attributes based on user input use a level of indirection.

Instead of:

```
window[userData] = "moreUserData";
```

Do the following instead:

```
if (userData==="location") {
   window.location = "static/path/or/properly/url/encoded/value";
}
```

7. When URL encoding in DOM be aware of character set issues as the character set in JavaScript DOM is not clearly defined (Mike Samuel).

8. Limit access to properties objects when using object[x] accessors. (Mike Samuel). In other words use a level of indirection between untrusted input and specified object properties.
Here is an example of the problem when using map types:

```
var myMapType = {};
myMapType[<%=untrustedData%>] = "moreUntrustedData";
```

Although the developer writing the code above was trying to add additional keyed elements to the `myMapType` object. This could be used by an attacker to subvert internal and external attributes of the `myMapType` object.

9. Run your JavaScript in an ECMAScript 5 canopy or sand box to make it harder for your JavaScript API to be compromised (Gareth Heyes and John Stevens).

10. Don't `eval()` JSON to convert it to native JavaScript objects. Instead use `JSON.toJSON()` and `JSON.parse()` (Chris Schmidt).

Common Problems Associated with Mitigating DOM Based XSS

Complex Contexts

In many cases the context isn't always strait forward to discern.

```
<a href="javascript:myFunction('<%=untrustedData%>', 'test');">Click
Me</a>
...
<script>
Function myFunction (url,name) {
    window.location = url;
}
</script>
```

In the above example, untrusted data started in the rendering URL context (`href` attribute of an `<a>` tag) then changed to a JavaScript execution context (`javascript:` protocol handler) which passed the untrusted data to an execution URL subcontext (`window.location` of myFunction). Because the data was introduced in JavaScript code and passed to a URL subcontext the appropriate server-side encoding would be the following:

```
<a href="javascript:myFunction('<%=Encoder.encodeForJS( ↩
              Encoder.encodeForURL(untrustedData))%>', 'test');">Click
Me</a>
…
```

Or if you were using ECMAScript 5 with an immutable JavaScript client-side encoding libraries you could do the following:

```
<!--server side URL encoding has been removed.  Now only JavaScript
encoding on server side. -->
<a
href="javascript:myFunction('<%=Encoder.encodeForJS(untrustedData)%>',
'test');">Click Me</a>
...
<script>
Function myFunction (url,name) {
    var encodedURL = ESAPI4JS.encodeForURL(url);  //URL encoding using
client-side scripts
    window.location = encodedURL;
}
</script>
```

Inconsistencies of Encoding Libraries

There are a number of open source encoding libraries out there:

1. ESAPI
2. Apache Commons String Utils
3. Jtidy
4. Your company's custom implementation.

Some work on a black list others ignore important characters like "<" and ">". ESAPI is one of the few which work on a whitelist and encode all non-alpha numeric characters. It is important to use an encoding library which understands which characters can be used to exploit vulnerabilities in their respective contexts. But there are misconceptions abound related to proper encoding.

Encoding Misconceptions

Many security training curriculums and papers advocate the blind usage of HTML encoding to resolve XSS. This logically seems to be prudent advice as the JavaScript parser does not understand HTML encoding. However, if the pages returned from your web application utilize a content type of "text/xhtml" or the file type extension of "*.xhtml" then HML encoding may not work to mitigate against XSS.

For example:

```
<script>
&#x61;lert(1);
</script>
```

The HTML encoded value above is still executable. If that isn't enough to keep in mind, you have to remember that encodings are lost when you retrieve them using the value attribute of a DOM element.

Let's look at the sample page and script:

```
<form name="myForm" …>
  <input type="text" name="lName"
value="<%=Encoder.encodeForHTML(last_name)%>">
…
</form>
<script>
var x = document.myForm.lName.value;  //when the value is retrieved
the encoding is reversed
document.writeln(x);  //any code passed into lName is now executable.
</script>
```

Finally there is the problem that certain methods in JavaScript which are usually safe can be unsafe in certain contexts.

Usually Safe Methods

One example of an attribute which is usually safe is innerText. Some papers or guides advocate its use as an alternative to innerHTML to mitigate against XSS in innerHTML. However, depending on the tag which innerText is applied, code can be executed.

```
<script>
var tag = document.createElement("script");
tag.innerText = "<%=untrustedData%>";  //executes code
</script>
```

Authors and Contributing Editors

Jim Manico - jim[at]owasp.org

Abraham Kang - abraham.kang[at]owasp.org

Gareth (Gaz) Heyes

Stefano Di Paola

Achim Hoffmann

Robert (RSnake) Hansen

Mario Heiderich

John Steven

Chris (Chris BEF) Schmidt

Mike Samuel

Jeremy Long

Edwardo (SirDarkCat) Alberto Vela Nava

Jeff Williams - jeff.williams[at]owasp.org

Erlend Oftedal

Other Articles in the OWASP Prevention Cheat Sheet Series

- Authentication Cheat Sheet
- Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet
- Forgot Password Cheat Sheet
- Cryptographic Storage Cheat Sheet
- SQL Injection Prevention Cheat Sheet
- Transport Layer Protection Cheat Sheet
- XSS (Cross Site Scripting) Prevention Cheat Sheet

OWASP FOUNDATION

ByLaws

Approved: 23-June-2011

ARTICLE I - OFFICES

Section 1.01. Offices The principal office of the Foundation in the State of Maryland, shall be located in County of Howard. The Foundation may have such other offices, either within or without the State of Maryland, as the Board of Directors may designate or as the business of the Foundation may require from time to time.

Section 1.02. Purpose. The OWASP Foundation will be the thriving global community that drives visibility and evolution in the safety and security of the world's software.

Section 1.03. Values. OPEN: Everything at OWASP is radically transparent from our finances to our code. **INNOVATION:** OWASP encourages and supports innovation/experiments for solutions to software security challenges. **GLOBAL:** Anyone around the world is encouraged to participate in the OWASP community. **INTEGRITY:** OWASP is an honest and truthful, vendor agnostic, global community.

ARTICLE II - AUTHORITY AND DUTIES OF OFFICERS

SECTION 2.01 Each Board Member will be assigned one of the following roles: Board Chair, Vice Chair, Secretary, Treasurer, or Board Member at large. These roles will carry the following responsibilities:

a. Board Chair - Provides leadership to the Board of Directors, who sets policy, Chairs meetings of the Board, encourages board's role in strategic planning, serves ex officio as a member of committees and attends their meetings when invited, helps guide and mediate board actions with respect to organizational priorities and governance concerns, monitors financial planning and financial reports, plays a leading role in fundraising activities, formally evaluates the performance of the Foundation Director and informally evaluates the effectiveness of the board members. Evaluates annually the performance of the organization in achieving its mission, performs other responsibilities assigned by the Board.

b. Vice Chair - performs Chair responsibilities when the Chair cannot be available, works closely with Chair and other Board Members, participates closely with Chair to develop and implement officer transition plans, performs other responsibilities as assigned by the Board.

c. Secretary - maintains records of the board and ensures effective management of organization's records, manages minutes of board meetings, ensures minutes are distributed shortly after each meeting, is sufficiently familiar with legal documents (articles, by-laws, IRS letters, etc.) to note applicability during meetings.

d. Treasurer - manages finances of the organization, administrates fiscal matters of the organization, provides annual budget to the board for member's approval, ensures development and board review of financial policies and procedures.

e. Board Member at large - regularly attends board meetings and important related meetings, volunteers for and willingly accepts assignments and completes them thoroughly and on time, stays informed about committee matters, prepares themselves well for meetings, and reviews and comments on minutes and reports, gets to know other committee members and builds a collegial working relationship that contributes to consensus, is an active participant in

the committee's annual evaluating and planning efforts, participates in fund raising for the organization.

SECTION 2.02 Election and Term of Office. Each Board member will serve for a term of 2 years. The role of the Board Members shall be elected by the Board of Directors at the first meeting following the election of the Board of Directors. If the election of officers shall not be held at such meeting, such election shall be held as soon thereafter as conveniently may be. Each officer shall hold that role until the next election has been completed.

SECTION 2.03 Resignation. Resignations are effective upon receipt by the Secretary of the Board of a written notification.

SECTION 2.04 Removal. Any officer, contractor, member, or director may be removed by a unanimous vote of the Board of Directors whenever, in its judgment, the best interests of the Foundation will be served thereby, but such removal shall be without prejudice to the contract rights, if any, of the person so removed. Election or appointment of an officer, agent, or director shall not of itself create contract rights, and such appointment shall be terminable at will.

SECTION 2.05 Vacancies. A vacancy in any office because of death, resignation, removal, disqualification or otherwise, may be filled by the Board of Directors for the unexpired portion of the term.

SECTION 2.06 Chairman of the Board. The Chairman of the Board shall be the principal executive officer of the Foundation and, subject to the control of the Board of Directors, shall in general supervise and control all of the business and affairs of the Foundation. He or she shall, when present, preside at all meetings of the Board of Directors, unless otherwise delegated. She or he may sign, with the Secretary or any other proper officer of the Foundation thereunto authorized by the Board of Directors, any deeds, mortgages, bonds, contracts, or other instruments which the Board of Directors has authorized to be executed, except in cases where the signing and execution thereof shall be expressly delegated by the Board of Directors or by these Bylaws to some other officer or agent of the Foundation, or shall be required by law to be otherwise signed or executed; and in general shall perform all duties incident to the office of Chairman of the Board and such other duties as may be prescribed by the Board of Directors from time to time.

SECTION 2.07 Secretary. The Secretary shall:
(a) Keep the minutes of the proceedings of the Board of Directors in one or more minute books provided for that purpose; (b) See that all notices are duly given in accordance with the provisions of these Bylaws or as required by law; (c) Be custodian of the corporate records and of the seal of the Foundation and see that the seal of the Foundation is affixed to all documents, the execution of which on behalf of the Foundation under its seal is duly authorized; (d) Keep a register of the post office address of each Director which shall be furnished to the Secretary by such Director; and (e) In general perform all duties incident to the office of the Secretary and such other duties as from time to time may be assigned to him by the Chairman of the Board or by the Board.

ARTICLE III - BOARD OF DIRECTORS

SECTION 3.01. General Powers and Authority. The business and affairs of the Foundation shall be managed by its Board of Directors

SECTION 3.02. Number, Tenure, and Qualifications. The number of directors of the Foundation shall be no less than five and no more than seven. Each director shall hold office for two years unless duly removed as prescribed in Section 5.5.03 and 5.04. Each director must be elected as prescribed in the election policy and procedure.

SECTION 3.03. Regular Meetings. The Board of Directors shall have regular meetings monthly. Meetings shall be at such dates, times, and places as the Board shall determine. These meetings will be open to public attendance. Attendance by board members is required at no less than 8 of the 12 meetings per year (1 per month) and shall meet in person at least once annually at a date to be announced and agreed upon.

SECTION 3.04 Special Meetings. Special meetings of the Board of Directors may be called by or at the request of the Chairman or any two directors. The person or persons authorized to call special meetings of the Board of Directors may fix the place for holding any special meeting of the Board of Directors called by them.

SECTION 3.05 Notice of Special Meetings. A special meeting may be called by the Chairman or at the request of any two (2) Board members by notice emailed, telephone, or telegraphed to each Board member not less one week before such meetings. Any directors may waive notice of any meeting. The attendance of a director at a meeting shall constitute a waiver of notice of such meeting, except where a director attends a meeting for the express purpose of objecting to the transaction of any business because the meeting is not lawfully called or convened.

SECTION 3.06 Quorum. A majority of the number of Directors fixed by Section 2 of this Article shall constitute a quorum for the transaction of business at any meeting of the Board of Directors. If less than such majority is present at a meeting, a majority of the Directors present may adjourn the meeting from time to time without further notice. All decisions will be made by majority vote of those present at a meeting at which a quorum is present. If a board of Directors vote results in a split decision, the Chairman of the Board, if present at the meeting, can decide the issue.

SECTION 3.07 Participation in Meeting by Conference Telephone. Members of the Board may participate in a meeting through use of conference telephone or similar communication equipment, so long as members participating in such meeting can hear one another. A quorum must be maintained at all times during the meeting or the meeting will not continue.

SECTION 3.08 Manner of Acting. The act of the majority of the directors present at a meeting at which a quorum is present shall be the act of the Board of Directors.

SECTION 3.09 Action Without a Meeting. Any action that may be taken by the Board of Directors at a meeting may be taken without a meeting if consent in writing, setting forth the

action so to be taken, shall be agreed to before such action by a majority of the directors. Such consent can be provided by email.

SECTION 3.10 Vacancies. Any vacancy occurring in the Board of Directors may be filled by the affirmative vote of a majority of the remaining directors though less than a quorum of the Board of Directors, unless otherwise provided by law. If there is an equal number of affirmative and negative votes then the ultimate determination shall be made by the then-sitting Chairman of the Board. A director elected to fill a vacancy shall be elected for the unexpired term of his predecessor in office. Any directorship to be filled by reason of an increase in the number of directors may be filled by election by the Board of Directors for a term of office continuing only until the next election of directors by the Directors.

SECTION 3.11 Employment. No paid employee can serve on the board of directors or in the role of Officer while they are employed in a paid position by the Foundation.

SECTION 3.12. Reimbursement. Directors shall serve without compensation with the exception that expenses incurred in the furtherance of the Foundation's business are allowed to be reimbursed with documentation and prior approval according to the Reimbursement Policy.

SECTION 3.13. Presumption of Assent A director of the Foundation who is present at a meeting of the Board of Directors at which action on any corporate matter is taken shall be presumed to have assented to the action taken unless his dissent shall be entered in the minutes of the meeting or unless he shall file his written dissent to such action with the person acting as the Secretary of the meeting before the adjournment thereof, or shall forward such dissent to the Secretary of the Foundation immediately after the adjournment of the meeting. Such right to dissent shall not apply to any director who voted in favor of such action.

ARTICLE IV - MEMBERS

SECTION 4.01. Membership Classes. There shall be three classes of OWASP members: Corporate, Individual, and Educational.

SECTION 4.02. Qualifications. Membership may be granted to any individual or organization that supports the mission and purposes of the Foundation, and who pays the annual dues as set by the Board of Directors or is approved by the Board of Directors as having provided a benefit to the organization deserving of membership.

SECTION 4.03. Termination of Membership. The Board of Directors, by affirmative vote of two-thirds of all members of the Board, may suspend or expel a member, and may, by a majority vote of those present at any regularly constituted meeting, terminate, suspend or expel the membership of any member who becomes ineligible for membership.

SECTION 4.04. Resignation. Any member may resign by filing a written resignation with the Secretary; however, such resignation shall not relieve the member so resigning of the obligation to pay any dues or other charges theretofore accrued and unpaid.

SECTION 4.05. Dues. Dues for members shall be established by the Board of Directors.

SECTION 4.06. Voting. Each member shall be entitled to vote on designated matters. The affirmative vote of a majority of the members or by proxy shall be the act of the members as a whole unless a greater number of members is required by law or stated otherwise in these Bylaws.

ARTICLE V - ADVISORY BOARDS, COMMITTEES AND LOCAL CHAPTERS

SECTION 5.01 Establishment The Board of Directors may, by resolution adopted by a majority of the Directors in office, establish one or more Advisory Boards or Committees. Committees will be held to the core purpose and core values as outlined in Sections 1.02 and 1.03. Committees will be structured according to the guidelines in Policy and Procedure.

SECTION 5.02 Local Chapters A local OWASP chapter may establish smaller, local chapters within the geographical boundary of a chapter, such as country or a city. The bylaws of a chapter must not contain anything that is at variance with the expressed purposes of the OWASP Foundation or with the OWASP Foundation Bylaws, and must be approved as specified by the OWASP Foundation Board of Directors before becoming effective. A chapter may not change its bylaws, its name, or its boundaries without approval as specified by the OWASP Foundation. Chapter Bylaws may be produced in the native language of a nation, but must be translated into English for submission to the OWASP Foundation.
The chapter leader and local chapter board has to manage the local chapter according to the guidance and rules defined in the Chapter Leader Handbook. The Global Chapters Committee provides the support required by the local chapters to thrive and contribute to the overall mission and goals of the OWASP Foundation.

The OWASP Foundation may, by affirmative vote of a majority of the Board of Directors, suspend or annul a chapter if, in the judgment of the Board of Directors, such action is in the best interests of the OWASP Foundation.

ARTICLE VI - INDEMNITY

SECTION 6.01 Indemnity. The Foundation shall indemnify the Officers of the Foundation including International Board Members and Employees, or agents as follows:
(a) Every Officer, Board Member, and employee of the Foundation shall be indemnified by the Foundation against all expenses and liabilities, including counsel fees, reasonably incurred by or imposed upon him or her in connection with any proceeding to which he or she may be made a party, or in which he or she may become involved, by reason of being or having been a director, officer, employee or agent of the Foundation or is or was serving at the request of the Foundation as a director, officer, employee or agent of the Foundation, partnership, joint venture, trust or enterprise, or any settlement thereof, whether or not he is a director, officer, employee or agent at the time such expenses are incurred, except in such cases wherein the director, officer, employee

or agent is adjudged guilty of willful misfeasance or malfeasance in the performance of his or her duties; provided that in the event of a settlement the indemnification herein shall apply only when the Board of Directors approves such settlement and reimbursement as being in the best interests of the Foundation.
(b) The Foundation shall provide to any person who is or was an officer, board member, or employee, or agent of the Foundation or is or was serving at the request of the Foundation as a director, officer, employee or agent of the Foundation, partnership, joint venture, trust or enterprise, the indemnity against expenses of suit, litigation or other proceedings which is specifically permissible under applicable law.
(c) The Board of Directors may, in its discretion, direct the purchase of liability insurance by way of implementing the provisions of this Article VI.

ARTICLE VII - CONFLICTS OF INTEREST

SECTION 7.01 Conflict defined. A conflict of interest may exist when any director, officer, or staff member may be seen as having interests which are adverse to the interests of the Foundation. Prior to any vote of the Board of Directors, a conflict of interest statement shall be made by any Board Member who is aware of any potential conflicts of interest to ensure that all parties are aware of any such conflicts.

SECTION 7.02. Disclosure required. Any conflict of interest shall be disclosed to the Board of Directors by the person concerned. When any conflict of interest is relevant to a matter requiring action by the Board of Directors, the interested person shall call it to the attention of the Board of Directors or its appropriate committee and such person shall not vote on the matter; provided however, any Director disclosing a possible conflict of interest may be counted in determining the presence of a quorum at a meeting of the Board of Directors or a committee thereof.

SECTION 7.03. Absence from discussion. The person having the conflict shall not participate in the decision regarding the matter under consideration.

SECTION 7.04. Minutes. The minutes of the meeting of the Board or committee shall reflect that the conflict of interest was disclosed and that the interested person did not vote. When there is doubt as to whether a conflict of interest exists, the matter shall be resolved by a vote of the Board of Directors or its committee, excluding the vote of the person concerning whose situation the doubt has arisen.

SECTION 7.05. Annual review. A copy of this conflict of interest statement shall be furnished to each director, officer, and staff member who is presently serving the Foundation, or who may hereafter become associated with the Foundation. This policy shall be reviewed periodically for the information and guidance of directors, officers, and staff members. Any new directors, officers, or staff members shall be advised of this policy upon undertaking the duties of such office.

ARTICLE VIII - CONTRACTS AND FINANCIAL ADMINISTRATION

SECTION 8.01 Fiscal Year. The fiscal year of the Foundation shall be January 1-December 31 but may be changed by resolution of the Board of Directors.

SECTION 8.02.**Contracts.** The Board of Directors may authorize any officer or officers, agent or agents, to enter into any contract or execute and deliver any instrument in the name of and on behalf of the Foundation, and such authority may be general or confined to specific instances. This authorization must be in writing (electronic communication is acceptable) in the minutes of any meeting that provides such limited authority.

SECTION 8.03. Loans. No loans shall be contracted on behalf of the Foundation and no evidences of indebtedness shall be issued in its name unless authorized by a resolution of the Board of Directors. Such authority may be general or confined to specific instances.

SECTION 8.04. Checks, Drafts, etc. All checks, drafts or other orders for the payment of money, notes or other evidences of indebtedness issued in the name of the Foundation, shall be signed by such officer or officers, agent or agents of the Foundation and in such manner as shall from time to time be determined by resolution of the Board of Directors.

SECTION 8.05. Deposits. All funds of the Foundation not otherwise employed shall be deposited from time to time to the credit of the Foundation in such banks, trust companies or other depositories as the Board of Directors may select.

ARTICLE IX - BOOKS AND RECORDS

SECTION 9.01. Books. Correct books of account of the activities and transactions of the Foundation shall be kept at the office of the Foundation and are available on demand in hard or electronic copy.

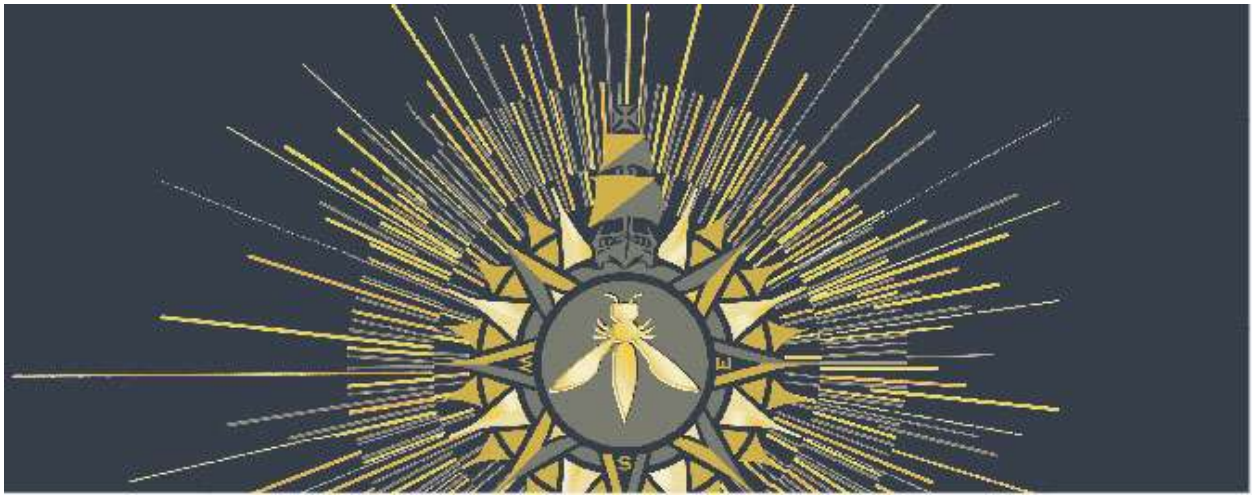
SECTION 9.02 Audit. A complete financial audit will be performed every 3 years by a third party, independent auditor.

ARTICLE X - AMENDMENT OF BYLAWS

SECTION 10.01. Amendments. These Bylaws may be amended by a majority vote of the Board of Directors, provided prior notice is given of the proposed amendment in the notice of the meeting at which such action is taken, or provided all members of the Board waive such notice, or by unanimous consent in writing without a meeting.

If you have comments on this document please email owasp@owasp.org.[99]

[99] The OWASP Foundation Bylaws are also available online at: http://sl.owasp.org/2012bylaws



Section IX: Appendix

References

All links listed in footnotes can also be found at:
https://www.owasp.org/index.php/Summit_2011_Outcomes

2011 Summit Attendee and Sponsor Details

30 Countries Represented at the 2011 Summit:

Belgium, Brazil, Canada, China, Croatia, Czech Republic, Finland, Germany, Greece, Hong Kong, India, Indonesia, Ireland, Israel, Italy, Malaysia, Mexico, Netherlands, Poland, Portugal, Saudi Arabia, Slovakia, Singapore, Spain, Sweden, Switzerland, Syria, United Kingdom, United States, and Uruguay

44 Local OWASP Chapters Represented at the 2011 Summit:

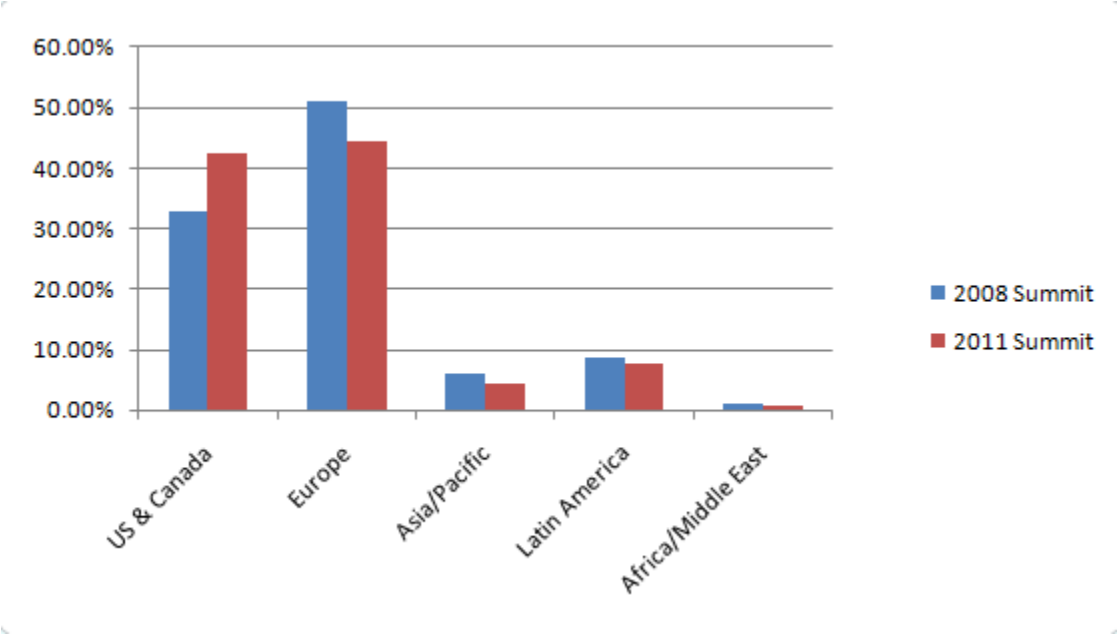
Alabama (US), Atlanta GA (US), Austin TX (US), Bay Area CA (US), Belgium, Brasilia (Brazil), Campinas (Brazil), Croatia, Dublin (Ireland), Geneva (Switzerland), Germany, Gibraltar, Goiano (Brazil), Greece, Hawaii, Hong Kong, India, Indonesia, Israel, Italy, London (UK), Long Island NY (US), Malaysia, Milwaukee WI (US), Minneapolis/St. Paul MN (US), NYNJ Metro (US), Netherlands, Orange County CA (US), Ottawa (Canada), Poland, Porto Alegre (Brazil), Portugal, Recife (Brazil), Rochester NY (US), Salt Lake UT (US), San Antonio TX (US), Sao Paulo (Brazil), Slovakia, Spain, Sweden, Syria, Uruguay, Virginia (US), and Washington D.C. (US)

Companies that Participated (Directly or Indirectly) in the 2011 Summit:

2008 vs. 2011 Summit Attendee Profiles

Metric	2008		2011	
Total # of Sponsored Attendees	76		103	
# of Attendees with Full Sponsorship	71		88	
# of Attendees with Partial Sponsorship	5		15	
# of Non-Sponsored Attendees	6		52	
Total Number of Attendees	82		155	
# of Countries Represented*	24		30	
Attendees from US and Canada # / %	27	32.93%	66	42.48%
Attendees from Europe # / %	42	51.22%	69	44.52%
Attendees from Asia/Pacific # / %	5	6.10%	7	4.52%
Attendees from Latin America # / %	7	8.54%	12	7.74%
Attendees from Africa/Middle East # / %	1	1.22%	1	0.65%

***Taiwan and Hong Kong treated as their own countries



In the above chart you can see **Summit attendee composition by region as a percentage of all attendees.** While there was small decline in the number of Europeans in attendance, and increase in the number of attendees from the US and Canada – these two regions still made up over 80% of the total attendee population.

2008 Summit Financial Details

Category	Cost	Notes
Travel - Diplomata Tours	$54,325.84	Includes flights for 65 attendees
Other Travel Costs	$12,563.72	Flights and other expenses submitted for reimbursement
Grande Real Santa Eulalia Hotel	$58,018.12	Includes accommodations for 74 and food for 76 attendees
AV Expenses – Eurologistix	$5,222.61	
Advertising – Generator	$1,261.50	
Summit Personnel	$960.00	
FedEx	$3,080.37	
Miscellaneous	$6,337.91	
Banking & Currency Corrections	$ 498.90	
SUBTOTAL	$142,268.97	
Income - Reimbursements/Donations	- $6,290.04	
TOTAL	$135,978.93	

Almost all OWASP participants (OWASP Project Leaders, Reviewers, and Contributors) at the 2008 Summit had their trip sponsored, at least in part, by the OWASP Foundation. To be considered a relevant OWASP participant, and, consequently, to qualify to have the Summit attendance expenses partially paid, attendees needed to fall into of the following categories:

1. OWASP Summer of Code 2008 project leaders & reviewers,
2. OWASP Summer of Code 2008 special project contributors,
3. OWASP Spring of Code 2007 project leaders & reviewers,
4. OWASP Autumn of Code 2006 project leaders & reviewers,
5. Active Project Leaders (not currently participating on SoC 08),
6. Active Chapter Leaders,
7. Member with significant past OWASP Contribution.

A list of OWASP sponsored attendees to the 2008 Summit as well as the reason for the sponsorship (i.e. the category from the above list that they fall into) can be found at:
http://spreadsheets.google.com/pub?key=pAX6n7m2zaTVLrPtR07riBA

Additionally, the following rules were established by the 2008 Summit planning committee to clarify which expenses and how much would be paid for by the OWASP Foundation:

1. With exceptions noted below, all accommodation and meals during the four-day event will be paid.
2. As we are still seeking out financial sponsorship support, until further notice, none of the dinners will be paid.
3. The meals consist of a pre-negotiated menu and only this menu will be paid.
4. The accommodation will consist in a place in a shared T1 (3 people) or T2 (5 people) apartment. Therefore, even though one can choose an individual room, OWASP will pay only for the cost associated with a shared stay. At the cost of +/- 60 Euros per night, there is the option to stay in an individual room (or in a double-room, in the cases where the partner - wife / husband - is also present).
5. Please note that the nights of 3 and 7 of Nov will be included in the paid accommodation for those individuals attending the whole event.
6. Regarding the flight expenses, OWASP will pay a maximum of 1000 US dollars for all non-European attendees and 600 US dollars for the European ones.

2011 Summit Financial Details

Category	Cost	Notes
EXPENSES		
Summit Venue Expenses		
Alentejo Room	$2,502.00	450€/day x 4 days = 1,800€
Campo Real 1	$3,614.00	650€/day x 4 days = 2,600€
Campo Real 2, 3, & 4	$3,614.00	650€/day x 4 days = 2,600€
Catering Supplement – dinners served in villas	$1,056.40	1.50€/person/day = 760€
Catering Supplement	$354.45	85€/day x 3 days = 255€
ASDL	$1,997.75	1,437.23€
Printer	$2,085.00	1,500€
Suite	$1,390.00	200€day x 5 days = 1,000€
AV Equipment	$16,853.75	12,125€
Drink Tickets	$2,636.83	7€/drink x 271 tickets = 1,897€
Cocktail Hour	$708.90	510€
Nuno Marco	$7,051.88	5,066.10€ (Optimus, Projector, PCs, Labor)
Food & Beverage Extras	$7,717.38	For Summit Team/Early Arrival 5,552.07€
CampoReal Total	**$51,572.34**	**37,107.40€**

Summit Giveaways		
Podcast CD & Book	$1,800.00	
Attendee Misc.	$5,254.17	Stickers, Passports, & Compasses

Summit Equipment & Services		
Operational Expenses	$1,384.22	Disposable cell phones, SIM cards, Netgear hub, baggage fees, ipad
OWASP Band Equipment Rental	$1,500	1,100€
Apparel – LX Studios & Polo Shirts	$2,858.96	

Category	Cost	Notes
EXPENSES (continued)		
Marketing – Hackers News Network	$250.00	
PR - Generator Beyond the Brand	$2,760.00	2,00€
SAPO (Additional Internet Connectivity)	$2,175.00	1,577€
Baltazar Martins (Summit Design/Marketing)	$3,210.00	2,327€

Summit Support Staff		
Sarah Baso (Summit Logistical Support)	$4,000	
Marta Pergorelli (Brazilian Delegation)	$5,000	
Sarah Cruz (Design)	$2,100	
Sandra Paiva (Working Session Editor)	$2,000	
Deb Brewer (Summit – On-site Event Planner)	$3,915.77	

Summit Expenses Subtotal	**$89.780.46**	
Summit Travel Subtotal	**$152,855.58**	http://sl.owasp.org/summit2011_travelcosts
TOTAL EXPENSES	**$242,636.04**	

INCOME		
OWASP Budget Allocation – Board Approved		
OWASP Funds for Operational Expenses	$50,000	$50,000 allocated by Board – Aug 2010
Summit Attendee Travel Budget	$50,000	$50,000 approved by Board in Dec 2010
$15,000 for Operational Costs and $25,000 for Summit Travel Expenses	$40,000	Approved by Board 23-Jan-2011

OWASP (Internal) Sponsorships		
Local Chapter Sponsorships	$44,095.65	Direct chapter donations & OSTR funds
Project Sponsorships	$2,000.00	Funds donated from project budgets

Category	Cost	Notes
INCOME (continued)		
External Sponsorships		
Wiki Donations	$1,310.11	
Praetorian	$1,942.14	$5000 Corporate membership with 40% ($2000 less fees) allocated to sponsor summit attendee
Security Innovation	$1,942.14	$5000 Corporate membership with 40% ($2000 less fees) allocated to sponsor summit attendee
(ISC)2	$1,947.09	Lunch Sponsorship ($2,000 less fees)
Trustwave	$1,975.00	Wireless Sponsorship ($2,000 less fees)

Accommodation Credit	$8,860.36	Credit from Diplomata Tours

Subtotal Internal Income	**$186,095.65**	
Subtotal External Income	**$16,029.75**	
TOTAL INCOME	**$202,125.40**	

PROFIT/LOSS	**-$40,510.64**	Total amount "over budget"

Total amount Spent by OWASP	**$226,606.29**	

The above details on the 2011 Summit Expenses and Income can be found at:
http://sl.owasp.org/summit2011_finalbudget

More details on Summit Travel and Accommodation costs, broken down by attendee can be found at:
http://sl.owasp.org/summit2011_travelcosts

2008 vs. 2011 Expense Comparison

Expense	2008	2011	Difference
Total amount spent by OWASP	$135,987.93	$233,775.68	+$97,787.75
Total amount spent by OWASP on flights	$62,860.37	$67,113.79	+$4,253.42
Number of flights paid by OWASP	71	85	+14
Average flight cost	$885.36	$789.57	($95.78)
Total cost of venue & accommodations (paid by OWASP)	$58,018.12	$126,314.25	+$68,296.35
AV Expenses	$5,222.61	$16,853.75	+$11,631.14
PR and Advertising	$1,261.50	$3,010.00	+$1,748.50
Total number of sponsored attendees	76	103	+27
Total number of attendees (sponsored & non)	82	155	+73
Average cost per sponsored attendee	$1,789.20	$2,269.67	+$480.47

There were many differences between the 2008 Summit and the 2011 Summit including the process for obtaining sponsorship for attending the Summit, the type and amount of resource used to run the event, and even the scope of attendees outside of OWASP leadership. Due these differences as well as some unknowns regarding the breakdown of expenses from the 2008 Summit, it is difficult to do much analysis or make conclusions based on a cost comparison between two events. In the future, in order to do a detailed analysis of the numbers it will be necessary to keep details (similar to that available 2011).

Nevertheless, it is noteworthy that in 2011 the average flight cost decreased by about $95.00 while the average distance traveled by attendees was likely more (based on a percentage of non-European attendees). Additionally, while the cost of the venue did not increase proportionate to the number of attendees at the event, the increase can be attributed to the fact that $51,500 was spent at the venue on large rooms (necessary to accommodate the large number of attendees – more than double than that which attended in 2008) and costs such as AV equipment were included in the venue cost (at the 2008 this was not included).

The total cost of the 2011 Summit was almost $100,000 more than the 2008 Summit, and while the number of sponsored attendees only increased by 27, the total number of attendees increased by 73. In 2008, only 6 individuals that attended were completely self-funded (not funded by OWASP). In 2011, however, 52 attendees were not sponsored by OWASP. While the summit planning team had hoped that this number would be higher (or the amount of money received by OWASP in corporate sponsorships for the Summit would be higher), this increase should be counted as a "success" for the event. For future Summits, the planning committee will need to consider the extra operational costs involved in handling a larger attendee base, whether they are sponsored by OWASP or not. It is likely that in order to put on a Summit in the future that is equal to or larger than the 2011 Summit, at least $100,000 should be set aside for operational costs alone (not including the cost to sponsor attendee travel and accommodation).

2011 Summit Attendees & Support Team

Adamski, Lucas

Lucas Adamski heads up the product security team at Mozilla, works on security architecture and features, and generally tries to make the Internet a happier and safer place. Previously, Lucas was a Security Architect at Adobe focused on Flash Player and AIR. He also worked at @stake and developed security managed services software at Breakwater Security.

Agarwal, Anurag

Anurag Agarwal, the founder of MyAppSecurity, has proven record in providing customers with solutions related to security risk management. Anurag is a former Director of Education Services at WhiteHat Security and has over 15 years of experience designing, developing, managing and securing web applications with companies like Citigroup, Cisco, HSBC Bank, and GE Medical Systems to name a few. He is an active contributor to the web application security field and has written several articles on secure design and coding for online magazines. A frequent speaker on web application security at various conferences, Anurag is actively involved with organizations such as the WASC (Web Application Security Consortium) and OWASP (Open Web Application Security Project). He started the project on Web Application Security Scanner Evaluation Criteria and is currently a project leader for OWASP developer's guide and OWASP Common Vulnerability List.

Aguilera, Vicente

Born in Badalona (Spain), Vicente is the OWASP Spain Chapter Leader, co-founder of Internet Security Auditors and member of the Technical Advisory Board in the RedSeguridad magazine. He is an enthusiastic supporter of the application security community, a regular speaker at industry conferences and has published several articles and vulnerabilities in specialized media.

Agustini, Alexandre

Alexandre Agustini is a senior lecturer and currently academic coordinator of Informatics Faculty at the Catholic University of Rio Grande do Sul (PUCRS). He has a Ph.D. in Computer Science from Universidade Nova de Lisboa (2006). Alexandre's primary research interest is in Natural Language Processing, acting on the following topics: text mining, machine learning, syntactic and semantic analysis of natural language.

Akhmad, Zaki

Born in Jakarta, Indonesia, 1982, Zaki holds a master degree from Bandung Institute of Technology, Indonesia, with major Electrical Engineering. Currently he works at indocisc, a small consultant company focus on information security, as a Junior Security Analyst. On professional certification, he had passed the CISA exam which he took on June 2010. He has led the OWASP Indonesia Chapter since December 2008. The first translation project completed by OWASP Indonesia Chapter team is the Top 10 OWASP 2010. He enjoys very much working on information security industry. On the leisure time, Zaki loves reading, writing, listening to music and for some time taking photos. He also enjoys sports, especially running and swimming. He can be contact at za at owasp dot org.

Alamri, Lorna

Lorna Alamri is a consultant at a large financial institution and resides in Minneapolis, Minnesota, USA. Lorna is Vice President of the Minneapolis/St. Paul, MN local OWASP Chapter, which is hosting the OWASP AppSec USA 2011 conference. She is also a member of the Global Industry Committee, Editor of the OWASP Newsletter, and a member of the Global Summit Planning Committee.

AlBasha, Talal

Eng. Talal Al-Basha currently works in the areas of Application Development Management, Application Security Consultation, and is GWAPT Certified. He is a Product Manager at Innovative Solutions, in addition to Alremh company at ICT Incubator and serving as the OWASP Syria Chapter Leader. Previously, Talal worked as a Presenter for Internet Security at ITDigest, Senior Developer at King Faisal Specialist Hospital, and Senior Developer at KFSHRC. He received his education at Damascus University.

Angal, Rajeev

Rajeev currently works as an Architect at Oracle (Sun Microsystems) and lives in the San Francisco Bay Area, California, USA. Prior to this, Rajeev was the Founder & VP Engineering at Intellifabric Inc, Director of Technology at Infospace Inc, and an Architect, Portal Server at SUN Microsystems. Rajeev received his education from the University of California, Santa Cruz and ITT Delhi.

Aniceto, Alexandre

Alexandre Aniceto, Information Security Consultant, CISSP, CISM, CISA, ISO27001/LA currently is a Partnerat Willway, S.A in the Lisbon Area, Portugal. Previously, Alexandre was a Senior Security Consultant at Glintt, Security Advisor at Archeocelis, Lda, and Security & Systems Engineer at Nokia Siemens Networks. He was educated at Royal Holloway, University of London, $(ISC)^2$, ISACA - Information Systems Audit and Control Association. Alexandre's specialties are Information Security Management, Security Architecture Design & Implementation, Auditing and Regulatory Compliance.

Aryavalli, Gandhi

Having Honors in Engineering (CS & Mech. Engg.) enriched by MBA (finance), have been working in Information Security space for the last 10+ years in the fields of Application Security, State Assessment, Data cum Network Security, Security Governance and Compliance areas. Currently part of McAfee family for the last 5+ years, providing technical expertise and support in the performance of architecture and application risk assessments for IT developed applications and third party solutions, review of applications for security vulnerabilities, perform penetration tests and enforcing Secure QA cum Coding practices. Key achievements include providing technical support to Department of Defense to install a Common Criteria lab in India for the first time, and established Vulnerability Assessment Center as per SSE-CMM Guidelines. Providing organization wide trainings and conducting secure code reviews, as a Secure Core Team member of McAfee. Has played a key role in Application security in various CMM companies like Microsoft (v-id), Mahindra BT, etc.

Barbato, L. Gustavo C.

Gustavo is Ph.D. (application security) and M.Sc. (intrusion detection) in Information System Security as well as Bachelor in Computer Science. He has worked in security projects for the Brazilian Government for many years involving software programming, network and systems administration, computer and network security, application and network penetration testing, software security assessments, code review, malware analysis, intrusion detection, forensics analysis and others activities. During that time, he has also worked as security professor at college and postgraduate by teaching subjects about network and information security. In the beginning, he used to work as software developer and system administrator. However, the last years were dedicated to security consulting on areas aforesaid. Nowadays, he is the Technical Application Security Lead at Dell and Secure Programming Professor at UNISINOS University. As voluntary work, he is the Porto Alegre (Brazil) OWASP Chapter Founder/Leader and member of OWASP Global Chapter Committee.

Barnett, Ryan

Ryan Barnett is a Senior Security Researcher at Trustwave. He is a member of Trustwave's SpiderLabs -the advanced security team focused on penetration testing, incident response, and application security where he focuses on web application defensive research and serves as the ModSecurity web application firewall project lead. In addition to his work at Trustwave, Ryan is also a SANS Institute certified instructor and a member of both the Top 20 Vulnerabilities and CWE/SANS Top 25 Most Dangerous Programming Errors teams. He is also a Web Application Security Consortium (WASC) Member where he leads the Web Hacking Incidents Database (WHID) and Distributed Web Honeypots Projects, as well as, the OWASP ModSecurity Core Rule Set (CRS) project leader. Mr. Barnett has also authored a Web security book for Addison/Wesley Publishing entitled *Preventing Web Attacks with Apache* and is a frequent speaker at industry conferences such as Blackhat and OWASP.

Baso, Sarah

Sarah is a licensed attorney living in Minneapolis, Minnesota, USA. Sarah has been involved with all aspects of the 2011 OWASP Global Summit – providing logistical support, booking attendee travel arrangements, updating wiki pages related to the 2011 Summit, and compiling Summit outcomes for a full Summit report. She currently works part time for OWASP providing operational support for the Global Chapters, Conferences, and Industry Committees. Sarah also works remotely as the Chapter Administrator for the local Los Angeles OWASP chapter.

Batista, Marco

Marco is a 26 year old from Portugal with a Network and Communications Engineer degree. He has worked for 2 years in Carrier Sales Support / Customer Premises Equipment (CPE) Broadband Access (xDSL, FTTH), and is currently taking a MSc in Information Security.

Bergling, Mattias

Mattias Bergling works as a Senior Security Consultant at 2Secure in Stockholm, Sweden. Mattias has been working with IT security for 12 years and has been focusing on security testing for the last 8 years. Mattias is the co-leader for the Swedish OWASP chapter and was on the Organizing Committee for AppSec EU 2010.

Bernik, Joe

Mr. Bernik is the Chief Information Security Officer for Fifth Third Bank, responsible for protecting Fifth Third Bank and its clients' information systems from risks. He is also responsible for defining and implementing Enterprise-wide information security strategies for the Bank.
Mr. Bernik has more than 16 years of experience as a risk professional. He has developed risk management practices, procedures and standards for several Fortune 100 companies including several global banking organizations.
Prior to his role at Fifth Third Bank, Mr. Bernik served in roles including Director of Operational Risk at the Royal Bank of Scotland and Chief Information Security Officer of ABN AMRO, and its subsidiary, LaSalle Bank.
Mr. Bernik received his bachelor's degree from the University of Mary Washington in Fredericksburg, Virginia, and completed graduate work in business administration at the City University of New York.
Mr. Bernik currently serves as an advisor to the Federal Reserve on matters of information security and is on the steering committee of the Financial Services Sharing and Analysis Center (FS-ISAC). Additionally, Mr. Bernik is Chair of the OWASP Global Industry Committee.

Biagiotti, Massimo

Massimo Biagiotti is the Project Manager and Business Developer of consulting activities for network and application security analyses concerning Ethical Hacking, Secure Software Development Lifecycle, Security Processes, Risk Analyses and Business Impact Analyses. Since 2009, Massimo is also responsible of the Internship Program of Business-e.

Bonver, Edward

Edward is a principal software engineer on the product security team under the Office of the CTO at Symantec Corporation. In this capacity, Edward is responsible for working with software developers and quality assurance (QA) professionals across Symantec to continuously enhance the company's software security practices through the adoption of methodologies, procedures and tools for secure coding and security testing. Within Symantec, Edward teaches secure coding and security testing classes for Symantec engineers, and also leads the company's QA Security Task Force, which he founded. Prior to joining Symantec, Edward held software engineering and QA roles at Digital Equipment Corporation, Nbase and Zuma Networks. Edward is a Certified Information Systems Security Professional (CISSP) and a Certified Secure Software Lifecycle Professional (CSSLP). He holds a master's degree in computer science from California State University, Northridge, and a bachelor's degree in computer science from Rochester Institute of Technology. Edward is a Ph.D. student at NOVA Southeastern University.

Booth, Rex

Rex is a Senior Manager in Grant Thornton's Public Sector practice and leads their Cybersecurity Solution group. He has over ten years of experience providing application development, risk management and information security services to government agencies, private industry, and financial institutions. Since joining Grant Thornton, Rex has led various information security and risk management engagements including FISMA, IV&V, SOX, and OMB A-123 engagements as well as identity management and system certification and accreditation efforts. During his tenure at previous employers, Rex designed and developed complex distributed web-based applications. As a member of a managed security services team performing research and development, he co-architected and implemented a scalable information detection and prevention information aggregation solution for use in a real-time 24/7 information security monitoring system, correlating and reporting on thousands of devices. He has presented on the topic of information security and assessment methodologies to various institutions and is currently a global committee member for the Open Web Application Security Project (OWASP).

Brennan, Tom

Tom started with technology in 1986 when 8-bit and CP/M was cool <grin>. After a career-ending injury with US Marines Corps., during Gulf War I Era, he dedicated his life to information security. Tom was elected and served with the FBI Infragard program 2002-2004, then founded the OWASP New Jersey Chapter that today includes NYC Metro. In 2007, Tom was appointed by his application security peers to the OWASP Global Board of Directors. Tom was the managing partner of Proactive Risk, which assessed technology, people and process used in finance, e-commerce, oil/gas, power generation/transmission, water, and global enterprise networks, before joining Trustwave Spiderlabs in 2011. Tom is a father of 4 great kids and is a frequent and entertaining speaker at information security conferences and bars around the world ;)

Brewer, Deb

Deb is the Owner/Director of LXstudios Inc, and has provided branding, corporate identity and collateral design solutions to institutional and retail clients for over twenty years. Deb attended Carnegie Mellon University in Pittsburgh, PA on a Fine Arts Scholarship and obtained a bachelor of Fine Arts in Graphic Design with a Minor in Professional Writing. She began her career as a Senior Designer in the Creative Services department at Thomson Financial in Boston, MA. After Thomson, Deb became a partner at Patric Ward Design in Boston, managing accounts such as Janus Institutional, Reebok, Standard & Poor's, and Thomson Financial. In 1999, Deb opened LXstudios, providing branding, corporate identity, print collateral, advertising, web, and event support to a wide clients in almost every commercial industry.

Bristow, Mark

Mark Bristow works as an Industrial Control Systems (ICS/SCADA) Security consultant with Securicon LLC for a US Government client. Before getting involved with ICS, Mark was heavily involved in web application vulnerability research, penetration testing and building application security programs as a consultant with SRA International. Mark is an active member of the Open Web Application Security Project (OWASP) as Global Conferences Committee Chair, AppSec DC Organizer, and Co-Chair of the OWASP DC chapter.

Brzozowski Daniel

Daniel is a web security enthusiast with broad knowledge in web applications development and web security. For the last few years, he has worked in the banking and financial industry. He is currently working towards his Masters Degree in Artificial Intelligence at Warsaw University of Technology and finishing his final master's thesis, "Web Application Penetration Tests". Daniel is based in London, UK and works for a worldwide financial company. His interests cover all aspects of web security, web development and public speaking. In Daniel's free time he enjoys practicing Krav Maga, listening to music, and following Web Security news.

Buetler, Ivan

Ivan is the Founder and CEO, Compass Security AG (since 1999), the Founder of Swiss Cyber Storm Security Conference (since 2007), the Founder of Hacking-Lab community site / Alias E1 (since 2006), the Founder and board member of Cyber Tycoons Foundation (since 2010), and Board Member of the Information Security Society of Switzerland ISSS (since 2010). After completing his degree in Electrical Engineering at the Technical College of Rapperswil focusing on computer science, control technology, electronics, energy engineering, and motion technology, Ivan Buetler worked for 2 years in St.Gallen at AGI Service, a company which provides services for banks. Then Ivan worked for 3r security engineering ag/Entrust Technologies supporting security consultants in technical matters, as well as analyzing clients' technical problems, local network and computer systems throughout Europe. During these activities, Ivan also completed post-graduate studies at the Management School of St.Gallen/Zurich in Business Management.

Calderon, Juan Carlos

Juan currently works as Application Security Research Leader/Sr Auditor at Softtek and lives in the Aguascalientes Area, Mexico. Previously he was a Project Leader at Softtek, as well as a Sr Application Security Auditor and Sr Web Developer at Soft tek. Juan also worked as a Web Application Security Specialist and Web Developer at GE DDEMESIS and as the IT Manager at Gabatti. Juan received his education from the Instituto Tecnológico y de Estudios Superiores de Monterrey and the Instituto Tecnológico de Zacatecas.

Casey, Larry

For the past 5+ years as OWASP's Director of IT, Larry has focused on everything OWASP. His ultimate goal has been and currently is to provide all the technologies needed for the OWASP community to grow. If your project or chapter has ideas, Larry encourages you to contact him to help move your goals along.

Causey, Brad

Brad is an active member of the security and forensics community worldwide. Brad tends to focus his time on Web Application security as it applies to global and enterprise arenas. He is currently employed at a major international financial institution as a security analyst. Brad is the President of the OWASP Alabama chapter, a member of the OWASP Global Projects Committee and a contributor to the OWASP Live CD. He is also the President of the International Information Systems Forensics Association chapter in Alabama. Brad is an avid author and writer with hundreds of publications and several books.

Chalmers, Matthew

Matthew has been doing information security and related work his entire professional career, since earning his bachelor's degree from MST. Matt has worked for large organizations in the defense, financial and manufacturing industries including the US Navy, the National Security Agency, JPMorgan Chase and, presently, Rockwell Automation. Matt currently performs risk, threat, control and vulnerability assessments; regulatory & policy/standard compliance audits; process improvement audits; and general & application control audits. Matt holds the CISA, GSNA, GCFA, CEH and CHS certifications and is ITIL v3 Foundation certified. Matt has been involved with OWASP since about 2002.

Chandra, Pravir

Pravir Chandra is Director of Strategic Services at Fortify where he leads software security assurance programs for Fortune 500 clients in a variety of verticals. He is responsible for standing up the most comprehensive and measurably effective programs in existence today. Creator and leader of the Open Software Assurance Maturity Model (OpenSAMM) project, Pravir also works extensively with OWASP and on other open projects to promote effective application security practices. As a thought leader in the security field for over 10 years, Pravir has written many articles, whitepapers, and books and is routinely invited to speak at businesses and conferences world-wide.

Cheng, Steven

Steven is currently the product manager for CodeSecure at Armorize Technologies, Inc. He has been with the company for more than five years spanning early from the development phase to current product management role. His job primarily involves requirement gathering and specification design. Recently the focus also shifted into development process in order to have better control of release schedule. In the past year Steven had led the CodeSecure team to undergo a major product transformation in terms of distribution method from appliance to pure software based, and complete UI redesign.

Clarke, Justin

Justin is a Director and Co-Founder of Gotham Digital Science, based in London. Justin has extensive international risk management, security and secure development consulting and testing experience in the United Kingdom, United States and New Zealand. He is the lead author/technical editor of "SQL Injection Attacks and Defenses" (Syngress), co-author of "Network Security Tools" (O'Reilly), and a contributor to "Network Security Assessment, 2nd Edition" (O'Reilly), as well as a speaker at various security conferences and events such as Black Hat, EuSecWest, ISACA, BruCON, OWASP, OSCON, RSA and SANS. Currently Chapter leader of the OWASP London chapter, and a member of the OWASP Connections Committee, he has a Bachelors degree in Computer Science from the University of Canterbury in New Zealand. He's also a CISSP, CISM, CISA, CEH, and still has his MCSE if you have a Windows NT 4.0/Exchange 5.5 network.

Coates, Michael

Michael Coates has extensive experience in application security, security code review and penetration assessments. He has conducted numerous security assessments for financial, enterprise and cellular customers worldwide. Michael holds a master's degree in Computer Security from DePaul University and a bachelor's degree in Computer Science from the University of Illinois. Michael is the creator and leader of the AppSensor project and a contributor to the 2010 OWASP Top 10. He is a frequent speaker at OWASP security conferences in the US and Europe and has also spoken at the Chicago Thotcon conference and provided security training at BlackHat. As the web security lead at Mozilla, Michael protects web applications used by millions of users each day.

Coimbra, Paulo

Paulo began working for OWASP in July 2007 assuming the Spring of Code closing process. In the beginning of 2008, be became an OWASP part-time employee assuming the role of Project Manager. After completing his IELTS course, his status changed again in July 2008 when he moved into a full-time position. Paulo answers directly to the OWASP Board and has been working closely with the OWASP Global Projects Committee since it was organized in November 2008.

Paulo Coimbra has a M.S. in Management (Technical University of Lisbon), a Post-Graduation in Political Science (University of Lisbon), and a B.S. in Management and Social Development (Portuguese Catholic University). Paulo has worked in management since 1992. He has performed different roles, from Economist (IAPMEI/Portuguese Ministry of Economy) to Teacher of Finances, Accountancy and M&A (Polytechnic Institutes of Setúbal and Santarém), to Marketing Director and Teacher of Project Finance, Corporate Communication and Political Science (Piaget Institute).

Cornell, Dan

Dan Cornell has over twelve years of experience architecting and developing web-based software systems. He leads Denim Group's security research team in investigating the application of secure coding and development techniques to improve web-based software development methodologies. Dan was the founding coordinator and chairman for the Java Users Group of San Antonio (JUGSA) and currently serves as the OWASP San Antonio chapter leader, member of the OWASP Global Membership Committee and co-lead of the OWASP Open Review Project. Dan has spoken at such international conferences as ROOTs in Norway and OWASP EU Summit in Portugal.

Corry, Bill

Bill is an Information Security Engineer at PayPal. He has extensive experience in information security, information technology and web application development. He brings integrity and accountability to all of his projects. Beyond Bill’s technical skills, he also has experience managing people and resources, budgeting, metrics, legal issues, strategic planning, and public speaking.

Cruz, Dinis

Dinis Cruz is a Security Consultant based in London (UK) and specialized in: ASP.NET/J2EE Application Security, Application Security audits and .NET Security Curriculum Development. For the past couple years Dinis has focused on the field of Static Source Code Analysis and Dynamic Website Assessments (aka penetration testing), and is the main developer of the OWASP O2 Platform which is an Open Source project that is focused on 'Automating Security Consultants Knowledge/Workflows' and 'Allowing non-security experts to access and consume Security Knowledge'. Dinis is currently focused on making the O2 Platform the industry standard for consuming, instrumenting and data-sharing between: the multiple WebAppSec tools, the Security consultants and the final users (from management to developers). Past industry experience include: running a small Software/Consultancy business, acting as CTO for a Portuguese University, being part of a Security Assessment team (Pentesting and Source Code Assessment) for a global Bank (ABN AMRO), taking the role of Directory of Advanced Technologies at Ounce Labs (acquired by IBM) performing Web Application security assessments on a large number of languages/technologies/frameworks and being a very active participant and enabler at OWASP.

Cruz, Sarah

Sarah Cruz is an award winning graphic designer working in London for Lewis Moberly www.lewismoberly.com. She Is responsible for the design of such global icons as Glenmorangie whisky, Johnnie Walker director's blend, Sport England, and the new Gatwick Airport identity. She designed the OWASP Summit '08, and the OWASP Summit 2011 identity. In 2008 she founded the charity Abundance London www.abundancelondon.com, which works with school groups to harvest surplus local fruit from city gardens and parks, and supplies it to local restaurants. English by birth, she grew up in the US. Sarah went to Choate and has a BA (honors) from Carnegie Mellon University. She has two daughters, ages 7 and 5, with husband Dinis Cruz, and can speak a bit of Portuguese.

Dawson, Isaac

Isaac is interested in all forms of application/network security, but primarily enjoys thinking of unique ways of breaking applications from a business logic stand point. He has published the following papers:

• *Blind Buffer Overflows in ISAPI Extensions*, which was released on the main page of the leading security news and information site, Security Focus in January 2005 (http://www.securityfocus.com/infocus/1819)

• *The Benefits of Combining Automated and Manual Penetration Testing*, a white paper written to aid a sales team in educating customers as to the benefits of combining manual testing with automated tools.

Isaac's specialties include: application assessments, network assessments, some reverse engineering.

De Win, Bart

Bart is a security enthusiast with an extensive academic background. He is a master in Computer Science. Afterwards, he has spent over a decade researching and improving techniques for the analysis and development of secure software, among others in the context of his Ph.D. He authored more than 60 articles published in international journals or conferences. He is specialized in methodological and constructive software security techniques, with a specific focus on application security. Because of his background, he has an in-depth knowledge of the state-of-the-art in the area. Bart currently works as a security consultant in the domain of application security. He works on a daily basis on application assessments and on helping customers improving their software security practices. Bart is one of the OWASP chapter leaders of the Belgian OWASP chapter. He co-organizes the OWASP BeNeLux events.

Deleersnyder, Seba

Sebastien Deleersnyder (Seba), Managing Technical Consultant SAIT Zenitel. Starting up the ICT Security business line for SAIT Zenitel BeNeLux-France (www.saitzenitel.com). Seba started the Belgian OWASP Chapter in 2005, started the OWASP Education project, and currently participates in the Global Chapters Committee in addition to being a member of the OWASP Foundation's Board of Directors. Seba is a co-organizer of BruCON, an annual security & hacker conference and trainings in Brussels (www.brucon.org). As security project leader and information security officer for multiple customers, Seba has built up extensive experience in Information Security related disciplines, both at strategic and tactical level. He specializes in (Web) Application Security, combining both his broad development and information security experience.

Di Paola, Stefano

Stefano Di Paola is the CTO and a cofounder of Minded Security, where he is responsible for Research and Development Lab. Prior to founding Minded Security, Stefano was a freelance security consultant, working for several private and public companies. He also worked in collaboration with University of Florence at the Faculty of Computer Engineering. Stefano is recognized as one of the top application security researchers. In the past years he released several advisories including the ones that are not publicly disclosed but patched and several open source tools. He has also contributed to OWASP testing guide and is also the Research & Development Director of OWASP Italian Chapter.

Donovan, Fred

Fred is an application security researcher and the founder of Attack Logic, a U.S. based AppSec consultancy. He spent 3 years as a private researcher on campus at UNL's Technology Park in the field of InfoSec and for the past 11 years has provided executive level IT services to public and private organizations. Application Security has been his exclusive focus for the past seven with a general focus on information warfare and the uses of counter intelligence for purposes of corporate defense. He is a regular guest lecturer and speaker at Universities, Conferences, and professional organizations. Mr. Donovan is alumni of the University of Missouri -- Columbia (Mizzou) and the American Military University (AMU).

Durkee, Ralph

Ralph Durkee, CISSP, GSEC, GCIH, GSNA, GCIA, GPEN is the principal security consultant and president of Durkee Consulting, Inc since 1996. Ralph founded the OWASP Rochester, NY chapter in 2004 and currently serves as a member of the OWASP Global Conferences Committee. Ralph also serves as president of the Rochester ISSA Chapter and chairs the annual Rochester Security Summit. He performs a variety of security audits and software security assessments and software development consultations for clients in the Rochester, NY area. His expertise in penetration testing, incident handling, secure software development and secure Internet and web applications is based on over 30 years of both hands-on and technical training experience. He has developed and taught a wide variety of professional security seminars including custom web application security training, and SANS SEC401 & SEC504 - Hacker Techniques and Incident Handling and CISSP bootcamp courses since 2004. Ralph regularly leads development of a wide variety of security standards such as application security, database encryption and security consulting for compliance with the Payment Card Industry Data Security Standard.

Dworakowski, Wojciech

Wojciech is a co-founder and Director at SecuRing – a company specializing in security testing services, based in Krakow, Poland. During last 8 years at SecuRing, he has managed many projects in domain of security testing for leading financial companies and public organizations. Wojciech is an OWASP Poland board member, ISMS Lead Auditor / BS7799 certified. Wojchiech's areas of interest include: Security testing management, ASVS, OWASP Testing Guide, Risk assessment vs. (web) applications, Security development lifecycle (OpenSAMM), Penetration testing & code review, Frameworks security.

Elias, Wagner

Wagner is the Manager of Research & Development and Co-Founder of Conviso Information Security Technical Services. Prior to this, he held the post of Director of Content and Education in Management 2006-2008; event manager of Brazil's 2008-2010 Chapter of ISSA (Information Systems Security Association) and in Brazil Project Leader OWASP (Open Web Application Security Project). Wagner has spent more than 10 years working in information technology and more recently with information security. He has gained some certifications in the area and has spoken at events such as H2HC (Hackers to Hackers Conference) GTS (Working Group on Security), and PHP Conference Microsoft Tech-Ed.

Eng, Chris

Chris Eng is Senior Director of Research at Veracode, where he helps define and implement the security analysis capabilities of Veracode's service offerings. He has over 12 years of experience in information security, including senior technical positions at Symantec and @stake, where he specialized in software security assessments, penetration testing, reverse engineering, and vulnerability research while also leading the development of @stake's WebProxy product. During this time, he advised numerous Fortune 100 companies on software security and served as a global leader for Symantec's Attack and Penetration Center of Excellence. He began his career with the US Department of Defense working on a variety of offensive-minded infosec projects. Chris speaks regularly at top information security conferences including BlackHat, OWASP, and RSA, discussing topics such as cryptographic attacks, application security metrics, secure coding, and the SDLC. He also serves on the advisory board for the SOURCE Boston and SOURCE Barcelona security conferences. Along with experts from more than 30 US and international cyber security organizations, he helped develop the CWE/SANS Top 25 Most Dangerous Programming Errors.

Evans, Arian

Arian is the VP of Operations at WhiteHat Security. In this role, Arian leads a team of application security engineers integral to delivering the WhiteHat Sentinel SaaS-based website vulnerability management service, currently assessing over 3000 production websites around the globe, primarily in e-commerce, financial services and healthcare verticals, and including many Fortune 500 companies. Arian's team also verifies all vulnerabilities identified by WhiteHat Sentinel, a unique feature of the service. Arian has worked at the forefront of Web application security for more than 10 years. His global projects include work with the Center for InternetSecurity, NIST, the FBI, the Secret Service, and many large commercial organizations in analyzing Web application security and providing hacking incident-response. Arian also researches and discloses new attack techniques and vulnerabilities in Web application software including commercial platforms like Cisco and Nokia. Previously, Arian led the Application Security Practice at FishNet Security, working with Fortune 500 clients and delivering software security services globally.

Falkenberg, Andreas

Andreas is currently a student at the Chair for Network and Data Security, Ruhr University Bochum Germany. His research interests include web service security, web service attacks, and XSS.

Fazli Azran, Mohd

Mohd Fazli Azran was OSS evangelist and are active use OSS from 1996. Join many OSS community and spread about OSS to public. Work as System Administrator almost 10 years and believe on OSS spirit "Sharing is Caring". Now move into Open Source Security for make awareness to public what is OSS security can do for community. Currently was Fedora Ambassador & openSUSE Ambassador. He also was CyberSafe Ambassador for Security Awareness by CyberSecurity Malaysia. He also was Secretariat for Open Source Developer Club Malaysia (OSDCMY) that organized Malaysia Open Source Conference (MOSC). Now active being OWASP Malaysia Chapter Leader.

Fedon, Giorgio

Giorgio Fedon is the COO and a cofounder of Minded Security, where he is responsible for running daily operations of the company and managing Professional Services. Prior to founding Minded Security, Giorgio was employed as senior security consultant and penetration tester at Emaze Networks S.p.a., delivered code auditing, Forensic and Log analysis, Malware Analysis and complex Penetration Testing services to some of the most important Companies as Banks and Public Agencies in Italy. He participated as speaker in many national and international events talking mainly about web security and malware obfuscation techniques. He was also employed at IBM System & Technology Group in Dublin (Ireland).

Feres Serrano Neves, Eduardo Jorge

Eduardo Jorge currently works for Dataprev in Brasil. Additionally, he serves as the OWASP Chapter Leader for Goiania, Brazil.

Ferraz, Felipe

Felipe Ferraz is a PhD candidate, has a Master Degree and Post Graduation on Software Engineering with emphasis on: Software Engineering, system architectures and Information Security. Worked with computer system for the last 8 years, experience in design and develop applications both web and mobile, especially with J2ME and Android Technologies. Has been Teaching Software Security Engineering on CESAR.EDU and FBV.

Ferreira, Lucas C.

Lucas has been a security professional for more than 15 years. He began working on network security and then security management. As he has several developers in the family, he got interested in secure development techniques. In 2008, he answered a Call for Trainings to be delivered at the first OWASP Summit and got the opportunity to go to Portugal and to know OWASP and its leaders. In 2009, he managed to put together the first AppSec Conference in South America and did it again in 2010. He is now more involved in OWASP than ever, having a seat at the Global Conferences Committee, leading the OWASP local chapter in Brasilia, DF, Brazil and leading the newborn OWASP Portuguese Project.

Fette, Ian

Ian is a Product Manager on the Google Chrome team. Responsible for ensuring the APIs we add to Google Chrome and to web standards provide a coherent development platform that meets the needs of Google's application developers and web developers at large. Ian has experience managing large globally distributed products, including currently managing a group split between N. America, Europe, and Asia. Previously, Ian worked as an Engineer with the U.S. Government, working on large highly available database applications, with security clearance. Ian specialties include product management, web standards, contract negotiations, security, phishing, malware.

Fitzgerald, Alexis

Alexis spent many years on the development side of the fence working on both thick client and web-based applications, mainly in the financial sector in Ireland and Switzerland. In the early nineties somebody asked Alexis if he had heard of this thing called "SQL Injection". That was when he began the transition from poacher to gamekeeper, working on the security end of things. He continues to do a good deal of development.
Alexis's first contact with OWASP was the AppSec Europe conference at Royal Holloway outside of London in 2005. Since then, he have mainly been a consumer of OWASP resources, apart from giving a few talks at various chapter meetings. His goal with OWASP is to help development teams build "enough" security into their projects and to raise general awareness about OWASP and application security, because he believes that outreach and education type initiatives must be key aspects in the future direction of OWASP.

Fitzhugh, Justin

Justin Fitzhugh is the VP of Engineering Operations for the Mozilla Corporation. He's responsible for all Mozilla's production and corporate infrastructure, including serving the Firefox product to more than 150 million users. In addition to Firefox distribution, his team designs, implements and supports the infrastructure for one of the largest open source organizations in the world. Prior to Mozilla, Justin managed Macromedia's global datacenter environment. He spends his spare time as an avid pilot, snowboarder and father in the Bay Area.

Flores, Mauro

Currently, Mauro works as a security consultant at Deloitte Uruguay. Mauro started working on security stuff at age 18, disassembling viruses and helping to develop AV technologies. After that he worked as a developer for companies related to the financial industry where he helped to develop credit card and home banking related applications. Finally, Mauro's background includes a move to the administration phase of his life where he worked as a security network administrator for the main TMT company in Uruguay. Also, he has done security research and development for companies in the UK and Brasil.

Fontes, Antonio

A.F. has over 10 years experience in the field of software development and risk management with private organizations. Member of the OWASP Switzerland board, he leads the Geneva chapter and contributes in several reference software security projects such as the "CWE Top 25 most dangerous programming errors." Antonio currently works at L7 Sécurité, a Swiss security & risk consultancy company he founded in 2010. His work strongly emphasizes on helping organizations better understand Internet threats and manage their risks

Fort, Julio Cesar

Julio Cesar Fort is just another guy living in Recife, Pernambuco, a very beautiful state located in northeast of Brazil. Currently he is an undergraduate student of Computer Engineering at CIn/UFPE (Pernambuco Federal University) and former undergraduate student in Mechanics Engineering at the same university. Julio was a scholarship holder of CNPq and acted as intern at C.E.S.A.R. learning secure coding techniques in C. Also, he worked as an intern for coadmin team at Tempest Technologies, a very nice market-leading company Brazilian information security industry.

Fortuna, Pedro

Pedro is a co-founder and CTO of AuditMark where he coordinates the R&D. AuditMark is a web-security start-up focused on two main areas: web traffic auditing and website protection. Pedro holds a degree in Computing Engineering and a MSc in Computer Networks. Furthermore, he has extensive knowledge and professional experience in R&D projects and software development, both at academic and industrial levels. Additionally, Pedro previously taught at the Faculty of Engineering of the University of Porto, and also gave training in computer security. Currently, he teaches Networks and Computer Security at the Engineering School of the Polytechnic Institute of Porto. He is also a member of INESC Porto L.A., a National R&D Laboratory, where he is working towards his PhD.

Frosch,Tilman

Tilman Frosch works as a researcher for the Horst Görtz Institute for IT-Security at Ruhr University Bochum, Germany. He is interested in everything that leverages the browser to compromise the system. In his spare time he stares at passive-DNS data and Ruby code. In the time left he creates noises from various instruments or spends said time outdoors.

Galvao, Pedro

Pedro has a five year degree in Information System and Computer Engineering (IST - Technical University of Lisbon), in addition to being an Oracle OCP (Oracle Certified Professional). He has about 7 years of experience as Oracle DBA and about 14 years of IT experience. Besides this, through Pedro's professional career, he has taken on multiple roles such as Trainer, Systems Administrator, Project Manager, and as a Programmer.

Gao, Helen

Helen has worked in the field of information security since 1991. She has worked as an application developer, manager as well as a software architect. Her employment history includes a financial institution, a market research company, a high-tech device manufacturer and a software company. Helen is a senior architect in TIBCO Software Inc. Her job duties include designing and developing complex event processing software.

Helen has taught math, physics and computer science in colleges in both United States and China. She graduated from Sun Yat-sen University in China and continued her studies of physics and computer science after she came to the United States. Helen has her Masters Degree in both physics and computer science. Helen founded the Long Island OWASP chapter in 2006. In addition to volunteering for OWASP, she serves as the president of Sun Yat-sun University Alumni Association. Helen helped found the Long Island Chinese School.

Garrancho, Bruno

Bruno is an information security professional with global experience in diverse environments. He holds a Msc in Information Technology - Information Security by Carnegie Mellon University. Bruno currently is the Security Practice Leader of Professional Services & Innovation for Logica Iberia.

Garg, Vishal

Vishal Garg is the Founder and Principal Security Consultant for AppSecure Labs Limited, a UK based company offering application security and penetration testing services. He specializes in conducting network and application security reviews, design reviews, and vulnerability research and analysis for web-based applications, cloud-based systems and COTS applications. In his 12-year career, he has offered software development and expert security advice to several recognized Fortune 500 and FTSE 100 companies including international financial institutions, retailers and multinationals. He has a master's degree in Information Security from Royal Holloway, University of London and is a Certified Information Systems Security Professional (CISSP) and a Certified Information Systems Auditor (CISA) and currently the project leader for the OWASP Development Guide.

Gomes, Leandro Resende

Leandro currently lives in Brasília, Brazil and works at SERPRO Brazilian Federal Data Processing Service, an organization that creates and maintains huge computer systems for critical public companies. Leandro works as part of a security development group that was responsible for addressing corporative security aspects during the SDLC. This group was created in 2006, and they discovered OWASP on that same year. This group has contributed to OWASP by translating ASVS and QuickRef Guide into Portuguese. The work of this group includes the dissemination of technical orientation, source code analysis and pen testing coordination and definition of security frameworks to be adopted. Most recently, Leandro attended BlackHat 2009 (Las Vegas), OWASP AppSec 2009 and ICCyber 2010 (Brazil). He also wrote the article "Securing web applications with fuzzing tests" for a SERPRO internal conference.

Gondrom,Tobias

Tobias is Managing Director of an IT Security & Risk Management Advisory based in the UK and Germany. He has twelve years of experience in software development, application security, cryptography, electronic signatures and global standardization organizations working for independent software vendors and large global corporations in the financial, technology and government sector, in America, EMEA and APAC. As the Lead of the Security Task Force at IXOS Software AG and then the Global Head of the Security Team at Open Text, Tobias was responsible for security, risk and incident management and introduced and implemented a secure SDLC used globally by development departments in the US, Canada, UK, Germany, and India. Since 2003, he has served as chair of the IETF working group “LTANS” in the security area, member of the IETF security directorate, and since 2010 chair of the web security WG at the IETF, and a former chapter lead of the German OWASP chapter from 2007 to 2008. Tobias is the author of the international standard RFC 4998 (Evidence Record Syntax) and co-author and contributor to a number of internet standards and papers on security and electronic signatures, as well as the co-author of the book “Secure Electronic Archiving”.

Hansen, Robert

Robert (CEO, Founder of SecTheory, Ltd) (CISSP) has worked for Digital Island, Exodus Communications and Cable & Wireless in varying roles from Sr. Security Architect and eventually product managing many of the managed security services product lines. He also worked at eBay as a Sr. Global Product Manager of Trust and Safety, focusing on anti-phishing, anti-DHTML malware and anti-virus strategies. Later he worked as a director of product management for Realtor.com. Robert sits on the advisory board for the Intrepidus Group, previously sat on the technical advisory board of ClickForensics and currently contributes to the security strategy of several startup companies.Robert wrote Detecting Malice authors content on O'Reilly and co-authored "XSS Exploits" by Syngress publishing. He sits on the NIST.gov Software Assurance Metrics and Tool Evaluation group focusing on web application security scanners and the Web Application Security Scanners Evaluation Criteria (WASC-WASSEC) group.

Hartmann, Kate

Kate has worked as Operations Director for the OWASP Foundation since May 2008. She works within the organization to supervise and facilitate a variety of operational tasks ranging from developing forms and designing surveys to planning events and serving as a liaison between committees and the Board of Directors. Kate has a Bachelors Degree with a Major in English/History from Virginia Polytechnic Institute and State University. In her free time, Kate enjoys gardening and referring soccer with her teenage son.

Heiderich, Mario

Mario Heiderich works as a researcher for the Ruhr-University in Bochum, Germany and currently focuses on HTML5, SVG security and security implications of the ES5 specification draft. Mario invoked the HTML5 security cheat-sheet and maintains the PHPIDS filter rules. In his spare time he delivers trainings and security consultancy for larger German and international companies. He is also one of the co-authors of Web Application Obfuscation: '-/WAFs..Evasion..Filters//alert(/Obfuscation/)-' – a book on how an attacker would bypass different types of security controls including IDS/IPS.

Heyes, Gareth

Gareth "Gaz" Heyes calls himself Chief Conspiracy theorist and is affiliated with Microsoft. He is the designer and developer behind JSReg – a Javascript sandbox which converts code using regular expressions; HTMLReg & CSSReg – converters of malicious HTML/CSS into a safe form of HTML. He is also one of the co-authors of Web Application Obfuscation: '-/WAFs..Evasion..Filters//alert(/Obfuscation/)-' – a book on how an attacker would bypass different types of security controls including IDS/IPS.

Hinojosa, Kuai

Currently, Kuai works at Cigital where he is responsible for black box and white box web application assessments, including enterprise web services and mobile devices. Kuai specializes in linking together technical risks and remediation advice, ensuring that developers can correctly interpret and act upon security findings. Recently, Kuai has been responsible for directly interfacing with large enterprise developers to guide and verify their remediation efforts. Before joining Cigital, Kuai worked as a technical lead at New York University's Information Technology Services groups where he led the implementation of New York University's main Content Management. Kuai has also worked as a database security administrator in the banking industry. In his free time, Kuai is a contributor to OWASP Global Education Committee and a member of the NYNJMetro OWASP Chapter board.

Hodges, Jeff

Jeff Hodges is a Security Engineer and Protocol Architect, working at PayPal in the areas of web security, identity, and distributed infrastructure. His interests lie in the areas of web security as well as the nature of "online identity" and its realization via composition of authentication, security, directory, and other technologies. Jeff participates in various IETF working groups including those whose topics involve HTTP, TLS/SSL, and those that touch upon security/identity. He also participates in various other Internet-based fora, e.g. Internet Identity Workshop (IIW), OASIS (SSTC/SAML committee), Kantara, Identity Commons, etc. Previously, he contributed to the Liberty Alliance effort as an editor and co-author of several of the Liberty ID-WSF and ID-FF protocol specifications. Earlier, he served as co-chair of the OASIS Security Services Technical Committee (SSTC/SAML), shepherding and contributing to the development of SAMLv1.0, as well as subsequently contributing to v1.1 and v2.0. His prior work includes contributions to the design of the LDAPv3 directory access protocol (in the areas of authentication and security), as well as the design and deployment of Stanford University's SUNet ID and Registry/Directory infrastructure. He's held architecture, engineering, and management positions at NeuStar, Sun Microsystems, Oblix, Stanford University, and Xerox.

Hoff, Jerry

Jerry Hoff is a Senior Application Security Engineer at Aspect Security. Jerry has led and performed numerous application security code reviews for clients across multiple industries. Jerry also provides training services for clients, and has over 10 years teaching and development experience. Jerry is also involved in the Open Web Application Security Project (OWASP) and was the lead developer of AntiSamy.net project. He has a master's degree in Computer Science from Washington University in St. Louis.

Hoffman, Achim

Achim currently is a senior security and network consultant. He has been developing software since early '80s; while his work used to commonly involve networking, around the turn of the century, he started focusing on web application security starting this millennium. Achim has had much involvement with WADFs and web application security scanners – anticipating their arrival, evaluating them, configuring and using them, and finally watching them disappear. In 2010, Achim founded sic[!]sec GmbH. Achim’s OWASP activities include: Participating in the German Chapter, German Chapter Board Member; Project leader, maintainer, developer of OWASP EnDe Project; reviewer for various other OWASP projects such as SoC 2008 and CAL9000; OWASP papers: Best Practices: WAF and Best Practice: Projektierung der Sicherheitsprüfung von Webanwendungen.

Hofmann, Chris

As Director of Engineering and then Special Projects at the Mozilla Foundation and Corporation since 2003, Chris Hofmann has spearheaded the research and development work of thousands of open source contributors around the world. A Netscape employee before joining Mozilla, Chris contributed to every Netscape and Mozilla browser release since 1996. As the first employee at the Mozilla Foundation in August 2003, Chris led a small but devoted team of the original ten engineers that established the Mozilla Foundation as an independent and self-sustaining organization. In 2004, Chris managed and executed the first worldwide release of Mozilla Firefox 1.0. Firefox 1.0 helped to fulfill the Mozilla Foundation's goal of supporting open Web standards and provide innovation and choice for Internet client software and set Firefox on a path to remarkable market share growth over the last several years.
Chris now helps to build and strengthen Mozilla communities around the world. These contributors and communities are involved with localization of Firefox in to over 70 languages, extend Firefox with Addons, and provide support to Firefox users. He engages with security researchers to help improve browser security and manages Mozilla's Security Bug Bounty Program. He is also interested in engaging, helping, and promoting the work done in companies and large institutions to deploy Firefox use and Mozilla technology.

Hogben, Giles

Dr Giles Hogben is programme manager for secure services at the European Network and Information Security Agency in Greece. He has led numerous studies on Network and Information security, including on topics such as Smartphone security, Cloud computing, Social Network security and European Identity card privacy. Before joining ENISA, he was a researcher at the Joint Research Centre in Ispra, Italy and led work on private credentials. He has a PhD in Computer Science from Gdansk University of Technology in Poland and graduated from Oxford University, UK in 1994 in Physics and Philosophy.

Ichnowski, Jeff

Jeff is currently the Principal Architect at SuccessFactors, where he has worked since September 2008. Prior to that he was the Director of Engineering, Web Technology at the same company. He has a Bachelors of Arts in Computer Science and Asian Studies (Japanese Language & History) from the University of California, Berkeley.

Jimenez, Juan Jose Rider

Juan Jose Rider Jimenez is the CEO of WUL4 in Spain. His experiences include:

• Financial industry: designer of computer solutions (ecommerce, PCI-DSS, etc)
• Healthcare system architect: ChipCard (https://www.chipcard-salud.es/)
• SOA-related technologies expert
• Web Services expert
• High-performance required application architect
• J2EE related-technologies expert
• IBM Websphere expert
• Payment methods and protocols, ecommerce, Internet, 3D-Secure, 3DSET, SPA/UCAF, etc
• JSF, RichFaces, Ajax
• Team Leadership.
• Business Development.

Kang, Abraham

Abraham currently works as part of the code review group for a large financial institution. He has worked on application security issues for over 8 years (focused on security code review for last 3+ years). Additionally he has authored articles related to enterprise application integration, scalability, and security. Lately Abraham has focused on XSS remediation and DOM based XSS. He is also interested in Unicode exploits and filter bypassing using character set mismatches. He recently contributed the candidate chapter for Output Encoding for the Web App Security Guide 3.0. Abraham is looking to contribute more to XSS, AJAX security, Unicode content on the OWASP site.

Keary, Eoin

Eoin is a Senior Manager with Ernst & Young Risk Advisory Services and responsible for Attack and Penetration services for EMEIA. He is a member of the Global Board of OWASP, the founder of the Irish chapter of OWASP and also editor/lead of the published OWASP Code Review (2007/2008) and Testing (V2.0) Guides 2007. He specializes in global large scale penetration testing services. He is also a coordinator for OWASP EU 2011 (to be held in June 2011) and previously organized OWASP Ireland 2009 & 2010

Knobloch, Martin

Martin is a independent Security Consultant at http://www.pervasec.nl. In his previous employment at Sogeti Netherlands B.V., Martin founded and led the Information security task-force PaSS (Proactive Security Strategy) addressing organization, infrastructure and software. Martin is member of the OWASP Netherlands Chapter Board and Chair of the Global Education Committee. He is leading and contributing to various OWASP Project and is member of the OWASP Summit organization team

Kosturjak, Vlatko

Vlatko is security consultant delivering his services in Europe, Middle East and Africa (EMEA) region. He holds multiple certs like PCI QSA, CISSP, CISA, C|EH, LPIC-3... He likes to contribute to open source (security) software and you can find his code in snort, OpenVAS, Nmap, Metasploit and w3af. He is OWASP Croatia chapter leader and OWASP favicon project leader.

Koussa, Sherif

Sherif is an application security independent consultant. Founder and Leader of OWASP Ottawa since 2006. Founder and principal consultant for Software Secured; an application security boutique shop.

Kuivenhoven, Marinus

Marinus works as a Senior Security Specialist at Sogeti Nederland BV. He has experience in developing and administration of multi-tier systems. Marinus is one of the founders and an active member of the Sogeti taskforce PaSS (Proactive Security Strategy), which focuses on implementations of the secure development lifecycle. He developed and teaches several courses in application security for educational institutes and customers. He is actively involved in OWASP. In the past years he has written articles for magazines like Computable and We Love IT. And he spoken on several international events including OWASP, ROOTs, Open Source Developer Conference and Engineering World.

Kumar, Nishi

Nishi is currently a Systems Architect at FIS with 20 years of broad industry experience. She is part of OWASP Global Education Committee and project lead for OWASP CBT (Computer based training) project. She is a committed contributor of OWASP. She has spearheaded Secure Code Initiative program in FIS Electronics Payment division. As part of that program, she has delivered OWASP based training to management and development teams to various groups in FIS. She has been involved with PA-DSS certification of several applications in FIS. Since joining FIS in 2004 she has worked as an architect and team lead for several financial payment and fraud applications. She has hands-on accomplishments in design, development and deployment of complex software systems on a variety of platforms. Prior to joining FIS, Nishi worked for Pavilion, HNC, Fair Isaac, Trajecta, Nationwide Insurance and Data Junction as Senior Software Engineer, Architect and in Project Management roles.

Lacerda, Filipe

Filipe is currently an IT Consultant and CIO/partner at Mipe/Lusolabs in Portugal. He has a degree in both Multimedia Engineering and Computer Science and his preferred programming language is PHP. Filipe is involved in the OWASP Academies project. For the last 7 years he has been teaching IT and this is an activity that he really enjoys. Additionally, he is a passionate person that loves technology and extreme sports such as white water kayaking.

Lauritão, Rogério Paulo Vicente

Rogério works for SAPO Portugal Telecom and assisted in taping and broadcasting the Global Summit Working Sessions to remote attendees around the world.

Li, Jason

Jason is an application security professional with experience in leading code review, penetration testing, and regulatory compliance assessments. He is also a proficient software developer including time spent as technical lead for Java and Java EE applications. He has a broad training background including development of courses about software development and application as well as delivery in live, virtual and eLearning formats. Jason is heavily involved in OWASP; his roles include:

- Co-Chair of the OWASP Global Projects and Tools Committee
- Frequent speaker at OWASP Conferences
- Project Lead for the OWASP JSP Testing Tool
- Core Contributor to the OWASP AntiSamy Project

Lindsay, David

David is a Senior Security Consultant with Cigital. His primary areas of interest include web application vulnerabilities, cryptography and web standards. His primary area of disinterest is writing bios.

Long, Jeremy

Jeremy is an Information Security Engineer for a large financial institution. He has been involved in drafting secure coding policies, delivering secure development training, and performing security code reviews. He has a MS in Information Security from James Madison University and currently holds the CISSP and GSSP-J certifications.

Loureiro, Nuno

Nuno has a MSc in Information Technology - Information Security from Carnegie Mellon University and currently works for SAPO where he's leading the Security Team. Besides his passion for Security and Web Security, he loves hiking and traveling.

Luptak, Pavol

Pavol gained his MSc in Computer Science at the Czech Technical University in Prague / Czech Republic with master thesis focused on ultra-secure systems. He holds many prestigious security certifications including CISSP and CEH, in addition to being the Slovak OWASP chapter leader, co-founder of the first Slovak hackerspace Progressbar and Society for Open Technologies (SOIT) where he is main responsible for IT security. Pavol has presented regularly at security conferences around the world. In the past, he demonstrated vulnerabilities in the public transport SMS tickets in all major cities in Europe, together with his colleague Norbert Szetei he practically demonstrated vulnerabilities in Mifare Classic RFID cards. He has 14 years experience in IT security, penetration testing and comprehensive OWASP security audits including social engineering and digital forensic analysis. Pavol is one of the co-author of the OWASP Testing Guide v3, has a deep knowledge of the OSSTMM, ISO17799/27001 and many years experience in seeking vulnerabilities. Currently, he is focused on web application obfuscation and GSM security.

Lyon, Chris

Chris Lyon is the Director of Infrastructure Security at Mozilla.

Manico, Jim

Jim Manico is the producer and host of the OWASP Podcast Series. He is also the project manager of the OWASP ESAPI project, a contributor to the OWASP Cheat-sheet Series, the chair of the OWASP Connections committee, and a member of the OWASP mobile project. Jim is currently an independent Application Security Architect and Educator. He has 15 years of experience developing Java-based data-driven web applications for organization such as FoxMedia (MySpace), GE, CitiBank, Sun Microsystems and Aspect Security. Jim has also provided Application Security Developer Education services for Fortune 10, Government, and NGO Institutions.

Maor, Ofer

CTO, Hacktics, Chairman, OWASP Israel

Ofer Maor has over fifteen years of experience in the Information Technology and Security. Mr. Maor is a pioneer in the Application Security field: he has been involved in leading research initiatives, has published numerous papers, appears regularly at leading conferences and is considered a leading authority by his peers. He also currently serves as the Chairman of OWASP Israel. Before founding Hacktics, Mr. Maor led Imperva's Application Defense Center, a research group focused on application security services and education. In this capacity, he advanced research activities and was responsible for all the application security services conducted by the company. He was previously a Senior Security Consultant at eDvice, an application security consulting firm, and served for three years as an Information Security Officer in the Israeli Defense Forces.

Mancini, Lucilla

Lucilla has a degree in Economics and extensive experience in finance, trading and derivatives. At some point in her career, Lucilla joined her financial experience with ICTmatters; and now after having worked for some years for Getronics both in Italy and in worldwide groups, leads a consulting team of about 25 people at Business-e. Lucilla's main duties involve in Governance, Audit and Ethical hacking with a group of 10 testers.
She has the following certifications: Cisa, Lead auditor ISO27001, Itil v3, CRISC, and Cobit.

Martinez, Mateo

Mateo's background includes many years of experience in Senior Information Security, Risk Management, Business Continuity Planning and Consultancy roles. Since 2007, he has been working at Tata Consultancy Services as the Information Security Manager. In this role, he is in charge of the Information Security Area, Implementing ISO 27001, Internal Audit, Security Incidents Management, Architecture & Design Review, Penetration Testing, Software Security for Latin American region and in charge of the Advisory of Security Services department. Mateo has his CISSP and has executed BCP and Information Security projects in the United States and in Dubai, UAE. Previously Mateo worked as a Senior BCP Consultant at PricewaterhouseCoopers. Mateo is one of the local chapter leaders for OWASP Uruguay.

Martorella, Christian

Christian has been working in the field of information security for the last 10 years, starting his career in Argentina IRS as security consultant, now he's Practice Leader in Threat and Vulnerability - EMEA in Verizon Business. He is co-founder an active member of Edge-Security team, where security tools and research is released. He has been speaker at What The Hack!, NoConName, FIST Conferences, OWASP Summit 2008 and OWASP Spain IV & VI, Source Conference Barcelona and Hack.LU. Christian has contributed with open source assessment tools like OWASP WebSlayer and Metagoofil. He likes all related to Information Gathering and Penetration testing. Christian currently holds the President position at the FIST Conferences board, and in the past taught Ethical Hacking at the IT Security Master of La Salle University.

Matatall, Neil

Neil is a Consultant for FishNet Security as part of the Application Security team. After starting off as a developer, Neil was asked to investigate application security and he hasn't looked back since. In OWASP, Neil has been a conference organizer (AppSec US 2010 and AppSec Academia '09), chapter leader (Orange County), project committer (ESAPI), and global conference committee member.

Melo, Ricardo

Ricardo is the CTO at DRI, a Portuguese company focused on open source environments. He has +10 years working with Linux and open source technologies like PHP and Mysql. He has been involved in a large number of projects, both web and non web applications, from small sized to +100 computer clusters both as developer, system administrator and software architect.

Mendo, Tiago

Tiago has worked in the security area for a few years, mostly in network security doing traffic analysis and network reverse engineering. He is a member of the Portuguese Honeynet Project and currently working for SAPO, which is the most visited site in Portugal, in the Web Security team. Tiago was part of the SAPO team that was involved in taping and broadcasting the Global Summit Working Sessions to remote attendees around the world.

Meucci, Matteo

Matteo has undergraduate degrees in Computer Science Engineering from the University of Bologna (Italy). He is the OWASP-Italy Founder and Chair from January 2005, leads the new OWASP Testing Guide from 2006, and he is starting the OWASP Common Vulnerability list with Anurag Agarwal and Eoin Keary. He is one of contributor of OWASP SAMM. He holds CISSP, CISA certification**,** Matteo is the CEO and a cofounder of Minded Security, an Application Security Consulting Company, with more than 10 years of specializing in information security and collaborates from several years at the OWASP project. Matteo is invited as speaker at many events all around the world talking about Web Application Security.

Nagra, Jasvir

Jasvir Nagra is a researcher and software engineer at Google. He is one of the designers and developers of Caja - a secure subset of HTML, CSS and JavaScript; co-author of Surreptitious Software - a book on obfuscation, software watermarking and tamper-proofing; contributor to Shindig - the reference implementation of OpenSocial; and an escaped perl hacker.

Neaves, Tom

Tom "c0redump" Neaves M.Sc, B.Sc (Hons) is a Principal Security Consultant at Verizon Business (formerly NetSec) where he is part of the Threat and Vulnerability Consulting EMEA Practice. Tom is also studying for a Ph.D in Information Security on a part-time basis back at Royal Holloway, University of London. Anything that speaks HTTP or gets transmitted over the air has his full attention!

Paiva, Sandra

Sandra took the position of OWASP Training Manager in October 2010 and was responsible for managing the OWASP 'Chapter-lead' Training activities and operationalizing the concept of 'OWASP Academies'. Throughout this process, she was managed by Dinis Cruz and report directly to the OWASP Board. Previously, Sandra was the Head of Customer Relationship Management (CRM) for Europe, Middle East and Africa at the Mergermarket Group (part of the Financial Times Group), having joined the company in July 2007 as a CRM Executive. She has a graduate degree in Statistics and Management of Information and a post-graduate degree in the same area..

Sandra has worked in several universities in Portugal where she taught Math and Statistics for about six years and thereafter, throughout an academic year, worked in the conceptualization, development and production of materials to support academic and scientific events and in the creation of methodologies to repackage contents and support academic and scientific activity.

Papapanagiotou, Konstantinos (Kostas)

Kostas has more than 7 years of experience in the field of Information Security both as a corporate consultant and as a researcher. Currently, he is Information Security Risk Management Services Manager of Syntax IT Inc and leader of the OWASP Greek Chapter. He holds a BSc from the Department of Informatics and Telecommunications, University of Athens, an MSc with distinction in Information Security from Royal Holloway, University of London and a PhD in Information and Network Security from the Department of Informatics and Telecommunications, University of Athens. He is the author of more than 10 scientific publications. He is a member of the ACM, IEEE and also a founding member of the Institute of Information Security Professionals (IISP). His current research interests are in the areas of application security, trust and security in pervasive and ubiquitous computing and steganography.

Pegorelli, Marta

Marta is a Strategist for corporate events and social events at Anggulo Eventos in Brasil. She is part of the Global Summit event team and her duties include organization of the Brazilian delegation as well as negotiation and liaising with the venue staff.

Potjes, Linda

Linda, from the Netherlands, is a Java Programmer in daily life. Living with an active OWASP member, she's been visiting a lot of conferences , slowly getting more and more interested in security. She is part of the OWASP Summit support team and assisting with miscellaneous tasks and errands – whatever needs to be done!

Reinhart, Ralf

Ralf is an expert in IT security focused on web application security. He has performed penetration tests on a large number of applications and systems at well-known companies, analyzed and reviewed the underlying architecture and hundreds of thousands lines of source code. He reverse engineered countless binaries and inspected a lot of log files.
As a child of the 80s Ralf used his 8 bit home computer, a black and white television set, an acoustic coupler and a rotary dial plate telephone to send his first email. Several years later he achieved an academic degree of a computer scientist (Diplom-Informatiker (FH)). He worked as a system and data base administrator, as a software designer and developer in the enterprise area where he engineered solutions on all tiers for the client, the server and the data base site. Furthermore he was IT project leader in the fields of software development, roll out, operations and maintenance. Accompanying his broad working experience he gained several certifications like ITIL v2 service manager, Oracle DBA and IT project manager.
Ralf is actively involved with the OWASP German Chapter, is founder and organizer of the Munich OWASP Stammtisch initiative, and for more than 20 years a signed in member of the Chaos Computer Club. In 2010 Ralf worked with his long term colleague Mr. Achim Hoffmann to found – the sic[!]sec GmbH – a company for IT security, process optimization and data protection. This is there he is employed currently as a principal consultant and general manager.

Richler, Heiko

Georg Simon Ohm University of Applied Sciences. OWASP University Chapter

Rohr, Matthias

Matthias is a consultant and software architect at BTC AG and a PhD student in the Research Training Group TrustSoft at the University of Oldenburg, Germany. He studied computer science at the Monash University, Melbourne (Australia) and at the University of Oldenburg (Germany). At present, he writes a PhD thesis on automatic failure diagnosis for large software systems based on timing behavior anomaly detection. His research interests include software performance, software reliability, and software dependability engineering.

Ross, David

David is a Principal Security Software Engineer on the MSRC Engineering team at Microsoft. Prior to joining MSRC Engineering in 2002, David spent his formative years on the Internet Explorer Security Team and wears the battle scars with pride. David's blog: http://blogs.msdn.com/dross

Roth-Mandutz, Elke

Elke is currently a Research Staff Member at Georg Simon Ohm University of Applied Sciences in Nuremberg Germany.

Saario, Mikko

Mikko is currently a Senior Specialist at Nokia Corp in Finland, where he works in a complex and diversified mobile/web environment. Mikkko is also a member of the board (in 2007) on the Finnish Information Security Association i.e. Tietoturva ry (www.tietoturva.org). Last but not least, Mikko founded and chaired the OWASP Helsinki Chapter.

Samuel, Michael

Mike is an engineer in Google's Applied Security group working on programming language based approaches to web application security. He is involved in the EcmaScript standards process and is one of the implementers of Caja, a system that allows for secure composition of web applications using existing standards. Lately he has been working on static type reasoning to make template languages robust against XSS.

Schmidt, Chris

Christopher Schmidt: GIS and Web Hacker
Chris is a professional web application developer, and has spent the past several years developing server and client side tools for the creation of web applications, especially applications which relate to mapping. Some of his most visible work over the past year is in the OpenLayers/TileCache/FeatureServer stack, a collection of open source tools designed to help users build mapping applications. Chris's has been involved in OWASP through Leading the ESAPI for Javascript Project and contribution to a number of other projects. He also serves as a member of the Global Projects Committee.

Schuh, Justin

Justin has held a variety of different positions across the IT spectrum, with most of his time focused on the security side of the industry. He likes interesting technical challenges solving unique problems. Justin's Specialties: Software reverse engineering, security assessment, exploit development. Software development on a wide range of languages, platforms and technologies. Management of software development and security consulting teams.

Schwartz, Stephen

Steve is currently the Director of Business Development at Stach & Liu; in addition to serving as the OWASP Atlanta local chapter Leader. Previously, Steve worked as Application Security Center Sales at HP Software, District Sales Manager at SPI Dynamics, and District Sales Manager Southeast at Trusted Network Technologies. He received a B.S. in marketing from Franklin Pierce College, where he also played Division II Baseball.

Searle, Justin

Justin Searle is a Senior Security Analyst with InGuardians, specializing in the penetration testing of web applications, networks, and embedded devices, especially those pertaining to the Smart Grid. Justin is an active member of ASAP-SG (Advanced Security Acceleration Project for the Smart Grid) and led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628. Previously, Justin served as JetBlue Airway's IT Security Architect, and has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities and corporations. Justin has presented at top security conferences including DEFCON, ToorCon, ShmooCon, and SANS. Justin co-leads prominent open source projects including the Samurai Web Testing Framework, Middler, Yokoso!, and Laudnum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

Secker, Tanya

Tanya is an Application Security Specialist at Trustwave and is the local Chapter Leader for OWASP Gibraltar.

Serrao, Carlos

Carlos is an Assistant Professor at ISCTE-IUL (Lisbon University Institute)/SoTA (School of Technology and Architecture)/DCTI, where he teach several subjects related to Information Systems, Information Security, IT/IS Project Management and Entrepreneurship (both on BSc and MSc programs). Additionally he is an ADETTI-IUL Researcher and Project Manager where I'm working mostly on the following research topics:
- Distributed Systems, Applications and Information Security
- Management and Protection of e-Intellectual Property and e-Contents
- Web-based and Mobile-based Information Systems
Projects. Experience in participation in multiple national and international co-operation IT/IS projects and provision of consulting services to different companies.
Carlos is also the OWASP Portugal Chapter Leader and is currently working to evangelize OWASP good practices and OWASP mission in improving the web applications security.

Stasinopoulos, Anastasios

Anastasios is a Certificated Network Administrator of CompTIA (Computing Technology Industry Association) computer-security enthusiast and also a hobbyist penetration tester. He is basically deals with Networking and Data Communications, Security as Fedora Security Spin Contributor and Penetration testing. He is also the developer of a set of Hackademic Challenges that anyone can practice for real world applications attacks and penetration tests (http://hackademic.s3cure.gr).

Sterne, Brandon

Brandon is the Security Program Manager at Mozilla where he works on security releases and designs and implements browser security features.

Steven, John

John is the Senior Director, Advanced Technology Consulting at Cigital with over a decade of hands-on experience in software security. John's expertise runs the gamut of software security from threat modeling and architectural risk analysis, through static analysis (with an emphasis on automation), to security testing. As a consultant, John has provided strategic direction as a trusted advisor to many multi-national corporations. John's keen interest in automation keeps Cigital technology at the cutting edge. He has served as co-editor of the Building Security In department of IEEE Security & Privacy magazine, speaks with regularity at conferences and trade shows, and is the leader of the Northern Virginia OWASP chapter. John holds a B.S. in Computer Engineering and an M.S. in Computer Science both from Case Western Reserve University.

Su, Cecil

Ever since Cecil began working in the financial services industry, his interest of information security (and especially of application security) was stoked. For his extra-curricular activities after office hours, he took every opportunity to learn about the craft. Now, after 10 years, Cecil's day job is as a director of Grant Thornton LLP in Singapore. As head of the Technology Advisory unit, he leads various engagement teams on diversified projects across vertical industries. His area of focus is in IT Assurance, IT Security Advisory and Digital Forensics. Aside from being a committee member of the OWASP GEC, he has also contributed to the OWASP Testing Guide, and coordinated efforts for the internationalization of Asian languages of OWASP materials. Cecil is also the current Chapter Lead for the Singapore Honeynet Project, ExCo member for the Association of Information Security Professionals (AISP), and a member of the security Controls and Security Services Working Group.

Tasar, Vehbi

Dr. Vehbi Tasar, CISSP, CSSLP, Director of Professional Programs Development - is in charge of all exam development at (ISC)². His responsibilities include exam question and content development, psychometric oversight of the exam questions, and maintenance of the ANSI certification for all (ISC)² credentials. Vehbi joined (ISC)² in June 2008 to develop a new security credential called Certified Secure Software Lifecycle Professional (CSSLP). Prior to joining (ISC)², Vehbi worked in software industry for over 30 years. He has a broad spectrum of application development expertise ranging from high performance computing to the database application development, and distributed enterprise computing for the IT infrastructure. Vehbi holds a B.S degree in Electrical Engineering from the Middle East Technical University from his native Ankara, Turkey. He received a M.S degree in Computer Science from the University of Missouri, Rolla, and a Doctor of Engineering Degree in Electrical Engineering from the University of Detroit, Mercy in Detroit, Michigan.

Taylor, Jason

Jason is the Chief Technology Officer at Security Innovation, where he leads the strategic direction for all technology initiatives and manages world-class development teams for the company's product lines. He has spent his career focused on application development and testing with a primary focus on application security. His unrivaled understanding of application behavior provided the impetus for Security Innovation’s industry pioneering fault injection tool, Holodeck Enterprise Edition, and critical enhancements to the company’s internal testing and development tools. Jason was the visionary and designer of the Company’s “Creating Secure Code” methodology and course which has been taught to several of the world's largest technology organizations.

Prior to joining Security Innovation, Jason served as test architect, security lead and development manager at Microsoft for various releases of Internet Explorer and Windows. He was the first member of the Internet Explorer security test team, and as the security team lead, he grew it from a solitary operation to the leading application security test team at Microsoft. Later, he built the Test Model Toolkit which became the standard model-based testing tool at Microsoft, winning a Best Practice Award along the way.

Tesauro, Matt

Matt has been involved in the Information Technology industry for more than 10 years. Prior to joining Praetorian, Matt was a Security Consultant at Trustwave's Spider Labs. Matt's focus has been in application security including testing, code reviews, design reviews and training. His background in web application development and system administration helped bring a holistic focus to Secure SDLC efforts he's driven. He has taught both graduate level university courses and for large financial institutions. Matt has presented and provided training at various industry events including DHS Software Assurance Workshop, AppSec EU, AppSec US, AppSec Academia, and AppSec Brazil.

Matt is currently on the board of the OWASP Foundation and highly involved in many OWASP projects and committees. Matt is the project leader of the OWASP WTE (Web Testing Environment) which is the source of the OWASP Live CD Project and Virtual Machines pre-configured with tools and documentation for testing web applications..

Thomas, Mark

Mark is a Staff Engineer with the SpringSource division of VMware. The majority of Mark's time is spent on the development of Apache Tomcat but he also provides expert Tomcat advice to the SpringSource support team and he leads the SpringSource security team as well as the integration of Tomcat with tc Server. Mark has been using and developing Apache Tomcat for more than seven years. He became involved in the development of Tomcat when he needed better control over the SSL configuration than was available at the time. After fixing that first Bugzilla issue, he started working his way through the remaining Tomcat issues and is still going. Along the way, Mark became a Tomcat committer and PMC member, undertook the majority of the Servlet 3.0, JSP 2.2 and EL 2.2 development for Tomcat 7, created the Tomcat security pages, became a member of the ASF, joined the Apache Security Committee and is an Apache Commons PMC member where he contributes to Commons Pool, DBCP and Daemon. He is currently the Tomcat 7 release manager and also helps maintain the ASF's Bugzilla and Jira instances. Mark has a MEng in Electronic and Electrical Engineering from the University of Birmingham,UK.

Tomhave, Benjamin

Ben is a Senior Security Analyst with Gemini Security Solutions in Chantilly, VA, specializing in solutions architecture, security planning, security program development and management, and other strategic security solutions.
Ben holds a Master of Science in Information Security Management from The George Washington University. He is a Certified Information Systems Security Professional (CISSP), co-vice chair of the American Bar Association Information Security Committee, member of ISSA, member of OWASP, and member of the IEEE Computer Society. He is a published author and an experienced public speaker. Prior to his current endeavor, Ben has worked in a variety of security roles for companies including BT Professional Services, AOL, Wells Fargo, ICSA Labs, and Ernst & Young.

Turpin, Keith

Over the years Keith has held a number of positions at the Boeing Company including: Application and Information Security Assessments team leader, lead IT security adviser for international operations, supplier security analyst, engineering systems integrator, software developer and senior manufacturing engineer on the 747 airplane program. Additionally, Keith represents Boeing at the International Committee for Information Technology Standard's cyber security technical committee. Currently, Keith serves as a delegate to the International Standards Organization's (ISO) subcommittee on cyber security and recently joined the national Software Assurance (SwA) Working Group Keith is the Project Leader for the OWASP Secure Coding Practices – Quick Reference Guide.

UcedaVelez, Tony

Tony develops and leads strategic IT & IS solutions for businesses that seek to mitigate IT operational and security risk through robust, cost effective programs, while maintaining a strategic alignment to key business objectives and providing overall value to the enterprise. His specialties include Security Risk Management, Risk Assessment Methodologies, Business Impact Analysis, Business Process Engineering, Maturity Modeling, Security Training, Vulnerability Assessment, Policy Management, Compliance Audits, Business Continuity Planning, Remediation Management

Uhley, Peleus

Peleus Uhley is the Platform Security Strategist within Adobe's Secure Software Engineering Team (ASSET). His primary focus is advancing Adobe's Secure Product Lifecycle (SPLC) within Adobe platform technologies, including Flash Player and AIR. Within OWASP, Peleus helps to maintain the OWASP Flash Security Project. Prior to joining Adobe, Peleus started in the security industry as a developer for Anonymizer, Inc., and went on to be a security consultant for @stake and Symantec.

van der Baan, Steven

Steven is a father of two and works as a Software Architect and Security Consultant for Sogeti Nederland BV. He has used computers for 27 years, starting with the ZX81 where he learned to program inside a memory of a whooping 1K. Steven saw every other computer thereafter as a bundle of joy and an adventure. This adventure is something that he's now trying to share with his kids. Steven was introduced to OWASP by Martin Knobloch and a colleague who was hosting CTF at Appsec DC 2009. This colleague called Steven due to some minor problems and (of course) Steven jumped in to help. Steven's involvement became more regular and eventually he took over leadership of the CTF project.

Vasilopoulos, Kyprianos

Kyprianos is a Senior Security Consultant at Atos Origin in Greece.

Vela, Eduardo

WebAppSec Researcher (sirdarckcat), Eduardo is an experienced web application security researcher, who has assisted companies such as Adobe, Apple, Google, Microsoft, Mozilla, Oracle, and Symantec in the resolution of security issues. Eduardo has also imparted courses and security conferences: DNS International, Microsoft Bluehat V8 (October 2008), BlackHat USA (2009), XCon (2009), BlackHat Europe (2010), OWASP day Mexico (2010), OWASP AppSec Sweden (2010). He is knowledgeable on SQL, PHP, Python and Ruby for web development and C/C++ for application development – exercising extreme caution on making fast and efficient code, but most of all, secure. He's also an enthusiast on Internet Culture and Social Networking research, music, literature, as well as a fan on solving algorithmic problems. Eduardo's specialties include Web Application Security, Programming (C/C++, PHP, Java, JavaScript, Python, Ruby, Batch/Bash, Perl)

Vilares Da Silva, Luis

Luis worked in the Portuguese central statistics office (INE) as systems and network engineer, software engineer 1990 to 1999. Worked as a webmaster, web developer and software engineer in the European police office (EUROPOL) in The Hague1999 to 2009. In that period did his MSc in IT Security and CISSP certification, MS training 70-340 and is MSTS for SharePoint 2007. He did audits and risk mitigation in the finance systems in Portugal in 2010 and is back to The Hague to work as a software architect within the Organization for the Prohibition of Chemical Weapons (OPCW) where he is trying to leverage some security into the various developed and under development applications. Last but not least, Luis is in the process of finalizing an MSc in forensic computing sand cybercrime investigations from UCD Dublin open to law enforcement only.

Vlachos, Vasileios

Dr. Vasileios Vlachos is lecturer at the department of Computer Science and Telecommunications of the Technological Educational Institutions (TEI) of Larissa. Previously, he was a senior R & D engineer at the ResearchAcademic Computer Technology Institute (R.A.C.T.I.) of Patras, Greece; and was a member of the Digital Awareness and Response to Threats (DART) team of the Special Secretariat for Digital Planning of the Hellenic Ministry of Economy and Finance. Dr. Vlachos holds a Diploma of Engineering in Electronic & Computer Engineering from Technical University of Crete, an MSc in Integrated Hardware and Software Systems from the Department of Computer Engineering and Informatics of the University of Patras and a PhD in Information Systems Security from the Department of Management Science and Technology of Athens University of Economics and Business. Dr. Vlachos has taught at the University of Thessalia the University of Central Greece and the University of Piraeus.

Vroom, Ferdinand

Ferdinand started as a FoxPro developer in 1995, but wanted to assume other roles in the development lifecycle.. The international part of his career started at Arthur D. Little, were he worked on many international projects in several countries like the US, UK, Germany, France, Italy, Spain and Belgium. Internet technologies, specifically web, have always been a large part of Ferdinand's daily work. After starting work at Nationale- Nederlanden in 2000 as coordinator of the Internet Development team he focused on the development lifecycle within this large Insurance company. Since 2005, Ferdinand has worked as a security officer and security architect, responsible for security related subjects in the development lifecycle and advising on security related matters in projects. Currently, Ferdinand works on security aspects of the new Financial Services Architecture integrating security measures in Cloud based infrastructures. Ferdinand enjoys sailing, skiing and car mechanics.

Watson, Colin

Colin is a consultant and co-founder of Watson Hall Ltd. Colin has a production and process engineering background, but has worked in information systems for fourteen years, concentrating exclusively on web application development, security and compliance. His work involves the management of application risk, building security and privacy into systems development and keeping abreast of relevant international legislation and standards. He has a particular interest in creating user trust in web systems and the relationships between security and usability. Colin has spoken at several OWASP chapter meetings and conferences on topics including web content accessibility guidelines, the Open Software Assurance Maturity Model and AppSensor. He is an OWASP project contributor and is a member of the OWASP Global Industry Committee, having been its chair for 2009-2010. He writes a blog about web security, usability and design under the pseudonym Clerkendweller. He holds a BSc in Chemical Engineering and an MSc in Computation from the University of Oxford.

Wichers, Dave

Dave has worked as an Information Security consultant continuously since 1989. He is currently focused on developer training, security code reviews, application penetration testing, technology selection, security policy development, infusing security into the software development lifecycle, and the development of standard security controls. He has particular expertise in security of web applications.
Dave also is currently an OWASP Board Member and coauthor and project lead of the OWASP Top Ten Most Critical Web Application Security Vulnerabilities (http://www.owasp.org/index.php?Top10).

Wilander, John

John is an application security researcher and consultant. He is a partner and evangelist at Omegapoint, a consultancy firm based in Sweden. John typically works as a security focused software developer. Java and JavaScript are his languages of choice. After his Master's degree in Computer Science and Engineering from Linköping University (Sweden) and Nanyang Technological University (Singapore) he pursued a PhD in application security. Last paper still pending but John's research publications can be found at: http://www.ida.liu.se/~johwi/research_publications/ John started the Swedish OWASP Chapter in 2007 and has since been leader and co-leader. In 2010 he chaired the most successful OWASP AppSec EU conference so far – OWASP AppSec Research 2010. John along with the Swedish chapter are listed as contributors to OWASP Top 10 2010.

Williams, Jeff

Jeff is the founder and CEO of Aspect Security, specializing in application security services including code review, penetration testing, training, and eLearning. Jeff also serves as the volunteer Chair of the Open Web Application Security Project (OWASP) where he has made extensive contributions, including the Top Ten, WebGoat, Secure Software Contract Annex, Enterprise Security API, Application Security Verification Standard, OWASP Risk Rating Methodology, starting the worldwide local chapters program, and starting the Rugged Software movement. Jeff holds advanced degrees in psychology, computer science, and human factors, and graduated cum laude from Georgetown Law. You can contact Jeff at jeff.williams@aspectsecurity.com.

Wilson, Doug

Doug is one of the co-chairs of the Washington DC OWASP chapter, and one of the organizers of the OWASP AppSec DC conference in Washington DC. He is a Principal Consultant for MANDIANT, a full service security company based out of the Washington DC area. Doug has been involved in information security for over a decade. He got his start in the Web 1.0 dot-com years working for web hosting companies, and ended up doing government contracting, with expertise in incident response and multi-tiered application architecture. He currently supports government contracts exploring ways of improving software assurance and confidence in COTS software. He has spoken at a wide variety of professional events in Washington DC, including Shmoocon, and the High Confidence Software and Systems (HCSS) conference.

Wuensch, Stefan

Starting as soon as he could grip a screwdriver, Stefan spent his formative years hacking and tinkering with anything run by electricity. Later Stefan joined the Boston-area hacker group L0pht, and was a member for five years. In 1998 Stefan and the other L0pht members testified before the United States Senate as part of a series of hearings on "Weak Computer Security in Government: Is the Public at Risk?" For the past 13 years Stefan has been working at Harvard University where he has been involved with security, high-performance research computing, networking, and systems infrastructure. His current role is Senior UNIX Engineer.

Wysopal, Chris

Chris Wysopal, Veracode's CTO and Co-Founder, is responsible for the company's software security analysis capabilities. In 2008 he was named one of InfoWorld's Top 25 CTO's and one of the 100 most influential people in IT by eWeek. One of the original vulnerability researchers and a member of L0pht Heavy Industries, he has testified on Capitol Hill in the US on the subjects of government computer security and how vulnerabilities are discovered in software. He is the author of "The Art of Software Security Testing" published by Addison-Wesley.

Yeo, John

John Yeo is Director of Trustwave's SpiderLabs for the EMEA region. SpiderLabs, one of the world's largest global security practices, is the advanced security division within Trustwave. SpiderLabs is focused on application security, incident response, penetration testing, physical security and security research. At Trustwave John is responsible for managing the various SpiderLabs teams and all aspects of service delivery within the EMEA region.

Zusman, Michael

Mike is a Managing Principal Consultant with the Intrepidus Group. At Intrepidus, his focus is on assisting clients in architecting secure mobile solutions and applications for various platforms including iOS, Android, and RIM. Prior to joining Intrepidus Group, Mike has held the positions of Escalation Engineer at Microsoft, Security Program Manager at Automatic Data Processing, and lead architect & developer at a number of smaller firms. In addition to his corporate experience, Mike is an independent security researcher, and has responsibly disclosed a number of critical vulnerabilities to commercial software vendors and other clients. He has spoken about mobile application security at a number of top industry events including Black Hat, CanSecWest, OWASP meetings and at local colleges including Polytechnic University. He has attained the CISSP certification, and is a co-leader of the OWASP Mobile Security Project.

About the OWASP Summit 2011 logo: