OWASP
SUMMIT
2011
LISBON
PORTUGAL
FEB 8-11

Outcomes & Operational Guide

Table of Contents

Introduction

Summit Statistics
# Attendees

30 Countries Represented

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
UK
United States
Uruguay

44 OWASP Chapters represented

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 (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
Washington D.C.

PRESS RELEASE

Hello World! OWASP Summit 2011 Kicks Off Massive Outreach Program

Lisbon, Portugal, February 15, 2011 - The Open Web Application Security Project (OWASP) today announced the results from its 2011 OWASP Summit. Over 180 application security experts from over 120 companies and 30 different countries joined forces to plan, build, and execute programs to improve 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.

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. Delegates gathered outside Lisbon, Portugal for a week of interactive working sessions and discussions. OWASP Summits are unlike conferences with static presentations. Instead, working sessions are used to author documents, create software, draft standards, and forge lasting relationships.

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.

- **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.

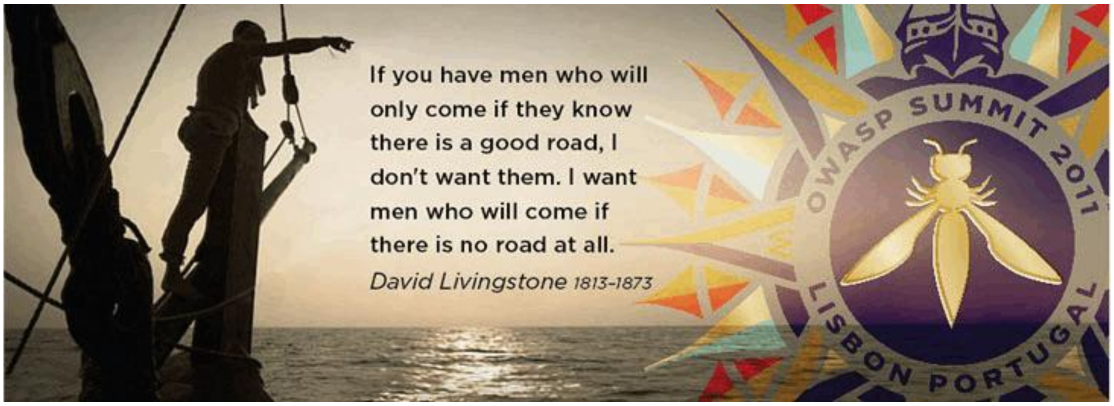
The full results of the Summit will be captured and released as an OWASP Report. The results will be released for comment and then ratified as a final deliverable. For more information, including notes, video, pictures, and other deliverables, please visit www.owasp.org.

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



If you have men who will only come if they know there is a good road, I don't want them. I want men who will come if there is no road at all.
David Livingstone 1813-1873

ABOUT THE OWASP SUMMIT

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.

The Summit is NOT a conference - there are no talks or training seminars. This is an opportunity to do actual work to further the field of application security. Participants will 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 the Summit! OWASP community members, application security experts, industry players, and developers are all welcome at the Summit. Attendees come ready to work and produce deliverables that advance the state-of-the-art in application security.

Many of the working sessions were created "dynamically" by the attendees. Anyone can propose a new working session, sign up for a room and time slot, and meet to work with other interested parties. Many of the main sessions ended up spawning multiple dynamic sessions to accomplish particular goals.

Much of the work that goes on at the Summit is at meals, social events, or hallways. We live together, eat together, and play together. We work hard and play hard for a solid week focused on application security. Even the OWASP Band is free and open for anyone to participate.

SUMMIT QUOTES

- *“I saw the ‘blossoming’ of OWASP in Portugal’s Spring. From an external viewpoint, OWASP has moved from niche to widely relevant, from localized to global, from pentesting to SDLC, from server to every component of the application’s delivery and use, from infosec to business process relevance.” – Colin Watson*

- *“I never would have found myself in a meaningful dialog with Google had it not been for this conference.” – Robert Hansen (RSnake)*

- *“I needed to discuss complex security problems that required input from a number of different people to solve it. At OWASP Summit we brought things together!” -- Tobias Gondrom, IETF*

- *“Seeing and meeting the world’s best-known security professionals at one place! Great party!” – Achim Huffmann*

- *“The Summit had an intense feeling of activity, information exchange, and planning” – Chris Wysopal, Veracode*

- *“It was interesting to see how much work got done in less than a week!” – Vishal Garg, AppSecureLabs*

- *“I’d like to say that the Summit has been absolutely a great experience. It’s the most useful security event that I’ve been to in the last few years. This most definitely was one of those events where things actually got done!” – Edward Bonver*

- *"The Summit is THE place to come together and transform great ideas into reality" – Cecil Su, Grant Thornton*

- *"Browser Security Track has made great progress in terms of outreach, involvement, and cross-company collaboration. Other groups should replicate this behaviour."*

- *"The system really works! The process is transparent and OWASPers are very committed in having a more secure world" – L. Gustavo C. Barbato - Dell*

- *"I saw the 'blossoming' of OWASP in Portugal's Spring. From an external viewpoint, OWASP has moved from niche to widely relevant, from localized to global, from pentesting to SDLC, from server to every component of the application's delivery and use, from infosec to business process relevance." – Colin Watson, Watson Hall*

- *"I enjoyed the sheer energy of the group"*

- *"I really liked the format of many sessions that were panel and open discussion around looking at problems and finding solutions"*

- *"It was a great summit and one of the best security event in the world" – Mohd Fazli Aaran – USDCMY*

- *"It worked democratically and made everyone give idea, complaint, planning, critic, and opinion" – Mohd Fazli Aaran – USDCMY*

- *"The small working groups got the conversation flowing between many people of different viewpoints" – Chris Wysopal, Veracode*

- *"It was so cool to get all these security experts under the same roof and you could pickup anybody's brain about any security issue"*

- *"For those who missed the Summit: you missed out, try to make the next one"*

- *"It is a great way to meet and exchange experience with some of the most important IT professionals of the world" – Massimo Biagiotti – Business.E*

- *"The best thing was the exceptional discussions generated from the main topics and continued into the late evenings." – Steve Schwartz, Stack and Liu*

- *“There were great discussions both inside and outside working sessions. I can’t wait to see the results of the seeds planted.” Juan Carlos Calderon, Softtek Mexico.*

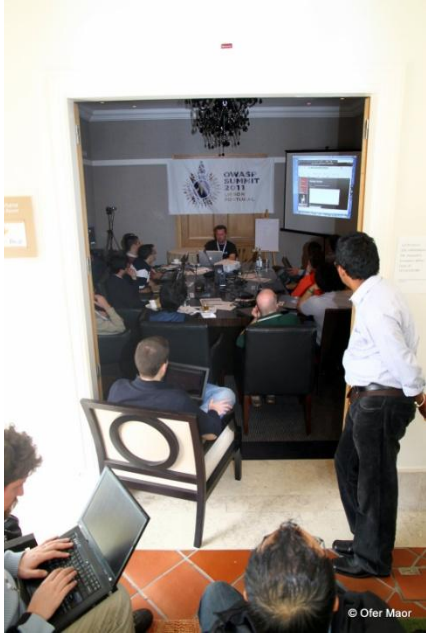
- *“The best was to see how ‘linking’ frameworks for education, government, and third-parties is taking shape and finally seems that it can materialize. It will be a huge enabler for OWASP mission.” Juan Carlos Calderon, Softtek Mexico.*

- *“Best part was being able to gather and talk with the best security minds in the world to solve difficult security problems.” – Abraham Kang*

- *“Attending the Summit was a unique experience because it was not about presentations, but actually having an active contribution to the discussions, knowing that all your contributions are going to make a difference to the future of OWASP.” – Vishal Garg, AppSecureLabs*

- *“The evening sessions are great. Highly productive, relaxed atmosphere, laughing, and beer.” –Bart De Win*

- *“The best experience was seeing so many companies like Microsoft, Google, Mozilla, etc… send large contingents to Portugal to participate in our Summit” – Dave Wichers, Aspect Security*



© Ofer Maor

- *"We arrived, we were impressed, and we were inspired!" – Cecil Su, Grant Thornton*

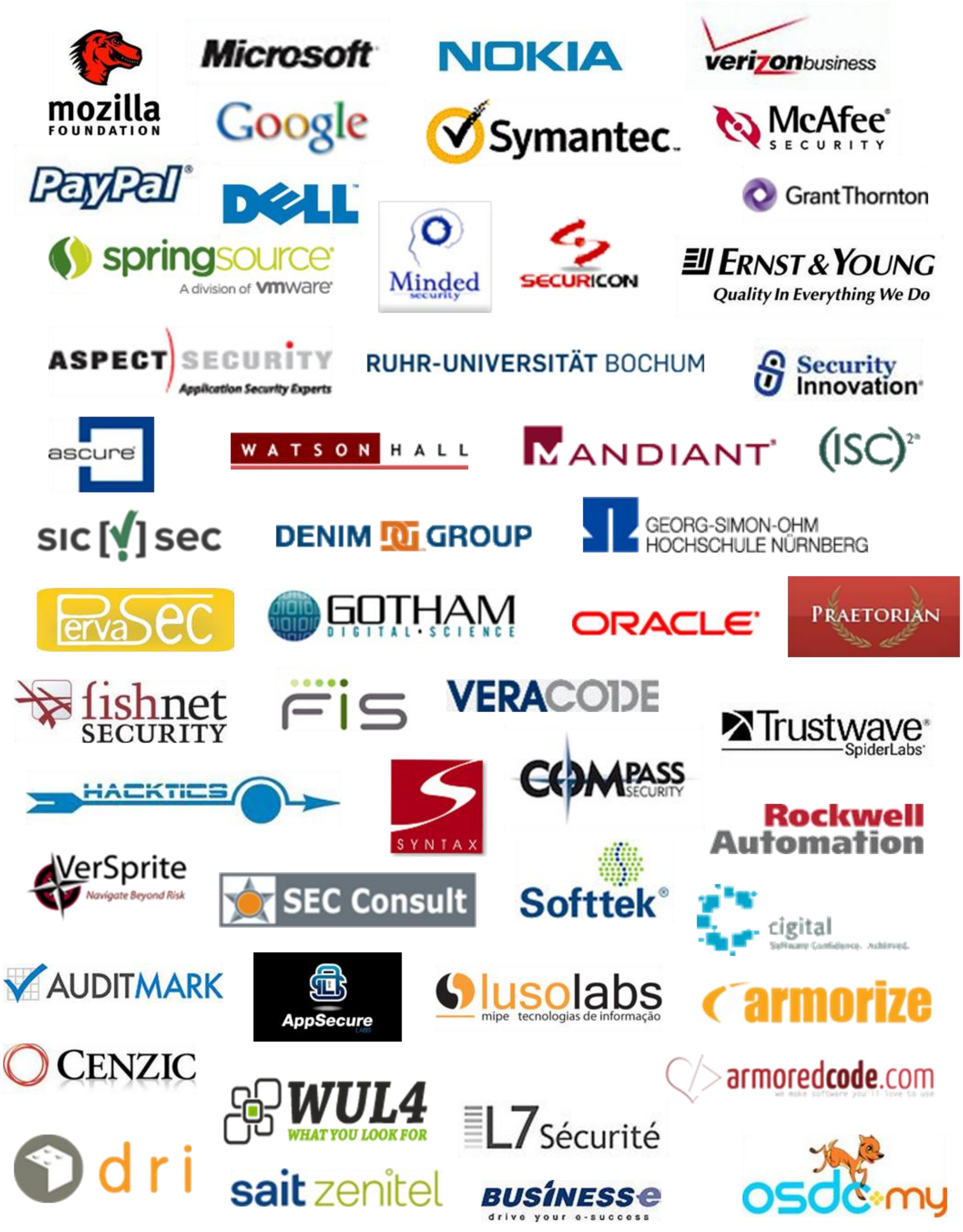
- *"The Summit is a place to work hard, play hard, and get things done." – Abraham Kang*

- *"Bringing together the best security experts and leaders from around the world and discussing solutions for the future of web application security" – Tobias Gondrom, IETF*

- *"Get to know and listen to the best of breed in app security in the world" – L.A. Vilares Da Silva, Open*

© Laurence Casey

COMPANIES PARTICIPATING IN OWASP SUMMIT



WORKING SESSIONS

The Working Sessions are how we actually produce results at the OWASP Summit. Each working session meets in a room where everyone participates to discuss, argue, collaborate, and most importantly produce a deliverable.

FIXED WORKING SESSIONS

Tuesday, February 8

XSS and the Frameworks
XSS - Awareness, Resources, and Partnerships
OWASP Training
OWASP Academies
WAF Mitigations for XSS
Virtual Patching Best Practices
OWASP Exams
University Outreach
Risk Metrics
Metrics and Labeling
Government Outreach
Counting & scoring application security defects
OWASP Secure Coding Practices Project
Enterprise Web Defense Roundtable
Threat Modeling

Wednesday , February 9

Protecting Information Stored Client-Side
Common structure and numbering for all guides
OWASP Common vulnerability list
Providing Access to Persisted Data
OWASP Testing Guide
Site Security Policy
OWASP Industry Outreach
Microsoft's SDL in 16 steps (and lessons learned)
OWASP Projects
DOM Sandboxing
Overhauling the OWASP Website

Thursday, February 10

Contextual Output Encoding
ESAPI-CORE
OWASP Board/Committee Governance
Board Structure
ESAPI for Ruby
Applying ESAPI Input Validation
Professionalize OWASP
OWASP funding and CEO discussion
EcmaScript 5 Security
OWASP Certification
HTML5 Security
What is an OWASP Leader?
Tracking OWASP Participation
Mobile Security
OWASP Licensing

DYNAMIC WORKING SESSIONS

Tuesday, February 8

OWASP vs Government vs Universities
Building the OWASP Brazilian Leaders Group
Common structure and numbering for all guides
OWASP Board/Committee Governance
XSS and the Frameworks
OWASP Academy Portal
Browser Security meet up

Wednesday, February 9

Formal Risk Assessment Methods
OWASP TOP 10 online training in Hacking-Lab
Defining AppSensor Detection Points
OWASP Asia/Pacific working group
Development Guide
Defining a minimal appsec program for universities, governments, and standards bodies
OWASP Portuguese Language Project
ASVS Project
Secure development guidelines for smartphone developers
Privacy - Personal Data/PII, Legislation and OWASP
Mobile Security
Should OWASP work directly with PCI-DSS?
OpenSAMM
Threat Modeling
Governance Part Two

Thursday , February 10

How can OWASP reach/talk/engage with auditors
Hackademic Challenges
OWASP Java Project
OWASP Exams
Industry - Healthcare
Industry - Banking/Finance
Developer Outreach
Scaling Web Application Security Testing
The future of OpenSAMM
Corporations at the Summit & funding opportunities
Conferences - Improving Conference Planner Support
OWASP College Chapter Program
Vulnerability Disclosure Policies
Global Conferences Committee Monthly Meeting
Planning South America/Central America AppSec Chapters
O2 Platform
ESAPI framework integration
Education

ATTENDEES

Adamski, Lucas
Agarwal, Anurag
Aguilera, Vicente
Agustini, Alexandre
Akhmad, Zaki
Alamri, Lorna
AlBasha, Talal
Angal, Rajeev
Aniceto, Alexandre
Aryavalli, Gandhi
Barbato, L. Gustavo C.
Barnett, Ryan
Baso, Sarah
Batista, Marco
Bergling, Mattias
Bernik, Joe
Biagiotti, Massimo
Bonver, Edward
Booth, Rex
Brennan, Tom
Brewer, Deb
Bristow, Mark
Brzozowski, Daniel
Buetler, Ivan
Calderon, Juan Carlos
Campbell, David
Casey, Larry
Causey, Brad
Chalmers, Matthew
Chandra, Pravir
Cheng, Steven
Clarke, Justin
Coates, Michael
Coimbra, Paulo
Cornell, Dan
Corry, Bil
Cruz, Dinis
Cruz, Sarah
Dawson,Isaac
De Win, Bart
Deleersnyder, Seba
DiPaola, Stefano
Donovan, Fred
Durkee, Ralph
Dworakowski, Wojciech
Elias, Wagner
Eng,Chris
Evans, Arian
Falkenberg, Andreas
Fazli Azran, Mohd
Fedon, Giorgio
Ferraz, Felipe
Ferreira, Lucas C.
Fette, Ian
Fitzgerald, Alexis
Fitzhugh, Justin
Flores, Mauro
Fontes, Antonio
Fort, Julio Cesar
Fortuna, Pedro
Frosch,Tilman
Galvao, Pedro
Gao, Helen
Garrancho, Bruno
Garg, Vishal
Gomes, Leandro
Gondrom, Tobias
Hansen, Robert
Hartmann, Kate
Heiderich, Mario
Heyes, Gareth
Hinojosa, Kuai
Hodges, Jeff
Hoff, Jerry
Hoffman, Achim
Hofmann, Chris
Hogben, Giles
Ichnowski, Jeff
Jorge, Eduardo
Jimenez, Juan Jose Rider
Kang, Abraham
Keary, Eoin
Knobloch, Martin
Kosturjak, Vlatko
Koussa, Sherif
Kuivenhoven, Marinus
Kumar, Nishi
Lacerda, Filipe
Lauritão, Rogério
Li, Jason
Lindsay, David
Long, Jeremy
Loureiro, Nuno
Luptak, Pavol
Lyon, Chris
Manico, Jim
Maor, Ofer
Mancini, Lucilla
Martinez, Mateo
Martorella, Christian
Matatall, Neil
Melo, Ricardo
Mendo, Tiago
Meucci, Matteo
Nagra, Jasvir
Neaves, Tom
Paiva, Sandra
Papapanagiotou, Kostas
Pegorelli, Marta
Perego, Paolo
Potjes, Linda
Reinhart, Ralf
Richler, Heiko
Rohr, Mathias
Ross, David
Roth-Mandutz, Elke
Saario, Mikko
Samuel, Michael
Schmidt, Chris
Schuh, Justin
Schwartz, Stephen
Searle, Justin
Secker, Tanya
Serrao, Carlos
Stasinopoulos, Anastasios
Sterne, Brandon
Steven, John
Su, Cecil
Tasar, Vehbi
Taylor, Jason
Tesauro, Matt
Thomas, Mark
Tomhave, Benjamin
Turpin, Keith
Tusha, Ervis
UcedaVelez, Tony
Uhley, Peleus
van der Baan, Steven
Vasilopoulos, Kyprianos
Vela, Eduardo
Vilares Da Silva, Luis
Vlachos, Vasileios
Vroom, Ferdinand
Watson, Colin
Weston, David
Wichers, Dave
Wilander, John
Williams, Jeff
Wilson, Doug
Wuensch, Stefan
Wysopal, Chris
Yeo, John
Zusman, Mike

SECTION I: Working Session Outcomes

Browser Security

Cross-Site Scripting Eradication

Outcome

[XSS Elimination sessions…]

Details

Coordinated efforts to eliminate cross-site scripting, including:

- Updated wiki to improve cross-referencing and have all resources in one place (e.g. a XSS landing page with links to external resources)
- Drafting an open letter and asking about open source resources to help solve this issues
- Mailing list for future communication on this issue

Appendix References

Outcome

Completion of the DOM Based XSS Cheat Sheet

Details

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

Appendix References

Outcome

Virtual Patching Best Practices

Details

- 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 – **Reducing both the time-to-fix interval and attack surface for exploiting a known vulnerability**
- Agreed upon potential drawbacks – **accuracy and coverage is variable depending on the vulnerability type, virtual patching tool deployment mode (3rd party 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 – we will create a table that lists virtual patching effectiveness for various attacks/vulnerabilities (OWASP Top 10, etc….).
- Action item – we will create an Incident Response type of process flow (Preparation, Identification, Analysis, Patch Creation, Testing, Deployment and Follow-Up)

Appendix References

Outcome	WAF Mitigation for XSS

Details

- 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 – to research if it possible to use Anti-Samy type functionality in a WAF

Appendix References

Virtual Patching Best Practices……………………………………………A15

WAF Mitigation for XSS…………………………………………………………A15

Metrics

TRACK:
METRICS

Outcome	[Metrics and Labeling]
Details	
Appendix References	

Outcome	[Counting and Scoring Application Security Defects]
Details	
Appendix References	

Outcome	[]
Details	
Appendix References	

University Outreach, Education, and Training

Outcome	Creation of OWASP Codes of Conduct for Educational Institutions, Government Institutions, and Standards Bodies
Details	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.
Appendix References	Working Session: OWASP vs. Government vs. Universities The OWASP Code of Conduct for Educational Institutions ("OWASP Blue Book") The OWASP Code of Conduct for Government Institutions ("OWASP Green Book") The OWASP Code of Conduct for Standards Bodies ("OWASP Yellow Book")

Outcome	Creation of OWASP Application Security Code of Conduct for Certifying Bodies ("OWASP Red Book")
Details	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.
Appendix References	Working Session: OWASP Certification..A14 The OWASP Application Security Code of Conduct for Certifying Bodies (The OWASP "Red Book")

Outcome	Hackademic Challenges
Details	1. Introduce the Hackademic Challenges as an OWASP project 2. Enhance the administrative frontend/framework and add features to facilitate teacher-student interaction and management 3. Develop additional challenges
Appendix References	

Outcome	Feedback on OWASP Exams...
Details	
Appendix References	

Outcome	OWASP Academies /OWASP Academy Portal
Details	1. Concluded on a specific structure for the portal and process for receiveing and reviewing material for blocks. 2. Decided to put up material for the first blocks asap 3. (After 1 and 2 have been accomplished) Issue a call for additional material/blocks.
Appendix References	

Outcome	OWASP Training
Details	
Appendix References	

Secure Coding Workshop

Outcome	Defining AppSensor Detection Points
Details	1. 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. 2. Identified what additional documentation is needed and desired by potential adopters in order to explain the project and drive adoption. 3. Identified methods of integrating AppSensor into existing framework code in order to drive adoption through a grass roots style approach.
Appendix References	

Outcome	Secure development guidelines for smartphone developers
Details	1) Commitment to smartphone developer guidelines from several attendees 2) Tentative collaboration agreements on several issues (e.g. univeristy curricula) 3) Updated understanding of web security issues.
Appendix References	

Outcome	Contextual Output Encoding
Details	Increase coverage and functionality of existing Output Encoding Codecs New drop in set of codecs for the ESAPI Encoder to use for additional contexts Implementation Guide for Framework Developers to integrate Output Encoding
Appendix References	

Outcome	Providing Access to Persisted Data
Details	Enumerated a variety of scenarios that could be used for creating coding examples Selected scenario for implementation (3 levels of authorization: channel, user, method) Selected scenario for implementation (Fundamentals of Crypto APU Usage)
Appendix References	

Outcome	Protecting Information stored Client side
Details	
Appendix References	

Outcome	
Details	
Appendix References	

Individual OWASP Projects

Summary of OWASP Projects/Process/Committee

Outcome

Creation of the OWASP Common Numbering Project

Details

Project Leader: Dave Wichers (ASVS)

Project Contributors:

Jeff Williams (ASVS)*
Vishal Garg (Development Guide)*
Eoin Keary (Code Review Guide)*
Matteo Meucci (Testing Guide)*
Keith Turpin (Secure Coding Quick Reference Guide)*
Brad Causey (Global Projects Committee)*
Rick Mitchell

Individuals also involved in the Global Summit working sessions from which this outcome arose are designated with an asterix (*)

Project Purpose:

An exciting development, a new numbering scheme that will be common across various OWASP Guides and References is being developed. This numbering scheme is loosely based on the OWASP ASVS section and detailed requirements numbering. The OWASP ASVS, Guide, and Reference project leads and contributors plan to work together to develop a numbering scheme that facilitates easier mapping between various OWASP Guides and References, and that would allow for a period of transition as the Guides and References are updated to reflect the new numbering scheme. This project will provide a centralized clearinghouse for mapping information. For more information on this project, or if you wish to contribute, please contact [mailto:dave.wichers@owasp.org Dave Wichers].

This common numbering scheme will be of requirements. A mapping of vulnerabilities to this requirements list will most likely be developed after the common requirements list is created. This common numbering scheme is intended to be independent of any particular OWASP project and is not intended to dictate how those projects are developed and organized. Its intent is to be a resource to facilitate cross referencing between related topics and to encourage, but not require, projects like the OWASP Guides to adopt a similar structure. But that decision is up to the respective project leads.

Appendix References

Common Structure and Numbering for All Guides
OWASP Common Vulnerability List
“Common Vulnerability List” ppt presentation created by Matteo Meucci

Outcome	OWASP Testing Guide
Details	
Appendix References	

Outcome

OWASP Development Guide

Details

- Collaborate with other guide leaders and come up with common numbering scheme and Restructure the guide to adhere to this numbering scheme to enable cross-referencing with other guides. The plans to release first draft of the numbering scheme is before the end of February 2011.

- Reveiew 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.

Appendix References

Outcome	Application Security Verification Standard (ASVS)
Details	
Appendix References	

Outcome	OWASP Secure Coding Practices Project
Details	
Appendix References	

Outcome	Mobile Security Project
Details	1. A list of 37 mobile risk items gathered from participants during the working session; these 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. 2. Relationships were established 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) 3. Sometimes-heated discussion leading to a general consensus on the mission, target audience, and key deliverables of the Mobile Security project. 4. Additional wiki content was created.
Appendix References	

Outcome	Threat Modeling
Details	1. A unanimous vote to having an OWASP threat modeling project. 2. Promotion of such a project to not only security consultants but also having contributors from an end user organization to provide their feedback on challenges and such. 3. OWASP to promote the methodology to establish it as a standard in the industry. 4. An insight into how people have been doing threat modeling individually. There is no set standard used by people but everyone has their own. 5. Discussion on having an OWASP threat modeling project and let OWASP drive build and drive a standard which can be adopted by the industry. Discussion on various components of threat modeling and how they fit into the process.
Appendix References	

Outcome	OWASP Java Project
Details	
Appendix References	

Outcome	BSIMM activities mapped to SAMM
Details	
Appendix References	

Outcome	
Details	
Appendix References	

Outcome

OWASP Portuguese Language Project

Details

1. We have defined priorities for the project (translation and revision)

2. Coordination strategy has been defined and will be detailed and posted on the wiki

3. We have a process to be used for translations defined

4. We need to build common language rules to be used by all translator, regardless of their home country

Appendix References

Outcome	
Details	
Appendix References	

Outcomes from “Birds of a Feather” Sessions

Outcome	Privacy - Personal Data/PII, Legislation, and OWASP
Details	1) A recognition that OWASP MUST (not should) be active in this space 2) Direct input into OWASP's response to the FTC staff report on consumer privacy 3) A consensus to try to document the drivers, issues, resources and relevant technical approaches
Appendix References	

Outcome	How can OWASP reach/talk/engage with auditors?
Details	
Appendix References	

Outcome	Should OWASP work directly with PCI-DSS?
Details	
Appendix References	

Outcome	
Details	
Appendix References	

Outcome	
Details	
Appendix References	

Outcome

Details

Appendix
References

Outcome	
Details	
Appendix References	

OWASP Governance and Global Committees

Outcome

Global Projects Committee solicited feedback on two GPC initiatives: OWASP Projects Hosting and OWASP Projects Lifecycle

Details

- 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 is an effort to help clarify the maturity of an OWASP Project in order to better serve users and help facilitate allocation of our resources to properly support our projects.
- These outcomes are encapsulated in a draft project hosting Request for Proposals and draft lifecycle diagrams.
- As a direct result of the Summit, the GPC also welcomed 2 new members: Chris Schmidt and Justin Searle.

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.

Appendix References

Project Hosting RFP
Project lifecycle diagrams

Outcome	Global Industry Committee
Details	
Appendix References	

Outcome	Global Education Committee
Details	
Appendix References	

Outcome	Global Chapters Committee
Details	
Appendix References	

Outcome	Global Conferences Committee
Details	
Appendix References	

Outcome	Global Membership Committee
Details	
Appendix References	

Outcome	OWASP Board/Committee Governance
Details	
Appendix References	

Outcome	Tracking OWASP participation
Details	
Appendix References	

Outcome	OWASP Funding (and CEO discussion)
Details	
Appendix References	

Outcome	Licensing
Details	**Licensing requirements for OWASP Documentation:** **List existing licenses used by OWASP Projects:** **Problem corporations face with adopting and utilizing OWASP materials and code:** **Recommendations for changes in the OWASP License** **OWASP: Licensing FAQ**
Appendix References	

Outcome	
Details	
Appendix References	

SECTION II: Summit Operations

Summit Budget

Roles and Responsibilities

Summit Timeline

The Working Session Model

APPENDIX

Working Sessions & Documentation:

Cross-Site Scripting Eradication

WORKING SESSION: XSS – Awareness, Resources, and Partnerships

Short Working Session Description:

Let’s make 2011 the OWASP year of XSS…eradication. As part of that effort, we need to get the word out as we never have before. To achieve this we are going to have to spread the word and knowledge through more than just OWASP – who can we partner with (commercial and non-commercial)? What freely available resources can we reference? How can we reach developers and get them what they need in order to be more effective with regards to XSS?

Related Project(s):

- XSS and the Frameworks

Chair(s): Justin Clarke

Objectives:

1. Work on what partners we can reach, and what resources they can provide us access to
2. Work on who we can work with to reach a maximum amount of developers writing web applications
3. Plan engagement with identified organizations
4. Plan a call to action for OWASP chapters for identified XSS resources

Outcomes/Deliverables proposed by working group:

- A concrete, specific business plan for investing OWASP funds in a campaign designated to ensure that every developer knows about XSS and what to do to prevent it. The plan should have specific goals, measures, and targets over time so we know if it is on track.

WORKING SESSION: XSS and the Frameworks

Short Working Session Description:

Can we work with the common web frameworks to prevent XSS at the framework level? If the framework that a developer uses handles the most common-occurring cases of XSS, the overall prevalence of XSS will be reduced significantly.

Related Project(s):

- OWASP Enterprise Security API (ESAPI)

Chair(s): Justin Clarke

Objectives:

5. Work on how OWASP can engage the major web frameworks to move toward a "secure by default" stance.
6. Work on OWASP resources to provide patches/design approaches in conjunction with the frameworks

Outcomes/Deliverables proposed by working group:

- OWASP statement or press release to publically ask the frameworks to build security in
- Engagement plan on how we'd work with (if at all) a framework to get ESAPI or similar functionally integrated
- White paper or standard for what we want the web frameworks to provide in terms of XSS defenses. Turning the XSS Prevention Cheat Sheet into a standard/metric for frameworks would be great.
- OWASP Standard defining an appraisal methodology for a framework's XSS prevention capability based on the other deliverable.

OWASP XSS

Just some notes – not a verbatim statement of what was said by whom, just an interpretation, and not necessarily documented or interpreted correctly!

(Beginning missed)

Address correctness issue... no real incentive to work around this system. People can wrap functions.

Lack of escaping in all places... requires education, tools (later discussion)... but escaping shoiuld not be the special case. It should be the default to get rid of XSS.

Jim Manico: Want to talk about XSS edge cases.... data in the middle of an HTML document, could place it as an attribute, a URL parameter,CSS parameter, sometimes multiple encodings. Is escaping the only answer? No, we need to consider CSP as well. Looking where escapingcan be turned off usually identifies where the problems are. We need to make it difficult to turn off escaping. Eg untrusted data, via CSS escaping, can still be vulnerable – use of expressions. IE6-8 and FF <4 had this functional aspect. Output encoding is not the full solution. Need a combination of contextual output encoding, and default to an HTML encoding. Edge cases are difficult. ESAPI doesn't always get it right. Certain places in an HTML body, it is not possible to put incorrectly coded data – is this achievable more widely? This may hurt, and break some functions.

Hex encoded JS variables can add to the problem. Need to look at flow of data throughout the DOM. Certain functions may 'pop' XSS.

Brandon Stern (Mozilla): CSP has been my main project over the last two years or so. Encouraging we are all tackling this problem at all different layers, which work together. CSP is not a silver bullet, but contributes to protection. Previewed at Irvine conference, and also spoke at AppSec DC. It is a policy driven mechanism shipping in FF4, but specifies what types of content and from where should be allowed. Policy specified as a custom HTTP header (but may also need META or LINK tag support), E.g. Sites A & B can serve JS, sites C&D can serve CSS and images, and everything else is not allowed. The browser enforces this whitelist. Important part that inline scripts, etc are turned off by default – a dramatic departure from the web model. Only valid scripts which can be executed are those which are inseparate files, andfrom a whitelisted host. But although this is the default, sites can change this to allow these types of inline scripting, to encourage update. Have some fairly large sites in the process of rolling it out (e.g. mobile.twitter.com) and other have already done so. While it can be a significant amount of work, it is a robust control against content injection. But coolest piece is reporting – you can specify a URL in the policy to which a report is sent every time the policy is violated – a “canary in a coalmine”. Site may be misconfigured, or something odd is going on. Real time notification as the violations occur.. adding values to other users, not just the CSP enabled browser users (FF4 now), because you can investigate and mitigate problems straight away. Mozilla contributing to Web Application Security Group at W3C and want CSP to become a standard feature.

Jim M – Is CSP the solution, or should it be applied in conjunction with other measures?

Brandon S – the latter, they work together.

Chris Eng (Veracode) – We come from a different angle – detection via static/dynamic analysis – at scale using a cloud service. But there is a disconnect within the security community, within OWASP, within software developers as to whether developers should have to think about security at all. But should developers have accountability... so it is good to have these different layers of protection, but accidents and mistakes still happen. Want to get people to look at the whole application inventory, and get developers to write secure code. About "secure coding"... is this a real term... even in the security community. We need to tackle this at all levels, and from all angles. But Veracode is launching a free service for developers to upload their binaries and have XSS flaws detected for free. Has to be a Java application, is not unlimited, and is not unlimited. This is to lower the barrier, and is easy to use. Hopefully this will take some XSS out of the system. Can you help publicize? Veracode.com/freeservice

Mike: Developer education is a great thing, but they should not have to be experts in all the aspects of XSS, or even every aspect of the language they are coding in.

Jim: Change turn off secure defaults should be "unsafe" or "hack me now". Emerging technoligies – we still have work to do?

Mike: It is possible to write XSSible templates even if you use all the protections.

Jim: Is it possible to write XSS templates?

Mike: Yes – Jeff's approach could do this, even with malicious template creators.

Jim: How about DOM, where data flows through various paths and files....

Mike: Watch my talk from OWASP Sweden on virtualizing the DOM. If you want to have code that uses published APIs, but want to limit what it can do. You can virtualize this, eg the DOM of JS API, and modify how it works. Mark Miller has been working with ECMAScript to get proxies into Harmony, to help make this code efficiently.

Justin C: We can talk for whole day, but how about the audience... we want to have the opportunity for everyone to contribute.

Jaz (Google) – work with Mike. I cannot add much to what has been said, but CSS and SQLinjection really are the same problem. String manipulation, and at some point the strings become code. Need to look at all the places where strings are manipulated and strings are used as code. We know where the problems are. Can we produce a list of all these places where (according to spec) strings become code, and browser manufacturers add functions for these, but we need a public list.... and then we can attenuate that list to make XSS go away.

Brandon S: Yes, absolutely agree. CSP turns off many of these string conversion functions by default. The policy switch used to be “allow inline scripts” but is now “disable XSS protection”.

Justin C: Does Google have any plans to release any of this research etc?

Jaz: One project (DOM HTML sandboxing – Caja project) is open source, so is available now. Our marketing on this isn't too great!

Justin C: This is what I like about OWASP.... there is a lot of commonality about the problems, does anyone else want to make a point.

Mike: Closure templates language will be open sourced... used in Google Docs.

[Audience]: If you want OWASP to be the single point for XSS eradication... we need a strategy and way to align OWASP's resources with this.

Justin C: Yes, what can we do now... we won't be able to come up anything like a strategy in this session, but we have other session opportunities to develop this further. Other organisations also have resources and plans... who do we reach out to, if we want to make a serious dent, and what would we say. The browserv security track has brought in some extra people to this session. Speaking to the vendors, I have been asking what can they contribute? We need to make the connections... eg I had never heard of JXLT until last night.

[Audience – Anurag]: My viewpoint. Based on training of developers, is that developer training alone won't work. Some companies enforce it, some developers want to learn it. Developers need help from the technologies, vendors, browsers, OWASP, etc. It is inconvenient for developers and takes a long time for developers to get into OWASP resources. The OWASP guide projects are working on aligning all of these, to make it as convenient and easily navigable. On frameworks, MS has .NET library, why doesn't Java have anything? Time to market pressures on developers mean they don't have time to hunt for solutions... training helps, but a lot of help is needed beyond training,

Chris: Well for Java, how about ESAPI? Why sisn't it working. We [Veracode] see ESAPI in about 1in20 applications.

Jim M: Static analysis is not perfect. Checks can be disabled in ESAPI. Training gives significant reduction in XSS, but not 99% or more. We need simple solutions for developers. Caja looks good, but it is complicated.

Justin C: We have lots of stuff to come out of this session, where can we start as OWASP? Eg templating languages – can we improve deployment/outreach to developers and other frameworks? How about XSS output encoding? Where should we put our effort? Do we need to support all the different approaches? We have more sessions about browser security... can we sum up what you each think OWASP should start on?

Mike: I am not going to answer your question... but what occurs to me, I have done this on one templating language, and would like to do it in another – does anyone have any metrics on templating language so I can prioritise.

Justin C: All of them?

Mike: Yes, but have to serialize.

Jeff: Education is not enough.... all the different contexts, so need tools as well. My project makes it very difficult not to escape.. since you end up with an invalid template. There are limitations, but are to make it secure as possible. Easier with a new project. Different techniques will have different benefits and pitfalls. On the OWASP side – just listing the technologies, the barriers of entry, pros and cons would really help.

Mike: With a million line codebase, applying output encoding manually may take until HTML6 is released.

Jaz: We have a choice between a rock and a hard place. Legacy applications have to be maintained and grow. Can push the copmplexity out to other tools, but have to deal with it. A hard place is... we can't solve all the problems with a templating systems, and look at transitioning developers to choose what is sufficiently flexible, to let them decide the benefit/disbenefit payoff.

Mike: Need to be ready for problems... eg a tool to help with an attack... this can lead to gradually infect a code base with security.

Jaz: The problem of education... not my background.... personally I believe in education with a stick.. a tool that yells at you every time you use escaping wrongly.

Jim M: JS is difficult – harder than people things. Eg JS function override. Legacy apps are rewritten as technology progresses, so they are not a real problem. Moving forward, privileged to sit with these panels, together we have the ability to solve the problem. We need: auto-escaping templates, server side policy, sandboxing, content security policy in the browser.

Brandon S: Jim's vision is great... no one silver bullet/choke point to get rid of the threat of XSS. My perspective is different.... mine is now browser security. The browser is a leverage point. We have half a dozen major browser vendors, but hundreds of thousands of developers. If we can add value by not forcing the majority of the burden on developers... eg sandboxing. W3C is an open group you can all contribute to. Try CSP and see what works, and what doesn't.

Chris E: I have been accused of being a pessimist... we haven't eradicated SQLinjection and that should be easier to prevent than XSS. So keep that in mind. I support everything discussed, but it it will be hard. On developer education, the technologies are evolving and merging, and it is so easy to shoot yourself in the foot. Who has presented appsec at a major security conference [quite a large number in the audience] and, then at a majkor developer conference [hardly anyone]. We need to be speaking at developer conferences – the unreached at the moment.

Anurag: No one size fits all... we need to work together. Education in combination with everything else. All the OWASP projects... do we have pilot customers? Can we reach out via pilots to let OWASP learn to make it better, and feed this back into other projects too. Eg ESAPI exists, but it seems we don't have many users. Can we get feedback and use that to improve our projects? Eg can ESAPI have pluggable modules, rather than a massive code change for existing applications?

Justin C: I would like to propose.... update the wiki to improve cross-referencing and have all resources in one place... eg a XSS landing page with links to external resources as well. I will put out an open letter asking about open source resources to help solve this issue. Step 1 is to have somewhere which defines what we have now. May also end up with a mailing list. Encourage everyone to join in. At some point I will reach out to the leaders list. Look to dynamic sessions, tonight or tomorrow. I would like to thank the panel, who did not offer to be on the panel in advance. Thank you [applause]... and now coffee.

WORKING SESSION: DOM Based XSS Prevention Cheat Sheet

Short Working Session Description:

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. The Global Summit will allow those drafting this cheat sheet to meet and bounce ideas of key individuals in the web security world.

Related Project(s):

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
- **DOM based XSS Prevention Cheat Sheet**

Chair(s): Abraham Kang, Jim Manico

Objectives:

7. Discuss and get feedback on DOM Based XSS Prevention from individuals in the web security world
8. Create a working draft and wiki page for the DOM Based XSS Prevention Cheat Sheet

Outcomes/Deliverables proposed by working group:

- Completion of the DOM Based XSS Prevention Cheat Sheet

- Set up a working group mailing list to work on resolving DOM based XSS: https://lists.owasp.org/mailman/listinfo/owasp-dom-xss

DOM based XSS Prevention Cheat Sheet

From OWASP

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(untrustedData))%
>”);
document.writeln(“<%=Encoder.encodeForJS(Encoder.encodeForHTML(untrustedData)
)%>”);
```

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 &amp; 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 an 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\u0049\u007
4;

           //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 possibily 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 (eg. `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 a 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 Mitgating 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>
```

Insonsistencies 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 vulnerabilies 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 retrived 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 Stevens

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
- **DOM based XSS Prevention Cheat Sheet**

WORKING SESSION: Virtual Patching Best Practices

Short Working Session Description:

The purpose of this session is to develop a framework methodology for organizations to use to help them to decided if/when/how to utilize virtual patching for identified web application vulnerabilities.

Related Project(s):

- OWASP Best Practices: Use of Web Application Firewalls
- Securing WebGoat with ModSecurity

Chair(s): Ryan Barnett

Objectives:

1. Identify which attacks/vulnerabilities are best suited for virtual patching
2. Identify which tools are best suited for virtual patching (appliance vs. embedded, WAFs vs IPS, etc...)
3. Identify who should be responsible for virtual patching
4. How to develop/test virtual patches

Outcomes/Deliverables proposed by working group:

- White paper on “Effective Virtual Patching” the discusses the scenarios above

WORKING SESSION: WAF Mitigations for XSS

Short Working Session Description:

To discuss if/when/how web application firewalls can help to prevent XSS attacks

Related Project(s):

- Blog post by Ryan Barnett on defending against XSS (http://blog.modsecurity.org/2010/09/advanced-topic-of-the-week-identifying-improper-output-handling-xss-flaws.html)
- Blog post by Ryan Barnett on using content injection to combat XSS (http://blog.modsecurity.org/2010/09/advanced-topic-of-the-week-xss-defense-via-content-injection.html)
- ModSecurity Demo (http://www.modsecurity.org/demo/demo-deny-noescape.html)

Chair(s): Ryan Barnett

Objectives:

1. Improve XSS Attack Payload Detection Techniques
2. Identifying Improper Output Handling Flaws in Web Apps
3. Feasibility of Profile Page Scripts/Iframes
4. Testing Injection of JS Sandbox Code in Responses

Outcomes/Deliverables proposed by working group:

- White paper describing “Next Generation WAF Capabilities” such as the ones described above. Include areas requiring additional research and funding.

OWASP Summit – Virtual Patching & WAF Mitigations for XSS

Just some notes – not a verbatim statement of what was said by whom, just an interpretation, and not necessarily documented or interpreted correctly!

Ryan B: We are talking about virtual patching as a process, not particular vendors of WAFs. Can we start at the top... can we have an official definition? Many customers are unclear... eg the word “patch” has certain connotations and this may not help.

Ryan: “A security filter designed to prevent the exploitation of a known vulnerability”? We can start with this and work from there.

[Audience: Mike]: Physical analogy: fixing a chink in your armour.

Ryan: We need to think from the customer's viewpoint. What is the benefit? I usually say minismising the time to fix. Sometimes you can't mitigate 100%, so maybe “reduce the impact”

Dan Cornell: Raises the bar so that we know what we have to address.

Ryan: We can make a page on the wiki, about this area, like the proposed one for XSS.

Ryan: If you go virtual patching, is this out of line or inline (transparent proxy or bridge). This choice impacts other functionality. The type of tool has an impact on what you can do. Could have an external device, or something closer to the app (e.g. ModSecurity), even closer (ESAPI WAF). So we need to document how we want to do this, and affects what categories we want to address. Say injection flaws might be applicable equally, but authorization may require you to be inside the code. A virtual patch inside the code is not necessary altering the code, but some sort of layer within it.

[Audience Juan Carlos Calderon]: A WAF in the code blurs the definition. Why not just fix the code?

Ryan: yes, we want to document the process, and keep the benefits in mind. Why don't people fix the code? Maybe a farmed out application, third party code elsewhere that impact your site, etc.

??: Should also document the downsides, weaknesses

[Audience]: Getting back to the session objectives... First is Improve XSS scripting attack payload techniques. Categorize the different attack techniques, filtering methods, WAF bypass techniques.

Ryan: I'd like to talk about virtual patching in general first, and then perhaps we can talk about XSS as a specific case. Also need to talk about who is responsible... often network security people. See German's chapter on best practices operating WAFs which has good information on the individual roles. For example need to take into account evasion practices, and this needs to include developers. The network people don't know the context, so the document mention the need for an “application manager” (someone with a development background who understands the application) to be involved. It is not as simple as banning a single tick – impedance mismatch between firewalls, proxies, web server, application server, database, browser etc is an example of how difficult this can be.

???: May be difficult, but not insurmountable. Can OWASP list an enumerate the considerations and contexts.

Ryan:

Dan: Would be both helpful and unhelpful. How do you relate an attack to the different detection techniques. Eg Snort vs ModSecurity vs ESAPI WAF. At these different levels of expressiveness in each language affect these. How does an attack appear, and how is this expressed in each. But a blacklist is never totally inclusive.

Ryan: Some action items... which categories of vulnerabilities are possibly suited for virtual patching, eg which Top Ten risks can be mitigated. Can we look at WebGoat... there was an attempt to mitigate the vulnerabilities using ModSecurity. The project was trying to attempt to mitigate 80% issues, and it would be good to go through these with all the techniques.

Dan: Interesting idea to categorize... maybe also can it be fixed in an automated or manual way. Some things can't be fixed. Some things are perhaps less cost-effective to do in a WAF... and it might still be better to fix in the code (if we can). At what point does this occur? WebGoat is a built up example, but interesting to understand where virtual patching is valuable.

Ryan: The German chapter's document (best practices for WAFs) has some interesting which compares the Top Ten 2007 with WAF virtual patching. It tried to estimate the workload of using a WAF or other techniques (e.g. XSS filters, input encoding code changes).

[Audience]: Haven't heard about enumerating vulnerabilities, but also what can't be stopped by each option.

Ryan: Yes, “deployment” is an aspect I think we need to include in our information... and highlight issues which may occur. On responsibilities, we can build on what's said in the German chapter's document.

[Audience]: Other objectives for this session are to Identify which tools are most suitable for virtual patching, identify who should be responsible, how to develop & test virtual patches.

Ryan: Some customers may ask can't Snort be used for virtual patching... Other tools may be right for the job... but the rules may not be accurate enough. Writing rules is tricky.

Dan: Blocking vs detecting is important issue. Most organizations do not want to undertake any blocking.... maybe we can define where it is appropriate to block.

Colin: Some things should be blocked eg not within the application's entry point.

Ryan: Do as much testing as you can, but production is the real battlefield. Yes detection only, non-blocking first. Later we can switch over to some form of blocking. The patch needs to be done quickly, so we need to allow for more rapid deployment. With ModSecurity, we are looking at anomaly scoring, where multiple factors can contribute to the final decision, and if it is blocking that is a dramatic decision.

Dan: Using virtual patch alerts as an input to knowledge, such as AppSensor which can make a broader decision.

Ryan: Form a process perspective, if an organisation already ahs an incident response framework, virtual patching should be part of tit and treated in the same way. It is not a real patch and therefore doesn'r necessarily go through all the same deployment practices, but from a tracking perspective it needs to be part of change control.

Dan: If we look at vulnerabilities, some may have virtual patches applied, but can we collect metrics on which have been attempted? The organisation needs a tight enough feedback loop to help make decisions.

Ryan: Now to move on to the specific of virtual patching for XSS. How can this help you? We know it's not the fix

[Audience - Jim M]: I used to be an anti WAFer, but am much more open to the help it can give.

Ryan. Let's talk virtual patching not WAF specifically – it could be some other tool. I looked at input validation first...

Jim M: WAF can help with input validation (depending upon the parameter type – numeric input).

[Audience]: Can't help more generally, eg persistent XSS.

Ryan: From experience, a lot of filtering improvements more recently, but now have a public demonstration page for ModSecurity. Has been interesting … traffic …evasions. The filters are good, but it is a blacklist approach, but have looked at PHP-IDS and exporting this to Lua for ModSecurity. It is a constant rat race to updates.

???: Yes filters can be evaded. The bad guys will win on this front. Is it possible for the WAF vendors to push a whitelisting approach?

Ryan: From learning systems perspective, very straightforward for numerical inputs, but for free text form fields or which allow HTML, the learning systems are not so good. There are some benefits, but the text fields are where the problems are.

???: Could OWASP push good architectures, to reduce the problems to begin with.

Ryan: We need to start with a negative security model, but yes these can be evaded. But if you are monitoring, maybe you can take some other actions.

???: Does the demo page allow attackers to fine tune their attacks.

Ryan: There is always around blacklisting... but need a better approach. How else can a WAF help. For SQLinjection, all you have is input. With XSS you also have outbound – we have two chances at it. Dynamic Taint Propagation (Fortify) is an interesting idea... in XSS (some reflected or stored)... if you can track this by flagging the data and see if it is reflected in the page. Sometimes it seems to work okay. But some apps change the data (eg encoding).

[Audience]: Similar to IE8 XSS filtering – maybe some lessons there.

Ryan: Yes looked at that, and wanted to move away from just blocking the inbound attack.

Juan Carlos: Another issue is where the data comes from some other channel, so you don't have anything to compare inbound and outbound. How can you tackle this outbound only?

Ryan: Yes, another example is malware on websites... where the source may be SSH, FTP, a widget, but you only see it on the way out. We have some rules in ModSecurity looking at this. Another pproach is ModSecurity using Lua, profiling the outbound page and monitoring it. Eg number of scripts and iframes. If a fullk payload is injected, might be able to detect that. But have to synchronise this type of monitoring with change control processes. But interesting, because you don't care about the inbound at all.

[Audience - ???]: Your honeypot project. Did you have any lessons learned about meta characaters. Eg did we ever see particular sequences of characters that were never good.

Ryan: It is an approach to look at....

Ryan: Would like to bring up... another approach since the browser is where the attack occurs, can we take the battle to the browser.

Jim: Not browser only. We need multiple tiers across the ecosystem.

Ryan: In ModSecurity we have the ability to append code to the respond. Could ModSecurity's content injection force sandboxing on the browser.. led to Eduardo's policy. ModSecurity appends this code.

Eduardo: This uses an HTML tag at the start. Originally idea was similar to CSP, but this idea enforced in the JS page. It disables HTML parsing in the document, and parses it itself within a snadbox. Uses browser parser to serialize the content, and problems were found with this. New version of ACS using Caja's HTML santisers. It also CSP rules. There are extensions.. you can input hashes of content.

Ryan: So those are the main ideas. Coming up to the end of the msession, but I'd love to talk with everyone who has more ideas about how we can use virtual patching against XSS.

Jim M: Could you wire in anti-samy for the HTML input, leaving just other strings to deal with?

Working Sessions & Documentation:

Metrics

WORKING SESSION: Risk Metrics

Short Working Session Description:

We all know that you can’t control what you can’t measure and that you need to measure the right things or you won’t be steering towards the right outcome. For this session we will define the right outcome as “low risk to an organization from vulnerabilities in applications.” This session will discuss assigning business risk to applications and it would also be great if this could be translated into monetary risk to determine if an organizations investment in applications is not too much or too little. This is a big unsolved problem so come prepared with ideas and be willing to take part in a discussion.

Chair(s): Chris Wysopal

Objectives:

1. Quantify business criticality of a deployed application
2. Translate technical risks into business risks (speak the language of management)
3. Translate technical risk into approximate financial risk

Outcomes/Deliverables proposed by working group:

- Paper describing definitions and formula for determining business criticality
- Paper translating technical language and risks into business language and monetary risk

WORKING SESSION: Metrics and Labeling

Short Working Session Description:

Consumers and organizations enlist the services of web-based services with no ability to make an informed decision on its security. This can include enterprise class websites such as payment processing, HR portals, benefits administration, and other corporate services, as well as consumer centric websites such as tax preparation, personal finance, social media, or medical records. While the companies providing these services are unlikely to share detailed information about known vulnerabilities in their systems, it would be beneficial to have a standardized mechanism for describing the security controls and processes in place. In other words, what are they doing right that should give consumers some level of confidence that the provider exercises application security best practices?

Chair(s): **Chris Eng**

Objectives:

1. Discuss positive security properties that should be tracked
2. Discuss options for consumer-friendly labeling
3. Discuss ways to encourage participation in risk labeling

Outcomes/Deliverables proposed by working group:

- White paper sketching out a standard for a software security label and a plan to finalize the standard

Metrics and Measurements Notes

2:34

How do we label these things on the software. for a level of criticality, does it meet the requirements
2:34

Chris W: Example - Federal US govt (NIST) specifying e-authentication systems - 4 different levels from password to mulitfactor
2:35

Chris W: US Govt went through the portfolio of systems and matched up to the appropriate authentication system
2:36

Chris W: Here's one example of multiple levels of risk - looking for feedback and what you've done
2:36

Chris W: Four different levels - 1 through 4 (little confidence through very high confidence)
2:38

Chris W: criteria - brand damage, liability or loss, harm to interests, sensitive information, personal safety, civil or criminal violations
2:38

Chris W: 6 areas of impact - low, moderate and high impact based on those criteria
2:39

Chris W: came up with a table - plug in answers and then come out with an assurance level 1 through 4
2:40

Chris W: this is a structure that we could use for app security - go through the criteria you define for the application
2:41

Chris W: what are some of the methods you've used?
2:41

Audience: interview senior business - then business impact assessments
2:42

Audience: business impact of an application. KFA (key financial applications) - idenfying. Financial/monetary impact.
2:42

Audience: do BIA exist in the business? (first question) Identify impact/existing measures
2:43

Chris W: Do BIA exist across businesses - for software labelling we need something we can use across businesses
2:44

Audience: rating (l/m/h) plus financial measure
2:45

Audience: example - issue with external ecommerce system? How do you measure financial impact?
2:45

Chris W: Loss if that system is compromised?
2:45

Chris W: Ponemon (?) model looked to quantify cost of a breach
2:46

Audience: SLE - single loss expectancy
2:47

Chris W: There are a lot of non-financial risks - in govt most of these aren't financial. Different from corporate world
2:48

Audience: We use BIA with SPRINT methodology. Have some standard methods for a BIA measure. Business games the system to get the BIA measure they're looking for
2:49

Chris W: Need for oversight in that case?
2:49

Audience: problem as business is ultimately signing off the risk
2:50

Chris E: reason we started with business risk - looking at putting risk labels on software. We need to say that software is safe for "what".
2:50

Chris E: example - RegOnline being used for OWASP site. There is no label saying what RegOnline has done with regards to security
2:51

Chris E: external statement needed for security on all software. Processes undergone, verification that has happened. To help quantify risk
2:52

Tobias G: is BIA gaming - distinction between outright gaming of BIA's and just signing off the risks
2:53

Tobias G: assets - may be valuable but not critical on all CIA aspects. Tailor security answer based on what aspects you are looking to protect
2:54

Audience: products are different to products - don't generally change. Software patches change the software
2:55

Chris W: big problem. SaaS and cloud change very frequently
Chris E: design properties not as likely to change
2:55

Chris E: different levels for each positive property. Tie rating to a specific release
2:56

Chris W: Past track record does give you some assurance.
2:57

Audience: similar to ASVS?
2:58

Audience: specific set of measures based on different levels
2:58

Chris W: different levels, different processes should happen
3:00

Audience: you can lie on the labelling?
Chris W: independent testing is one approach. Or a regulator that can punish those lying on labels
3:03

Arian E: on subject of measuring. Talked to hundreds of orgs - no consistent way of measuring risk. Even within orgs different way. Looked at development standards/principles - some exist, as move away from dev orgs less likely. DRC (disaster recovery) as a measure of criticality.
3:03

Arian E: criticality mapped to other measures
3:05

Arian E: want period of risk exposure etc
3:05

Arian E: wire into criticality - simple scoring system
3:06

Arian E: changes less than other measures
3:07

Chris W: example historical restaurant reviews vs continuous reviews (like Yelp etc)
3:07

Arian E: hopefully less subjective
3:08

Chris W: What are assurance guarantees?
3:09

Chris W: At Veracode we broke into 5 levels - level 1 no requirements. Move up when you achieve the level of assurance set
3:10

Chris W: Example - if certain criteria met - put certain level on a label
3:11

Audience: have you guys found consistent processes at customers for that?
3:12

Chris W: we need an all or nothing process. Nothing for low criticality, and do for high criticality
3:13

Chris W (correction): We see all or nothing approaches
3:15

Tobias G: what do we want to protect, and who are we doing it for?
3:16

Tobias G: might have different levels based on audience - consumer vs IT
3:16

Chris E: business chooses how to act on the label
3:16

Chris E: environmental stuff doesn't need to be reflected. Label should reflect objective information about the code
3:17

Chris W: example - banks think differently about internal v Internet apps. Test external apps, but don't fix XSS if internally
3:18

Chris E: OWASP an org that can help define the labels, not enforce
3:19

Chris E: govts could choose to enforce. OWASP could do something accurate, usable
3:20

Chris W: example (Software Facts Label) - could show results of testing, ala crash testing of cars
3:21

Chris W: vendors ship with known security defects. Maybe when safety - we need to disclose those elements
3:22

Audience: agility of software a problem.
3:22

Audience: values at a point in time.
Chris W: some value as old version still used
3:23

Audience: how long windows of vuln also give you that
Chris E: could include that on label as well
3:23

Chris E: how long to fix for this software
3:23

Audience: hard to construct and measure that detail. Data is there
Chris W: small sliver of real data though
3:25

Chris W: security features, mechanisms on labels - how to standardize?

3:25

Audience: subjective - performing processes, but what quality/depth?
3:26

Chris W: labelling on a scale - among a peer group on an ordinal scale
3:27

Chris W: relative scale may work for certain things
3:37

Next session - Counting and scoring application security defects

WORKING SESSION: Counting and Scoring Application Security Defects

Short Working Session Description:

One of the biggest challenges of running an application security program is assembling the vulnerability findings from disparate tools, services, and consultants in a meaningful fashion. There are numerous standards for classifying vulnerabilities but little agreement on severity, exploitability, and/or business impact. One consultant may subjectively rate a vulnerability as critical while another will call it moderate. Some tools will attempt to gauge exploitability levels (which can be a black art in and of itself), others won't. Tools use everything from CWE to the OWASP Top Ten to the WASC TC to CAPEC. Security consultants often disregard vulnerability classification taxonomies in favor of their own "proprietary" systems. Sophisticated organizations may create their own internal system for normalizing output, but others can't afford to undertake such an effort. Until tool vendors and service providers can standardize on one methodology -- or maybe a couple -- for counting and scoring application defects, they are doing their customers a disservice.

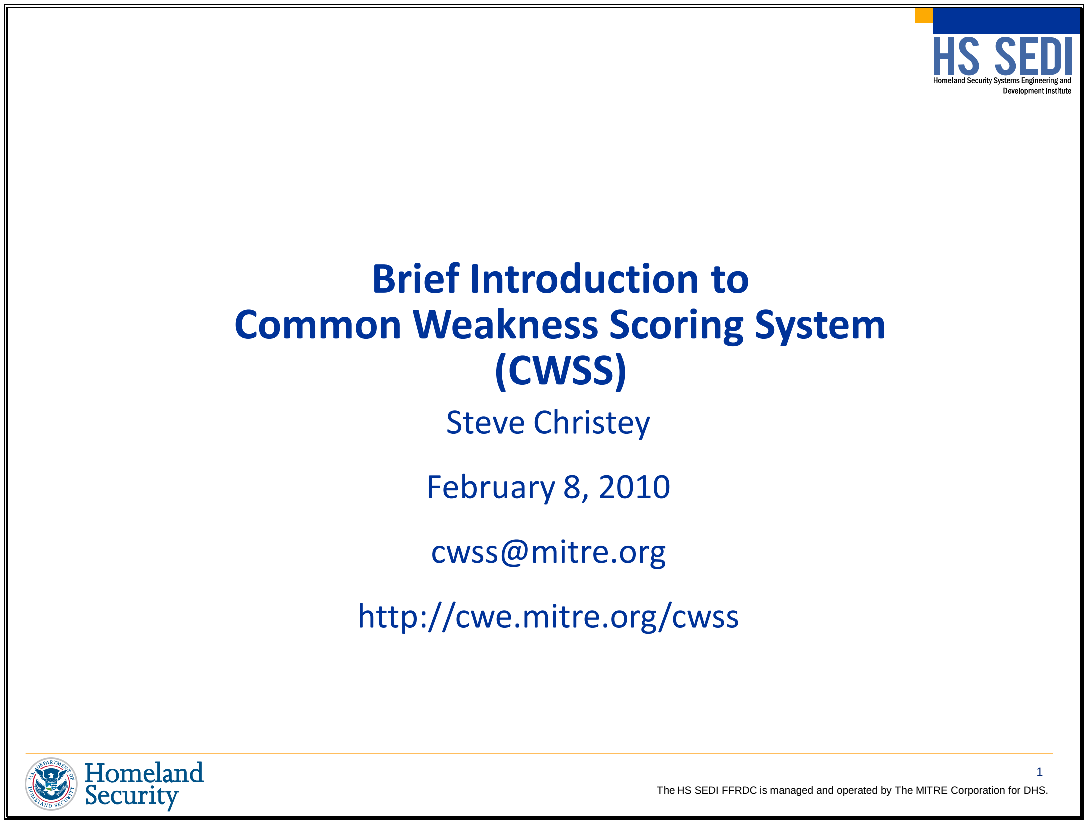
Chair(s): **Chris Eng, Chris Wysopal**

Objectives:

1. Discuss existing methods for counting and scoring defects, by vendors and practitioners willing to share their methodologies.
2. Discuss advantages and disadvantages of a standardized approach.
3. Discuss the CWSS 0.1 draft and how it might be incorporated into a standard.

Outcomes/Deliverables proposed by working group:

- White paper sketching out a standard for rating risks that accommodates individual minor defects all the way through architectural flaws (that may represent many individual defects)



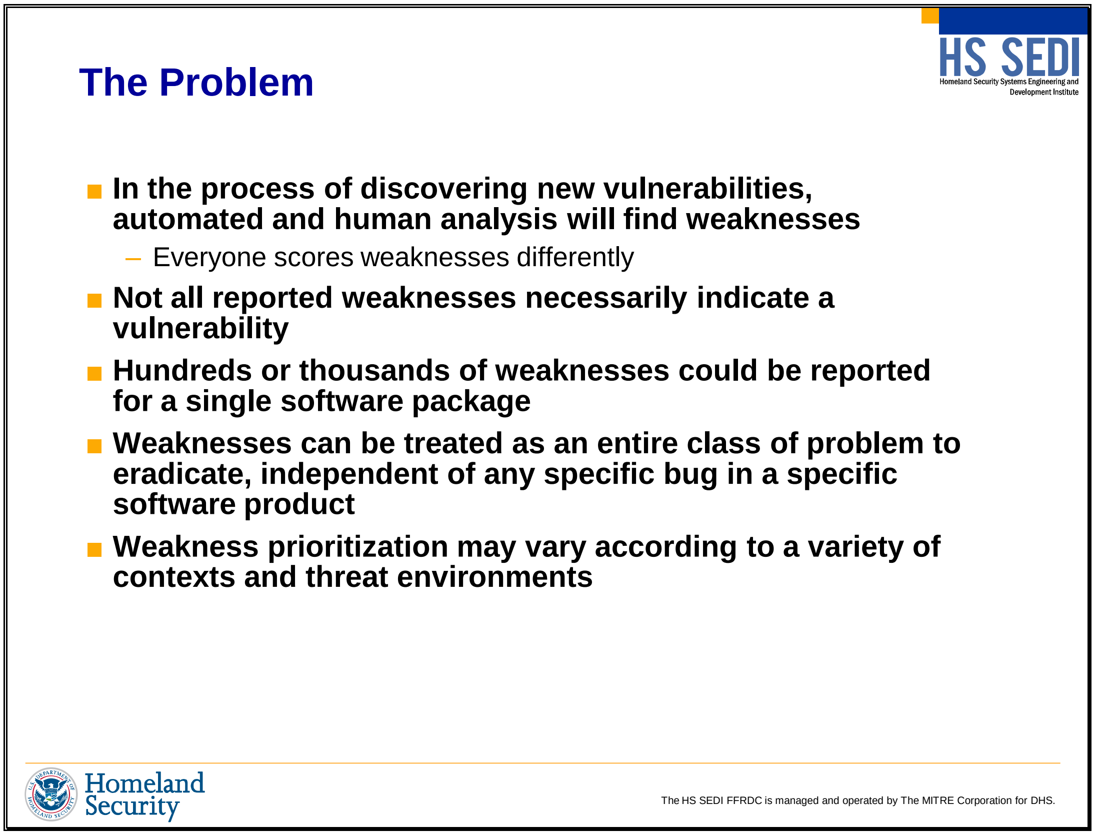
Brief Introduction to Common Weakness Scoring System (CWSS)

Steve Christey

February 8, 2010

cwss@mitre.org

http://cwe.mitre.org/cwss



The Problem

- **In the process of discovering new vulnerabilities, automated and human analysis will find weaknesses**
  - Everyone scores weaknesses differently
- **Not all reported weaknesses necessarily indicate a vulnerability**
- **Hundreds or thousands of weaknesses could be reported for a single software package**
- **Weaknesses can be treated as an entire class of problem to eradicate, independent of any specific bug in a specific software product**
- **Weakness prioritization may vary according to a variety of contexts and threat environments**

Beginnings

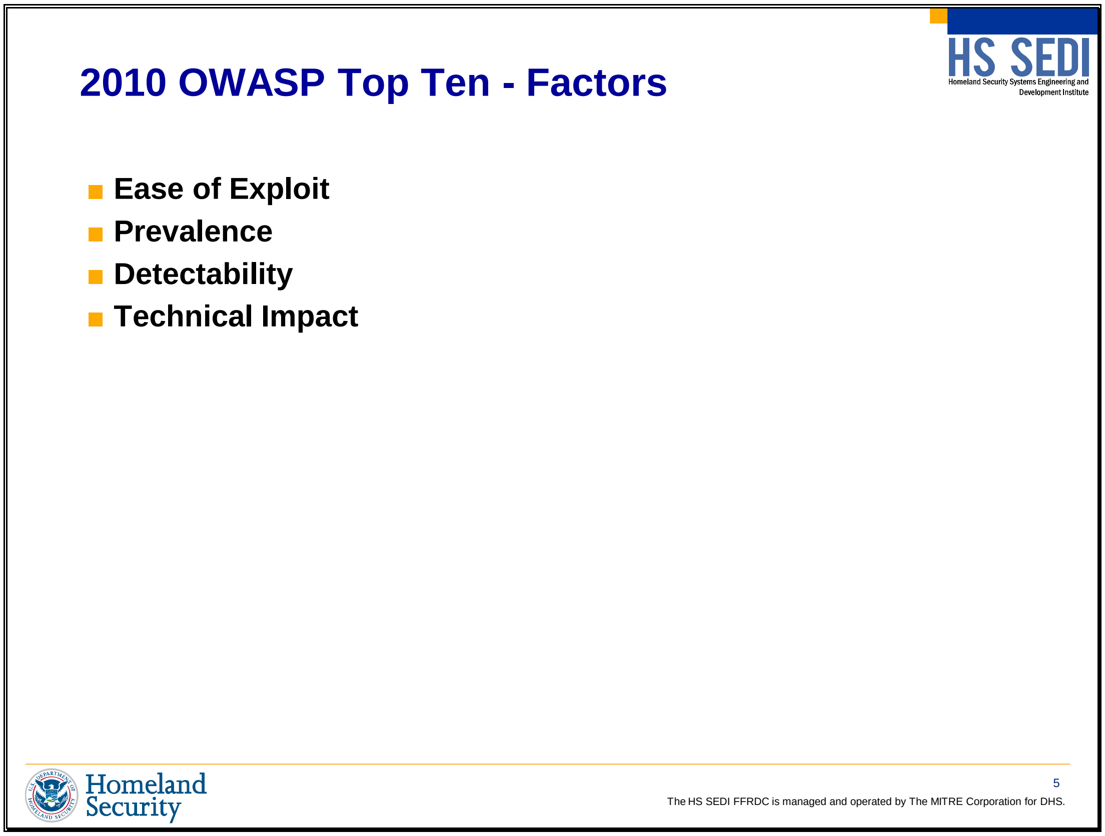
- CWSS Kickoff Meeting – Oct 24, 2008
- Briefing to SwA Working Groups – July 2010
- Start with CVSS
  - Try to address some of CVSS' limitations
  - Examine other metrics
- Environment / Context is critical
  - Business/mission priorities, how SW is deployed, …
- Ideally supports tools and humans
- Must be usable even when there is limited information

- Public white paper, December 2010
- 2nd version of white paper – February 2010 (soon)

2010 SANS/CWE Top 25

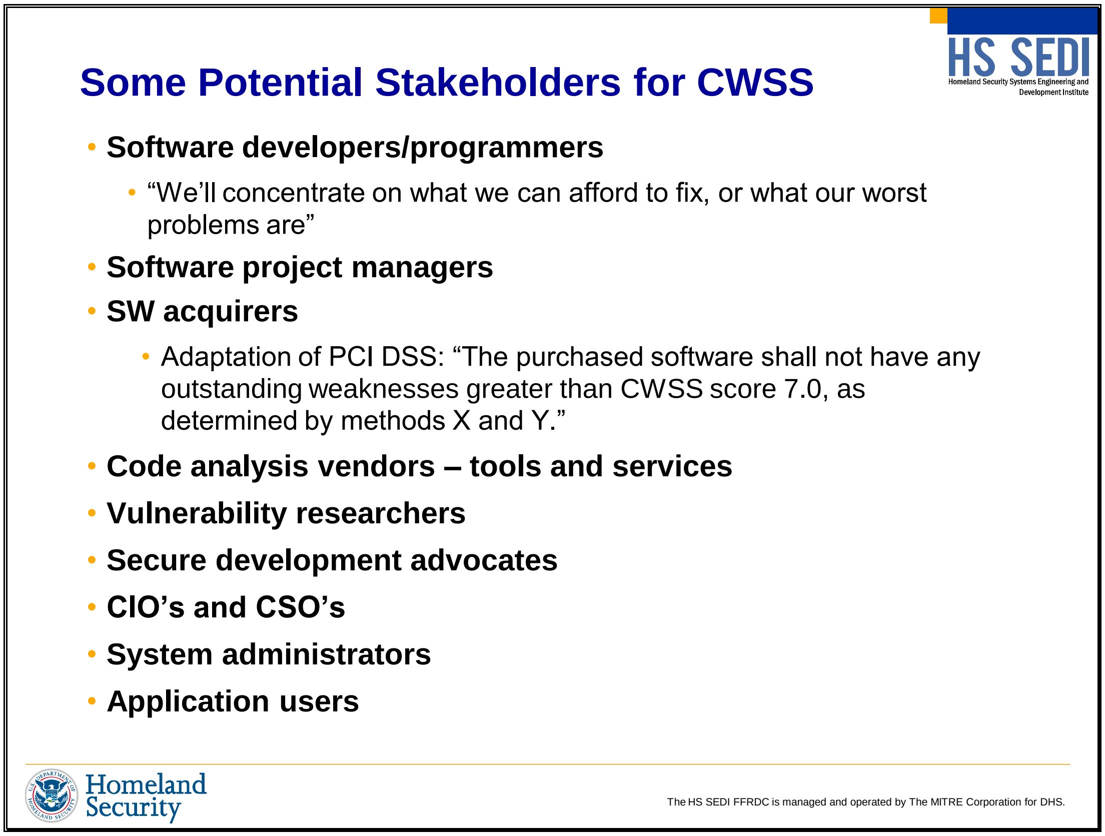
- Real-world, raw data is still very difficult to find
- Prioritized items based on "Prevalence" and "Importance" (4 values each)
- 25 participating organizations evaluated 41 nominee CWE entries
  - Developers, researchers, educators
- Focus profiles allowed alternate ranking
  - E.g. educational emphasis, importance to software consumers

http://cwe.mitre.org/top25/#AppendixC



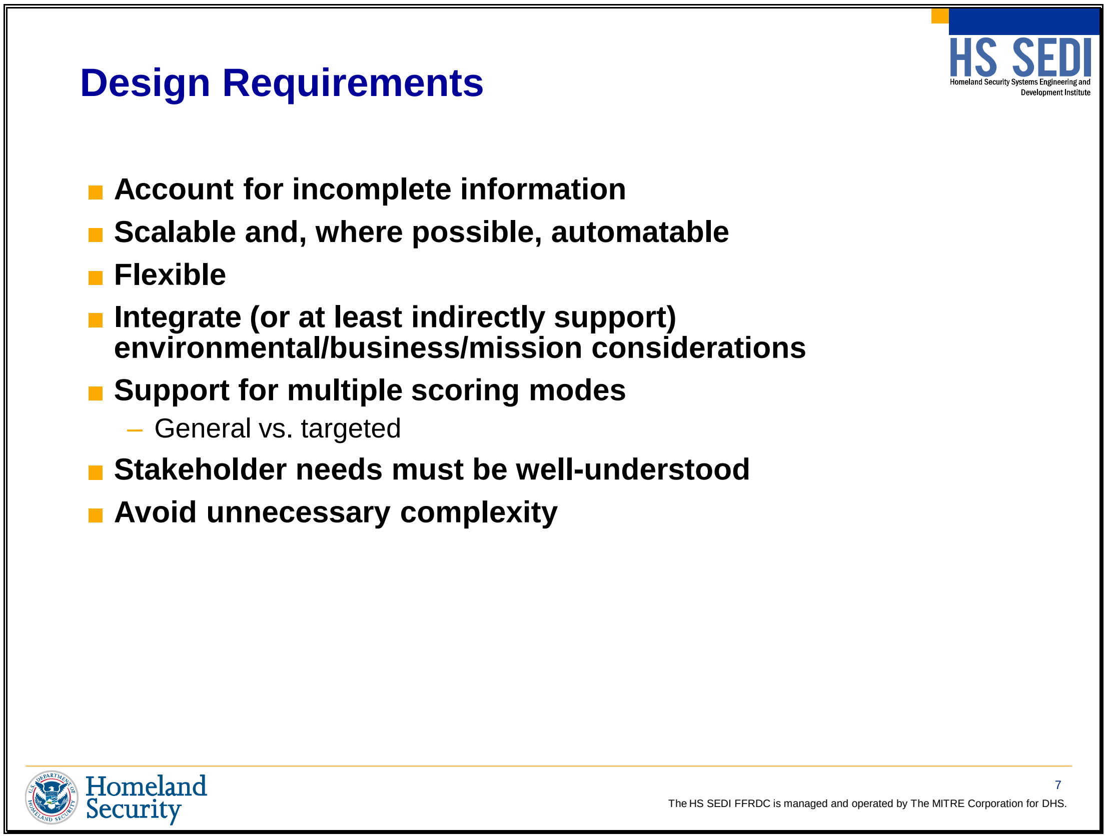
2010 OWASP Top Ten - Factors

- Ease of Exploit
- Prevalence
- Detectability
- Technical Impact



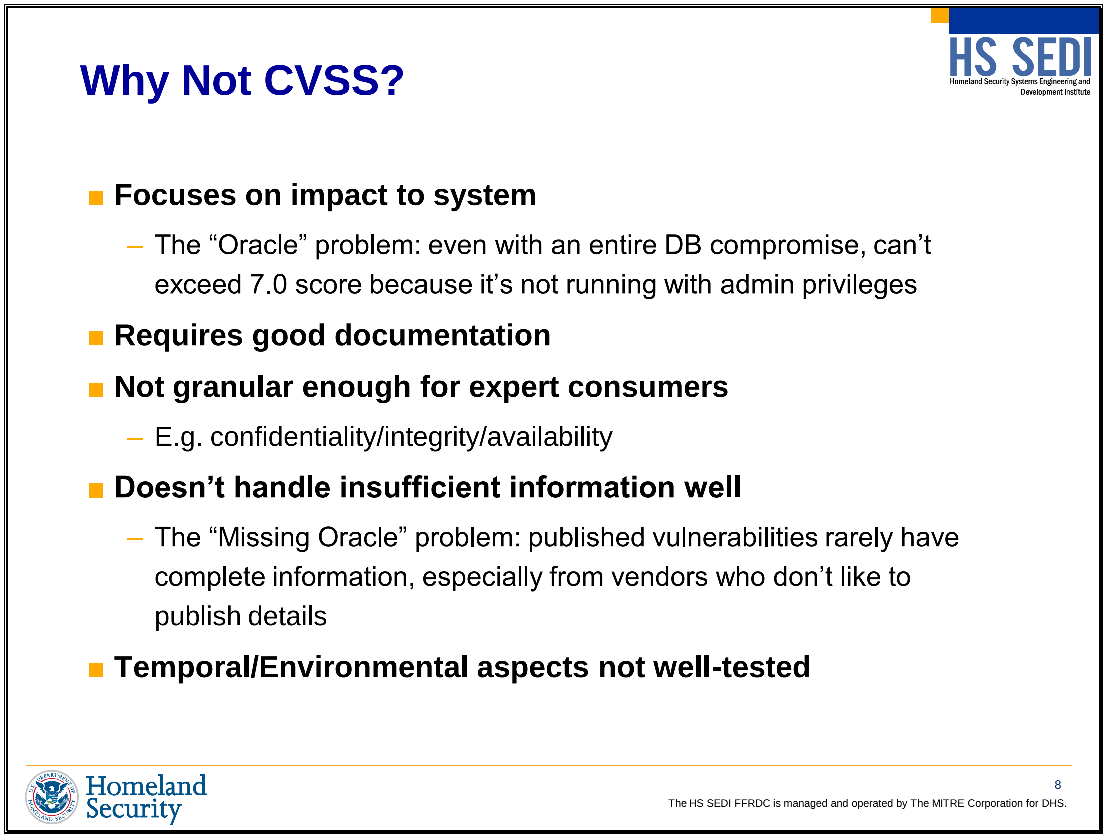
Some Potential Stakeholders for CWSS

- **Software developers/programmers**
  - "We'll concentrate on what we can afford to fix, or what our worst problems are"
- **Software project managers**
- **SW acquirers**
  - Adaptation of PCI DSS: "The purchased software shall not have any outstanding weaknesses greater than CWSS score 7.0, as determined by methods X and Y."
- **Code analysis vendors – tools and services**
- **Vulnerability researchers**
- **Secure development advocates**
- **CIO's and CSO's**
- **System administrators**
- **Application users**



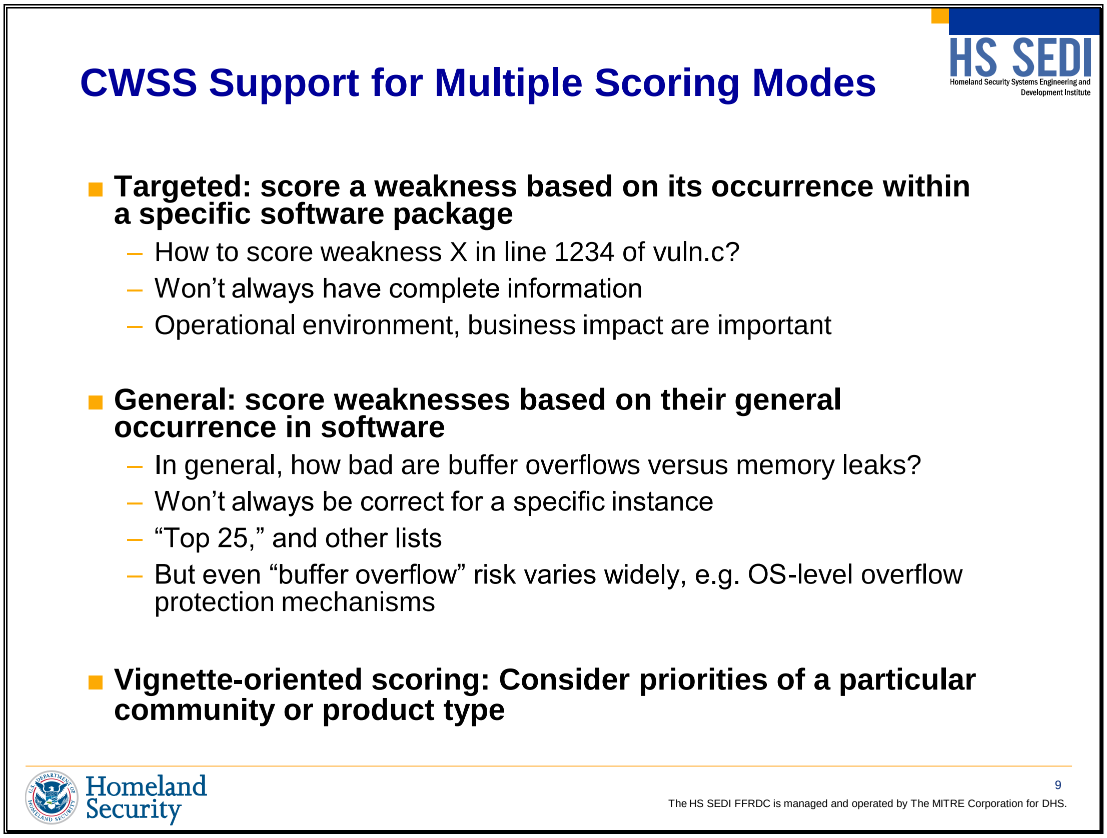
Design Requirements

- Account for incomplete information
- Scalable and, where possible, automatable
- Flexible
- Integrate (or at least indirectly support) environmental/business/mission considerations
- Support for multiple scoring modes
  - General vs. targeted
- Stakeholder needs must be well-understood
- Avoid unnecessary complexity



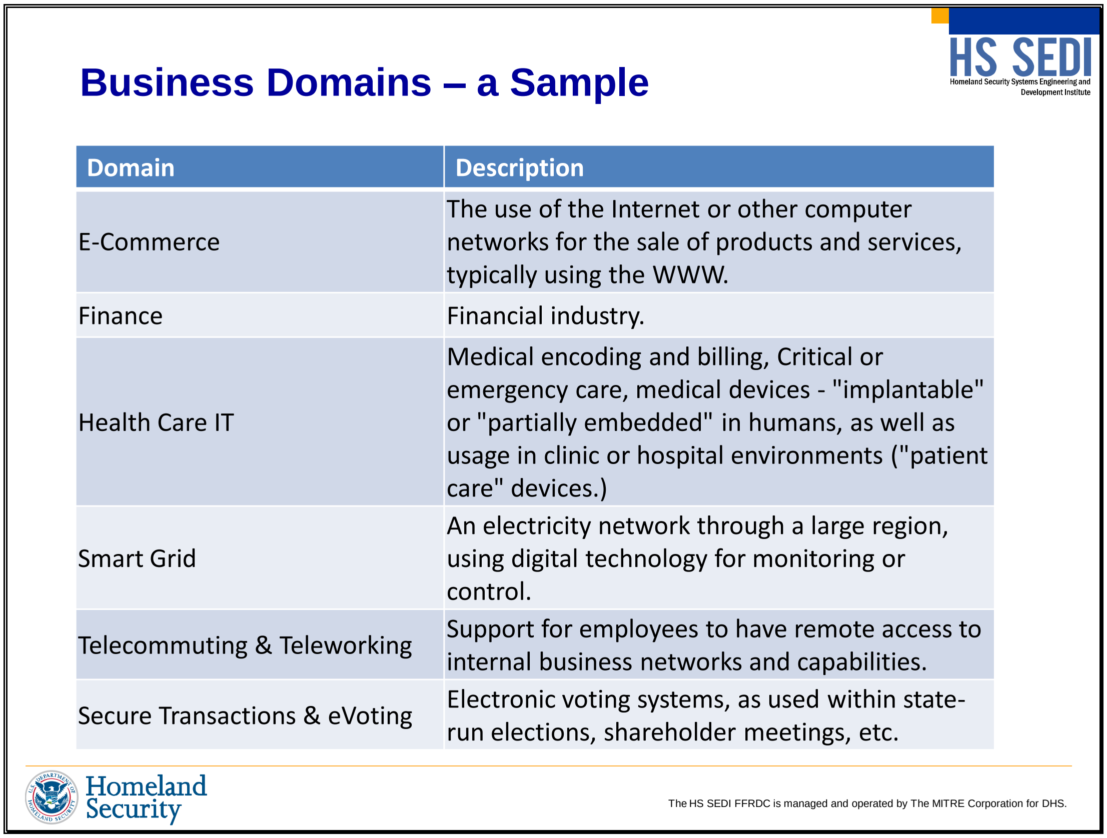
Why Not CVSS?

- Focuses on impact to system
  - The “Oracle” problem: even with an entire DB compromise, can’t exceed 7.0 score because it’s not running with admin privileges
- Requires good documentation
- Not granular enough for expert consumers
  - E.g. confidentiality/integrity/availability
- Doesn’t handle insufficient information well
  - The “Missing Oracle” problem: published vulnerabilities rarely have complete information, especially from vendors who don’t like to publish details
- Temporal/Environmental aspects not well-tested



CWSS Support for Multiple Scoring Modes

- **Targeted: score a weakness based on its occurrence within a specific software package**
  - How to score weakness X in line 1234 of vuln.c?
  - Won’t always have complete information
  - Operational environment, business impact are important
- **General: score weaknesses based on their general occurrence in software**
  - In general, how bad are buffer overflows versus memory leaks?
  - Won’t always be correct for a specific instance
  - “Top 25,” and other lists
  - But even “buffer overflow” risk varies widely, e.g. OS-level overflow protection mechanisms
- **Vignette-oriented scoring: Consider priorities of a particular community or product type**



Business Domains – a Sample

Domain	Description
E-Commerce	The use of the Internet or other computer networks for the sale of products and services, typically using the WWW.
Finance	Financial industry.
Health Care IT	Medical encoding and billing, Critical or emergency care, medical devices - "implantable" or "partially embedded" in humans, as well as usage in clinic or hospital environments ("patient care" devices.)
Smart Grid	An electricity network through a large region, using digital technology for monitoring or control.
Telecommuting & Teleworking	Support for employees to have remote access to internal business networks and capabilities.
Secure Transactions & eVoting	Electronic voting systems, as used within state-run elections, shareholder meetings, etc.

Archetypes

- Often used in different domains
- Linked together to address a particular area of functionality
  - Database
  - General-purpose operating system
  - Web browser
  - Programmable Logic Controller
  - Smartphone

Vignettes

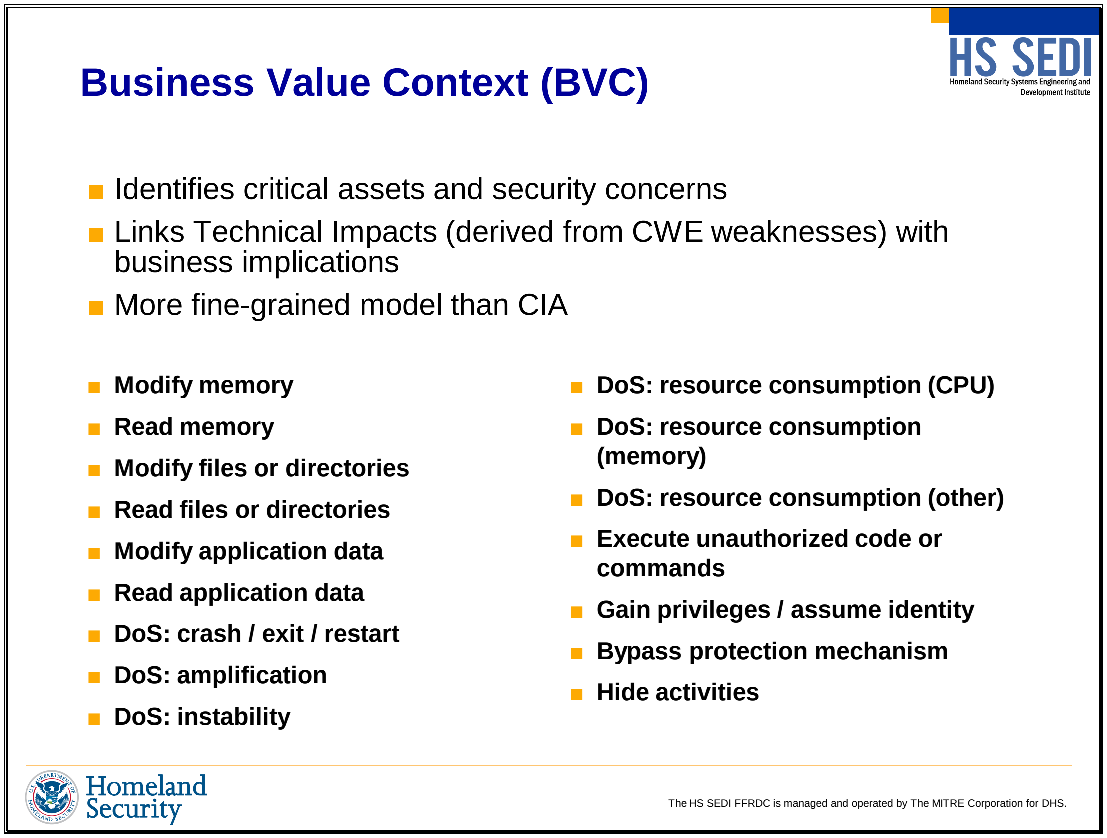
- **Define a particular environment and its priorities**
- **Essential Resources / Capabilities**
- **Confidentiality/Integrity/Availability importance**
  - Read application data, execute code, crash…
- **Link these technical impacts to business impacts**
- **Use technical impacts from CWE entries as the basis for more specific scoring**
- **Initial focus on CWE/SANS Top 25**

Vignette: Web-based Retail Provider

- **Business Domain: E-Commerce**
- **Internet-facing, E-commerce provider of retail goods or services**
- **Data-centric - PII, credit card numbers, order history**
- **Archetypes: Database, Web client/server, General-purpose OS**
- **Business Value Context:**
  - Confidentiality essential from a financial PII perspective
  - Identity PII usually less important.
  - PCI compliance a factor.
  - Security incidents might have organizational impacts including financial loss, legal liability, compliance/regulatory concerns, and reputation/brand damage.

Vignette: Smart Meters (Smart Grid)

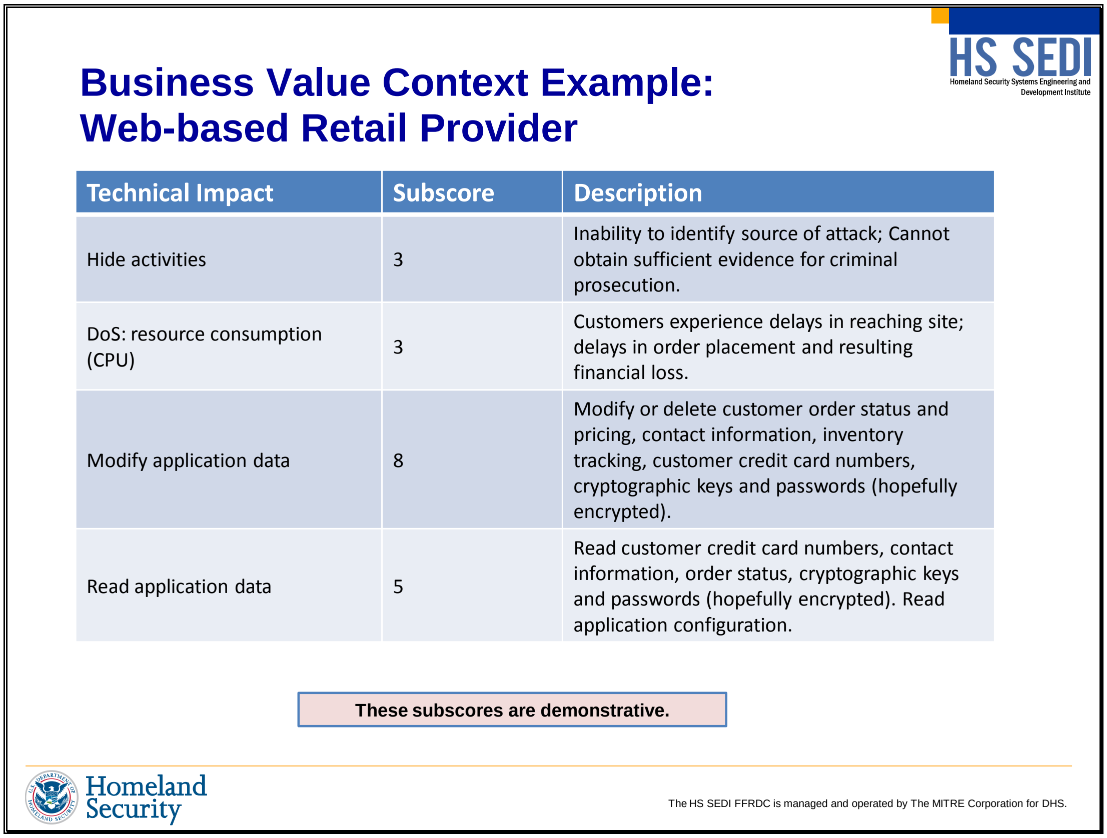
- **Business Domain: Smart Grid**
- **Meter that records electrical consumption and communicates this information to the supplier on a regular basis.**
- **Archetypes: Web Applications, Real-Time Embedded System, Process Control System, End-point Computing Device**
- **Business Value Context (BVC):**
  - Confidentiality of customer energy usage statistics is important - could be used for marketing or illegal purposes. For example, hourly usage statistics could be useful for monitoring activities.
  - Integrity of metering data is important because of the financial impact on stakeholders (consumers manipulating energy costs).
  - Availability typically is not needed for real-time; other avenues exist (e.g. site visit) if communications are disrupted.



Business Value Context (BVC)

- Identifies critical assets and security concerns
- Links Technical Impacts (derived from CWE weaknesses) with business implications
- More fine-grained model than CIA

- **Modify memory**
- **Read memory**
- **Modify files or directories**
- **Read files or directories**
- **Modify application data**
- **Read application data**
- **DoS: crash / exit / restart**
- **DoS: amplification**
- **DoS: instability**
- **DoS: resource consumption (CPU)**
- **DoS: resource consumption (memory)**
- **DoS: resource consumption (other)**
- **Execute unauthorized code or commands**
- **Gain privileges / assume identity**
- **Bypass protection mechanism**
- **Hide activities**



Business Value Context Example: Web-based Retail Provider

Technical Impact	Subscore	Description
Hide activities	3	Inability to identify source of attack; Cannot obtain sufficient evidence for criminal prosecution.
DoS: resource consumption (CPU)	3	Customers experience delays in reaching site; delays in order placement and resulting financial loss.
Modify application data	8	Modify or delete customer order status and pricing, contact information, inventory tracking, customer credit card numbers, cryptographic keys and passwords (hopefully encrypted).
Read application data	5	Read customer credit card numbers, contact information, order status, cryptographic keys and passwords (hopefully encrypted). Read application configuration.

These subscores are demonstrative.

CWSS 0.2 Scoring

Impact * Prevalence * Attackability * Confidence * RemediationCost

- **Prevalence is 1.0 in “targeted” scoring for weaknesses found in a specific application**
- **Attackability**
  - Attack Surface
  - Exploitability
- **Individual factors not yet defined**
  - Possibly informed by Business Value Context
  - Customers don’t really care about remediation cost
- **Scores for weaknesses may vary across vignettes or business domains**
  - But why would you compare the “weakness surface” of a SCADA system with that of a mobile phone app?

CWSS 0.2 Factors

- **“Unknown”/“Not Applicable” values supported everywhere**
- **Impact (I)**
- **Finding Confidence (FC)**
  - Proven True, Proven Locally True, Proven False
- **Remediation Cost (RC)**
  - Systemic, Localized, Minimal
- **Universality (UN)**
  - All, Moderate, Rare, Potentially Reachable
- **Access Vector (AV)**
  - Remote, Local, Network-adjacent, Physical
- **Required Privilege Level (RP)**
  - None, Guest, User, Partially Privileged User, Administrator

CWSS 0.2 Factors - Continued

- **Authentication Strength (AS)**
  - High, Medium, Low, None
- **Authentication Instances (AI)**
  - None, One, Multiple
- **Likelihood of Discovery (DI)**
  - High, Medium, Low
- **Likelihood of Exploit (EX)**
  - High, Medium, Low
- **Level of Interaction (IN)**
  - Automated, Limited, Moderate, Opportunistic, High
- **Internal Control Effectiveness (IC)**
  - None, Limited, Moderate, Complete
- **External Control Effectiveness (EC)**
  - None, Limited, Moderate, Complete

Aggregated Scoring

- **For a software package, how to combine all reported weaknesses to get an overall score?**
  - Individual score of the worst weakness
  - Combined score of all weaknesses
  - Account for size of code?
- **How to account for non-zero false positive / false negative rates?**
- **“Weakness Surface”**
- **One step closer to the Software Facts Label**

Technical Impacts for Individual CWE Entries - Example

- **Retail WWW Vignette**
- **CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**
  - Read application data (subscore: 8)
  - Bypass protection mechanism (subscore: 7)
  - Modify application data (subscore: 8)
  - *Maximum impact score: 8*
- **CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')**
  - Execute unauthorized code or commands (subscore: 10)
  - DoS: crash / exit / restart (subscore: 4)
  - *Maximum impact score: 10*

Yes, SQL Injection can allow code execution…

Prevalence Estimates per CWE

CWE	Name	Prevalence (1-10)
CWE-79	XSS	9.46
CWE-89	SQL injection	7.43
CWE-120	Classic overflow	6.04
CWE-352	Cross-site Request Forgery	7.75
CWE-285	Insufficient Authorization	6.04
…	…	…

- Prevalence data is rarely available at this level of detail
- Borrowed data from 2010 CWE Top 25 votes
- Normalize 1-4 scores to 1-10 range

http://cwe.mitre.org/cwss/vignettes.html#votesum

Considerations for CWSS beyond 0.1

- **Technical impact model is limited**
  - “code execution” applies to XSS, SQL injection, OS command injection, buffer overflows…
- **Factors for scores might change regularly**
  - Prevalence may change
  - Vignettes may change
  - Technical impacts may change
  - CWE will change
  - “Versioning” for CWSS when factors change
  - Is this manageable when sharing CWSS scores?
- **If maximum impact is chosen instead of the average, then scores will trend upwards as more vignettes are added**
- **Targeted and generalized scoring require different factors**

Considerations (Continued)

- **Scores could be adjusted downward based on environmental considerations**
  - Still need to model these
  - “this is a config file only readable by admin”
  - “this input is externally validated using Struts”
- **How to score a potentially-insecure API function that’s currently used safely?**
- **How to score software-wide design issues, e.g. “not using an input validation framework”?**
  - “worth” more than 100 XSS

Recent Activities

- **http://cwe.mitre.org/cwss**
- **White paper published**
  - Vignettes available for review
- **Community recruitment underway**
  - Working with SANS
  - Talked with several software security capability vendors
  - Software security tool vendors
  - Developers
  - End users / consumers
  - Vignette-oriented experts (e.g. SCADA)
  - CVSS SIG
  - OWASP
- **Associated CWE content changes**

Working Sessions & Documentation: Individual OWASP Projects

WORKING SESSION: Common Structure and Numbering for All Guides

Short Working Session Description:

The purpose of this session is to bring together the various document project leaders and other interested parties to discuss the establishment of a common document numbering system. This will also require that applicable document projects have a similar structure, at least in the areas associated with the numbering. That means this session will drive revisions to current projects. Additionally, this is an opportunity to discuss the overall alignment of the release document projects and how they fit into a secure development life cycle.

Some of the document projects that would benefit from this activity include the following, but there are several others not listed:

- OWASP Secure Coding Practices - Quick Reference Guide.........(What to do - Requirements),
- OWASP Development Guide......................................(How to do it – Coding guidance),
- OWASP Ruby on Rails Security Guide V2.........................(How to do it – Ruby specific),
- OWASP Testing Guide..(How to test it – Pen Testing),
- OWASP Code Review Guide......................................(How to test it – Code Review),
- OWASP Application Security Verification Standard Project......(Verify and rate what was done),

Chair(s): **Keith Turpin, Matteo Meucci, Vishal Garg**

Objectives:

1. Discuss and review current document project structures and key elements.
2. Review proposal to align to ASVS and discuss whether the current version of ASVS provides an adequate baseline.
3. Review other options for structure and numbering.
4. Develop a draft structure and numbering plan.
5. Discuss any dependencies which may exist, such as common nomenclature and definitions.

Outcomes/Deliverables proposed by working group:

1. A written recommendation for a unified category and numbering system for applicable document projects.
2. Agreement from applicable project leaders to adopt the finalized version of the system.
3. An implementation plan discussing when projects will implement the new system.

WORKING SESSION: OWASP Common Vulnerability List

Short Working Session Description:

There are many OWASP projects like OWASP Testing Guide, OWASP Code Review Guide, OWASP Developers Guide, etc which discuss on how to look for and remediate various vulnerabilities in a web application. For e.g., people using OWASP Testing Guide to test for vulnerabilities in their application can go through a list of vulnerabilities and test for it but there is no easy way for them to cross reference to dev guide to jump to a specific section and be able to access the relevant information quickly. These vulnerabilities are discussed as individual list in all the guides and there is no easy way to cross-reference all of them.

OWASP Common Vulnerability List will be a lightweight list, which will contain only the vulnerability ID, category, vulnerability name and a brief description. The main objective of this list is to provide a common platform for other guides and tools to provide a link to each other.

Related Project(s):

- OWASP Common Vulnerability List
- OWASP Testing Project
- OWASP Code Review Guide
- OWASP Building Guide

Chair(s): **Matteo Meucci, Eoin Keary, Anurag Agarwal**

Objectives:

1. Build the first version of the OWASP Common Vulnerability List

Outcomes/Deliverables proposed by working group:

1. Debating the vulnerability list and deliver the first version of the project

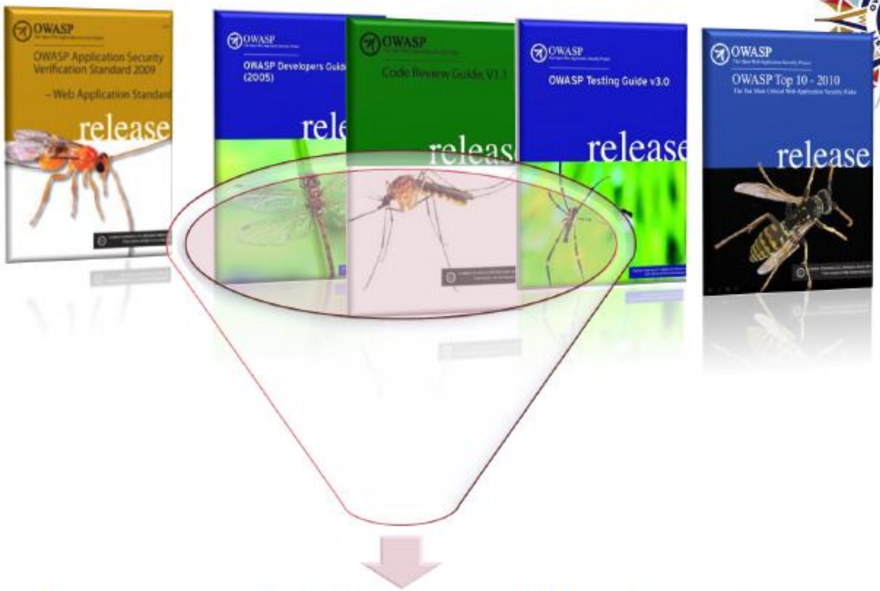
OWASP
Common Vulnerability list

AGENDA

- Why do we need a common vulnerability list?
- What are the status of the OWASP Guides?
- What the CVL can do to improve the Guides

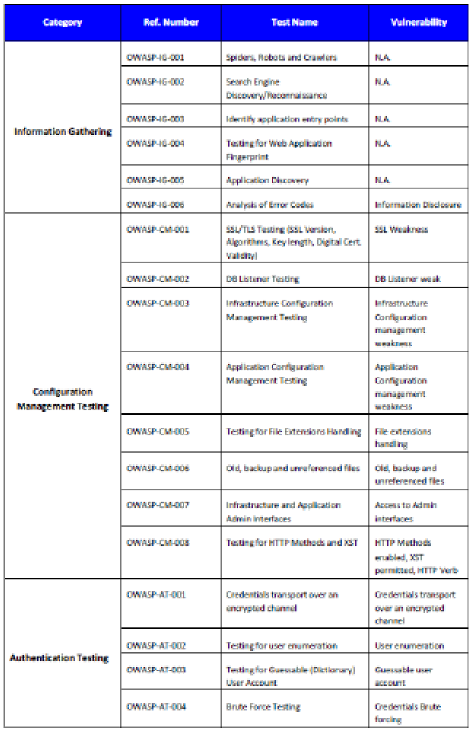
A Few words about the status of the Guides

OWASP Common Vulnerability List


OWASP
OWASP Application Security Verification Standard 2009
– Web Application Standard
release
OWASP
OWASP Developers Guide (2005)
rele
OWASP
Code Review Guide V1.1
releas
OWASP
OWASP Testing Guide v3.0
release
OWASP
OWASP Top 10 - 2010
The Ten Most Critical Web Application Security Risks
release

We need a common vulnerability list to talk the same language

Looking at the Testing Guide Categories & vulnerability list



Category	Ref. Number	Test Name	Vulnerability
Information Gathering	OWASP-IG-001	Spiders, Robots and Crawlers	N.A.
	OWASP-IG-002	Search Engine Discovery/Reconnaissance	N.A.
	OWASP-IG-003	Identify application entry points	N.A.
	OWASP-IG-004	Testing for Web Application Fingerprint	N.A.
	OWASP-IG-005	Application Discovery	N.A.
	OWASP-IG-006	Analysis of Error Codes	Information Disclosure
Configuration Management Testing	OWASP-CM-001	SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity)	SSL Weakness
	OWASP-CM-002	DB Listener Testing	DB Listener weak
	OWASP-CM-003	Infrastructure Configuration Management Testing	Infrastructure Configuration management weakness
	OWASP-CM-004	Application Configuration Management Testing	Application Configuration management weakness
	OWASP-CM-005	Testing for File Extensions Handling	File extensions handling
	OWASP-CM-006	Old, backup and unreferenced files	Old, backup and unreferenced files
	OWASP-CM-007	Infrastructure and Application Admin Interfaces	Access to Admin interfaces
	OWASP-CM-008	Testing for HTTP Methods and XST	HTTP Methods enabled, XST permitted, HTTP Verb
Authentication Testing	OWASP-AT-001	Credentials transport over an encrypted channel	Credentials transport over an encrypted channel
	OWASP-AT-002	Testing for user enumeration	User enumeration
	OWASP-AT-003	Testing for Guessable (Dictionary) User Account	Guessable user account
	OWASP-AT-004	Brute Force Testing	Credentials Brute forcing

From the list to the Guides 2011

Authentication	Credentials transport over an unencrypted channel User enumeration (also Guessable user account) Default passwords Weak lock out mechanism ...

Next step

- Subscribe to:
- http://www.owasp.org/index.php/Common_OWASP_Numbering mailing list (coming soon)
- Let's continuing the discussion of the project on the mailing list
- Deadline: February 2011
- Deadline for the new guides: end 2011

Thanks!

matteo.meucci@owasp.org

WORKING SESSION: OWASP Testing Guide

Short Working Session Description:

We need to define:

- An updated vulnerability list to test (from the OWASP Common Vulnerability List),
- Create a more readable guide, eliminating some sections that are not really useful,
- Insert new testing techniques: HTTP Verb tampering, HTTP Parameter Pollutions, etc.,
- Rationalize some new sections as Session Management Testing,
- Debate if whether to create a new section: Client side security and Firefox extensions testing.

Related Project(s):

- OWASP Testing Project
- OWASP Common Structure and Numbering for All Guides

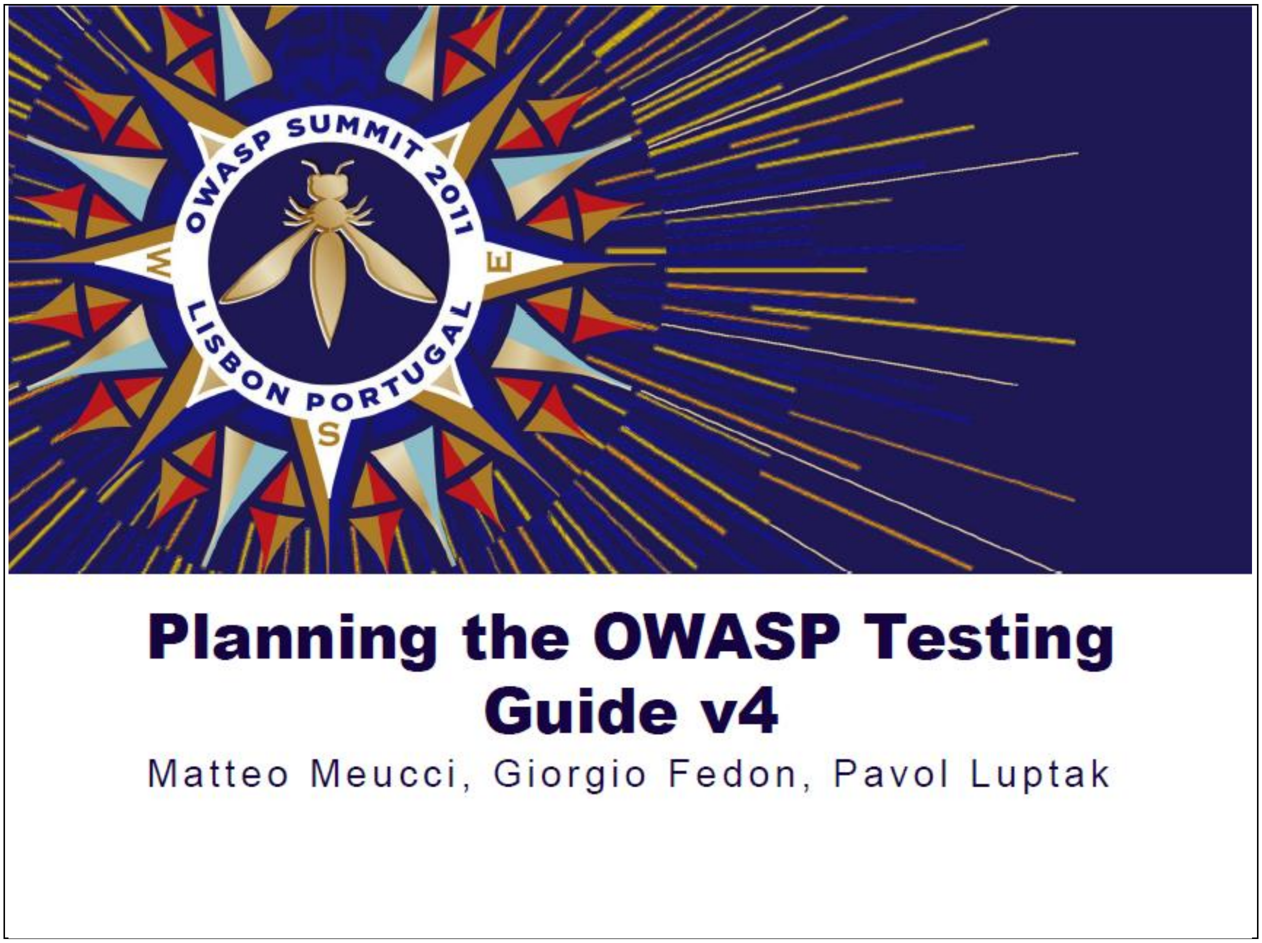
Chair(s): **Matteo Meucci**

Objectives:

1. Show the v3, and debating what we need to do to create an excellent v4.

Outcomes/Deliverables proposed by working group:

1. An updated outline for the testing guide that is tied into the OWASP common numbering scheme
2. A short white paper with ideas for revisions to the Testing Guide for evaluation and discussion by the community at large
3. A committed project manager who can reach out to experts to get the document completed.


OWASP SUMMIT 2011
LISBON PORTUGAL
W
E
S

Planning the OWASP Testing Guide v4

Matteo Meucci, Giorgio Fedon, Pavol Luptak

AGENDA

- Few words about the TG history and adoption by the Companies
- Why we need the Common Numbering and Common Vulnerability list
- Update the set of test
- V4 Roadmap

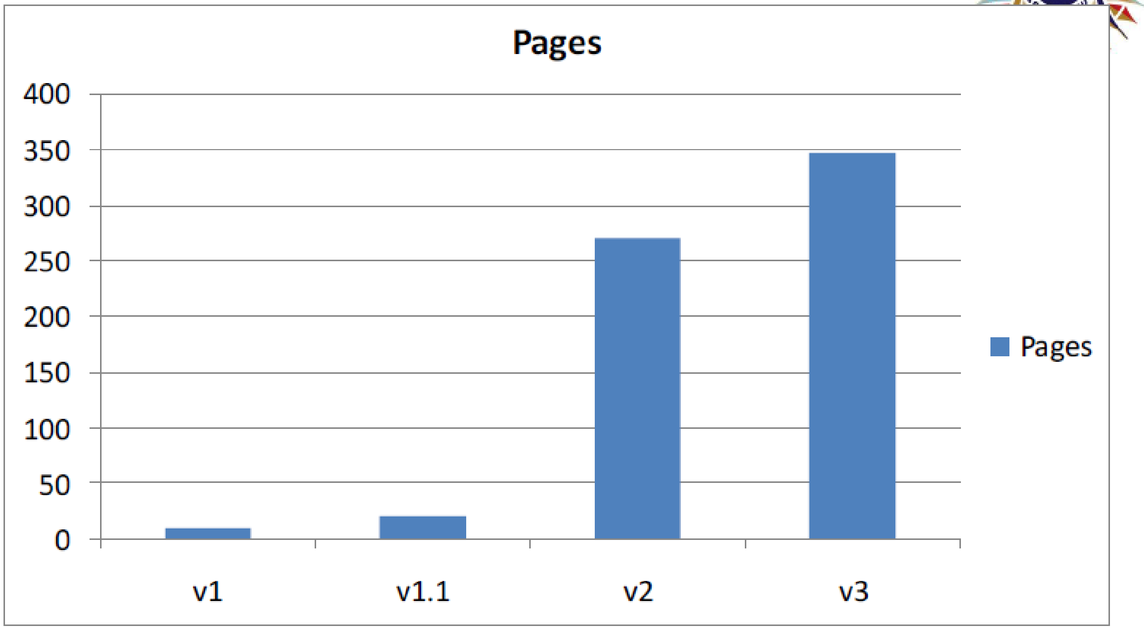
What is the OWASP Testing Guide?

Where are we now?

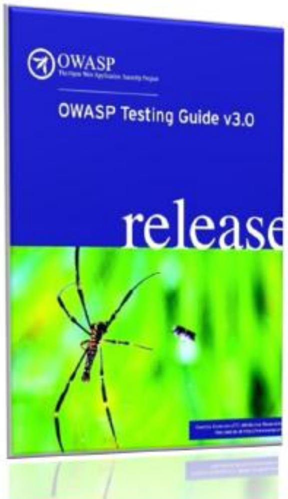
Testing Guide history

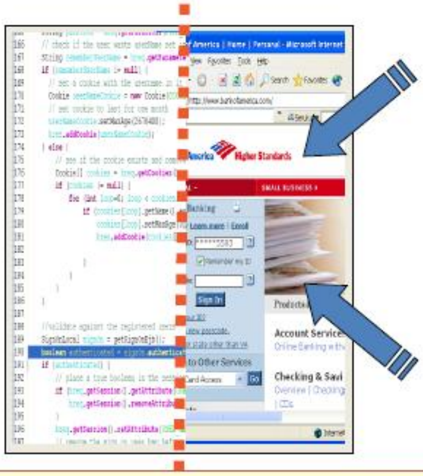
- January 2004
  - "The OWASP Testing Guide", Version 1.0
- July 14, 2004
  - "OWASP Web Application Penetration Checklist", Version 1.1
- December 25, 2006
  - "OWASP Testing Guide", Version 2.0
- December 16, 2008
  - "OWASP Testing Guide", Version 3.0 – Released at the OWASP Summit 08

Project Complexity



OWASP Testing Guide v3





```
// check if the user wants userName set
String rememberUserName = hreq.getParame
if (rememberUserName != null) {
  // set a cookie with the username in it
  Cookie userNameCookie = new Cookie(
  // set cookie to last for one month
  userNameCookie.setMaxAge(2678400);
  hres.addCookie(userNameCookie);
} else {
  // see if the cookie exists and remo
  Cookie[] cookies = hreq.getCookies(
  if (cookies != null) {
    for (int loop=0; loop < cookies
      if (cookies[loop].getName().
        cookies[loop].setMaxAge(
        hres.addCookie(cookies[
      }
    }
  }
}

//validate against the registered users
SignOnLocal signOn = getSignOnEjb();
boolean authenticated = signOn.authentica
if (authenticated) {
  // place a true boolean in the sessi
  if (hreq.getSession().getAttribute(
    hreq.getSession().removeAttribu
  }
  hreq.getSession().setAttribute(SIG
  // remove the sign on user key bef
```

- SANS Top 20 2007
- NIST “Technical Guide to Information Security Testing (Draft)”
- Gary McGraw (CTO Cigital) says: “In my opinion it is the strongest piece of Intellectual Property in the OWASP portfolio” – OWASP Podcast by Jim Manico

Testing Guide v3: Index

1. Frontispiece
2. Introduction
3. The OWASP Testing Framework
4. Web Application Penetration Testing
5. Writing Reports: value the real risk

Appendix A: Testing Tools

Appendix B: Suggested Reading

Appendix C: Fuzz Vectors

Appendix D: Encoded Injection

What are the difference between the OWASP Testing Guide and another book about WebApp PenTesting?

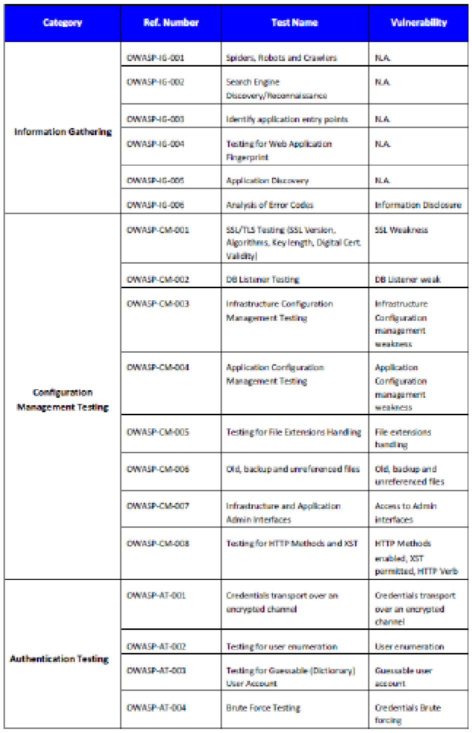
Web Application Penetration Testing

- OWASP Testing Guide is driven by our Community
- It’s related to the other OWASP guides

- Our approach in writing this guide
  - Open
  - Collaborative

- Defined testing methodology
  - Consistent
  - Repeatable
  - Under quality

Testing Guide Categories & vulnerability list



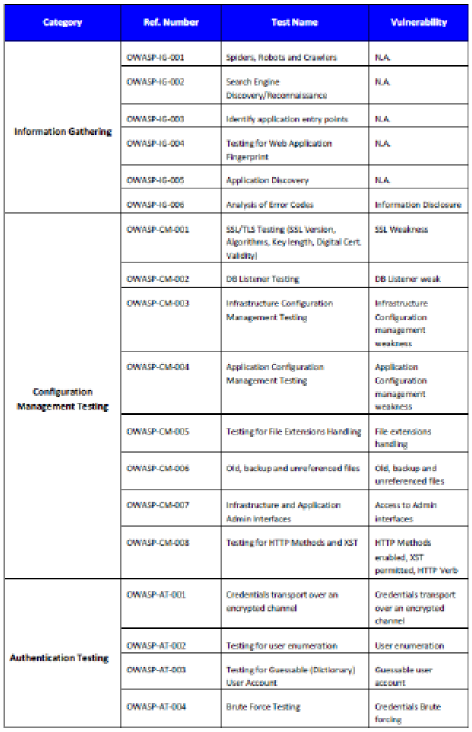
Category	Ref. Number	Test Name	Vulnerability
Information Gathering	OWASP-IG-001	Spiders, Robots and Crawlers	N.A.
	OWASP-IG-002	Search Engine Discovery/Reconnaissance	N.A.
	OWASP-IG-003	Identify application entry points	N.A.
	OWASP-IG-004	Testing for Web Application Fingerprint	N.A.
	OWASP-IG-005	Application Discovery	N.A.
	OWASP-IG-006	Analysis of Error Codes	Information Disclosure
Configuration Management Testing	OWASP-CM-001	SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity)	SSL Weakness
	OWASP-CM-002	DB Listener Testing	DB Listener weak
	OWASP-CM-003	Infrastructure Configuration Management Testing	Infrastructure Configuration management weakness
	OWASP-CM-004	Application Configuration Management Testing	Application Configuration management weakness
	OWASP-CM-005	Testing for File Extensions Handling	File extensions handling
	OWASP-CM-006	Old, backup and unreferenced files	Old, backup and unreferenced files
	OWASP-CM-007	Infrastructure and Application Admin Interfaces	Access to Admin interfaces
	OWASP-CM-008	Testing for HTTP Methods and XST	HTTP Methods enabled, XST permitted, HTTP Verb
Authentication Testing	OWASP-AT-001	Credentials transport over an encrypted channel	Credentials transport over an encrypted channel
	OWASP-AT-002	Testing for user enumeration	User enumeration
	OWASP-AT-003	Testing for Guessable (Dictionary) User Account	Guessable user account
	OWASP-AT-004	Brute Force Testing	Credentials Brute forcing

What we need now to improve the v3 and plan the v4?

OWASP Common Vulnerability List

We need a common vulnerability list

Looking at the Testing Guide Categories & vulnerability list

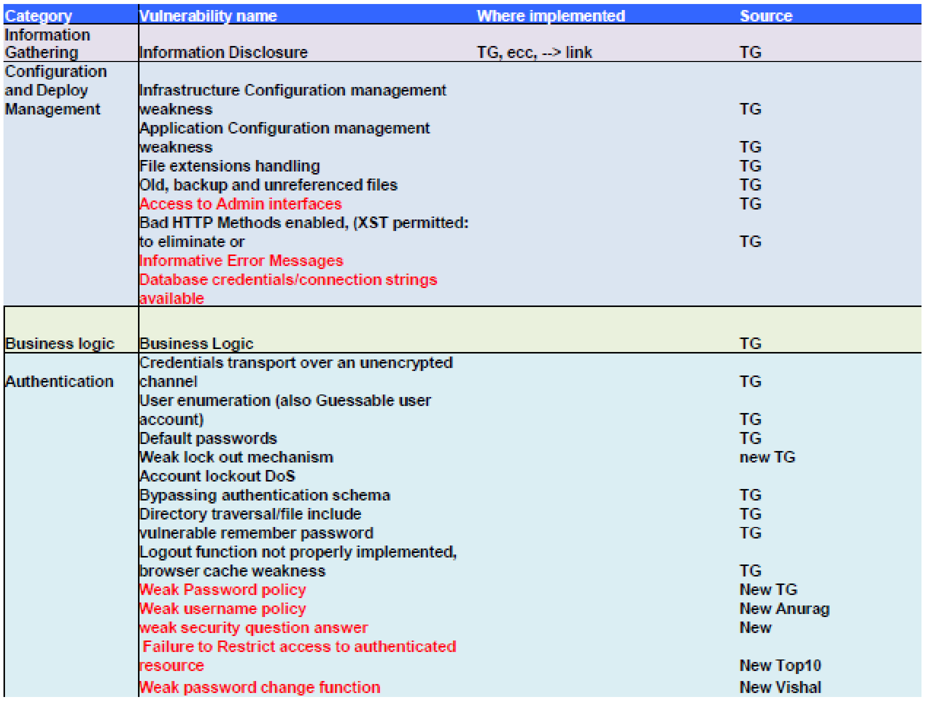


Category	Ref. Number	Test Name	Vulnerability
Information Gathering	OWASP-IG-001	Spiders, Robots and Crawlers	N.A.
	OWASP-IG-002	Search Engine Discovery/Reconnaissance	N.A.
	OWASP-IG-003	Identify application entry points	N.A.
	OWASP-IG-004	Testing for Web Application Fingerprint	N.A.
	OWASP-IG-005	Application Discovery	N.A.
	OWASP-IG-006	Analysis of Error Codes	Information Disclosure
Configuration Management Testing	OWASP-CM-001	SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity)	SSL Weakness
	OWASP-CM-002	DB Listener Testing	DB Listener weak
	OWASP-CM-003	Infrastructure Configuration Management Testing	Infrastructure Configuration management weakness
	OWASP-CM-004	Application Configuration Management Testing	Application Configuration management weakness
	OWASP-CM-005	Testing for File Extensions Handling	File extensions handling
	OWASP-CM-006	Old, backup and unreferenced files	Old, backup and unreferenced files
	OWASP-CM-007	Infrastructure and Application Admin Interfaces	Access to Admin interfaces
	OWASP-CM-008	Testing for HTTP Methods and XST	HTTP Methods enabled, XST permitted, HTTP Verb
Authentication Testing	OWASP-AT-001	Credentials transport over an encrypted channel	Credentials transport over an encrypted channel
	OWASP-AT-002	Testing for user enumeration	User enumeration
	OWASP-AT-003	Testing for Guessable (Dictionary) User Account	Guessable user account
	OWASP-AT-004	Brute Force Testing	Credentials Brute forcing

The new team

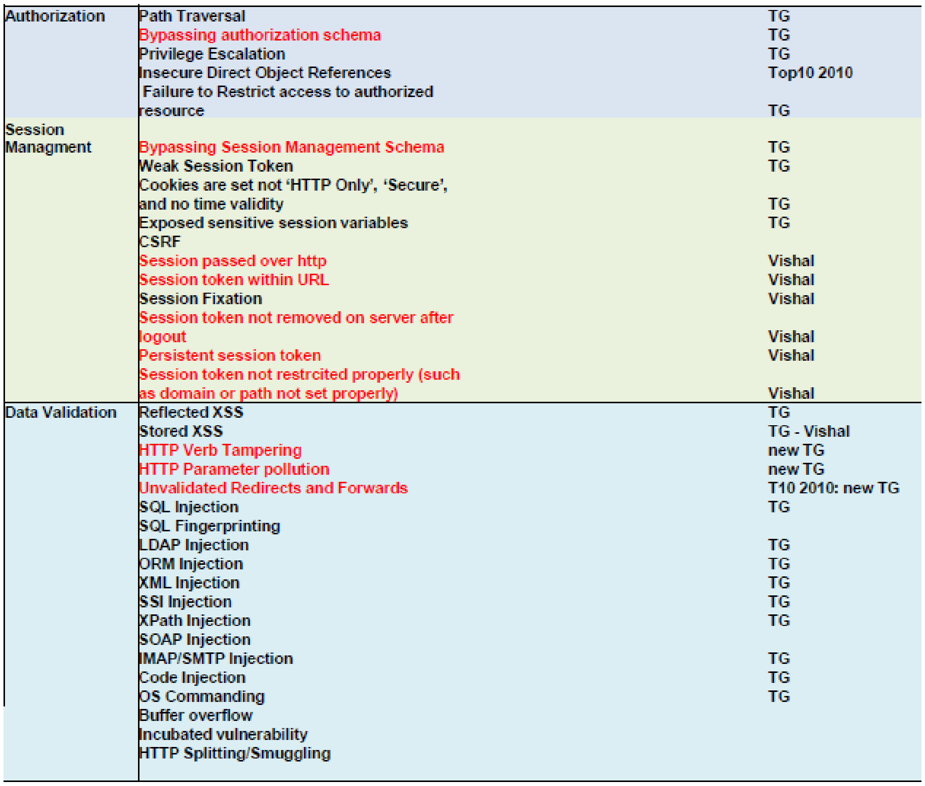
Andrew Muller
Aung KhAnt
Cecil Su
Colin Watson
Daniel Cuthbert
Giorgio Fedon
Jason Flood
Javier Marcos de Prado
Juan Galiana Lara
Kenan Gursoy
Kevin Horvat
Lode Vanstechelman
Marco Morana
Matt Churchy
Matteo Meucci
Michael Boman
Mike Hryekewicz
Nick Freeman
Norbert Szetei
Paolo Perego
Pavol Luptak
Psiinon
Ray Schippers
Robert Smith
Robert Winkel
Roberto Suggi Liverani
Sebastien Gioria
Stefano Di Paola
Sumit Siddharth
Thomas Ryan
Tim Bertels
Tripurari Rai
Wagner Elias

Proposed v4 list: let's discuss it



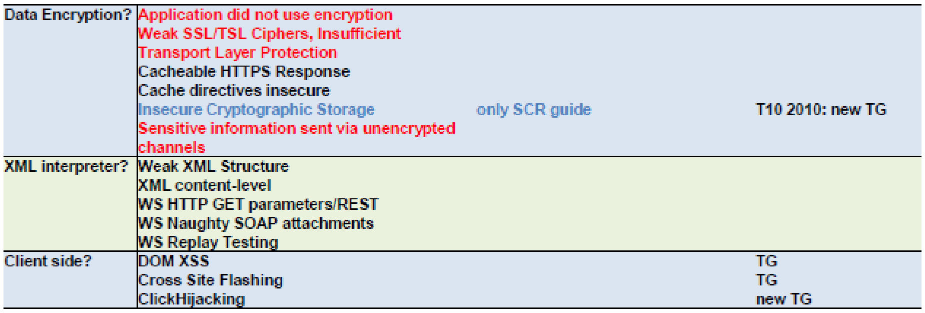
Category	Vulnerability name	Where implemented	Source
Information Gathering	Information Disclosure	TG, ecc, --> link	TG
Configuration and Deploy Management	Infrastructure Configuration management weakness		TG
	Application Configuration management weakness		TG
	File extensions handling		TG
	Old, backup and unreferenced files		TG
	Access to Admin interfaces		TG
	Bad HTTP Methods enabled, (XST permitted: to eliminate or		TG
	Informative Error Messages		
	Database credentials/connection strings available		
Business logic	Business Logic		TG
Authentication	Credentials transport over an unencrypted channel		TG
	User enumeration (also Guessable user account)		TG
	Default passwords		TG
	Weak lock out mechanism		new TG
	Account lockout DoS		
	Bypassing authentication schema		TG
	Directory traversal/file include		TG
	vulnerable remember password		TG
	Logout function not properly implemented, browser cache weakness		TG
	Weak Password policy		New TG
	Weak username policy		New Anurag
	weak security question answer		New
	Failure to Restrict access to authenticated resource		New Top10
	Weak password change function		New Vishal

Proposed v4 list: let's discuss it (2)



Authorization	Path Traversal	TG
	Bypassing authorization schema	TG
	Privilege Escalation	TG
	Insecure Direct Object References	Top10 2010
	Failure to Restrict access to authorized resource	TG
Session Managment	Bypassing Session Management Schema	TG
	Weak Session Token	TG
	Cookies are set not 'HTTP Only', 'Secure', and no time validity	TG
	Exposed sensitive session variables	TG
	CSRF	
	Session passed over http	Vishal
	Session token within URL	Vishal
	Session Fixation	Vishal
	Session token not removed on server after logout	Vishal
	Persistent session token	Vishal
	Session token not restrcited properly (such as domain or path not set properly)	Vishal
Data Validation	Reflected XSS	TG
	Stored XSS	TG - Vishal
	HTTP Verb Tampering	new TG
	HTTP Parameter pollution	new TG
	Unvalidated Redirects and Forwards	T10 2010: new TG
	SQL Injection	TG
	SQL Fingerprinting	
	LDAP Injection	TG
	ORM Injection	TG
	XML Injection	TG
	SSI Injection	TG
	XPath Injection	TG
	SOAP Injection	
	IMAP/SMTP Injection	TG
	Code Injection	TG
	OS Commanding	TG
	Buffer overflow	
	Incubated vulnerability	
	HTTP Splitting/Smuggling	

Proposed v4 list: let's discuss it (3)



Data Encryption?	Application did not use encryption		
	Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection		
	Cacheable HTTPS Response		
	Cache directives insecure		
	Insecure Cryptographic Storage	only SCR guide	T10 2010: new TG
	Sensitive information sent via unencrypted channels		
XML interpreter?	Weak XML Structure		
	XML content-level		
	WS HTTP GET parameters/REST		
	WS Naughty SOAP attachments		
	WS Replay Testing		
Client side?	DOM XSS		TG
	Cross Site Flashing		TG
	ClickHijacking		new TG

Proposed v4 news from Pavol

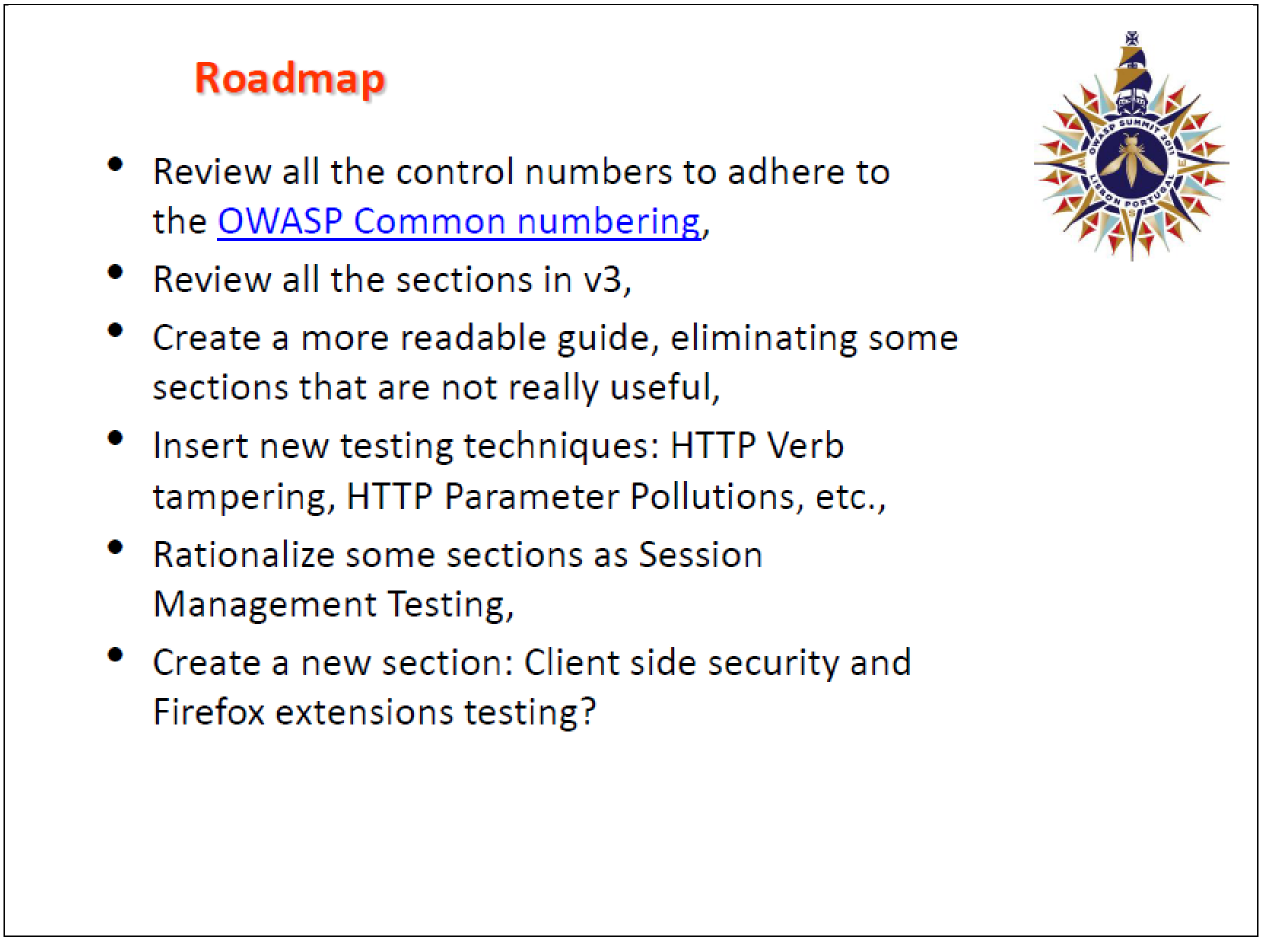
- add new opensource testing tools that appeared during last 3 years (and are missing in the OWASP Testing Guide v3)

- add few useful and life-scenarios of possible vulnerabilities in Bussiness Logic Testing (many testers have no idea what vulnerabilities in Business Logic exactly mean)

- "Brute force testing" of "session ID" is missing in "Session Management Testing", describe other tools for Session ID entropy analysis (e.g. Stompy)

- in "Data Validation Testing" describe some basic obfuscation methods for malicious code injection including the statements how it is possible to detect it (web application obfuscation is quite succesfull in bypassing many data validation controls)

- split the phase Logout and Browser Cache Management" into two sections



Roadmap

- Review all the control numbers to adhere to the OWASP Common numbering,
- Review all the sections in v3,
- Create a more readable guide, eliminating some sections that are not really useful,
- Insert new testing techniques: HTTP Verb tampering, HTTP Parameter Pollutions, etc.,
- Rationalize some sections as Session Management Testing,
- Create a new section: Client side security and Firefox extensions testing?

Questions?

http://www.owasp.org/index.php/OWASP_Testing_Project

matteo.meucci@owasp.org

Thanks!!

Owasp Summit 2011 - Portugal - Testing Guide Session

Notes taken by Giorgio Fedon

Matteo Meucci: Testing Guide is very important from a black box and grey box point of view. We would like to continue this approach in the new Owasp Testing Guide for extending even more Web Application Penetration Testing Methodology. So we are planning the new version 4. Owasp Testing guide is driven by the community and is strongly related to other Owasp guides like the Code Review Guide and the Building Guide. That's why we have a strong commitment in finding an Owasp Common Vulnerability List for all the guides.

Matteo Meucci: For the new Testing Guide we proposed new tests to better aligning the actual table of content to the one of the other guides. Secure cryptographic storage is a good example: it was included in the Owasp Top Ten 2010 and not in the Testing Guide. Owasp testing Guide Team will update and improve each single chapter for the new version. A very important chapter to extend is the one about Web Configuration Problems.

Stefano Di Paola: I would suggest to change the name of Configuration issues category to "Configuration and Deploy".

Nishi: I would suggest to specify for each category the group in charge for that. For example in the company where I work Infrastructure and Application teams are very different.

Response: Infrastructure and Application is not necessarily divided between different group of people. About the names of the categories I would simplify the one about unsafe methods… a name like "Extended HTTP Methods like WebDav and Trace Methods" would be fine for me.

Luptak: I think that Insecure Cryptographic Storage is not necessarily important in Testing guide which relates to Black Box testing. From my point of view it would better fit the code review guide.

Stefano Di Paola: Password Encryption is something you can be aware of during testing… imagine a recovery password feature that sends you original password in plain text. That would be a problem

Anurag: I think that in the description of the issues there is a commixture of Attack Names with Vulnerabilities. I think that we should choose vulnerabilities or Attacks, not both.

Giorgio Fedon: From my point of view, sometimes the attacks describes better the vulnerability and vice versa. "Padding Oracle Attack" sounds better that "the encrypted string is not protected by a digital signature and the state of the invalid padding is somehow visible through response analysis".

Matteo: Testing guide is to create a Methodology not just controls to test… That's why I think that talking about test cases or Attacks is very important. This practice simplifies testing cases.

Nishi: For Automation is important defining strings for test cases. For example SQL Injection attacks, we need standard patterns.

Matteo: We already did that… I think

Anurag: I would suggest to add for each paragraph 3 lines, to describe better which is the vulnerability, and the attack impact if correctly exploited. In addition, call the structure by the correct names, it would make it easier to link the guides.

Colin: There are some more extra details I would like to talk about, in particular some about configuration

Matteo: Your list of suggestion is one excellent contribution and is very detailed, I invite all the people in the mailing list to read it and to discuss your points.

Luptak: There are a lot of new and great open source tools missing that should be mentioned. Business validation section is not so clear, I would like if we could discuss a little about it. For me an example of Business Logic issue is like History Hack in facebook. It's not directly connected, but in the session management paragraph I would add also add weak session Ids brute forcing.

Giorgio: Business Logic tricky vulnerability, I suggest to better describe the methodology to Identify and classify Business Vulnerabilities as we intend in the Testing Guide. A tester should choose any other issue that could fit his finding before mapping it to this particular category. Only Afterwards he can define it a Business Logic issue.

Stefano: An example of a business logic vulnerability, is usually something not conventional. Do you remember the 1 dollar subscribing bonus hack? A user register 10K user accounts that were linked to the same bank account and earned 10k dollars overnight. System administrators discovered hundreds of "Mickey Mouse" family accounts the day after.

Giorgio: In Penetration Testing Methodology for Business Logic could be helpful examples of real test Cases which describe business logic issues. Since these vulnerabilities are application specific, they go past the scope of the testing guide, I think.

Anurag: For the Threat modeling I think that a list of tests to add to this guide as well could be helpful

Luptak: A very useful technique for testing is also obfuscation.

Giorgio: I agree with you, but maybe in the Appendix. Testing guide is for spotting vulnerabilities, not for exploiting them. Obfuscation is usually helpful to bypass controls and Web IDS/IPS for inserting payload and exploiting vulnerabilities.

Stefano: I would suggest external references in the appendix.

Giorgio: From the testing Guide is missing a lot about client side methodology before testing. For example understanding the Client, for a Java applet or a Flex application is very important. In addition are also missing controls like Click Jacking, HPP attacks.

Nishi: Should be important to add a paragraph about remediation and client side fixing.

Giorgio: In the unity model of unifying all the guides using a common vulnerability list, OCVL (Owasp Common Vulnerability List) may help to find important information across all the guides. Testing Guide is for testing, Development Guide is for developing an application securely and for fixing.

Luptak: Browser Cache management is also to fix, it is in 2 sections

Public: We ask you to improve the Denial of service methodology also, this is an important part of testing, but we need to better clarify the risks and that timeframes must be agreed and coordinated with the customer.

Matteo: Good Idea, Updating Denial of Service testing. Java Double.Parse(Double) is a good example, thank you Jim for pointing this out.

Nishi: Improving methodology for clients is important also: Frameworks Flex application, different from Web Applications

Stefano: Also important Firefox Extension Testing vendor develops from time to time very specific extensions for the browsers. However these extensions are not so common.

Public: It's important to differentiate between common and uncommon issues.

Matteo: There is only one minute left, thank you all for participating to this Working Session, see you online on the mailing list.

WORKING SESSION: OWASP Development Guide

Short Working Session Description:

If done from the earliest stages, secure applications cost about the same to develop as insecure applications, but are far more cost effective in the long run. The primary aim of the OWASP Development Guide is to help businesses, developers, designers and solution architects to build secure web applications from the outset. The next version of the guide is an extension from the existing version with further enhancements to make it more usable for all stake holders. The aim of the working session is to have a discussion on the shortcomings of the existing guide and to make it a basis for further enhancements, alignment of the guide to ASVS Standard and OWASP common numbering scheme, potential for alignment of all three OWASP guides (DG, CRG and TG) and the ways to improve the usefulness of the guide to all the stake holders.

Related Project(s):

- OWASP Guide Project

Chair(s): **Vishal Garg**

Objectives:

1. Discussion on major enhancements to the next version of the development guide
2. Discussion on aligning the guide to ASVS standard and OWASP common numbering scheme
3. Discussion on improving the usefulness of the guide to all stakeholders
4. Collaboration with other OWASP guides - Top 10, ASDR, CRG and TG

Outcomes/Deliverables proposed by working group:

- An updated outline for the development guide that is tied into the OWASP common numbering scheme
- A short white paper with ideas for revisions to the Development Guide for evaluation and discussion by the community at large
- A committed project manager who can reach out to exert to get the document completed.

WORKING SESSION: ASVS Project

Short Working Session Description:

Discussion on the Application Security Verification Standard (experiences, ideas for improvement, etc.)

Related Project(s):

- Application Security Verification Standard (ASVS)

Chair(s): **Matthias Rohr**

Objectives:

1. Discuss experiences with using ASVS
2. Discuss specific requirements and ideas for improvement
3. Create a white paper with ideas for revisions to the ASVS

Outcomes/Deliverables proposed by working group:

- A short white paper with ideas for revisions to the ASVS, ready for evaluation by the community at large. Actual suggested revisions to the document are helpful, but not required if time does not allow.

WORKING SESSION: OWASP Secure Coding Practices Project

Short Working Session Description:

The purpose of this session is three fold:

1. Introduce the project to those who are not yet familiar with it;
2. Discuss what improvements can be made to the guide;
3. Discuss what is needed to align the guide to the new common numbering structure being developed.

Related Project(s):

- OWASP Secure Coding Practices – Quick Reference Guide

Chair(s): **Keith Turpin**

Objectives:

1. Improve visibility of this project to other document project leaders
2. Discussion and documenting suggested enhancements to the next version of the guide
3. Collaboration with other OWASP guides
4. Plan for implementation of common numbering schema

Outcomes/Deliverables proposed by working group:

- An updated outline for the Quick Reference Guide that is tied into the new OWASP Common Numbering Scheme
- A short white paper with ideas for revisions to the Quick Reference Guide

OWASP – Secure Coding Practices - 2011 Global Summit

Top three accomplishments of the session:

1. Got broader exposure of the Secure Coding Practices guide, including to other document project leaders
2. Clarified the purpose of the Secure Coding Practices guide
3. Identified some areas of improvement for the next release and got additional members volunteering to be contributors

Some changes planned for next release:

1. Renaming the guide. Proposed new title "Secure Software Requirements 2011"
2. Update project references
3. Incorporate contributions from new contributors
4. Implement number system based on common numbering schema, to be defined

Session Notes: *Courtesy of Colin Watson*

Disclaimer: Not a verbatim statement of what was said by whom, just an interpretation, and not necessarily documented or interpreted correctly!

Keith Turpin: “Secure Software Requirements” would be a better description since system, database and framework configuration included. Compact 17 pages, in a language suitable for developers. Does not attempt to rank practices.

KT: Still a relatively new project, so will walk through it and discuss changes required.

[Audience: Colin Watson]: Change CLASP to SAMM?

KT: Yes, that is a pending change.

[Audience 2]: I guess you have to be generic enough for all systems, but too easy for people to agree on the intent.

[Audience - Dave Wichers]: We want to develop a set of requirements standards, so maybe use ASVS for what to verify. These should be linked to the other documents.

[Audience – Anurag]: We are working on pulling the guides together by cross referencing, but not all in one.

[Audience – 5]: Not just “the guide” which is confusing.

[Audience – 6]: This would have helped me when I had to write a developer guide years ago. 20 pages is probably the max – good.

KT: This document says what to do, not how to do it. Hence it needs to be short, otherwise it is too complex.

[Audience – 7]: So is the common numbering enough, or do we need links?

KT: We are looking in a another session at standardisation across ASVS, Code Review, Development and testing Guides. Probably want to use numbering, rather than linking to make sure they can be updated independently.

[Audience – 8]: This seems like a good starting point. The next thing is build it out.

KT: yes, decide which requirements you are going to use (and for the others why not). Then look for standards elsewhere, or tools, or frameworks, etc.

[Audience – John Wilander]: Will developers catch on... the security guys have cooked up something again. Will this produce more secure code, or a way to get back to them when things go wrong.

[Audience – Dave W]: It is a starting point.

[Audience – John W]: We need code snippets.

[Audience – Dave W]: Yes we need that too, but the unification project.

[Audience – 9]: The developers need to know the overview/goals too. Not just examples... but they need those too.

[Audience – Nishi]: Who is the audience?

KT: Depends on your team/processes. It is the equivalent of functional requirements for security. Someone needs to review them and decide what is required. Then feed those into the workflow tool... and the developers see functional reqs, just some of which are security. Or developers can go over this and use it as a discussion “tool” about what is software security?

[Audience – John Steven]: We look at coding index, on how much code is included. But it is broader and applicable across sectors. It will last longer too. We do need to look at these as requirements. But this does not meet traceability and testability needs. We need generic standards, but make sure they are contextualised in development scenarios, to lead to testable and traceable specifications and code.

KT: I understand. I tried to collect generically, all the requirements. You need to go in and look at the context, to look at which apply. It is a starting point list. Some may be contradictory, so it does require interpretation (eg security architect) and map out how it is done.

[Audience – 11]: If we could code our requirements, why would we write requirements.

[Audience - Nishsi]: Every situation is different.

[Audience – John W]: Who could write some code to show canonicalization? [Small number of hands] Don't tell me what to do that you don't know about.

[Audience – Nishi]: Cross references with other docs and code will make it more usable.

[Audience – Tobias]: Fully agree. If I were to implement it, I would know the team, I would add some code snippets and give it to developers.

KT: My goal is to make this as usable as possible. If there's something incorrect in the document, tell us.

[Audience – 12]: There are some implied requirements like defining data types, defining all inputs, etc. Some developers may not think about all of these.

KT: Yes some of these would need to be explained.

[Audience – 13]: I'd like to wean the developers off the security folk. Going forward, it would be better if it were all ties in.

KT: As the five documents are updated, there will be links for more information. The goal is for this to be used for requirements, and then step into other resources.

[Audience – Anurag]: I want to mention the common numbering scheme again, but there is so much information on the OWASP site... say we had one common number for a vulnerability, this might reference tests, tools, code review, articles, etc. Session is tomorrow at 10am.

[Audience – Vishal]: We have a development guide session tomorrow, and this is the type of feedback we need from you, so we can implement this into the guide.

[Audience – 14]: I have been working on this for a number of client. It is important to have a high-level document which is relatively static (eg a coding policy), and then have technology specific guidelines for language, framework, etc (eg on a wiki where developers can contribute).

KT: The name is important here, not all apply. A list of good practices, to select from. But will probably say “requirements” rather than “practices”.

[Audience – 15]: It is a joint responsibility – not just the security team or the development team. It is important to work together with the developers to explain and discuss how a solution can be implemented.

KT: The document came from developer feedback, when they asked for security to form part of requirements.

[Audience – Nishi]: Could this be mapped to Top ten?

[Audience – Dave W]: Yes – you can!

KT: Requirements can apply to multiple vulnerabilities at the same time. It may not be the only solution, but may contribute. So the relationships may be complex.

[Audience – 16]: Some people point to Top Ten now, but in the future may start looking at this.

KT: It was a good promotional document, but it can blind some companies.

[Audience – 17]: Develops may get confused over server vs. client, the different tiers, etc.

[Audience – Dave W]: I want a really good set of requirements, and this is really good.

[Audience – 18]: Mitre have put a lot of work into CWE..

KT: That's vulnerabilities, this document does not mention them at all.

WORKING SESSION: OWASP Java Project

Short Working Session Description:

The OWASP Java Project needs to be restarted. This session will attempt to gather momentum around the project again.

Related Project(s):

- OWASP Java Project

Chair(s): **Lucas C. Ferreira**

Objectives:

1. Restart the Java Project
2. Find new leadership
3. Recruit volunteers
4. Build a new roadmap for the project

Outcomes/Deliverables proposed by working group:

- Action plan for the project
- New project leader

WORKING SESSION: Threat Modeling

Short Working Session Description:

Discussion on various components of threat modeling, threat modeling methodologies and their challenges.

Chair(s): **Anurag Agarwal**

Objectives:

1. Reviewing existing methodologies and their pros and cons
2. Assigning business impacts to threats
3. Assigning technical impacts to threats
4. Threat Rating System.
5. Can we bring attack trees into main stream threat modeling methodology?

Outcomes/Deliverables proposed by working group:

- A document with a public recommendation on the use of threat modeling.
- An OWASP standard defining what a threat model is.
- An OWASP standard defining what a threat model is.
- An OWASP standard defining a workflow for creating and maintaining a threat model.
- A white paper providing recommendations on how organizations can use threat modeling to achieve better security earlier in the process. Including a business-case rationale for threat modeling would be excellent.

Threat Modeling Working Sessions (2) -- Discussion Points:

1. Threat Modeling – Existing Challenges
2. Taxonomy
3. Threat Modeling Approaches (Asset Centric, System Centric, Attacker centric)
4. Methodology
    a. Existing Methodologies
        i. Microsoft
        ii. Trike
        iii. PASTA
    b. Classifying threats into Risk
    c. Technical Impact vs Business Impact
5. Input to Threat Modeling
6. Components of a Threat Model (Asset, Threat Agent, Actors, Threats, etc)
7. Output of Threat Modeling
8. Consumers of Threat Model
9. Attack Trees – Advantages and Disadvantages
10. Application Decomposition and DFDs
11. Threat Modeling Tools (TAM, PTA, ThreatModeler)
12. Threat Modeling and Abuse Case Modeling
13. Threat Library (more focused threats as opposed to Top 10, WASC TC)
14. Do we need an OWASP Threat Modeling project?

Accomplishments:

1. An insight into how people have been doing threat modeling individually. There is no set standard used by people but everyone has their own.
2. Discussion on having an OWASP threat modeling project and let OWASP drive build and drive a standard which can be adopted by the industry.
3. Discussion on various components of threat modeling and how they fit into the process.

Output:

1. A unanimous vote to having an OWASP threat modeling project.
2. Promotion of such a project to not only security consultants but also having contributors from an end user organization to provide their feedback on challenges and such.
3. OWASP to promote the methodology to establish it as a standard in the industry.

WORKING SESSION: Mobile Security

Short Working Session Description:

Working session to establish baseline knowledge repository for mobile security testing within OWASP.

Related Project(s):

- OWASP Mobile Security Project

Chair(s): **Mike Zusman**

Objectives:

1. **Primary: Create core knowledge base on project wiki site**
2. Recruit volunteers to contribute to project
3. Establish relationships with key players (i.e. Apple/Google/etc)
4. Create the OWASP Mobile Top 10

Outcomes/Deliverables proposed by working group:

- Project wiki page
- OWASP Ecosystem concept to see what all you should have in place.
- Mobile Top 10

Mobile Working Session Summit Results

Activities Performed at Summit

1. Dynamic Working Session - Duration: 90 minutes. Attendance: ~20

   Open discussion regarding the general mission of the OWASP Mobile project, and the methodology for creating an official OWASP Top 10 Risks List.

   Key outcomes:

   - OWASP mobile needs to provide for policy makers at organizations, mobile application security testers, and mobile application developers
   - The Top 10 list should be data driven and crowd sourced. Initiative is underway.
   - ENISA/OWASP to work together on producing secure development guidelines
   - Symbian is low priority. Priority platforms: iOS, Android, RIM, WinPhone7

2. Official Working Session -Duration: 90 minutes (we went over a bit). Attendance: ~40

   Open discussion regarding the general mission and target audiences of the OWASP mobile project. Participants who represented companies other than consultancies and security product/service organizations were queried as to what their mobile application security shortcomings are, and what they would like to see come out of the project. In general, feedback matched closely to what was identified during the dynamic session: guidance for policy makers, testers, and developers.

   After this open discussion, the summit participants were split into 3 groups. Each group was tasked with coming up with their own version of the OWASP Top 10 Mobile Risks list. The outcome of this exercise was two Top-10 lists and one Top-17 list. Each small group had a representative present their list to the work group, and the finer points of some risks were discussed.

   The outcome of the group exercise has been compiled into a spreadsheet to be used by Jerry to survey penetration testing/application assessment companies in an effort to create a data driven/crowd sourced OWASP Top 10 Mobile Risks list.

   Key outcomes:

   - 37 Mobile Risks identified and documented by summit participants
   - General consensus on the mission, target audience, and key deliverables of Mobile Project
   - Relationships established project participants
   - Need to establish relationships with platform vendors, in order to express the need for security specific features & functionality

Deliverables Identified Prior to Summit

1. Primary: Create core knowledge base on project wiki site

Status: Achieved. Additional content added to wiki.

2. Recruit volunteers to contribute to project

Status: Achieved. Specific volunteered initiatives include:

- Giles Hogben (ENISA) - Giles will establish a relationship with OWASP to help produce ENISA/OWASP branded mobile platform specific secure development guidelines
- Jerry Hoff - Volunteered to survey pen-testing companies on mobile app assessment data in order to create a data driven OWASP mobile Top 10

3. Establish relationships with key players (i.e. Apple/Google/etc)

Status: fail

4. Create the OWASP Mobile Top 10

Status: Partial Success. While an official Top 10 list was not ratified, much discuss was had, and an initiative is underway to create an official OWASP Mobile Top 10.

5. Community Outreach

Status: Success. Numerous summit participants expressed an interest in contributing to the product. Moving beyond the summit, it is critical to maintain momentum and keep participants engaged in the project.

6. Formalized Road Map

Status: Partial Success. While an official road map document is pending, there was consensus among summit participants on the key initiatives that OWASP mobile must undertake. These will help formulate the official road map, and include:

- Produce the OWASP top 10 for mobile
- Produce materials & methodologies useful for app assessment
- Produce materials for app developers

WORKING SESSION:

Short Working Session Description:

Discussion on the Application Security Verification Standard (experiences, ideas for improvement, etc.)

Related Project(s):

- Application Security Verification Standard (ASVS)

Chair(s): **Matthias Rohr**

Objectives:

4. Discuss experiences with using ASVS
5. Discuss specific requirements and ideas for improvement
6. Create a white paper with ideas for revisions to the ASVS

Outcomes/Deliverables proposed by working group:

- A short white paper with ideas for revisions to the ASVS, ready for evaluation by the community at large. Actual suggested revisions to the document are helpful, but not required if time does not allow.

Working Sessions & Documentation:

University Outreach, Education and Training

WORKING SESSION: OWASP vs Government vs Universities

Short Working Session Description:

Besides addressing our community, Prof. Luís Magalhães has kindly agreed on discussing again with us in a round table format about ways of cross collaboration. Dinis Cruz and Paulo Coimbra have already met him roughly a year ago and it was discussed the potential shared interest in working together on Education matters maybe through an Academy vehicle. Through this WS, while we may have the opportunity of a partnership push, we aim discussing with the Portuguese Knowledge Society Agency, with both other national Government Agencies' and with a few Euro-American Universities representatives the potential interest in working together on Web AppSec Education and in applying, also in partnership, for European funding designed to support Transatlantic Education

Related Project(s):

- OWASP Training
- OWASP Academies
- OWASP Academy Portal Project
- OWASP Exams Project
- OWASP Secure Coding Summer School (as a concept still being draft)

Chair(s): **Dinis Cruz, Jeff Williams**

Objectives:

9. First steps on the goal of building partnerships involving Euro/American Goverment Agencies + Euro/American Universities + OWASP Foundation to push forward web appsec education goals.
10. To assess the potential of the European funding currently available and designed to support 'Transatlantic Education' - Call for proposals 2011

Outcomes/Deliverables proposed by working group:

1. Defining a minimal appsec program for universities, governments, and standards bodies

The OWASP Application Security Code of Conduct Idea

This document is a PRELIMINARY DRAFT intended for discussion and comment. Anyone interested in participating should send questions, comments, and ideas to _____TBD______.

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 minimum baseline, and that they are not difficult to achieve.

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”)

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")

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")

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 SHOULD 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 SHOULD 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 SHOULD 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.

WORKING SESSION: OWASP Certification

Short Working Session Description:

This session aims to establish the model by which a certification/exam based on OWASP materials could be created. The topics of discussion will include:

- What is a workable/acceptable certification model for OWASP's Community?
- What types of certification should there be?
- What would a CC-licensed exam look like (as executed by others)?
- Since OWASP is not interested or able to administer certifications itself who could run/administer such CC certifications/exams?
- What should OWASP's official position be on entities that provide OWASP based certifications?

Chair(s): **Jason Taylor, Jason Li, Dinis Cruz**

Objectives:

2. Determine whether certification would have value for OWASP's community
3. Determine a model by which certification based on OWASP materials could succeed
4. Determine a model for creation and distribution of a CC-licensed certification exam based on OWASP materials
5. (if agreed) Determine a model for supporting the administration of certification based on OWASP materials

Outcomes/Deliverables proposed by working group:

2. A business plan for evaluation by the community at large.

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

8. **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.*

9. **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.*

10. **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.

11. **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.*

12. **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.

13. **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

WORKING SESSION: OWASP Exams

Short Working Session Description:

This session aims to establish the model by which a certification/exam based on OWASP materials could be created. The topics of discussion will include:

- What is a workable/acceptable certification model for OWASP's Community?
- What types of certification should there be?
- What would a CC-licensed exam look like (as executed by others)?
- Since OWASP is not interested or able to administer certifications itself who could run/administer such CC certifications/exams?
- What should OWASP's official position be on entities that provide OWASP based certifications?

Chair(s): **Jason Taylor , Jason Li, Dinis Cruz**

Objectives:

1. Determine whether certification would have value for OWASP's community
2. Determine a model by which certification based on OWASP materials could succeed
3. Determine a model for creation and distribution of a CC-licensed certification exam based on OWASP materials
4. (if agreed) Determine a model for supporting the administration of certification based on OWASP materials

Outcomes/Deliverables proposed by working group:

1. A business plan for evaluation by the community at large.

WORKING SESSION: OWASP Academies

Short Working Session Description:

This session aimed to present and promote the discussion and consolidation of the OWASP Academies model proposed in January 2011 to support OWASP's strategy of penetrating and influencing the Academy – OWASP Academy Portal Project.

More information can be found on the OWASP Academies wiki page:
http://www.owasp.org/index.php/OWASP_Academies

Related Project(s):

- OWASP Academy Portal Project
- OWASP AppSec Tutorial Series

Chair(s): **Sandra Paiva**

Objectives:

1. Presentation of the discussion had in January – what we were looking for, what conclusions were reached and why
2. The OWASP Academic Portal Project – what it is, advantages, contributors, roadmap
3. Alternative ways of working with Universities when possible -- Summer School proposal (ISCTE)
4. OWASP Appsec Tutorial Series – How to best disseminate it and use it

Outcomes/Deliverables proposed by working group:

- Deliver the above as a fundable business plan complete with financial and resource requirements, timelines, metrics, etc.

WORKING SESSION: OWASP Training

Short Working Session Description:

This session aimed to present the OWASP Training Model and the initiatives undertaken to operationalize it. Furthermore, this session intended to promote the consolidation of this model as a base for Chapter-lead training initiatives and define what would be the next steps to take order to maintain and keep this model alive and active.

Related Project(s):

- OWASP Training

Chair(s): Sandra Paiva

Objectives:

1. Presentation and Consolidation of the OWASP Training Model
2. How to keep the initiative alive – people, methodologies, contents, and materials
3. Trainers Database – assessment of quality and who is ready to deliver what
4. Connection with Paid/Commercial Training Model
5. Set up a strategy to apply for currently available state European funding
6. Production of training materials – training modules, publications, videos, CDs

Outcomes/Deliverables proposed by working group:

- Deliver the above as a fundable business plan complete with financial and resource requirements, timelines, metrics, etc…
- Team and Model to apply for currently available state European funding.

WORKING SESSION: University Outreach

Short Working Session Description:

This working session aimed at bringing together educational supporters together and addressing questions such as:

- What security education programs currently exist in university settings around the world?
- How can OWASP participate and influence the curricula of these educational programs?
- How can we foster relationships between OWASP and universities?
- How can the relationship between OWASP and universities be standardized?
- What can OWASP offer universities and what can they, in turn, expect from each other?

Related Project(s):

Chair(s): Martin Knobloch

Objectives:

1. Estimation of security programs currently existing in university settings around the world.
2. Determine how OWASP can participate and influence the curricula of these educational programs.
3. Determine how OWASP can foster relationships between OWASP and universities.
4. Determine how the relationship between OWASP and universities can be standardized.
5. Discuss what OWASP can offer universities and what they can expect from each other.
6. Discuss a plan to set up and run an OWASP Secure Coding Summer School (or something similarly named).

Outcomes/Deliverables proposed by working group:

- A study with facts, numbers, and other metrics about application security in academia – the OWASP Academic State of the World
- A white paper with strategies for infiltrating academia with OWASP's priorities

WORKING SESSION: OWASP Top 10 Online Training in Hacking-Lab

Short Working Session Description:

Related Project(s):

Chair(s):

Objectives:

Outcomes/Deliverables proposed by working group:

OWASP GOVERNANCE/COMMITTEES

WORKING SESSION – OWASP LICENSING

Licensing requirements for OWASP Documentation:
OWASP only asks that contributors utilize an approved Open Source License.
However, the preferred license for wiki content is the Creative Commons 3.0 SA Attribution.

List existing licenses used by OWASP Projects:
The most popular licenses used at OWASP are
GNU Free Documentation License
LGPL ang GPL
Creative Commons 3.0 SA Attribution (all wiki content is this)
BSD

Problem 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)?

Recommendations for changes in the OWASP License
Clarify the term "distribution" so that it does not include affiliates and partners of enterprises. This would help enterprises who modify OWASP documents to use them for internal operations with occasional distribution to affiliates and partners.

OWASP: Licensing FAQ
OWASP Licensing FAQ (Frequently Asked Questions) -- Deliverable from OWASP Summit meeting in Lisbon 2011
Disclaimer: The following is not legal advice. It is highly recommended for a licensed lawyer to review your specific situation and ascertain all relevant issues when selecting and understanding license agreements.
1. Who own the content and code submitted to OWASP?
a. The author of the submitted code or content owns the code. However, the author submitting the creative work agrees to open source their work under an approved open source license. The author also has the option of completely assigning all rights in his work to OWASP. Under copyright law the author of a creative work gains copyright protection once the creative work is put into a tangible form.
2. Can I take back from OWASP the code/documentation I had previously submitted?
a. Technically no, because you open sourced your code/documentation. However, you can fork your documentation/code and close source your additional changes as the owner of the original documentation/code.
3. Does OWASP require you to share back your changes?
a. It depends on the license associated with the code/documentation you are modifying. Some licenses require you to share back any code changes the instant you make then. Other licenses require you to use the same license as the parent code/document which you used. Some are triggered upon distribution and others are triggered on modification or use.
4. What is the default license for information posted on the OWASP wiki?
a. Creative Commons 3.0 SA Attribution
5. Can you override the default license which OWASP runs under?

a. Yes, but you have to follow the directions in the license you are selecting to abide by the selected license. If the license you selected for your code/document does not include placement directions. Add a license section in the header comments of a code file or the appendix of a document.
6. Which license should I use if I want to give enterprises free will to build products on top of your submitted code or make and use changes to your submitted documents?
a. BSD
7. Which license should I use to control distribution, sale or modification of the submitted code/documentation?
a. It depends on the limitations you want to enforce in your submitted code/documentation. So read the license and talk to an attorney to understand what you are getting into. Remember that the more restrictive the license then the less likely that an enterprise will want to use it.
8. Is it possible to change my license after my document/code is released to the public?
a. If you are the sole contributor for the document/code then you can make changes to the license at any time. If there are multiple contributors to a document or code base you will need go get agreement for the license change from all contributors.

Insert PPT Presentation

Summit Bios

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 lead 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 enjoy 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. She is Vice President of the Minneapolis OWASP Chapter, 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 Defence to install a Common Criteria lab in India for the first time, and established Vulnerability Accessment Center as per SSE-CMM Guidelines. Providing organisation 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. She currently works as a teacher for at risk youth (grades 5-8) at an after school and summer kids program, in addition to volunteering at an ESL school that provides English, computer, math, and citizenship classes to immigrants and refugees. Most recently, Sarah has been involved with OWASP, providing logistical support, travel planning and wiki foo for the Global Summit and serving as the secretary for the Global Industry Committee.

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).

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 Lyfecycle, 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).

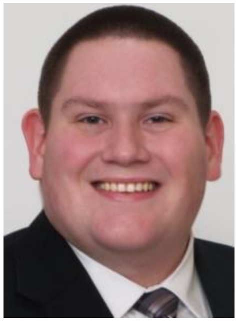
Brennan, Tom

Brennan started with technology in 1986 when 8-bit and CP/M was cool <grin>. After a career ending injury with United States Marines Corps., during Gulf War I Era he has dedicated his life to information security. Was elected and served with the FBI Infragard program 2002-2004 and then founded the OWASP New Jersey Chapter that today includes NYC Metro. In 2007 Brennan was appointed by his application security peers to the OWASP Global Board of Directors. Tom was the managing partner of Proactive Risk that routinely 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. 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. On a Fine Arts Scholarship, she obtained a bachelor of Fine Arts in Graphic Design with a Minor in Professional Writing from Carnegie Mellon University in Pittsburgh, PA. 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 financial services, medical, technology, management consulting, mortgage/banking and retail clients.

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. He has been working in banking and financial industry for the last few years. He is doing his Masters Degree in Artificial Intelligence at Warsaw University of Technology. He is currently working on his final master’s thesis, whose title is “Web Application Penetration Tests”. Right now he is based in London, UK and works for a worldwide financial company. His interests covers all aspects of web security, web development and public speaking. In his free time he enjoys practicing Krav Maga, listening to music and following Web Security news.

Buetler, Ivan

Founder and CEO, Compass Security AG (since 1999)
Founder of Swiss Cyber Storm Security Conference (since 2007)
Founder of Hacking-Lab community site / Alias E1 (since 2006)
Founder and board member of Cyber Tycoons foundation (since 2010)
Board member Information Security Society Swizerland ISSS (since 2010)
Member /ch/open foundation. 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. He provided plans for high-availability Unix and NT server systems including, among other things, a platform for the stock market and foreign exchange dealers based on Reuters, Bloomberg and FIMS (Telekurs). Afterwards, while working for 3r security engineering ag/Entrust Technologies, Ivan supported security consultants in technical matters, analysed clients' technical problems, local network and computer systems throughout Europe. This security work included penetration tests, security reviews, the development of secure architectures, Internet and Intranet security, as well as security solutions for e-Commerce. In particular, he was involved in the cross-certification of the Canadian Entrust PKI with Europe. During these activities he 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. Prior to this 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 Developmer 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. Juan Specializes in: Application Security, Security Source Code Review, Vulnerability assessments, security trends analysis, Penetration Testing, Secure SDLC, App Sec consultancy.

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 Causey 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. Brad currently holds certifications in the following arenas: MCSA, MCDBA, MCSE, MCT, MCP, GBLC, GGSC100, C|EH, CIFI, CCNA,IT Project Management+, Security+, A+, Network+, CISSP, CGSP.

Chalmers, Matthew

Matthew Chalmers 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 and can be reached at matthew dot chalmers at owasp dot org.

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 Cheng 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. The beta version is now available for download and final release date is scheduled on 4th March.

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.

A few of Paulo's OWASP contributions are as follows:

- OWASP Spring of Code 2007,
- OWASP Summer of Code 2008,
- OWASP EU Summit 2008,
- OWASP Assessment Criteria 1.0 & 2.0,
- OWASP 'Project About' Templates,
- OWASP Projects Dashboard,
- OWASP Project Reviewers Database,
- OWASP Training.

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 Corry 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.

Information Security: access controls, disaster recovery, network security, web application security, HIPAA, PCI, application lifecycle, penetration testing, auditing, security research and more.

Information Technology: server administration, hardware/software installation/configuration, help desk/technical support, product evaluation, and more.

Web Application Development: entire development cycle, from design to implementation to quality assurance to deployment.

Specialties: Contributor to HTML5 and WASC Threat Classification v2

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 (hons) from Carnegie Mellon University. She can speak a bit of Portuguese. Sarah has two daughters 7 and 5 with husband Dinis Cruz.

Dawson, Isaac

I am interested in all forms of application/network security. I mainly enjoy trying to think of unique ways of breaking applications from a business logic stand point.
I have published the following papers:
• Blind Buffer Overflows in ISAPI extensions:
http://www.securityfocus.com/infocus/1819 - This article was released on the main page of the leading security news and information site, Security Focus in January 2005.
• The Benefits of Combining Automated and Manual Penetration Testing (Japanese Only): https://www4.symantec.com/Vrt/offer?_requestid=22090&a_id=42747 – This
white paper was written to aid our sales team in educating our customers as to the benefits of combining manual testing with automated tools. I felt that the Japanese market relied too heavily on tool based analysis so the paper was written to show what automated tools cannot find.
Specialties: 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 bussines line for SAIT Zenitel BeNeLux-France (www.saitzenitel.com). I started the Belgian OWASP Chapter in 2005, have started the OWASP Education project and participate in the global chapters committee and the Board of the OWASP Foundation. I co-organize the yearly security & hacker BruCON conference and trainings in Brussels (www.brucon.org). As security project leader and information security officer for multiple customers I have build up extensive experience in Information Security related disciplines, both at strategic and tactical level. I specialise in (Web) Application Security, combining both my 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. Wojchiech's areas of interest include:Security testing management.

- ASVS.
- OWASP Testing Guide, etc.
- Risk assessment vs. (web) applications.
- Security development lifecycle (OpenSAMM).
- Penetration testing & code review.
- Frameworks security.

Wojciech is an OWASP Poland board member, ISMS Lead Auditor / BS7799 certified.

Elias, Wagner

Wagner Elias is the Manager of Research and 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; Events in the management 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 speaking at events like 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 Evans 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

Student at the Chair for Network and Data Security, Ruhr University Bochum Germany.
Research interests include:
- Web Service Security
- Web Service Attacks
- XSS

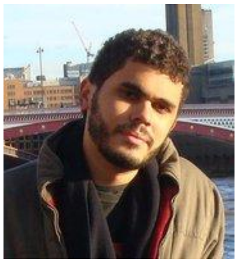
Fazli Azran, Mohd

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).

Ferraz, Felipe



Felipe Ferraz is 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, specially 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 answer 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

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. Experience managing large globally distributed products, currently managing a group split between N. America, Europe, and Asia.
Engineer with the U.S. Government, working on large highly available database applications, with security clearance.
Specialties: Product management, web standards, contract negotiations, security, phishing, malware

Fitzgerald, Alexis

I spent many years on the development side of the fence working on both thick client and web-based applications. That was mainly in the financial sector in Ireland and Switzerland. In the early noughties somebody asked me if I had heard of this thing called "SQL Injection". That was when I began the transition from poacher to gamekeeper, working on the security end of things. I continue to do a good deal of development.
My first contact with OWASP was the AppSec Europe conference at Royal Holloway outside of London in 2005. Since then I have mainly been a consumer of OWASP resources, apart from giving a few talks at various chapter meetings. My goal with OWASP is to help development teams build "enough" security into their projects and to raise general awareness about OWASP and application security. That is why I believe 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

I start working on security stuff at the age of 18 disassembling viruses and helping to develop AV technologies. After that I work as a developer for companies related to the financial industry where I help to develop credit card related applications, home bankings and stuff like that.
Then I move to the administration phase of my life where I work as a security network administrator for the main TMT company of my country.
At the same time I did security research and develop for companies on the United Kingdom and Brasil.
Now I work as a security consultant in Deloitte Uruguay.

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

My name is Julio Cesar Fort, 24, yet another guy living in Recife, Pernambuco, a very beautiful state located in northeast of Brazil. Currently I am an undergraduate student of Computer Engineering at CIn/UFPE (Pernambuco Federal University) and former undergraduate student in Mechanics Engineering at the same university. I was a scholarship holder of CNPq and acted as intern at C.E.S.A.R. learning secure coding techniques in C. I worked, also as intern, in coadmin team at Tempest Technologies, a very nice market-leading company Brazilian information security industry.

Fortuna, Pedro

He 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.

Holds a degree in Computing Engineering and a MSc in Computer Networks. Extensive knowledge and professional experience in R&D projects and software development, both at academic and industrial levels. Teached at the Faculty of Engineering of the University of Porto, and also gave training in computer security. Currently, 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

I have a five years degree in Information System and Computer Engineering (IST - Technical University of Lisbon), being a Oracle OCP (Oracle Certified Professional), about 7 years of experience as Oracle DBA and about 14 years of IT experience. Besides this, through my professional career, I had been in several 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. Helen graduated from Sun Yat-sen University in China. She continued her studies of physics and computer science after she came to the United States. Helen has masters degrees in both physics and computer science. Helen founded the Long Island OWASP chapter in 2006. Besides 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

Information security professional with global experience in diverse environments. I hold a Msc in Information Technology - Information Security by Carnegie Mellon University. I'm currently the Security Practice Leader of Professinal 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 specialises 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 recognised Fortune 500 and FTSE 100 companies including international financial institutions, retailers and multinationals. He has a masters 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 Resende Gomes lives in Brasília, capital of Brazil. He works at SERPRO, Brazilian Federal Data Processing Service, organization that creates and maintains huge computer systems for critical public companies. Leandro works on a security development group, responsible to address corporative security aspects during the SDLC. This group was created in 2006, and they discovered OWASP on that same year. The main contribution to OWASP was the translation of ASVS and QuickRef Guide. The work of this group includes the dissemination of technical orientation, source code analysis and pen testing coordination and definition of security components/frameworks to be adopted.

The last events Leandro participated was BlackHat 2009 conference in Las Vegas, OWASP AppSec 2009 and ICCyber 2010, Brazil. He wrote an article about "Securing web applications with fuzzing tests" for a SERPRO internal conference.

Gondrom,Tobias

Tobias Gondrom is Managing Director of an IT Security & Risk Management Advisory based in the United Kingdom 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 Global Head of the Security Team at Open Text (2005-2007) and from 2000-2004 as the lead of the Security Task Force at IXOS Software AG, he 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 is the 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“ (ISBN 3-87081-427-6).

Hansen, Robert

Robert Hansen (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.

Mr. Hansen 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. He also has briefed the DoD at the Pentagon and speaks at SourceBoston, Secure360, GFIRST/US-CERT, CSI, Toorcon, APWG, ISSA, TRISC, World OWASP/WASC conferences, SANS, Microsoft's Bluehat, Blackhat, DefCon, SecTor, BSides, Networld+Interop, and has been the keynote speaker at the New York Cyber Security Conference, NITES, OWASP Appsec Asia and OWASP Appsec Brazil. Mr. Hansen is a member of Infragard, West Austin Rotary, WASC, IACSP, APWG, contributed to the OWASP 2.0 guide and is on the OWASP Connections Committee.

Hartmann, Kate

Operations Director at OWASP

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

Software Security Consultant, Cigital, Inc.
Kuai Hinojosa has been developing and securing web applications for over a decade. At Cigital, Kuai 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. In addition, He led ITS eServices application security initiatives. Kuai has also worked as a database security administrator in the banking industry protecting company's assets. In his time off, He volunteers his time leading the OWASP Global Education Committee's education efforts and He is a current member of the New York and New Jersey Metro OWASP Chapter board.

Hodges, Jeff

Jeff Hodges is a practicing 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.

In the recent past, 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 has included contributions to the design of the LDAPv3 directory access protocol (in the areas of authentication and security), as well as contributing to 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

***"some"* Security ..** It's difficult to describe my knowledge in the security world without being subjective, hence replace *some* by whatever your feel happy with. The official title on the v-card will be senior security and network consultant, which means something too.

(Short) CV

I'm doing software development since early '80s, used to networking all the time, and focused on web application security starting this millennium. Meanwhile I've seen coming, have evaluated, have configured and used, and have seen disappearing a lot of WAFs and web application security scanners. Founded sic[!]sec GmbH in 2010.

OWASP Activities

- Participating in the German Chapter, German Chapter Board Member
- Project leader, maintainer, developer of OWASP EnDe Project
- Reviewer on some other OWASP projects (SoC 2008)
- CAL9000 (added some en-/decoding and request/response functionality; 2006)
- 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

Principal Architect at SuccessFactors

Jimenez, Juan Jose Rider

CEO at WUL4, Spain
• 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.

Specialties: E-Invoice expert(facturae, etc), PCI-DSS, Security for Web Applications, Web Services, e-commerce, SOA, J2EE,...

Jorge, Eduardo

Kang, Abraham

Work for financial institution in their code review group
Have been working on application security issues for over 8 years (focused on security code review for last 3+ years). Published articles related to enterprise application integration, scalability, and security. Been recently focused on XSS remediation and DOM based XSS. Also interested in Unicode exploits and filter bypassing using character set mismatches. Recently contributed the candidate chapter for Output Encoding for the Web App Security Guide 3.0. 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 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 Knobloch is a independent Security Consultant at http://www.pervasec.nl. In his previous employment at Sogeti Netherlands B.V., Martin founded and lead 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 Kosturjak 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 Koussa 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 Kuivenhoven 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.

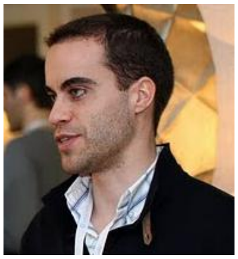
Kumar, Nishi

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

I have a degree in both Multimedia Engineering and Computer Science. My programming language of election is PHP and on a daily basis I am an IT Consultant and CIO / partner at Mipe / Lusolabs, Portugal. Currently, I am working on OWASP Academies project. For the last 7 years I have been teaching IT and this is an activity that I really enjoy. Apart from that, I am a passionate person that just loves Technology and extreme sports such as white water kayak!

Lauritão, Rogério Paulo Vicente



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. Heavy involvement in the Open Web Application Security Project (OWASP) Foundation including:

- 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 Lindsay 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 Long 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, he is 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 uses to have regular presentations at various worldwide security conferences (in Netherlands, Luxembourg, Berlin, Warsaw, Krakow, Prague). 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.

He 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.

At this time 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. For more information, please see http://www.manico.net. Jim has also provided Application Security Developer Education services for Fortune 10, Government, and NGO Institutions.

Maor, Ofer

CTO, Hacktics, Chairman, OWASP Isarel -- 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

Degree in Economics and large experience in finance, trading and derivatives. Later I joined this experience with ICT matters; and now after having worked for some years for Getronics both in Italy and in worldwide groups, now I lead in Business-e e the consulting team of about 25 persons.
Main activities are in Governance, Audit and Ethical hacking with a group of 10 testers.
My main certificates are Cisa, Lead auditor ISO27001, Itil v3, CRISC , Cobit

Martinez, Mateo

Mateo has many years of experience in a variety of challenging 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, where he oversees 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. In addition to his CISSP, Mateo has BCP and Information Security projects executed in Chicago, US and in Dubai, UAE. Previously he worked for PricewaterhouseCoopers as a Senior BCP Consultant.

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 cofounder 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 is the President of the FIST Conferences board, and in the past taught Ethical Hacking at the IT Security Master of La Salle University.

Matatall, Neil

Neil Matatall is a Consultant for FishNet Security as part of the Applicaiton 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

I'm the CTO at DRI, a Portuguese company focused on on open source environments. I have +10 years working with Linux and open source technologies like PHP and Mysql. I've been involved on 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

I've worked in the security area for a few years, mostly in network security doing traffic analysis and network reverse engineering. I'm a member of the Portuguese Honeynet Project and I'm currently working for SAPO, which is the most visited site in Portugal, in the Web Security team.

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; contributer 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

In October 2010 Sandra assumed the position of OWASP Training Manager, where she was responsible for managing the OWASP ‘Chapter-lead’ Training activities and building the concept of 'OWASP Academies'. Prior to this work with OWASP, Sandra was 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. Before joining Mergermarket, she worked for two years at Dealogic on the Mergers & Acquisitions and Loan Markets products. 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 teaching Math and Statistics and also, for 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)

Dr Konstantinos Papapanagiotou 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

Strategist for corporate events and social events at Anggulo Eventos

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.This week, she's on the support team for the OWASP summit, helping out with 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. Additionally, Ralf has worked on numerous reports, guidelines and policies for big customers on topics such as awareness, counter measures, secure coding, and secure deployment.

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 collegue 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 Rohr 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 Ross 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

GSM, UMTS (UTRAN)
Requirement definition for PM counter based on customers requests, field demands and 3GPP standards.
KPI (metrics) definition for network supervision, network optimization, trouble shooting.
PM OAM definition and support.
Technical customer negotiations and support.
Evaluation of measurement / KPI results.
Specialties: Requirement definition, 3GPP standards, XML, DOORS

Saario, Mikko

Currently a Sr Specialist at Nokia Corp in Finland
* Working in a complex and diversified mobile/web environment.
* Member of the board (in 2007) in the Finnish Information Security Association i.e. Tietoturva ry (www.tietoturva.org).
* Founded and chaired the OWASP Helsinki Chapter (www.owasp.org).

Samuel, Michael

Mike Samuel 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 implementors 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

I am a professional web application developer, and have 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 my 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.

Schuh, Justin

I've held a variety of different positions across the IT spectrum, with most of my time focused on the security side of the industry. I like interesting technical challenges solving unique problems.

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

Application Security Specialist - Trustwave

Serrao, Carlos

Assistant Professor at ISCTE-IUL (Lisbon University Institute)/SoTA (School of Technology and Architecture)/DCTI, where I teach several subjects related to Information Systems, Information Security, IT/IS Project Management and Entrepreneurship (both on BSc and MSc programs).
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.
OWASP.PT leader. Currently working to evangelize OWASP good practices and OWASP mission in improving the web applications security.
Author. I'm the author and co-author of several articles published on scientific conferences, proceedings, journals and project deliverables. Also the co-author of one of the best selling portuguese books about PHP programming. Geek. Love technology. Huge fan of gadgets.
OS agnostic. Linux, Mac OS X, Windows. Bring them all!!!

Stasinopoulos, Anastasios

Anastasios Stasinopoulos is a Certificated Network Administrator of CompTIA (Computing Technology Industry Association) computer-security enthusiast and also a hobbist penetration tester. He is basically deals with Networking and Data Communications, Security as Fedora Security Spin Contributor (http://fedoraproject.org/wiki/Security_Lab) 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 Sterne is the Security Program Manager at Mozilla where he works on security releases and designs and implements browser security features.

Steven, John

John Steven 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 Su 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, ten years on, 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 internationalisation 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 - Vehbi 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 has 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

Mr. Taylor is the Chief Technology Officer at Secure 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. Mr. Taylor 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, Mr. Taylor 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.

Mr. Taylor is an external reviewer, contributor and primary author for Microsoft patterns & practices security guidance. He has published several whitepapers including "Web Services Risk Assessment and Recommendations" and "Security Threats: Risks, Protection & Limitations" for CIO Update. He is co-author of "Team Development with Visual Studio Team Foundation Server" and "Improving Web Services Security" with J.D. Meier of Microsoft. Mr. Taylor received his C.S. degree from Montana State University.

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 a 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.

Industry designations include the Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH). Matt Tesauro has a B.S. in Economics and a M.S in Management Information Systems from Texas A&M University.

Thomas, Mark

Mark Thomas 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, United Kingdom.

Tomhave, Benjamin

Ben Tomhave 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.
Some of his achievements include:

- Representing Boeing at the International Committee for Information Technology Standard's cyber security technical committee.
- Representing the United States as a delegate to the International Standards Organization's (ISO) sub committee on cyber security.
- Joining the national Software Assurance (SwA)Working Group
- Serving as the Director of the HPPV Northwest regional engineering competition.
- Working with college engineering education, which led to a 2005 national award from the American Society of Engineering Education.
- Leading the OWASP project on secure coding practices
- Presenting on Building Security Assessment at OWASP AppSec USA 2009

UcedaVelez, Tony

Develop and lead 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.

Specialties - 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

Senior Security Consultant Greece at Atos Origin

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 Sweeden (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 Vilares da Silva worked in the Portuguese central statistics office (INE) as systems and network engineer, software engineer from 1990 to 1999. Worked as a webmaster, web developer and software engineer in the European police office (EUROPOL) in The Hague from 1999 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 some 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 Organisation 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 a 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, a 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. Working for KPMG Management Consultants as Knowledge & IT Expert gave him the opportunity to solve all kinds of IT, Knowledge Management and other Business and IT related issues. 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. His previous employers include IBM, TreeStar Automation, KPMG MC, Arthur D. Little.

Ferdinand enjoys sailing, skiing and car mechanics.

Watson, Colin

Colin Watson 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 contributes to a number of OWASP projects 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

Information Security consultant continuously since 1989. Current focus area is in Application Security Consulting, including 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. Particular expertise in Security of Web Applications.

Currently member of the OWASP Board, the OWASP Conferences Chair, and coauthor and project lead of the OWASP Top Ten Most Critical Web Application Security Vulnerabilities (http://www.owasp.org/index.php?Top10).

Early career focused on InfoSec for DoD, including C&A, Trusted Product Evaluations, Multilevel Security, and Cross Domain Solutions (e.g., Guards) for product vendors, large DoD integrators, and the NSA.

Specialties - Application Security Consulting (specialty focus on Web Application Security), Information Security, Certification & Accreditation, Multilevel Security, Cross Domain Solutions (Guards), Secure Software Development in Java

Wilander, John

John Wilander 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 Williams 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 Wilson 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. Mike brings 12 years of security, technology, and business experience to Intrepidus Group. He has attained the CISSP certification, and is a co-leader of the OWASP Mobile Security Project.