OWASP

The Open Web Application Security Project

Annual Report 2009

OWASP Annual Report

2009

"The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit worldwide charitable organization focused on improving the security of application software. Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. "

OWASP AppSec DC 2009 Conference

Jeff Williams, OWASP Board Chair

The OWASP Mission

First I'd like to introduce the OWASP Board

Tom, Dave, Dinis, Seba, and myself

The board runs the OWASP Foundation, the 501c3 nonprofit which provides support for all the activities that happen at OWASP. Like all the people involved in OWASP, we volunteer our time to make the project a success. I'd like to take this opportunity to thank each of you for all the hard work you do to make OWASP a success.

If you combine all the materials available through his program and what's available at OWASP, we've got ALL the right stuff out there. But we are still losing ground.

For years, we have watched as the software market fails to produce secure applications.

Increasingly, this situation is worsening and there are two key factors. First, the reliance that we put on our software infrastructure increases every day. Application software controls our finances, healthcare information, legal records, and even our military defenses. Secondly, application software is growing and interconnecting at an unprecedented rate. The sheer size and complexity of our software infrastructure are staggering and present novel security challenges every day.

While we have made some progress in security over the last decade, our efforts have been almost completely eclipsed by these factors. The software market and security experts still struggle to eliminate even simple well-understood problems. Take cross-site scripting (XSS) for example. In the last decade, XSS has grown from a curiosity to a problem to an epidemic. Today, XSS has surpassed the buffer overflow as the most prevalent security vulnerability of all time.

It's the same for SQL injection. And CSRF will follow the same pattern too.

These problems, while technically simple, have proven extraordinarily difficult to eradicate. We can no longer afford to tolerate software that contains this kind of easily discovered and exploited vulnerabilities. Read about the RBS WorldPay attack – the level of coordination and sophistication required to pull off this attack are stunning.

In addition to risks like this, we are already seriously limiting innovation in the development of applications that can improve the world.

Why doesn't the software market produce secure software?

It's possible that the risks we focus on are overblown and that the market is actually working to produce an optimal level of security in our applications. But the other possibility is that the software market is broken. Despite what you might hear in economics class, markets are not perfect. They have failures like monopolies, price-fixing, and speculative bubbles.

One classic market problem was detailed in a Nobel Prize winning paper by George Akerlof called "The Market for Lemons." Basically he showed that when sellers have more information than buyers – like when you're selling your used car that barely runs – buyers will discount the price they're willing to pay. That means people with good cars can't get a fair price and so they won't sell. And that means you can only buy lemons in the used car market.

Now think about that for software. Buyers really can't tell the difference between secure software and insecure software. So they're not willing to pay more for security.

We need radical innovative ideas to fix the software market. We are not going to "hack our way secure" – it's going to take a culture change.

The automobile industry made the change over at 30 year period after Ralph Nader exposed the industry….and today we have cars that have safety features. The food industry made the change but only after the FDA started the Nutrition Facts program. Even the cigarette industry has been dramatically changed through campaigns like the "Truth…" campaign.

The OWASP mission is to make application security visible. Creating transparency goes directly to the heart of what is wrong with the software market and has the potential to actually change the game.

Why is OWASP the right approach?

OWASP is a worldwide free and open community focused on improving the security of application software. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

In many ways, we're like public radio. This allows us to reach a very broad audience and it makes it possible for us to avoid difficult commercial relationships that influence our activities. This freedom from commercial pressures allows us to provide unbiased, practical, cost-effective information about application security.

I believe this objectivity is absolutely critical. For too long, much of the application security information in the market has come from people selling stuff, and our message has been lost.

What is OWASP doing?

In November 2009, OWASP Leaders from around the world got together to discuss our progress and set our priorities for 2010. Each of our Global Committees reviewed their accomplishments and we discussed OWASP's agenda for the future. We just established these committees in 2008 and they are already making huge progress establishing the foundation needed to achieve OWASP's mission.

I'd like to encourage all of you to figure out something you can do to change the culture in your team, company, or industry. In this organization are some of the greatest minds in application security. I challenge you to focus your efforts on those things that will actually change the world and allow us to fulfill the potential of what we can achieve with software.

New OWASP Board Members for 2010

At the 2009 Global Summit OWASP members voted in two additional OWASP board members. Matt Tesauro and Eoin Keary.

Matt Tesauro

OWASP Live CD Project Lead

OWASP Global Projects Committee Member

OWASP Testing Guide classes (3)

OWASP Podcast “roving reporter”

Eoin Keary

OWASP Ireland Chapter leader & Founder since 2004

OWASP Testing Guide leader (2005-2007)

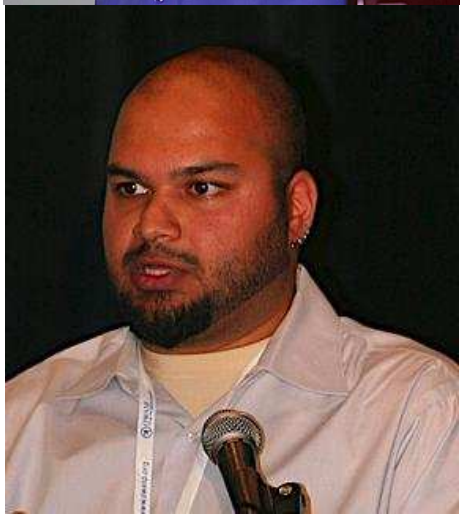
Code Review Guide (V1.1) leader

OWASP ASVS Reviewer

OWASP SAMM Contributor

OWASP Ireland 2009

The following National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice were released in 2009 and reference OWASP



- The CIS Security Metrics - Consensus Metric Definitions
- Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing (2 versions)
- Club de la Sécurité de l'Information Français (CLUSIF), France, Sécurité des applications Web, Comment maîtriser les risques liés à la sécurité des applications Web?
- Defense Information Systems Agency (DISA), USA, Application Security and Development Checklist
- European Network and Information Security Agency (ENISA), Cloud Computing Risk Assessment
- Federal Chief Information Officers (CIO) Council, USA, Guidelines for Secure Use of Social Media by Federal Departments and Agencies
- GovCertUK, UK, SQL Injection
- Ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire, France, Guide de réalisation Java
- Ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire, France, Guide de réalisation PHP
- National Institute of Standards and Technology (NIST), USA, Framework and Roadmap for Smart Grid Interoperability Standards
- National Institute of Standards and Technology (NIST), USA, Interagency Report 7628 (draft) - Smart Grid Cyber Security Strategy and Requirements
- National Security Agency/Central Security Service, USA, Manageable Network Plan

Further details at http://www.owasp.org/index.php/Industry:Citations

OWASP by the Numbers

The OWASP worldwide community is growing rapidly:
There are **21,000** people who are actively involved with OWASP. These are the people who attend chapter meetings, participate in mailing lists, and have accounts on our wiki.
There are **326** OWASP mailing lists (projects, committees, events and chapters)

- **7** Global Committees
- **39** Committee Volunteers
- **159** chapters
- **117** projects
- **17** OWASP Books
- **18** full day or multi-day events and conferences around the world
- **3** employees (Kate, Paulo & Alison)

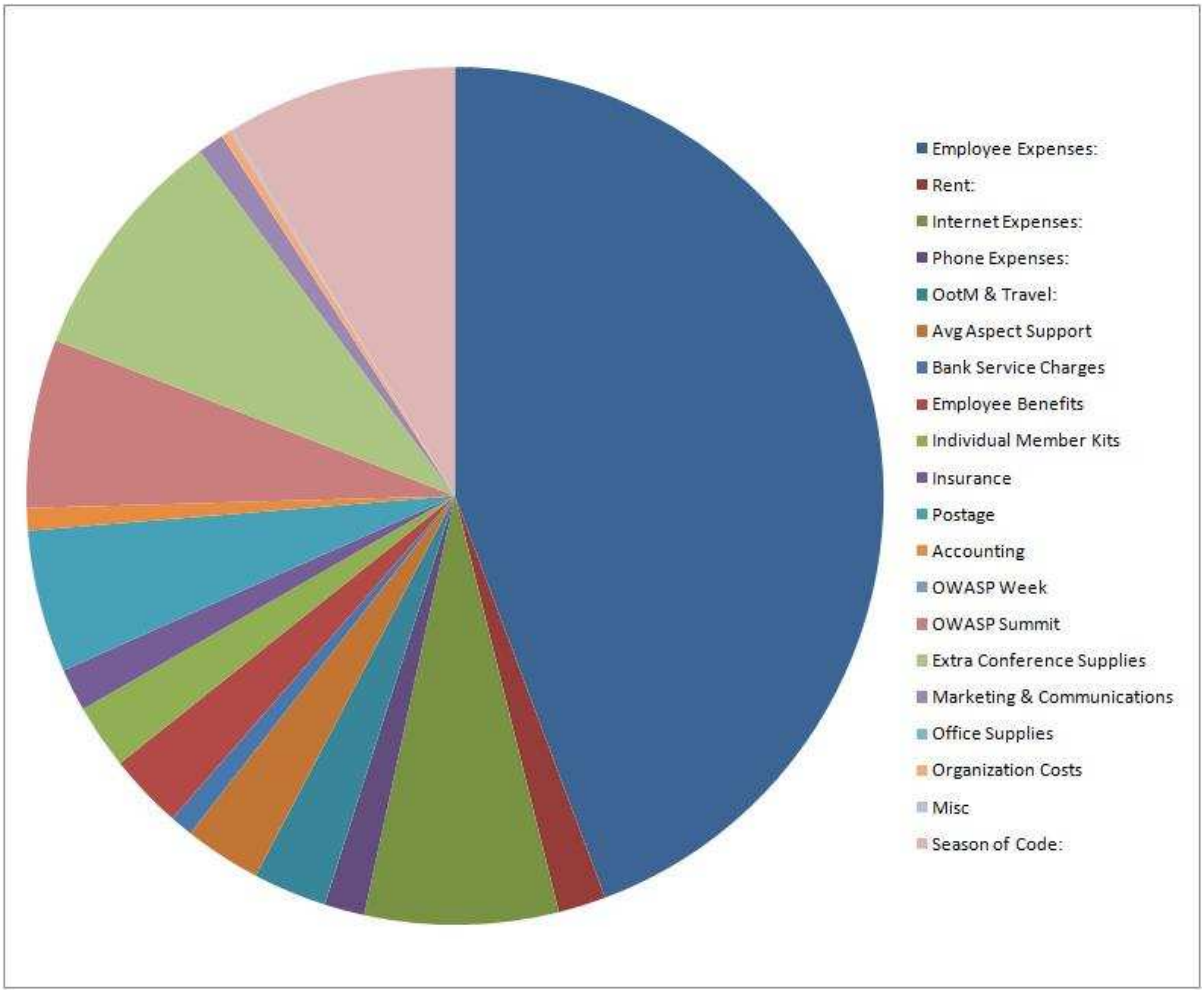
Wiki Page edits since the wiki was set up: **76,865** and **6,381** articles

OWASP is the largest knowledgebase of application security information anywhere.

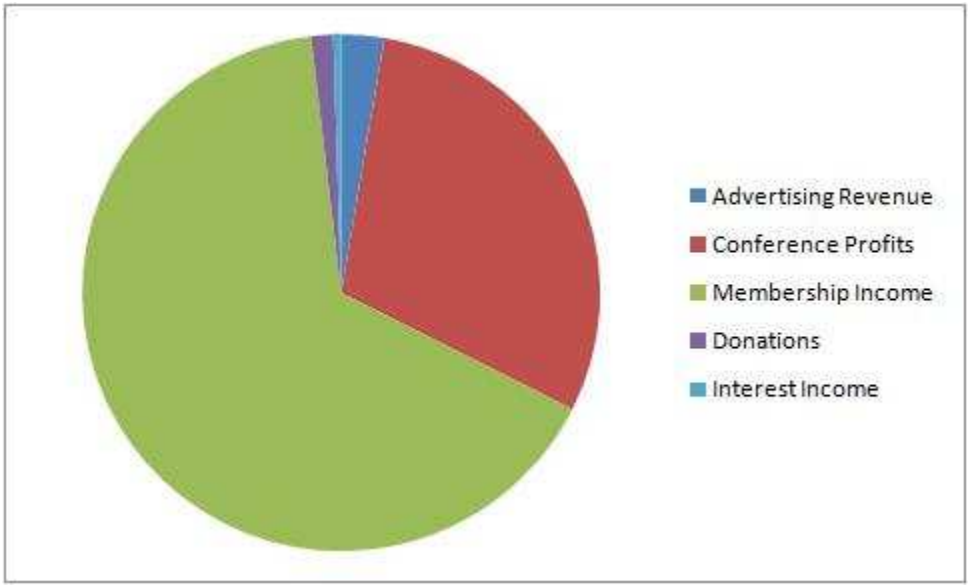
With an average of **200** updates to the wiki everyday. Over **100,000** page views per week. Total views: **31,903,633**

OWASP Foundation 2009 Financials

2009 Expenses $299,445.04



2009 Income $204,089.21



http://www.owasp.org/index.php/File:2009_Final_Numbers.xlsx

OWASP as an authoritative reference for web application security

OWASP continues to be referenced as the leading authority on web application security. OWASP begun maintaining a record of important references to OWASP and its resources. A number of OWASP projects maintain their own lists of citations, quotations, recommendations, testimonials and users, and but this process has so far identified 48 national & international legislation, standards, guidelines, committees and industry codes of practice which reference OWASP. The oldest sources found are some Japanese government documents from 2002, and include well-known references such as requirements from the Payment Card Industry Security Standards Council (PCI SSC) in the 2006 and 2008.

- A quarter of the citations relate to documents issued during 2009-2010 that show an increasing diversity in organizations and subject matter:
- Center for Internet Security (CIS), The CIS Security Metrics - Consensus Metric Definitions
- Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing (2 versions).
- Club de la Sécurité de l'Information Français (CLUSIF), France, Sécurité des applications Web, Comment maîtriser les risques liés à la sécurité des applications Web?
- Defense Information Systems Agency (DISA), USA, Application Security and Development Checklist.
- European Network and Information Security Agency (ENISA), Cloud Computing Risk Assessment.
- Federal Chief Information Officers (CIO) Council, USA, Guidelines for Secure Use of Social Media by Federal Departments and Agencies.
- GovCertUK, UK, SQL Injection.
- Ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire, France, Guide de réalisation Java.
- Ministère de l'Écologie, de l'Énergie, du Développement durable et de l'Aménagement du territoire, France, Guide de réalisation PHP.
- National Institute of Standards and Technology (NIST), USA, Framework and Roadmap for Smart Grid Interoperability Standards.
- National Institute of Standards and Technology (NIST), USA, Interagency Report 7628 (draft) - Smart Grid Cyber Security Strategy and Requirements.
- National Security Agency/Central Security Service, USA, Manageable Network Plan.

Further details at:

http://www.owasp.org/index.php/Industry:Citations

OWASP will continue to maintain this record and plans to document testimonials from individuals in a wide range of business sectors.

2009 Global OWASP AppSec Events

OWASP AppSec Australia 2009
February 25th-27th, training & conference, Gold Coast Convention Center, QLD Australia

OWASP AppSec Europe 2009
May 11th-14th , 3 track conference and 8 tutorials, Part In Hoetl, Krakow, Poland

OWASP AppSec Ireland 2009
September 2009, conference and tutorials, Trinity University, Dublin, Ireland

OWASP AppSec Brazil 2009
October 27-30th, Conference and tutorials, Camara dos Deputados, Anexo II, Praca Dos Tres Poderes

OWASP AppSec US 2009
November 10th-13th, Conference and tutorials, Walter E Washington Convention Center, Washington, D.C.

OWASP AppSec India 2009
November 17th-20th, New Delhi, India

OWASP Global Summit
November 11th, 2009
Walter E. Washington Convention Center, Washington, D.C.

Regional and Local OWASP Events for 2009:
March 13, 2009 - **OWASP Software Assurance Day DC 2009,** McLean, VA USA
March 2009 - **Front Range OWASP Conference 2009 (aka SNOWFroc),** Denver, CO USA
February 23, 2009 - Feb 23rd - **OWASP Day III: "Web Application Security: research meets industry"** - Bari (Italy)
July 13 2009 - **OWASP New Zealand Day 2009** – Auckland, New Zealand
August 24, 2009 **Minneapolis/St Paul half day event** Minneapolis, MN USA
August 26, 2009 - **AppSec Academia Symposium** Irvine, CA USA
October 12-13, 2009 - **German Conference** Nurnberg, Germany
October 28-29 2009 - **4th annual Rochester Security Summit** Rochester, NY USA
November 6, 2009 - **Italy OWASP Day 4** Milan, Italy
December 2, 2009 - **BeNeLux Day** Belgium
December 10-11, 2009 - **IBWAS '09** Madrid, Spain

OWASP TOP 10 FOR 2010

Will You Help Us Reach Every Web Developer in the World?

Columbia, MD 4/19/2010 —

Since 2003, application security researchers and experts from all over the world at the Open Web Application Security Project (OWASP) have carefully monitored the state of web application security and produced an awareness document that is acknowledged and relied on by organizations worldwide, including the PCI Council, DoD, FTC, and countless others.

Today, OWASP has released an updated report capturing the top ten risks associated with the use of web applications in an enterprise. This colorful 22 page report is packed with examples and details that explain these risks to software developers, managers, and anyone interested in the future of web security. Everything at OWASP is free and open to everyone, and you can download the latest OWASP Top 10 report for free at:

http://www.owasp.org/index.php/Top_10

The time has come to get application security awareness out of the security community and directly to the people who need to know it most. This year, our audacious goal is to get the OWASP Top 10 into the hands of **every web developer in the world** – but we need your help. We ask anyone reading this; would you be willing to do one simple thing to help protect the future of the Internet? If you know people who write code for the web, could you forward them the OWASP Top 10 and ask them kindly…

Are you familiar with all of the risks in the OWASP Top 10?

Will you make a commitment today to protect your code against the OWASP Top 10?

For too long, many organizations have relied exclusively on an occasional scan or penetration test to gain assurance for their internal and external web applications. This approach is expensive and doesn't provide much in the way of coverage. Like other types of security, application security requires a risk management program that provides visibility across the entire portfolio and strategic controls to improve security. If your organization is ready to tackle application security, there are dozens of free books, tools, projects, forums, mailing lists, and more at OWASP. You can also join one of over 180 local chapters worldwide or attend our high quality and inexpensive AppSec conferences.

The OWASP Top 10 for 2010 are:

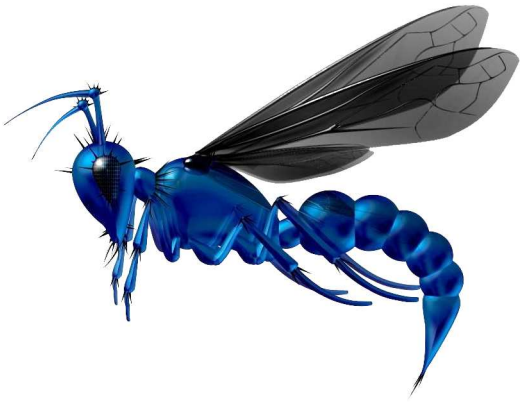
A1: Injection
A2: Cross-Site Scripting (XSS)
A3: Broken Authentication and Session Management
A4: Insecure Direct Object References
A5: Cross-Site Request Forgery (CSRF)
A6: Security Misconfiguration
A7: Insecure Cryptographic Storage
A8: Failure to Restrict URL Access
A9: Insufficient Transport Layer Protection
A10: Unvalidated Redirects and Forwards

The 2010 update is based on more sources of web application vulnerability information than the previous versions were when determining the new Top 10. It also presents this information in a more concise, compelling, and consumable manner, and includes strong references to the many new openly available resources that can help address each issue, particularly OWASP's new Enterprise Security API (ESAPI) and Application Security Verification Standard (ASVS) projects.

Global Industry Committee

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

Goals



The Global Industry Committee (GIC) was formed during the summit in Portugal in November 2008. Its mission is to expand awareness and advance the inclusion of application security best practices in the public and private sectors, including professional associations, trade bodies and standards organisations. The committee also aims to become a voice for these external organisations within OWASP, promoting their views and requirements to the Board, committees, project leaders and other OWASP participants.

To accomplish this, the GIC undertakes outreach work including presentations, contribution to other organisation's work and collaborative efforts where these can be identified and resources are available.

Achievements during 2009

During 2009 the GIC undertook 19 outreach actions, led or assisted with responses to 9 draft guidance documents, discussion papers and standards, and began to document resources elsewhere that reference OWASP and its projects. This has raised OWASP's profile and exposed new people to its efforts and materials. Most members of the committee were also heavily involved with conferences described elsewhere and running local chapters.

Objectives for 2010

At the start of 2010 the GIC has been joined by three new members and a new board representative Dave Wichers.

The GIC is looking to take a more pro-active role in reaching out to non-IT and non-security people in sectors such as:

- Energy
- Medical
- Financial
- Government

In particular, the GIC plans to create new, and nurture existing, relationships between OWASP and other organizations, especially with organizations that have some participation within OWASP already.

The GIC will continue to promote OWASP's projects and resources to a wider community. It will also identify and facilitate working with other organizations and contributing to their initiatives where suitable opportunities exist.

2009 OWASP Global Projects Committee

The Global Projects Committee was created during the OWASP EU Summit in Portugal 2008. The primary mission of the committee is to oversee the prioritization and execution of current projects, support and provide direction for new tools and documentation, and foster a community that facilitate contributions from OWASP community members and adoption of OWASP Projects by the global community at large. At the end of the 2009, OWASP had 86 active projects and 17 orphaned projects.

In 2009 the committee focused on the following goals:

Inventory existing OWASP projects
The Projects Committee solicited OWASP project leaders through the OWASP Projects Spring 2009 Self Update survey to identify existing projects and their statuses, details, licenses, and availability. The survey also asked leaders to self assess their status as an OWASP project. The effort obtained 61 responses and the responses were used to populate the OWASP projects metadata.

Identify orphaned and inactive projects for adoption
The Projects Committee took the results of the OWASP Projects Spring 2009 Self Update survey and followed up with 51 projects leaders that did not reply to the original survey. Of these projects, 27 projects remained inactive or abandoned after attempts to follow up with the project leader. These "orphan" projects were advertised to OWASP leaders for adoption. Of these projects, 10 have been or are in the process of being adopted by new leaders.

Establish Project Assessment Criteria and apply to existing projects
One of the long term visions of the Projects Committee is to establish consistent quality across OWASP's entire portfolio of projects. To that end, the Projects Committee created the Project Assessment Criteria v2. This criterion is an extension of the existing Project Assessment Criteria that were previously applied to Season of Code projects. The biggest addition to the Project Assessment Criteria v2 is the separation of the assessment of the quality of individual project releases and the overall health and activity of a project as a whole. The Projects Committee has started an ongoing effort to apply the new Project Assessment Criteria v2 to all OWASP projects.

Establish Season of Code and OWASP Grant Framework
In 2009, the OWASP Board elected to alter the traditional strategy of the Season of Code to support development of OWASP projects. To facilitate this shift, the Projects Committee was delegated the task of establishing the framework for OWASP grants, including Season of Code grants. While the 2009 Season of Code was not launched, the framework was created and leverages the Project Assessment Criteria v2 as a means of establishing accountability and progress.

Integrate Project Assessment metadata into OWASP website
Another long term vision of the Projects Committee is to improve the brand quality and presence of the OWASP project pages and OWASP website in general. The Projects Committee has taken the first steps towards this goal by creating wiki-templates with associated Project Assessment metadata. These templates help establish a consistent look and feel and aid potential OWASP users to easily find key details about OWASP projects. The majority of the core wiki-templates are complete and integration into existing projects pages will commence shortly.

In 2010 the Projects Committee plans to:

- Integrate all remaining Project Assessment metadata into OWASP project pages
- Redesign the OWASP projects page and related web pages with dynamic, metadata driven content in order to: simplify navigation of the OWASP projects portfolio, establish look-and-feel consistency of OWASP projects, and create an incentive for project leaders by awarding rotating high-profile status in the OWASP projects page for top projects
- Investigate the usage of a centralized OWASP project repository for all OWASP projects
- Continue soliciting leaders to adopt orphaned OWASP projects
- Launch and administer future Seasons of Code as conditions merit

2009 Global Membership Committee

The Global Membership Committee was created during the OWASP EU Summit in Portugal 2008. The primary mission of the committee is to recommend policies, procedures, and strategies for increasing the value of OWASP membership to individuals and organizations and enhancing the membership in OWASP both numerically and qualitatively. Current committee members are Sebastien Deleersnyder (Board Representative, Belgium), Dan Cornell (Chair, US), Michael Coates (US), Stephen Craig Evans (US), and Kate Hartmann (Operations Director, US). At the end of the 2009 calendar year OWASP had 770 individual members and 27 organizational supporters. In 2009 the committee focused on the following goals:

- Rework and streamline the membership model
- Re-evaluate the benefits OWASP provides to members

In order to rework and streamline the membership model, the number of classifications of member types was reduced to three: Individual membership who pay $50/year, Organization Supporters who pay $5,000-/year and University Supporters who pay nothing, but provide meeting space for OWASP events. Previously there were several different classes of organizational supporters based on the size and mission of the organization.

The benefits were updated so all new individual members receive a membership pack with OWASP materials such as a membership card, OWASP book, OWASP DVD, and other OWASP-branded tchotchkes. Organization supporters receive a month's worth of banner advertising on the OWASP site, get a company logo on the OWAPS Members page, and have access to the OWASP Job Board.

In addition the Membership Committee set up and ran the 2009 election for two new board members that was initiated at the Summit prior to AppSec DC. This election resulted in the selection of Matt Tesauro and Eoin Keary to join the OWASP Board.

In 2010 The committee plans to:

- Implement a program to communicate with all organization supporters once per quarter
- Provide materials to chapter leaders to help them identify and recruit additional individual members, organization supporters, and university supporters
- Clarify how organization supporter can have their support provided to specific projects
- Increase the individual member count to 1500
- Retail all current organization supporters and increase the total count to 35
- Generate $250,000 in revenue for OWASP via membership fees (this money will be split 60/40 between OWASP and the originating chapter)

2009 Global Education Committee

The Global Education Committee was created during the OWASP EU Summit in Portugal 2008. The primary purpose of the Global Education Committee is: to work with the OWASP Education Project to provide educational materials for both internal and external users, develop liaisons with educational institutions worldwide.

Mission

Provide awareness, training and educational services to corporate, government and educational institutions on application security.

Vision

Make OWASP educational material globally available as a well known resource in easily consumable form mapped to a framework tied specifically to user roles and responsibilities

The Global Education Committee continues to make an impact in our OWASP community by earning the support of academic institutions at the local level and around the world. This year to mention a few new EDU supporters we have: NYU-Poly, Rutgers (our thanks to Rutgers university and the local NYC/NJ Metro chapter for making this possible), ISCTE-IUL (thanks to Carlos Serrao and OWASP supporters in Portugal) and ISEP (our thanks to Sebastien Gioria in France for making this possible). It is also worth mentioning that will soon announce the support of new EDU supporters. In addition, we are working in a few efforts to provide training days and training materials at the location of some of the EDU supporters mentioned above.

Nishi Kumar project leader of the Computer Based Training Project and Kuai Hinojosa one of CBT's project contributor have been working in organizing a set of training materials that can be easily downloaded and provide a great format for an OWASP training session. This was a result of Dinis and the London's chapter efforts to offer an OWASP Training day base on all OWASP training materials such as: An OWASP Tour, the OWASP Top 10, Testing Guide, Code Review Guide to mention a few.

Sebastien Gioria, Cecil Su and Carlos Serrao have been leading the translation of guides such as the OWASP Top 10 in languages such as French, Portuguese, Chinese, Taiwanese and some other Asian languages. They both are also working on organizing local events.

Kuai Hinojosa will be delivering an OWASP tour at the next EDUCAUSE Security Task Force meeting in May 30th (for more information about this group see http://www.educause.edu/security). He started working on gaining support from this group and opening channels in the academic community at the local and global level.

Martin Knobloch and Fabio Cerullo continue to lead efforts in Europe participating and helping organize events such as the IBWAS (AppSec Iberia conference) event organized by Carlos Serrao and Vicente Aguilera.

Our committee continues to face the challenge of meeting regularly due to having one of the largest and most diverse committees. It has been difficult to meet with so many different time zones therefore our new strategy will be to split our meetings in two regions, Europe and Asia lead by Martin and the American Region lead by Kuai Hinojosa. Our main focus for this year is to continue to build relationships and the right channels to get the support of the academic community, and work with the education project to build and improve training resources and initiatives to educate others. For more information about the Global Education Committee see: http://www.owasp.org/index.php/Global_Education_Committee

2009 OWASP Global Conferences Committee

The Global Conferences Committee was created during the OWASP EU Summit in Portugal 2008. The primary mission of the committee is to determine location, frequency and to oversee and direct global conferences, speakers and training. Current committee members are Eoin Keary (Board Representative, Ireland), Mark Bristow (Chair, US), Kate Hartmann (Operations Director, US), Wayne Huang (Taiwan), Dhruv Soi (India), John Wilander (Sweden) and Lucas Ferreira (Brazil). In the 2009 calendar year we hosted 18 OWASP events! In 2009 the committee focused on the following goals:

- Establish standard guidelines for conference chairs to follow when planning events

In order to have a cohesive understanding across the organization, the committee started out by defining the three different types of OWASP events: AppSec Conference, Regional Conference, and an OWASP Event. These definitions are critical to setting expectations for the different types of events that take place with the OWASP brand. The committee also revamped the OWASP How to Host a conference page. The new page includes a tabbed layout to make it easier to find the relevant information. One critical addition to the page is the Conference Planner's Toolkit. This tab includes a brand new Budget Tool, revised Sponsorship Document, standardized call for papers and call for training provider templates, a training provider agreement, a speaker's agreement, and a standard presentation template.

Identify budget guidelines for conference chairs to follow

In 2009 the committee released the OWASP Conference Budget Planning Tool. The initial version of the tool was piloted for the 2009 AppSec DC conference. Budget tool 2.0 will release 2010. We also established a new profit sharing model with the local chapter so that 30% of the revenue from the events will be distributed to the local chapter to continue local evangelism efforts.

Create a sponsorship package

A brand new, revamped sample sponsorship package was developed in 2009. This new package includes a more attractive design and a standard set of sponsorship levels to promote consistency for our sponsors across events.

Examine current conference planning tool (Cvent) and determine plan for 2010

The committee conducted an evaluation and decided that OWASP will continue to use CVENT then migrate to salesforce when the application is ready and thoroughly tested.

In 2010 The committee plans to:

- Centralize management of all OWASP events via the conferences committee
- Completely revisit the How to Host a Conference page content
- Further relationships with other like minded organizations and perhaps host some joint events
- Release in Q1 2010 a 2011 Call for AppSec Conferences
- Investigate the possibility of creating sponsorship packages for corporations
- In conjunction with the education committee create an OWASP Training Roadshow
- Work with the education committee to evaluate the training and presenter resources available to the OWASP community

2009 OWASP Global Chapter Committee

With 163 chapters worldwide, chapter activity is one of the important foundations of OWASP, being the link between the OWASP core members and security and IT practitioners around the globe. To that end, the Global Chpater Committee is committed to supporting local communities to start and operate a successful OWASP chapters. As the outreach of OWASP chapters is large, the Global Chapter Committee must also set guidelines and exercise governance that will ensure that OWASP goals and values are maintained while not limiting the open source spirit in which chapters operate.

Current committee members include Tom Brennan (Board Representative, USA), Ofer Shezaf (Chair, Israel), Matthew Chalmers (USA) and Puneet Mehta (India) and Kate Hartmann (OWASP Operations Director, USA)

In 2009 the committee focused on:

- Creating formal guidelines for chapter activity.

Restarting dormant chapters by or locating new leadership.

To facilitate these goals the committee has created the chapter handbook which includes chapter rules and useful information for chapter leaders. The committee has also performed a chapter survey to learn about the needs of chapter leaders and find dormant chapters.

In 2010 The committee plans to focus on providing tools for chapter leaders to help in making chapters mode successful and easier to run, including tools for setting up and running meetings, a repository of presentations for chapter meetings and matching speakers to events. Additionally the committee will work to find geographical areas that are not covered today by OWASP and look for leaders to start chapters in the area.

Global Connections Committee

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

Goals

The Global Connections Committee (GCC) was formed during the summit in Washington DC in November 2009. Its mission is to expand awareness and advance the understanding of the OWASP foundation. The committee also aims to become a voice for the OWASP Global Committees within OWASP and externally to the population in general.

To accomplish this, the GCC has set forth several goals to attain during 2010.

Objectives for 2010

- Help facilitate an increase in growth of the OWASP foundation through increased membership, sponsors, media recognition and conference involvement.
- Broaden the acceptance of OWASP through greater participation at non-OWASP conferences.
- Increase awareness of OWASP among the developer community.
- Release an updated OWASP.org website which is more user friendly.

At the start of 2010 the GCC has kicked off with new members: Lorna Alamri, Justin Clarke, Robert Hansen and Jim Manico. Board members are Dinis Cruz and Tom Brennan.

The GCC responsibilities include:

- Making connections between the OWASP Community and the materials it creates
- PR and Promotion of the OWASP Foundation, projects and events
- OWASP Newsletter
- OWASP "collaboration tools" – LinkedIn, Twitter Feeds, etc.
- Expand OWASP's influence into Developer Groups
- Expand OWASP's participation at non-OWASP conferences
- Develop and OWASP Speaker Bureau.
- Work with OWASP Website project to create a new "User-focused" OWASP website.

The GCC will actively promote the OWASP foundation, projects and events to the media, non- OWASP conferences, developer groups and wider community. It will also identify and facilitate working with other organisations and contributing to their initiatives where suitable opportunities exist.

Organizational Supporters of OWASP's mission

Educational Supporters of OWASP's mission

Contact:

OWASP Foundation
9175 Guilford Road,
Suite #300
Columbia, MD 21046

OWASP Foundation

Kate.hartmann@owasp.org

paulo.coimbra@owasp.org

alison.shrader@owasp.org

OWASP Foundation Board

Jeff.williams@owasp.org

seba@owasp.org

tomb@owasp.org

eoin.keary@owasp.org

dave.wichers@owasp.org

matt.tesauro@owasp.org

dinis.cruz@owasp.org