OWASP AppSec Conferences

December 1st-2nd, 2010
BeNeLux 2010
Eindhove, The Netherlands

December 16th & 17th, 2010
IBWAS '10
Lisbon, Portugal

February 8th—February 11th, 2011
OWASP Global Summit 2011
Lisbon, Portugal

AppSec EU, Dublin
June, 2011

AppSec USA Minneapolis
September 19th-23rd, 2011

OWASP
The Open Web Application Security Project

OWASP AppSec USA 2011—Minneapolis

A big thank you to IBM for being the 1st Sponsor of AppSec USA 2011 and signing up as a Gold Sponsor.

Get your CFP responses ready. The Call for Papers will go out March 15, 2011.

We will be using the http://appsecusa.org site coming soon.

IBWAS '10

Carlos Serrao

IBWAS '10, the 2nd. OWASP Ibero-American Web Application Security conference will be held in Lisbon, Portugal on the 16th and 17th of December, 2010. The conference will take place at the ISCTE—Lisbon University Institute. Training will be held on the 16th and Conference on the 17th.

This conference aims to bring together application security experts, researchers, educators and practitioners from the industry, academia and international communities such as OWASP, in order to discuss openly problems and new solutions in application security. In the context of this track academic researchers will be able to combine interesting results wit the experience of practitioners and software engineers.

OWASP Summit 2011

Tom Brennan

The OWASP Summit 2011 is fast approaching, http://www.owasp.org/index.php/Summit_2011 if you have been involved with OWASP for awhile you might recall that we announced the OWASP Elections at the OWASP Summit 2008 and they were held on November 11th 2009.

* Wiki archive reminder see: http://www.owasp.org/index.php/Board_member

The next cycle will start at OWASP Summit 2011 with elections to take place on November 11th 2011 by the current OWASP Members http://www.owasp.org/index.php/Member-ship#Categories_of_Membership_.26_Supporters

If you have the cycles and want to be a candidate for consideration we encourage you meet the pre-req., and get involved with a OWASP Global Committee http://www.owasp.org/index.php/Global_Committee_Pages today.

OWASP Podcasts Series

Hosted by Jim Manico

Ep 77 Rafal Los

Ep 78 AppSec Roundtable with Jeff Williams, Andrew van der Stock, Tom Brennan, Samy Kamkar, Jeremiah Grossman and Jim Manico (Complete Chaos)

Ep 79 Tony UV (Threat Modeling)

Follow OWASP on Twitter

@OWASP

OWASP Project Update

Paulo Coimbra

Please see below a few items regarding OWASP Projects developments made since we last issued the OWASP Newsletter.

1. General OWASP projects news

1.1 - The **ASVS** project's leadership has been put under an application process and OWASP community has responded with enthusiasm – five candidates have shown interest in leading or co-leading this OWASP flagship project. The GPC is currently on its way to produce a recommendation for OWASP Board decision.

http://www.owasp.org/index.php/Request_For_Proposals/Seeking_New_Project_Leader_For/ASVS

1.2 - In a record time the **OWASP Secure Coding Practices - Quick Reference Guide** has produced and has had its third release assessed and consequently rated as Stable Quality. We thank and congratulate the project leader, Keith Turpin, and the release reviewers and contributors.

http://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

1.3 - The OWASP AppSensor Project, led by Michael Coates, has important developments (new tool) and is currently under review targeting a Stable Release rating.
http://www.owasp.org/index.php/Category:OWASP_AppSensor_Project

1.4 - The **OWASP O2 Platform, led by Dinis Cruz,** has important developments **(new release)** and is **currently** under review targeting a Stable Release rating.

http://www.owasp.org/index.php/OWASP_O2_Platform

1.5 - The **OWASP JBroFuzz Project** has a new leadership. We thank Yiannis Pavlosoglou for all the work he has done to push this project forward and welcome and wish all the best to the new leader, Ranulf Green.

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

2. Projects recently set up

2.1 - **OWASP Uniform Reporting Guidelines, led by Vlad Gostomelsky.**

This project will complement the OWASP Testing Guide as well as the OWASP RFP Template. This is going to be a reporting template for vulnerability findings which will be free, base on industry best practices and hopefully will become the de facto standard.

- http://www.owasp.org/index.php/OWASP_Uniform_Reporting_Guidelines

2.2 - **OWASP Zed Attack Proxy Project, led by Psiinon.**

This project provides an easy to use integrated penetration testing tool for testing web applications and provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.

- http://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project#tab=Project_About

2.3 - **OWASP Secure Web Application Framework Manifesto, led Rohit Sethi.**

This project is a document detailing a specific set of security requirements for developers of web application frameworks to adhere to.

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

2.4 - **OWASP Mobile Security Project, led by Jack Mannino and Mike Zusman.**

The OWASP Mobile Security Project will help the community better understand the risks present in mobile applications, and learn to defend against them.

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

2.5 - **OWASP Fiddler Addons for Security Testing Project, led by Chris Weber.**

This project (aka OWASP FAST) is the umbrella for two complementary projects i.e. the **Watcher Project,** a passive vulnerability scanner, and the **X5s Project**, an active XSS testing and input/output encoding detection. http://www.owasp.org/index.php/OWASP_Fiddler_Addons_for_Security_Testing_Project

2.6 - **OWASP Application Security Skills Assessment, led by Neil Smithline.**

This project (aka OWASP ASSA) is an online multiple-choice quiz built to help individuals understand their strengths and weaknesses in specific application security skills.

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

- **OWASP Browser Security Project, created by initiative of Dave Wichers & Michael Coates.**

This project still has no clear leadership but the main effort has been made by the above referred. Further clarification will be soon available.

http://www.owasp.org/index.php/OWASP_Browser_Security_Project#tab=Project_About

3. Projects to be soon set up:

3.1 – OWASP ESAPI Objective C

3.2 - OWASP PASSWD

3.3 - OWASP Eclipse plug-in

4. Projects to be soon reset up:

All the Cross-Site Request Forgery (CSRF) related contents.

3.4 -OWASP Open-sourcing JXT

OWASP A10-Unvalidated Forwards

ESAPI -
* New Leader for .Net ESAPI – Michael Weber
* Java ESAPI currently undergoing code review for General Availability Release

OWASP Top 10 now available in Spanish and Italian

The OWASP Top 10 2010 has been translated to Spanish thanks to the fantastic work from the team below:

Project Lead: Fabio Cerullo (Far Left) Team: Juan Carlos Calderon (2nd Left) , Rodrigo Marcos (Center), Vicente Aguilera (2nd Right). Edgar Sanchez (Far Right) Not pictured: Daniel Cabezas Molina, Jose Antonio Guasch, Paulo Corondo.

You could find both versions in PPT & PDF at the following location:

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Spanish_Translation

Link to Italian version:

http://www.owasp.org/images/f/f9/OWASP_Top_10_-_2010_ITA.pdf

Thank you to our Corporate Members who renewed their support of the OWASP Foundation!

mnemonic
-securing your business

New Corporate sponsors in November and December Thank you for your support!

ADP

AppliedTrust

ORACLE

OWASP searching for a new home for www.owasp.org (the website) if someone would like to bid on hosting the web server email owasp@owasp.org for details.

OWASP Training Model
Sandra Paiva

In the context of the effort we are making to stabilize and consolidate an OWASP Training model that can be used as a powerful tool to spread OWASP's knowledge and message, OWASP is looking for trainers to deliver training under the flag "**OWASP projects and resources you can use today**". This is a model of training which is **free for OWASP members**, **delivered by OWASP Leaders** (with only travel expenses paid) and **covering OWASP modules and/or projects If you are an OWASP Leader and would like to be included in OWASP's pool of trainers, this is your chance - add your name and info to the OWASP Trainers Database and be counted!**

Do it now and become an OWASP Trainer! Check the Database and conditions here: http://www.owasp.org/index.php/OWASP_Training#tab=Trainers_Database_-_Call_for_Trainers.21

Follow all the developments on the OWASP Training here http://www.owasp.org/index.php/OWASP_Training.

Follow all the developments on the OWASP Training here http://www.owasp.org/index.php/OWASP_Training.

OWASP College Chapters Program, led by Jeff Williams. This initiative will help to extend application security into colleges and universities worldwide.**2. OWASP Alchemist Project**, co-lead by Bishan Singh, Chandrakanth Narreddy and Naveen Rudrappa. This project enables a software development team in realization of highly secure and defensible application with built-in defences/controls against security-related design, coding and implementation flaws.

OWASP China
Helen Gao

The first OWASP China conference took place in Beijing on Oct. 20-23, 2010. More than 500 people attended this event. OWASP board member Tom Brennen kicked off the convention with a call for participation. Information security experts from the United States, mainland China, Taiwan, Hong Kong, Singapore and other areas presented the latest information on the most important security issues. Forester analyst Dr. Chenxi Wang and OWASP project leader Pravir Chandra were among the speakers . Since the conference was such a success, we anticipate scheduling another conference next year.

First OWASP Uruguay Day

The 1st OWASP event held in Uruguay was held on Dec. 9th. 2011. Mateo Martinez, Mauricio Campiglia and Cristian Borghello were speakers. More information on the event can be found here: http://www.owasp.org/index.php?title=OWASP_Day_Uruguay_2010

Along with images from the event. Thank you to Mateo Martinez, Fabio Cerullo, Roberto Ambrosoni and Kate Hartmann for planning this event.

OWASP CTF Poject
Steven van der Baan

The Capture the Flag project has been held this year at 8 separate events (ranging from AppSec-EU in Stockholm, Sweden through GovCert in Singapore to OWASP BeNeLux in Eindhoven). The CTF also has obtained it's own logo now (http://www.owasp.org/images/8/87/CTFLogo.jpg) and received a complete overhaul to the framework which supports the CTF. This framework will soon be released. Steven van der Baan has replaced Martin Knobloch as the lead for the CTF project.

OWASP Modsecurity CRS v2.0.9
Ryan Barnett

I am pleased to announce the release of the OWASP ModSecurity Core Rule Set (CRS) v2.0.9.

The most significant change is that users can now easily toggle between Traditional or Anomaly Scoring Detection modes. http://blog.modsecurity.org/2010/11/advanced-topic-of-the-week-traditional-vs-anomaly-scoring-detection-modes.html

Improvements:
- Changed the name of the main config file to modsecurity_crs_10_config.conf.example so that it will not overwrite existing config settings. Users should rename this file to activate it.
- Traditional detection mode is now the current default
- Users can now more easily toggle between traditional/standard mode vs. anomaly scoring mode by editing the modsecurity_crs_10_config.conf file
- Updated the disruptive actions in most rules to use "block" action instead of "pass". This is to allow for the toggling between traditional vs. anomaly scoring modes.
- Removed logging actions from most rules so that it can be controlled from the SecDefaultAction setting in the modsecurity_crs_10_config.conf file
- Updated the anomaly scores in the modsecurity_crs_10_config.conf file to more closely match what is used in the PHPIDS rules. These still have the same factor of severity even though the numbers themselves are smaller.
- Updated the 49 and 59 blocking rules to include the matched logdata
- Updated the TAG data to further classify attack/vuln categories.
- Updated the SQL Injection filters to detect more boolean logic attacks
- Moved some files to optional_rules directory (phpids, Emerging Threats rules)

Bug Fixes:
- Fixed Rule ID 960023 in optional_rules/modsecurity_crs_40_experimental.conf is missing 1 single quote https://www.modsecurity.org/tracker/browse/CORERULES-63
- Moved all skipAfter actions in chained rules to the rule starter line (must have ModSec v2.5.13 or higher) https://www.modsecurity.org/tracker/browse/MODSEC-159
- Fixed restricted file extension bug with macro expansion https://www.modsecurity.org/tracker/browse/CORERULES-60
- Updated the SQLI TX variable macro expansion data in the 49 and 60 files so that it matches what is being set in the sql injection conf file
- Fixed typo in SQL Injection regexs - missing backslash for word boundary (\b) https://www.modsecurity.org/tracker/browse/CORERULES-62

OWASP Site Statistics for November 2010

258, 568 visits

654,677 pageviews

00:03:03 Avg. Time on Site

58.28% New Visits

Mark Bristow at AppSec DC.

OWASP Foundation

9175 Guilford Road
Suite #300
Columbia, MD 21046

Phone: 301-275-9403
Fax: 301-604-8033
E-mail:
Kate.Hartman@owasp.org

The free and open application security community

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas. We can be found at www.owasp.org.

OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, cost-effective information about application security.

OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. Similar to many open-source software projects, OWASP produces many types of materials in a collaborative, open way.

The OWASP Foundation is a not-for-profit entity that ensures the project's long-term success.

OWASP Organizational Sponsors

Newsletter Editor: Lorna Alamri Contributors: Leonel Navarro & Jayanthi Srinivasan