January 18, 2010

OWASP AppSec Conferences

June 21-24, 2010
AppSec Research 2010
Stockholm

AppSec USA 2010 Announcement

The Global Conferences Committee is excited to announce the date and location of the OWASP AppSec US 2010 Conference. AppSec US 2010 will be held September 7th through September 10th, 2010 and hosted by Los Angeles and Orange County Chapters at the University of California, Irvine, the only school in the University of California system with a dedicated school of Information and Computer Science. More information, including the call for speakers & the call for training will be sent shortly. The committee extends congratulations to the MSP Chapter for their outstanding proposal submission. While not selected for AppSec US 2010 we are looking forward to arriving in the Midwest and Central US corridor for events in the near future.

OWASP AppSec Research 2010 Call for Papers

The OWASP AppSec Research Conference is looking for submissions which fall into three categories:

Publish or Perish: Research papers for peer-review. Submit: Max 12 pages, LNCS format

Demo or Die: Presentation and Demo. Submit: 1 page abstract + screenshot

Present or Repent: Presentation only. Submit: 2 pages extended abstract.

http://tinyurl.com/yjv2otg Deadline: Febuary 7th.

IBWAS 09

Around 40 participants and several dozen technology students and their teachers attended the Iberic Web Application Security conference (IBWAS'09) that was held at the Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Universidad Politécnica de Madrid, Spain, on the 10th and 11th of December 2009.

The conference, which was a massive success, was organized by the Spanish and Portuguese OWASP chapters with the aim of bringing together application security experts, researchers, educators and practitioners from the industry and academia to openly discuss problems and new solutions in application security.

Through the passionate discussion held during the "**Web Application Security: What should Governments do in 2010?**" panel, several conclusions have been reached.

These conclusions reflect the decisions made by the panel and should be debated, updated and eventually published by OWASP as a set of recommendations.

1. We challenge governments to work with OWASP to increase the transparency of web application security, particularly with respect to financial, health and all other systems where data privacy and confidentiality requirements are fundamental;
2. OWASP will seek participation with governments around the globe to develop recommendations for the incorporation of specific application security requirements and the development of suitable certification frameworks within the government software acquisition processes;
3. We offer our assistance to clarify and modernize computer security laws, allowing the Government, citizens and organizations to make informed decisions about security;
4. We ask governments to encourage companies to adopt application security standards that, where followed, will help protect us all from security breaches, which might expose confidential information, enable fraudulent transactions and incur legal liability;
5. We offer to work with local and national governments to establish application security dashboards providing visibility into spending and support for application security.

OWASP Board Members 2010

Jeff Williams
Dinis Cruz
Dave Wichers
Tom Brennan
Sebastien Deleersnyder
Eoin Keary
Matt Tesauro

OWASP Podcasts Series

Hosted by Jim Manico

Ep 57 David Linthicum (cloud Computing)

Ep 56 Adar Weidman (Regular Expression DOS)

Ep 55 AppSec Justification Roundtable with Boaz Gelbord, Jason Lam, Jim Manico and Jeff Williams

Ep 54 George Hesse

Ep 53 Amichai Shulman (WAF)

Looking for an AppSec job? Check out the OWASP Job Page

Have an AppSec job you need posted?

Contact:

Kate Hartmann

WASC Threat Classification v2/ OWASP Top Ten 2010 RC1 Mapping Jeremiah Grossman's Blog

Reprinted with permission from Jeremiah Grossman's Blog http://jeremiah-grossman.blogspot.com/

"With most of the work done by Bil Corry (@bilcorry), here is a solid first pass at creating a mapping between the newly released WASC's Threat Classification v2 and OWASP's Top Ten 2010 RC1. This should help those actively using one or both of use documents. "

WASC Threat Classification v2	OWASP Top Ten 2010 RC1
WASC-19 SQL Injection	A1 - Injection
WASC-23 XML Injection	
WASC-28 Null Byte Injection	
WASC-29 LDAP Injection	
WASC-30 Mail Command Injection	
WASC-31 OS Commanding	
WASC-39 XPath Injection	
WASC-46 XQuery Injection	
WASC-08 Cross-Site Scripting	A2 –Cross Site Scripting (XSS)
WASC-01 Insufficient Authentication	A3 - Broken Authentication and Session
WASC-18 Credential/Session Prediction	
WASC-37 Session Fixation	
WASC-47 Insufficient Session Expiration	
WASC-01 Insufficient Authentication	A4 - Insecure Direct Object References
WASC-02 Insufficient Authorization	
WASC-33 Path Traversal	
WASC-09 Cross-site Request Forgery	A5 - Cross-Site Request Forgery
WASC-14 Server Misconfiguration	A6 - Security Misconfiguration
WASC-15 Application Misconfiguration	
WASC-02 Insufficient Authorization	A7 - Failure to Restrict URL Access
WASC-10 Denial of Service	
WASC-11 Brute Force	
WASC-21 Insufficient Anti-automation	
WASC-34 Predictable Resource Location	
WASC-38 URL Redirector Abuse	A8 - Unvalidated Redirects and Forwards
WASC-50 Insufficient Data Protection	A9 - Insecure Cryptographic Storage
WASC-04 Insufficient Transport Layer Protection	A10 -Insufficient Transport Layer Protection

OWASP TOP 10 2010 RC1—Update Dave Wichers

The OWASP Top 10 2010 RCI was released at AppSec DC . The comment period ended 12/31/09. The project team hopes to release the update 2/4/10.

More information can be found at the top of the Top 10 project page: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP JBroFuzz

OWASP JBroFuzz project has been recently assessed against the OWASP Assessment Criteria 2.0 and its ultimate release (JBroFuzz 1.7) has been considered a Stable one **as of 12/2/09**

http://www.owasp.org/index.php/Category:OWASP_JBroFuzz

http://www.owasp.org/index.php/Category:OWASP_JBroFuzz_Project_-_Version_1.7_Release_-_Assessment

http://www.owasp.org/index.php/Assessment_Criteria_v2.0

Congratulations to the project leader, Yiannis Pavlosoglou, and to the team, Matt Tesauro and Leonardo Cavallari Militelli, that performed the very first review against the new OWASP assessment criteria.

Global Industry Committee
Colin Watson

The Industry Committee's mission is to expand awareness and promote the inclusion of software security best practices in the public and private sectors, including organizations that promote standards and best practices. The committee also wants to become a voice for these organizations within OWASP, promoting their views and requirements.

To accomplish this we undertake outreach including presentations, contribution to other organization's efforts and collaborative efforts wher these can be identified and resources are available.

During 2009 Rex Booth and David Campbell in North America, and Georg Hess, Eoin Keary and Colin Watson in Europe, together with our OWASP board representative Tom Brennan 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. In 2010 we have been joined by three new members Joe Bernik, Alexander Fry and Yiannis Pavlosoglou, and our new board representative Dave Wichers. We are 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 and government as well as promoting OWASP's projects and resources to the wider community. Where other OWASP people have existing contacts, we want to help them develop a dialogue between the organizations.

Key links:

OWASP Global Industry Committee:
http://www.owasp.org/index.php/Global_Industry_Committee

Industry Committee Mailing List
http://lists.owasp.org/mailman/listinfo/global_industry_committee

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

Dinis Cruz presenting at IBWAS 09

IBWAS 09 Panel Speakers:

OWASP Project Update
Paulo Coimbra

New Project:

OWASP Computer Based Training Project *(OWASP CBT Project)*, led by *Nishi Kumar*

Releases:

OWASP ModSecurity Core Rule Set Project - ModSecurity 2.0.3 To be assessed by: Ivan Ristic & Leonardo Cavallari.

The OWASP EnDe Project
OWASP Vicnum Project OWASP Vicnum - Release 1.4 (12/31/2009) .

OWASP Content Validation using Java Annotations Project

OWASP Application Security Verification Standard (ASVS) – Draft versions of its Japanese & French translations. Under development: German & Chinese translations.

Reviewers drive: The GPC is on its way to launch a Reviewers Drive .

releases will be assessed in accordance with the OWASP Assessment Criteria 2.0.

Membership

Individual Memberships: 767

- New Memberships in December: 26
- Renewals in December: 0
- Lost memberships in December (did not renew): 9
- Individual Memberships: $900

Organizational Memberships: 27

- New Memberships in December: 0
- Renewals in December: 1 (Nokia)
- Lost memberships in December (did not renew): 1 (Corporate One Federal Credit Union)

Membership income for December: $5,900

Thank you to Nokia who renewed their support of the OWASP Foundation in December.

NOKIA

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.

Newsletter Editor: Lorna Alamri, IBWAS images: Carlos Serrao