November 20, 2009

OWASP AppSec Conferences:

Nov 17th-20th App Sec India

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

Dec 2nd 2009 BeNeLux Day College De Valck
http://www.owasp.org/index.php/BeNe-Lux_OWASP_Day_2009

Dec 10th-11th IBWAS, Madrid
http://www.ibwas.com/

AppSec Research 2010 - Stockholm, Sweden

OWASP Board Members

Jeff Williams

Dinis Cruz

Dave Wichers

Tom Brennan

Sebastien Deleersnyder

Congratulations to the two new OWASP Board Members:

Eoin Keary &

Matt Tesauro

OWASP
The Open Web Application Security Project

OWASP TOP 10 2010 RC1 - Dave Wichers

The OWASP Top 10 2010 RCI was released at AppSec DC . Dave Wichers as project lead made the presentation. He has uploaded both the presentation and the Top 10 itself to the OWASP wiki. The presentation is in .pptx format, and the Top 10 is a PDF document.

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

Since this is a release candidate, it is up for open comment until the end of the year. So, please review and provide Dave Wichers with comments.

And the Top 10 for 2010 (rc1) is ...

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: Failure to Restrict URL Access
A8: Unvalidated Redirects and Forwards
A9: Insecure Cryptographic Storage
A10: Insufficient Transport Layer

This update is based on more sources of web application vulnerability information than the previous versions were when determining the new Top 10. It will also present this information in a more concise, compelling, and consumable manner, and include 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. A significant change for this update will be that the OWASP Top 10 will be focused on the Top 10 **Risks** to Web Applications, not just the most common vulnerabilities. http://www.owasp.org/index.php/OWASP_Top_10_2010_AppSecDC

OWASP AppSec DC 2009 Lorna Alamri

AppSec DC featured Joe Jarzombek, Director for Software Assurance at the Department of Homeland Security National Cyber Security Division as Keynote to kick off the conference. A panel discussion made up of federal CISOs (Earl Crane—Branch Chief for Security Strategy, DHS, Gary Galloway—Deputy Director of the Office of Information Assurance, Dept. of State, Timothy Ruland—CISO, US Census Bureau, and Richard Smithon—CISO TSA covered topics such as:

- Level of application security program maturity
- Integration of application security inside existing security management frameworks
- Building an application security team
- Web 2.0,
- Transparency

Another well attended panel was on Securing the SDLC process and the importance of software security assurance, panelists were: Dan Cornell, Michael Craigue, Dennis Hurst, Joey Peloquin & Keth Turpin. Pravir Chandra served as moderator.

OWASP AppSec DC was the App Sec event in the US to be at in 2009.

OWASP Podcasts Series

Hosted by Jim Manico

Sandro Gauci (wafwoof)

Michael Coates (Real Time Defensese, OWASP AppSensor)

Eladad Chai (Business Logic Attacks)

Andre Riancho (OWASP w3af)

Giorgio Fedon (Browser Security in Banking)

OWASP Development Guide—Andrew van der Stock

Mike Boberski is the new Development Guide's PM. Mike's other OWASP efforts includes the
Application Security Verification Standard, various cheat sheets, and
ESAPI for PHP.

His duties will include:
* Volunteer coordination - allocation of work, etc
* Maintaining the Guide's Wiki project pages, road map, etc
* Status updates - encouraging folks to check in regularly
* Quality Control
Andrew van der Stock proposes that the Development Guide move to be the detailed design guide for the Application Security Verification Standard's requirements. At a minimum, he would like to cover every single control mentioned in the ASVS.

The Plan:

1. Workable roadmap with realistic timeline.
2. Call for volunteers

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

Mike.boberski@owasp.org

NIST SP 800-53
David Campbell

Rex Booth of the industry committee successfully organized an effort earlier this year to provide cohesive comments to the recently released 3rd revision of NIST's special publication 800-53. Federal folks will recognize this document, entitled "*Recommended Security Controls for Federal Information Systems and Organizations*" as the heart and soul of FISMA, which is the process by which federal agencies earn their infosec "letter grades".

We were very pleased to see that several of the revisions and updates provided by OWASP were included in the release document.

The Global Industry Committee continues to monitor draft documents released by NIST and other relevant organizations and provides feedback to ensure that the AppSec community is properly represented.

AppSec DC 2009 Exhibit hall and break service

Enterprise Security API - Project News

Project News

- ESAPI Python version project possibly starting up. Please contact jeff.williams@owasp.org for more information.
- ESAPI Java 2.0 is nearing completion. Release in a few weeks. Please check SVN and send any last minute requests to the ESAPI list.
- We've had a request for an ESAPI ColdFusion edition. If there are any interested developers, please contact jeff.williams@owasp.org to volunteer.
- ESAPI has been through a line-by-line review by a major systems integrator. We will post all the findings soon but they are pretty minor.
- OWASP ESAPI has been integrated into the OWASP Secure Software Contract Annex in the OWASP Legal Project.
- OWASP ESAPI is presented by Jeff Williams at OWASP Software Assurance Day DC 2009 in conjunction with the Software Assurance Forum sponsored by the US Department of Homeland Security, Department of Defense and National Institute of Standards and Technology.

Project Mail List

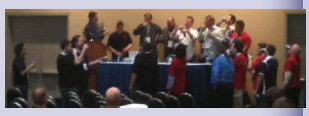
Subscribe here
Use here

Weekly Status

- ESAPI Doc Weekly Status 2009-11-13.pdf

For the most recent project news:

http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=News



Cloudy with a chance of 0-Day. Start of presentation delivered by Jon Rose and Tom Leavey from Trustwave/ Spiderlabs.

Become a member

The professional association of OWASP Foundation is a not-for-profit 501c3 charitable organization not associated with any commercial product or service. OWASP is an open source project dedicated to finding and fighting the causes of insecure software to be successful we need your support. OWASP individuals, supporting educational and commercial organization form an application security community that works together to create articles, methodologies, documentation, tools, and technologies ("OWASP Materials"). - 2009 Membership Powerpoint

Why Become a Supporting Member?

- As a member of the internet community do you agree with the ethics and principals of OWASP Foundation?
- Do you want to underscore your awareness of web application software security?
- Do you want to continue to increase your knowledge and expand your skills when attending OWASP conferences at a discount?
- Do you want to expand your personal network of contacts? OWASP Linked'In Group

A portion of your membership fee directly supports the local chapter of your choice.

Contact: Kate Hartmann

Kate.Hartmann@owasp.org

"As a Direct result of the AppSec DC 2009 Conference OWASP gained over 70 new members."
Kate Hartmann

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 Project News –
Paulo Coimbra, OWASP Project Manager

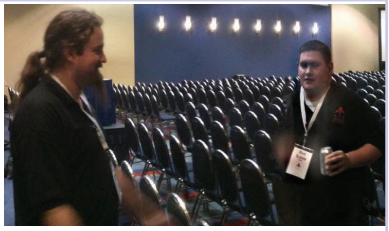
New Projects;

OWASP Security Assurance Testing of Virtual Worlds, led by ***Rick Zhong***.

Updates:

The OWASP Content Validation using Java Annotations Project has recently launched its first release (SHIP Validator 0.3 Release) which is now ready to be assessed and its leadership is actively looking for a Project or Chapter Leader to act as First Reviewer.

The OWASP EnDe Project http://www.owasp.org/index.php/Category:OWASP_EnDe#tab=Project_Details has just launched a new Release, its Version - 0.1.68.



Doug Wilson & Mark Bristow getting ready for the start of AppSec DC 2009. Rex Booth is behind the camera.

Rocket war. Photo courtesy of Kate Hartmann.

Newsletter Editor: Lorna Alamri
Special thanks to Rex Booth & Kate Hartmann: images, Adam Baso: editing help & Colin Watson: content suggestions.