May 17, 2010

OWASP AppSec Conferences

June 2nd, 2010
[Froc 2010]
Denver, Colorado

June 3rd—4th, 2010
[OWASP Day Mexico]
Aguascalientes, Mexico

June 21st—24th, 2010
[AppSec Research 2010]
Stockholm, Sweden

June 30th, 2010
[OWASP Argentina Day]
Buenos Aires, Argentina

September 7th–10th, 2010
[AppSec USA 2010]
Irvine, California

September 17th, 2010
[AppSec Ireland]
Dublin, Ireland

November 16th–19th, 2010
[AppSec Brasil 2010]
Campinas, Brasil

OWASP
The Open Web Application Security Project

OWASP AppSec Research 2010

The full conference and training program is available. The Gala Dinner will be on Wednesday June 23rd at the city hall, This is where the Nobel Prizes are awarded. Check it out here: [City Hall]

OWASP AppSec USA, California 2010 Keynotes

AppSec USA will take place at the UC Irvine Conference Center in Orange County, CA on September 7th—10th, 2010.

Key notes will be:

Bill Cheswick—AT&T Research
HD Moore—Metasploit/Rapid7
David Rice—Geekonomics
Jeff Williams—Aspect Security

The conference website will be release soon and will be available at:

[www.appsecusa.org]

OWASP AppSec, Brasil 2010 Keynotes

OWASP AppSec Brasil announces their Keynotes for the conference are Bruce Schneier and Jeremiah Grossman. The event will be held November 16th—19th, 2010. For more information on the conference:

www.owasp.org/index.php/AppSec_Brasil_2010).

OWASP Top 10 2010 Released

OWASP Top 10 2010 was released on April 19th, 2010. OWASP received great press coverage on the release. Here are just a few links from the international news media attention OWASP received. If you haven't already please take a moment to review the Top 10 for 2010 and accept the challenge to make application security more visible.

To read the Press Release:

[http://www.owasp.org/index.php/OWASPTop10-2010-PressRelease]

Articles:
[Logic Flaws and the OWASP Top 10, Steve Ragan—The Tech Herald]

[Top 10 Most Critical Web App Security Risks, Ericka Chickowski—Channel Insider]

[Injection tops list of web application security risks, Angela Moscaritolo—SC Magazine]

[OWASP Issues Top 10 Web Application Security Risks List, Kelly Jackson—DarkReading]

[Security: 10 Most Dangerous Web App Security Risks, Brian Prince—eWEEK]

OWASP Newsletter—Call for Articles

OWASP is looking for article submissions around application security to be published in the OWASP newsletter. All submissions should be non-commercial in content.

Please contact Lorna.Alamri@owasp.org for further information or with submittals.

Interview with Jim Manico

Lorna Alamri

One of the most exceptional things about OWASP is it allows people who are passionate about application security a forum. Jim Manico has put together a renowned podcast series where he interviews known application security experts. He has been able to use his talents to develop an OWASP Podcast Series , grow his career and increase the OWASP knowledge base and awareness around application security.

Why did you decide to do the first podcast?

Back in October of 2008 I was witnessing several interractions between OWASP volunteers over the OWASP eLists and I was just blown away with the depth of the discourse. I thought, someone needs to capture this. I thought podcasting would be easy.. so without really asking permission, I just started recording. :) Arshan, Jeff Williams and Jeremiah Grossman offered to be my first victims - and I've been podcasting for OWASP ever since. :)

What was your original goal with the podcast? Has that changed? If so how?

My original goal was to record "easy style" over a free telephone conference service and just publish the final mp3. Now, I'm purchasing a very high end studio microphone and am focusing on quality of the final production as best I can through careful editing and professional mastering. This is a full 360 from my original intentions, but I'm constantly trying to evolve the quality of the show.

How has the project developed?

Today (Mid March) I'm editing the 63rd show. I have several shows completed and waiting for the new Top Ten press release.

How do you prepare for an interview?

I start by scheduling with various guest. I also have a monthly reoccurring invite for the round-table show. I work out questions with guests ahead of time. I'm looking for smart commentary, not surprises for my guests.

What was the most popular podcast? the most controversial? your favorite?

The roundtables are the most popular shows. We did have one guest call all of OWASP "a bunch of communists" which raised a few eyebrows. My favorite show was with Billy Hoffman from HP - he said my grandmother deserves to be hacked. ;) Dave Aitel came on the show was just the coolest cat of them all. Richard Stallman came on the show and slammed me hard after I asked him what his Skype account was. (PS: I only released Stallmans interview in ogg! Promise!) But I'm especially grateful to Andre Gironda, Jeff Williams and Boaz for all of their help in supporting the show. And frankly, all of my **guests have been fantastic!**

Knowing what you know now what would you do differently, if anything?

I would never have claimed that a free telephone conference service would be good enough to record a podcast! :)

What was your biggest challenge to starting the podcast?

Just doing it. One we got started, the spirit of the podcast took over. :)

Why do you feel it's been successful?

Guests. I have had the pleasure of having some incredibly smart and talented guests on the show. We could not do this without that community.

If you could interview anyone for the podcast - who would that person be?

OWASP Podcasts Series

Hosted by Jim Manico

Ep 61 Richard Bejtlich (Network Monitoring)

Ep 62 Amichai Shulman (WAF)

Ep 63 Ed Bellis (eCommerce)

Ep 64 Andy Ellis (Availability)

Ep 65 AppSec Round Table: Boaz Gelbord, Dan Cornell, Jeff Williams, Johannes Ullrich & Jim Manico

Ep 66 Brad Arkin (Adobe)

Ep 67 Top Ten– Jeff Williams (XSS)

Ep 68 Top Ten—Kevin Kenan (Cryptographic Storage)

Ep 69 Top Ten—Eric Sheridan (CSRF)

Ep 70 Top Ten—Michael Coates (TLS)

Ep 71 Top Ten—Robert Hansen (Redirects)

I would like to interview the MS employee who invented HTTP Only! :) But really, Bruce Schneier is one of the only folks that I'm still chasing to be on the show. I recorded Bruce in the early days of the podcast, but (my fault) the recording quality was so bad that I could not push it live. Bruce! I'm sorry! Please give me a second chance. :)

What's next?

The show must go on! Several companies have been kind enough to make donations to OWASP through being on the show - and that has given me a little budget to buy professional studio equipment for future shows. Thank you to Tenable, Adobe, Orbitz and Akamai for your generous OWASP donations!

Are there any lessons learned that you would like to share? Anything else you would like to share with your audience?

I have published my equipment list and process at http://www.owasp.org/index.php/Talk:OWASP_Podcast This list is a result of many lessons learned over the past few years.

Most importantly, thank you for listening! The show would not be a success if it was not for our fantastic listeners!

If you have any comments, please drop me a line at podcast@owasp.org.

Can you help OWASP make *every* application developer knowledgeable about the OWASP Top 10?
Share this link:
OWASP Top 10 - 2010.pdf

London OWASP Chapter
OWASP AppSec Training Project

The London OWASP Chapter just completed their 1st training event on April 16th. They have compiled a day of presentations to address the following gaps:

- Apart from OWASP's Top 10, most OWASP Projects are not widely used and understood. In most cases this is not due to lack of quality and usefulness of those Document & Tool projects, but due to a lack of understanding of where they fit in an Enterprise's security ecosystem or in the Web Application Development Life-cycle.
- This course aims to change that by providing a selection of mature and enterprise ready projects together with practical examples of how to use them.
- The course will be very practical where demonstration and hands-on exercises will be provided for the tools covered.

Materials can be downloaded at:

OWASP Projects and Resources you can use today.

Now looking for OWASP chapters to take the materials and replicate the classes for the markets they serve.

Thank you to our Corporate Members who renewed their support of the OWASP Foundation in March and April

Booz | Allen | Hamilton

cigital

symantec.

fishnet SECURITY

New Corporate sponsor in April: Qualys
Thank you for your support!

QUALYS

Follow OWASP

OWASP has a Twitter feed

http://twitter.com/statuses/user_timeline/16048357.rss

IBWAS '10—Call for Papers

Carlos Serrão, Ph.D.

IBWAS'10, the 2nd. Ibero-American Web Application Security conference will be held in Lisbon (Portugal), on the 11th and 12th November 2010. 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 open problems and new solutions in application security. In the context of this track academic researchers will be able to combine interesting results with the experience of practitioners and software engineers.

The conference organizers have already published the Call for Papers (CfP) and anyone interested in submitting a paper to the conference should do so, according to the instructions detailed in the CfP, until the 24th. September 2010.

Suggested topics for papers submission include (but are not limited to):

- Secure application development
- Security of service oriented architectures
- Security of development frameworks
- Threat modeling of web applications
- Cloud computing security
- Web applications vulnerabilities and analysis (code review, pen-test, static analysis etc.)
- Metrics for application security
- Secure coding techniques
- Platform or language security features that help secure web applications
- Secure database usage in web applications
- Access control in web applications
- Privacy in web applications
- Standards, certifications and security evaluation criteria for web applications
- Application security awareness and education
- Attacks and Vulnerability Exploitation

All accepted papers will be published in the conference proceedings, under an ISBN reference. Conference proceedings will be published by Springer in the Communications in Computer and Information Science (CCIS) series.

For more information please check:
Call for Papers: http://www.owasp.org/index.php/IBWAS10#tab=Call_for_Papers
Conference web-site: http://www.ibwas.com

OWASP Projects Update

Paulo Coimbra, OWASP Project Manager

New projects

Hungarian Translation Project

http://www.owasp.org/index.php/OWASP_Hungarian_Translation_Project#tab=Project_Details

RFP– Criteria

http://www.owasp.org/index.php/Projects/RFP-Criteria

New Releases

JSReg: JavaScript regular expression based sandbox

https://code.google.com/p/jsreg/

HTML Reg: Java Script regular expression based sandbox for HTML

http://code.google.com/p/htmlreg/

JavaScript regular expression based sandbox for CSS

http://code.google.com/p/cssreg/

OWASP Training

London Training: OWASP projects and resources you can use today May 28th, 2010

London Training: OWASP projects and resources you can use today April 16th, 2010

Training Video Links

http://www.youtube.com/watch?v=pYp-kJTrzCE&feature=player_embedded

http://www.youtube.com/watch?v=eRRwaAmKhVg&feature=player_embedded

ASVS Translations & ESAPI for PHP Project updates
Mike Boberski

The count of completed translations of ASVS is now up to three:
French, German, Japanese
Here is the link:
ASVS Translations
Other languages under development:
Malay, Chinese, Hungarian, Persian, Spanish, and Thai.

The ESAPI for PHP project is nearing its first release, putting finishing touches on like updating the codebase to be PEAR compliant, adding phpdoc, and going the last mile for a few controls.

Here is the link: http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=PHP

OWASP
Making Application Security More Visible

This year OWASP is focusing on making application security more visible. One way to do so is to focus on speaking as OWASP at non– OWASP events. Her are just a few upcoming events where OWASP will be taking their message about application security to security and application development organizations.

France: French Chapter will be at RMML 2010:
http://2010.rmll.info/OWASP.html?lang=en
About RMLL2010 :
The Libre Software Meeting (LSM or RMLL in French for Rencontres Mondiales du Logiciel Libre) is conferences cycle about Free Software. LSM is an annual event born in 2000 and since 2003, it occurs in a different town each year. LSM are free as in beer and as a speech :-) No fees, no places limit.
2010 LSM will take place in Bordeaux from 6 to 11 July. 2010 LSM will have 7 main topics (each topic will host several more focused sessions) :
We will presents some tools and appsec tricks (like a small ersatz of the OWASP london Training) : Top10 2010 + WebGoat/WebScraba examples.

Greece: Greek Chapter supports AthCon (http://www.athcon.org/), a conference that will be held in Athens, Greece on June 3rd-4th, 2010. OWASP Members receive a 15% discount on registration.

Malaysia: Malaysia OWASP chapter will be at the Malaysia Open Source Conference 2010. http://conf.oss.my

Singapore: OWASP Singapore is supporting the following events:
1) ISC2's SecureAsia@Singappore on 26-27 July 2010
Their website is http://www.informationsecurityasia.com/
2) Singapore Ministry of Home Affairs' GovernmentWare on 28-30 September 2010
Their website is http://www.govware.sg

Slovenia: OWASP Slovenia is joining OTS 2010 conference (http://cot.uni-mb.si/ots2010/) that will be held in Maribor, Slovenia, June 15th-16th. OTS is celebrating their 15th anniversary and OWASP Slovenia is proud to take care for Application Security Section on Wednesday, on June 16th, at 16:15.

USA: OWASP will have a featured speakers at ICCS. http://www.iccs.fordham.edu/ The International Conference on Cyber Security is a joint effort between the FBI and Fordham University. It will take place at the Fordham Law Center in New York, NY from August 2nd-5th, 2010

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

Have an AppSec job you need posted?

Contact:

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 Organizational Sponsors

Newsletter Editor: Lorna Alamri