July 17, 2010

OWASP
The Open Web Application Security Project

Application Security Conferences

September 7-10, 2010, Irvine, CA - USA Registration OPEN! http://www.appsecusa.org/register-now.html

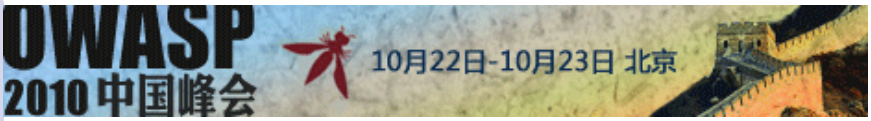
September 16-17, 2010, Dublin Ireland

CFP and CFT OPEN – http://www.owasp.org/index.php/OWASP_IRELAND_2010#Call_for_Papers REGISTRATION OPEN - http://www.owasp.org/index.php/OWASP_IRELAND_2010#Registration

October 20-21, 2010, Rochester, NY – USA CFP OPEN - http://www.rochestersecurity.org/call-for-presentations

October 20, 2010, Nurnberg, Germany

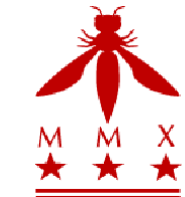
CPF OPEN - http://www.owasp.org/index.php/OWASP_AppSec_Germany_2010_Conference#tab=Call_for_Papers_-_English_Version



October 20-23, 2010, Beijing, China CFP/CFT OPEN - http://www.owasp.org/index.php/OWASP_China_Summit_2010#tab=Call_For_Paper

October 29, 2010, Austin, TX - USA

CFP OPEN - http://www.owasp.org/index.php/Lonestar_Application_Security_Conference_2010#tab=Call_for_Papers



November 8-11, 2010, Washington, DC – USA

CFP/CFT OPEN - http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=CFP

Registration OPEN - http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=Registration

November 11-12, 2010, Lisbon, Portugal

CFP OPEN - http://www.owasp.org/index.php/IBWAS10#tab=Call_for_Papers

November 16-19, 2010, Campinas, SP, Brazil

CFP and CFT OPEN - http://www.owasp.org/index.php/AppSec_Brasil_2010#tab=Calls

[OWASP Podcasts Series](#)

Hosted by Jim Manico

Ep 72 [Interview with Ivan Ristic (WAF)](#)

Ep 73 [Jeremiah Grossman and Robert Hansen](#)

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

Interview with Matt Tesauro

Lorna Alamri

One of the most exceptional things about OWASP is it allows people who are passionate about application security a forum. Matt Tesauro is project lead for the LiveCD project. His involvement in OWASP has allowed him to grow his career and increase the OWASP knowledge base and awareness around application security.

Why did you decide to do the first LiveCD?

I did the OWASP Live CD as part of the OWASP Summer of Code 2008. I got the email from OWASP about the SoC and when I read about a project which combined application security and Linux, I knew it was for me as those are two of my favorite things.

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

The original goal of the Live CD was to get a working one by the SoC deadline. ;)

In reality, I was trying to gather the best app sec tools together in one easy to use package. I kept the tools focused on app sec instead of doing a general "hacking" tools CD.

The Live CD has definitely changed since that first version in September 2008. The first big change were several sub-projects which grew out of the Live CD. The first of those were virtual installs for VMware and VirtualBox. We also got a working, but painfully slow, VM on a USB drive version working.

Truth is that it grew to be much more then just a Live CD. For that reason, the latest version has been renamed to OWASP WTE or Web Testing Environment. We've taken the base of the OWASP Live CD, migrated that from SLAX to Ubuntu Linux and created individual, separately installable packages for all the tools on WTE.

The big improvement this will allow is easier development of methods of getting testing tools into the hands of security professionals. With the latest packages, you can take a standard Ubuntu installation, point it at the WTE repository and, in a few minutes, install all the WTE tools installed.

How has the project developed?

As I mentioned above, its morphed from just a bootable CD to a bunch of different methods to get the tools you want. As soon as we complete the migration from SLAX to Ubuntu, we'll have a ton of different methods to get WTE to end users:

- Live CD
- Virtual Installations (VMware, VirtualBox, Parallels, ...)
- Adding packages to existing Ubuntu installs
- WTE on a USB Stick
- Wubi - a method to dual boot Windows and Ubuntu without repartiioning
- Custom version such as a Java static tools collection, a version with tools and attack targets, etc
- New categories of tools like static analysis tools

I've also been fortunate to have several people contribute to the project. Nishi Kumar did the graphics for the releases. Brad Causey and Drew Beebe have contributed many, many hours to the project as well. They also deserve a mention for the help they've provided.

I have to admit that since I moved to Trustwave's SpiderLabs, I've spentmore time getting used to a new and wonderful place to work then updating the project. I've really enjoyed the caliber of my co-workers at SpiderLabs and spent more time talking shop then making Debian packages for WTE. Never fear though, I keep finding myself firing up a virtual install of WTE for work so its only a matter of time before I start scratching that itch again.

What was the most popular Application on the LiveCD? the most controversial? your favorite?

By a long way, the most commented, asked about and probably used application on the Live CD has been WebGoat. I think the fact that a WebGoat was only a quick boot away from being ready to go was a huge boon for many people either learning application security or those teaching a class.

I'm not sure there's been a truly controversial application added - perhaps Metasploit which isn't strictly a web app security tool. Also, I've gotten a bit of grief about Maltego CE which is a closed sourced trial version. Maltego sales is what is keeping a roof over the head of the guy who wrote it so I won't hold that against him.

As for a personal favorite - I hate to single out only one. Some of the ones I use most frequently are WebScarab, Burp Suite, JBroFuzz, Nikto, and Dir-

Buster. There's also some new favorites which will be added to WTE in the next release.

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

I really liked SLAX for making a Live CD. It was great for that purpose. However, the minute we branched out to VMs and trying to update the Live CD dynamically, it just wasn't the right fit.

So, if I had anything to do over, I'd start with a version of Linux with proper package management system. Debian has had years to work out the wrinkles of managing packages so why not stand on the shoulders of those giants? BTW, RPM is also a fine package management system. If you're a RPM wizard, I'd love to work with you to get RPMs made from the .deb packages for WTE.

What was your biggest challenge to starting the LiveCD Project

One of my initial challenges was keeping the scope sane. I started out looking at various tools for app sec and came up with a list of over 330 tools. Getting that paired down to a sane number took a while. Also, learning how to properly create packages is painful upfront, but once you get it, you can automate updating packages when new versions of the tools are created so there's a long-term payoff.

Why do you feel the Live CD has been successful?

Last time I counted the downloads, which was November of 2009, the total was just over 330,000 downloads from the first SoC release. That's a huge number of people who've got to know OWASP and application security. I've also heard from several instructors who've used it for training classes. One of the most surprising developments was the inclusion of the OWASP Live CD in a college text. In fact a few weeks ago at AppSec EU 2010 in Stockholm, I had one of the attendees recognize me and thank me for the latest WTE release so how can I complain?

How has the LiveCD Project affected your career?

First, just being active and involved in OWASP has been HUGE. For me, the OWASP Live CD was a great way to get into and involved with the OWASP community. Because of the Live CD and speaking I've done about the project, I've been to Portugal, Poland, Brazil and multiple places within the US. I've met a ton of really brilliant OWASP people and, got my name out into the application security community.

I also believe the work on the Live CD and with the Global Projects Committee helped me to become a OWASP Foundation board member. Helping the other OWASP board members work on fulfilling OWASP mission has been a wonderful experience.

On a pragmatic level, I've been a paid trainer multiple times because of the Live CD. Not to mention that having active involvement with OWASP and being on the OWASP board are very beneficial resume material. I am certain that my OWASP experience was a large factor in my current position with Trustwave's SpiderLabs.

What's next?

For WTE, I'd like to grow the number of contributors so that I don't become a bottle neck as I've been earlier this year. I'd also like to expand the packages that are part of WTE to include static analysis tools, Flash tools, and perhaps some vulnerable applications too.

As for my role with the OWASP board, I'm actively working on the infrastructure which runs OWASP's operations. Hopefully, OWASP will have a new, enterprise-grade infrastructure to help move the community to a whole new level of success.

Anything else you would like to share with the Project fans?

I can't say enough for those that make licensing easy to find and one of the common open source licenses like GPL, Apache or BSD. Trying to figure out if I can safely include tools on WTE turned out to be a MUCH bigger pain that I expected. You have no idea how many projects I had to download and explore before I could figure out the license.

The one thing to share with the project fans is please send feedback, suggestions, complaints or whatever to the mail list or on the project forums. The best way for the project to get better is for those of us working on the project to know what works and what doesn't.

Follow OWASP

OWASP has a Twitter feed

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

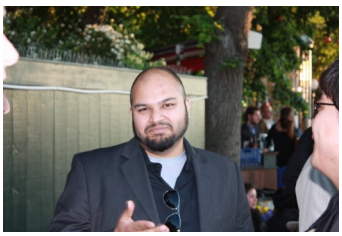
Can you help OWASP make *every* application developer knowledgeable about the OWASP Top 10? Share this link: OWASP_Top_10_-_2010.pdf

ESAPI Update
Jeff Williams

The NSA has offered to perform an in-depth security review of ESAPI and make the results available. For those who don't have much experience with the NSA, a major part of their mission is defense. In the past, they supported the National Computer Security Conference, created the Rainbow Series, and sponsored the SSE-CMM. More recently they've been involved in SCAP and SE-Linux.

The NSA team supporting OWASP is very experienced in cryptography and application reviews lined up already and they will be starting their work very soon. They are going to focus on the Java ESAPI version first, and may support other language versions when they're ready – meaning their crypto is at least up to the Java 2.0 level. Their initial estimate is that the review will take several months to complete.

I'm extremely excited about this development, and I'll keep you posted on their progress.


OWASP Projects Update
Paulo Coimbra, OWASP Project Manager

New projects

http://www.owasp.org/index.php/Projects/ESAPI_Swingset-

http://www.owasp.org/index.php/Projects/Owasp_Esapi_Ruby

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

Project with new releases recently launched

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

Project seeking contributors to launch new release

http://www.owasp.org/index.php/Category:OWASP_Testing_Project#tab=Project_About (Testing Guide V 4.0)

Project that has been re-launched

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

OWASP ESAPI Swingset Project has a new leader

Cathal Courtney. Please welcome him!

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

This project has already produced a release, the ESAPI Swingset RC 4, which has been made available right now – please glance at it.

http://www.owasp.org/index.php/Projects/ESAPI_Swingset/Rzeleases/Current

OWASP Site
Google Analytics

Site visits for May: 233,765
Pageviews: 573,144
Pages/Visit: 2.45
Average Time on Site: 00:02:57
58.3% New Visits
http://conf.oss.my
Content overview:
/index.php/Main_Page 63,070 page views
/index.php/
Category:OWASP_Top_Ten_Project 21,610 page views
/index.php/
Category:OWASP_WebScarab_Project
16,615 page views
/index.php/Category:
OWASP_WebGoat_Project
13,502 page views
/index.php/Category:OWASP_Project
10,915 page views
Top Keywords:
Owasp, webscarb, owasp top 10, webgoat, sql injection.

OWASP O2 Platform
Dinis Cruz

I'm happy to announce that I finally published a first major release of the OWASP O2 Platform (with an installer, documentation+videos and a number of key/unique capabilities).

There is a brand new GUI which makes a massive difference in finding the available scripts, tools and APIS that exist inside O2 (if you tried the previous versions you will really appreciate this) . You can see the new GUI and access the download link at this page: http://www.o2platform.com/wiki/O2_Release/v1.1_Beta

PLEASE TRY IT, and provide feedback on: what you like, what works, what doesn't work, what could be improved, etc... (if you want to file a bug, please use this web interface http://code.google.com/p/o2platform/issues/list)

There is enough functionality + capabilities + power in this version of O2, that I finally have the confidence to make this direct request for you, knowing that no matter what area of Web Application Security you are involved in, there will be an O2 Script/Module/Tool that will make you more productive.

Since the new GUI is very recent, most documentation and videos available start with the previous GUI. But since I can now easily create detailed WIKI documentation pages and/or videos using O2 , my plan is to reply to your questions that way (i.e. with a video or wiki page)

OWASP AppSEc Research Summary
John Wilander

The upsized European OWASP AppSec conference took place in Stockholm, June 21-24. Three chapters – Sweden, Norway, and Denmark – together with Stockholm University hosted the event and welcomed 275 attendees to a sunny Scandinavia.

The first two days offered training in secure development, pen testing, malware analysis, and architecture review. During the joint dinner Monday evening American guests learnt how to eat hamburgers with fork and knife – a Swedish specialty :).

The conference days had three parallel tracks with talks and demos from both industry and academia. Keynotes were given on the future of browser security and the development of the SDL since the nineties. The sponsor expo featured 12 companies headlined by Diamond sponsor Microsoft.
On Wednesday night conference attendees along with significant others were welcomed to Stockholm City Hall and a three course gala dinner with entertainment. A fabulous community celebration sponsored by Google. During dinner the tables competed for champagne in three categories – culture, geekiness, and arts. The final challenge of building an OWASP -inspired statue out of pipe cleaners spurred a lot of creativity. Or was it the wine?

The organizers would like to thank everyone who supported and took part in the first OWASP AppSec Research conference. See you next year in Dublin!

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, AppSec Research Stockholm photos: Boris Hemkemeier