September, 2010

OWASP

The Open Web Application Security Project

OWASP AppSec Conferences

October 8th
OWASP 1-day event
Minneapolis, MN

October 20th, 2010
AppSec Germany 2010
Nurnberg, Germany

October 20th—23rd, 2010
OWASP China Summit 2010

October 29th, 2010
LASCON
Austin, TX

November 8th-11th, 2010
AppSec DC 2010
Washington, DC

November 5th
OWASP Day V-2010
Trento, Italy

November 9th, 2010
CONSIP
Rome, Italy

November 11-12th, 2010
IBWAS
Lisbon, Portugal

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

November 20th, 2010
BASC
Boston, MA

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

OWASP AppSec USA 2011—Minneapolis

Mark your calendars: OWASP AppSec USA 2011 will be held in Minneapolis, MN at the Minneapolis Convention Center from September 20th –23rd, 2011. Follow @owasp and AppSec USA Linkedin group for upcoming news.

Samy Kamkar—OWASP Europe Tour 2010 & More

OWASP Leeds—September 15th, 2010

OWASP Ireland—September 16 –20th, 2010

OWASP Belgium—September 21, 2010

OWASP Netherlands—September 23, 2010

BruCON 2010—September 23-25th, 2010

OWASP London—October 1st, 2010

OWASP Sweden—October 4th, 2010

OWASP Denmark—October 6th, 2010

Athens Digital Week - October 7-8th, 2010

OWASP Slovakia—October 11th, 2010

OWASP Portugal - October 15th, 2010.

LASCON 2010—October 29-31st, 2010

AppSec Brazil 2010—Nov 16th-19th, 2010

"OWASP on the Move " and OWASP Chapter funds were used to drive attendance at OWASP chapters in the EU and more. The tour has had great success and been very well received.

OWASP APPSEC DC 2010 Nov 8th - 11th

M M X

AppSec DC 2010 is the East Coast's premiere Information Security Conference for 2010.

Building on the success of last year's AppSec DC 2009, the AppSec DC team is working to further the OWASP conference mission of hosting the best minds in application security in a forum to share innovations and ideas. AppSec DC's unique location and relationship with federal entities in the Washington DC area also allows OWASP and its affiliates to continue to reach out to and interact with the federal government in this time of ever-increasing National Security concerns.

This year, in addition to content from industry leaders in application security research, entities within the Department of Homeland Security (DHS), the Department of Defense (DoD), the National Security Agency (NSA), the National Institute of Standards and Technology (NIST) and other government agencies will be contributing content focusing on Software Assurance and the role that that plays areas of extreme concern in the current climate, such as protecting Critical Infrastructure or Supply Chain Risk Management. If you work in or with the federal government, regardless of branch or service, this is likely a critical concern for some subset of your workplace, and the combination of content at this event will provide an incredible value to your and your employer.

In addition to two days of great speaking content, keynotes and panels, AppSec DC will also provide two days of world class training on applications security from a variety of vendors at a fraction of the cost found at other events. This year featured panels will not only include federal "what works" in application security, but several other areas of interest so that there will be engaging discussion for all types of attendees. The AppSec DC crew is also working a great vendor space and engaging contests, including a hacking competition built specifically for our event.

AppSec DC will take place at the Walter E. Washington Convention Center in Washington DC on November 8-11. Training will be on the 8th and 9th, talks will be on the 10th and 11th. Our partner hotel is the Grand Hyatt again this year, and a discounted rate will be available for attendees who register in Advance.

Mozilla at AppSec USA 2010

At AppSec USA OWASP leaders met the Mozilla team in attendance and engaged in a working discussion browser lunch. This is just one example of an OWASP event and its role played in bringing great application security minds together to discuss real problems - and more importantly real solutions to application security issues.

Here is a link to Sid Stamm's of Mozilla's blog.

http://blog.sidstamm.com/2010/09/appsec-usa-was-great.html

During AppSec USA 2010 Mozilla introduced Content Security Policy (CSP). Content Security Policy mitigates the risk of Cross Site Scripting (XSS), clickjacking, and packet sniffing attacks. The following link includes and introductory overview of Content Security Policy which has a reference section which includes links to the spec and how to deploy CSP on a site.

https://developer.mozilla.org/en/Introducing_Content_Security_Policy

As a result of the browser security lunch at AppSecUSA 2010 a new browser security project has been created. This project is still in its infancy, but you can find lots of good links related to security features in Firefox.

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

Jim Manico interviewed Brandon Sterne on the Content Security Policy release at AppSec 2010 in Ep 75,

OWASP in support of Mozilla has a XSS project in the works - http://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OWASP-DV-001) The Cross Site Scripting Prevention Cheat Sheet http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

and is putting together an OWASP awareness week.

For more information on the most recent XSS attacks: http://xssed.com/archive/special=1

OWASP New Project and Releases

New Project:

OWASP Alchemist Project, co-lead by Bishan Singh, Chandrakanth Narreddy and Naveen Rudrappa.

New Releases:

The Top Ten - French Version has been released.

The ModSecurity 2.0.6 version has been 'formally' reviewed and rated as a Stable Release. http://www.owasp.org/index.php/Projects/OWASP_ModSecurity_Core_Rule_Set_Project/Releases/ModSecurity_2.0.6/Assessment

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

Project contributor and the reviewers - Ryan Barnet, Brian Rectanus, Ivan Ristic and Leonardo Cavallari.

OWASP Podcasts Series

Hosted by Jim Manico

Ep 71 Top Ten— Robert Hansen (Redirects)

Ep 72 Ivan Ristic (WAF)

Ep 73 Jeremiah and Robert Hansen

Ep 74 Eoin Keary (Code Review)

Ep 75 Brandon Sterne (Content Security Policy)

Ep 76 Bill Cheswick (Account Lockout)

Follow OWASP

OWASP has a Twitter feed

Www.twitter.com/owasp

OWASP cited in W3C's Mobile Web Application

OWASP is being cited in W3C's forthcoming Mobile Web Application Working Document released in September 2010

Best Practices document.

http://www.w3.org/2005/MWI/BPWG/Group/Drafts/BestPractices-2.0/latest

OWASP Singapore

Cecil Su

OWASP Singapore is co-organizing a CtF competition with SITSA (Singapore IT Security Authority) which is part of the Ministry of Home Affairs. The CtF is opened to all the mainstream institutes of higher learning in Singapore. This is the First time that the game is hosted in this GovernmentWare 2010 Conference & Exhibition, an annual event since 1991.

http://www.govware.sg

It will be a competition where tertiary students can test their IT security skills in a safe and realistic environment. SITSA and OWASP maintain that information security should not be a privileged skill and everyone should have the opportunity to learn about it in this internet age.

National Seminar on Information Security and Cryptography

Lucas Fereira

The Security Office of the Brazilian Presidency is organizing the III Senasic (National Seminar on Information Security and Cryptography - https://wiki.planalto.gov.br/comsic/bin/view/ComSic/IIISENaSIC). This seminar aims to gather the Brazilian Infosec community to work together and exchange information on a variety of important topics.
The seminar will contain a few presentations by Brazilian and international speakers and a series of panels to discuss themes such as:

- Randomicity
- UAV communications security
- Quantum theory applications
- Important projects for the National Network on Information Security and Cryptography
- Parameter definition for a Brazilian Cyber Defense Exercise

The OWASP Brazilian Chapter will be represented in the seminar by Lucas C. Ferreira and Wagner Elias, which will, respectively, coordinate and participate in the panel that will define the parameters for a Brazilian Cyber Defense Exercise.

The main objective of this panel is to define the needs and possibilities for an exercise of defending important infrastructures and networks. The panel will gather specialist from industry and academia in a cooperative environment to discuss the ENaPI (National Exercise on Infrastructure Defense). The resulting ideas should be

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

DENIM GROUP

art of defence

WhiteHat SECURITY

HARRIS CONNECT

DREAMLAB TECHNOLOGIES

New Corporate sponsors in August and September: Thank you for your support!

mozilla Firefox

amazon

Digital River

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 Project Updates

Paulo Coimbra

The OWASP Development Guide has new project leaders. Vishal Garg and Anurag Agarwal are currently assuming the role previously performed by Andrew van der Stock. We thank the latter for his relevant contribution and wish the best to the new leaders.

http://www.owasp.org/index.php/User:Vishal_Garg

http://www.owasp.org/index.php/User:Vanderaj

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

Three major OWASP Guides – Development, Testing and Code Review – are being pushed by their leaders and contributors to reasonably soon publish a new release. Each of them has been funded with 5,000 dollars.

http://www.owasp.org/index.php/Category:OWASP_Testing_Project#tab=Project_About http://www.owasp.org/index.php/Category:OWASP_Guide_Project#tab=Project_About

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

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

The OWASP CTF Project has a new leader. Martin Knobloch has been replaced by Steven van der Baan. We thank Martin for his relevant contribution and wish the best to the new leader.

http://www.owasp.org/index.php/User:Knoblochmartin

http://www.owasp.org/index.php/User:Steven_van_der_Baan

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

OWASP ModSecurity CRS Project has been under intense work development and has produced recently various releases. Its version ModSecurity2.0.6 has been reviewed and assessed and was consequently rated Stable Quality Release. We thank and congratulate Ryan Barnett and the release reviewers, Ivan Ristic and Leonardo Cavallari

http://www.owasp.org/index.php/User:Rcbarnett

http://www.owasp.org/index.php/User:Ivanr

http://www.owasp.org/index.php/User:Leocavallari

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

The OWASP Alchemist Project, co-lead by Bishan Singh, Chandrakanth Narreddy and Naveen Rudrappa, has been recently set up. Please welcome them!

http://www.owasp.org/index.php/User:Bishan_Singh

http://www.owasp.org/index.php/User:Chandrakanth_Reddy_Narreddy

http://www.owasp.org/index.php/User:Naveen_Rudrappa

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

In a record time the OWASP Secure Coding Practices - Quick Reference Guide has been setup and has had its second release assessed and consequently rated as Stable Quality. We thank and congratulate the project leader, Keith Turpin, and the release reviewers, Ludovic Petit and Brad Causey.

http://www.owasp.org/index.php/User:Keith_Turpin

http://www.owasp.org/index.php/User:Ludovic_Petit

http://www.owasp.org/index.php/User:Bradcausey

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

The OWASP Enterprise Application Security Project has been recently adopted by Alexander Polyakov. We thank him and wish him the best of success.

http://www.owasp.org/index.php/User:Alexander

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

OWASP College Chapters Program has been recently setup and is being led by Jeff Williams. This initiative will help to extend application security into colleges and universities worldwide.

http://www.owasp.org/index.php/User:Jeff_Williams

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

The OWASP AppSensor Project has important developments and is under review targeting a Stable Release rating.

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

http://www.owasp.org/index.php/User:MichaelCoates

The Google Hacking Project's Inquiry has been concluded with the publication of the OWASP Global Projects Committee's Report and the OWASP Board Resolution.

http://www.owasp.org/index.php/OWASP_Inquiries/Google_Hacking_Project

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

Projects to be soon set up:

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

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

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

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

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

Lonestar Application Security Conference (LASCON) 2010

Well over 100 people have registered so far for the Lonestar Application Security Conference (LASCON) happening in Austin, TX at the Norris Conference Center on October 29, 2010.

Keynote: Matt Tesauro (OWASP Foundation Board Member) and four excellent tracks: Technical Track, Management Track, OWASP Etcetera Track and Speed Debates.

Speakers include:

- Robert Hansen,
- Samy Kamkar
- Dan Cornell
- Chris Eng
- Josh Sokol
- James Flom
- And many others

Registration is easy. Just go to http://guest.cvent.com/d/vdqf7g/4W and enter your name and e-mail address. Tell us whether you're an OWASP member or not (LASCON will validate against OWASP membership list.) If not you pay an extrat $50 which just the cost of a full year of OWASP membership.

OWASP Foundation

9175 Guilford Road
Suite #300
Columbia, MD 21046

Phone: 301-275-9403
Fax: 301-604-8033
E-mail: owasp@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 USA 2010 photos: Chuck Espinoza