OWASP
SUMMIT
2011
LISBON
PORTUGAL
FEB 8-11

HELLO WORLD!

OWASP SUMMIT 2011 KICKS OFF MASSIVE APPLICATION SECURITY OUTREACH PROGRAM

"I saw the 'blossoming' of OWASP in Portugal's Spring. From an external viewpoint, OWASP has moved from niche to widely relevant, from localized to global, from pentesting to SDLC, from server to every component of the application's delivery and use, from infosec to business process relevance." – Colin Watson

PRESS RELEASE

Hello World! OWASP Summit 2011 Kicks Off Massive Outreach Program

Lisbon, Portugal, February 15, 2011 - The Open Web Application Security Project (OWASP) today announced the results from its 2011 OWASP Summit. Over 180 application security experts from over 120 companies and 30 different countries joined forces to plan, build, and execute programs to improve the security of the world's software applications. The Summit was a significant step towards OWASP's mission to ensure all types of organizations are empowered to build, select, and use software applications securely.

OWASP launched and advanced dozens of concrete initiatives to bring application security to governments, educational institutions, browser vendors, standards bodies, software development teams, and mobile platform vendors. Delegates gathered outside Lisbon, Portugal for a week of interactive working sessions and discussions. OWASP Summits are unlike conferences with static presentations. Instead, working sessions are used to author documents, create software, draft standards, and forge lasting relationships.

Some highlights from the 2011 OWASP Summit include:

- **OWASP-Portugal Partnership** – OWASP has been working to establish relationships with various governments around the world, particularly the United States, Brazil, Portugal, and Greece. At the Summit, OWASP representatives worked directly with senior Portuguese IT officials to establish a protocol for working with Portugal to improve their application security capabilities.

- **OWASP Outreach to Educational Institutions** – Reaching students is a unique opportunity to reach developers early in their development. At the Summit, delegates drafted an OWASP Code of Conduct for Educational Institutions, created a detailed plan for OWASP Student Chapters and continued development of the OWASP "Academies" Portal with extensive education and training materials.

- **OWASP Industry Outreach** – OWASP resolved to develop industry working sessions to be held at major OWASP conferences starting with OWASP EU 2011 in Dublin, Ireland. The objective of these sessions will be to solicit feedback from industry players to help better focus OWASP efforts and make sure OWASP deliverables are relevant to industry concerns.

- **OWASP Browser Security Project** – The Summit brought representatives from browser vendors Mozilla, Google, and Microsoft together with leading security researchers to discuss, and strategize about browser security issues. Several new OWASP initiatives were launched, including a browser security scorecard project based on OWASP's recently created browser testing framework. There were extensive discussions on browser initiatives such as Mozilla's Content Security Policy (CSP) and browser sandboxes.

- **OWASP-Apache Partnership** – OWASP forged a relationship with the Apache Software Foundation (ASF) to start the process of sharing OWASP software projects with the ASF with the intention of including OWASP-provided code in Apache projects. The intention of this collaboration is to improve the security of the widely-used ASF Open Source software, as well to improve visibility for OWASP efforts.

- **OWASP Mobile Security Initiative** – OWASP made progress on their upcoming Top 10 Mobile Vulnerabilities and Top 10 Mobile Defenses lists. In addition, OWASP resolved to reach out to mobile platform vendors to work with them on integrating better security into their environments.

- **OWASP Governance Expansion** – OWASP updated its Charter and worked out procedures for the upcoming Board elections. These governance updates will help best support the dynamic and growing OWASP community.

- **International Focus** – OWASP reaffirmed a commitment to be a truly international organization. Delegations from several countries and regions around the world including Asia-Pacific and South America participated in outreach workshops. Addition focus has been given to expanding international representation on OWASP's Board and Global Committees.

- **Application Security Programs** – To help organizations actually implement application security programs, we are mapping OWASP projects to all major approaches, including OWASP OpenSAMM, Microsoft's SDL, and BSIMM.

- **Application Security Certification** – OWASP reaffirmed its commitment to avoid becoming a certification body. Instead, it created the OWASP Code of Conduct for Certification Bodies that defines what application security certification program should entail.

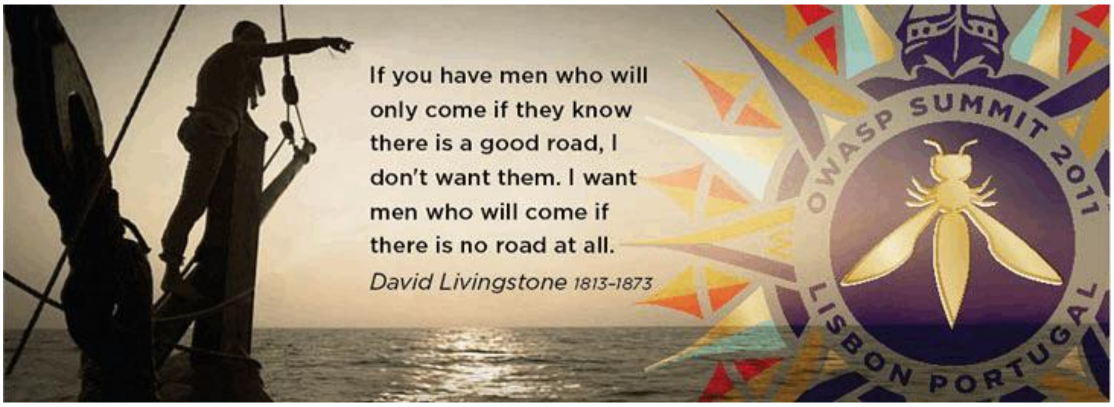
The full results of the Summit will be captured and released as an OWASP Report. The results will be released for comment and then ratified as a final deliverable. For more information, including notes, video, pictures, and other deliverables, please visit www.owasp.org.

About OWASP

The Open Web Application Security Project (OWASP) is a worldwide free and open community dedicated to improving the security of application software worldwide. OWASP's mission is to make application security visible so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. Find out more at www.owasp.org.

Reader Contact Information:

OWASP Foundation, 9175 Guilford Road, Suite #300; Columbia, MD 21046,
Tel: (301) 275-9403, Fax: (301) 604-8033, www.owasp.org,
kate.hartmann@owasp.org


If you have men who will only come if they know there is a good road, I don't want them. I want men who will come if there is no road at all.
David Livingstone 1813-1873
OWASP SUMMIT 2011
LISBON PORTUGAL

ABOUT THE OWASP SUMMIT

OWASP Summits are where application security experts can meet in a neutral non-commercial setting to discuss plans, projects and solutions for the future of application security.

<u>The Summit is NOT a conference</u> - there are no talks or training seminars. This is an opportunity to do actual work to further the field of application security. Participants will stay in shared accommodations and collaborate to produce tangible progress towards influencing standards, establishing roadmaps, and setting the tone for OWASP and application security for the coming years.

Anyone can attend the Summit! OWASP community members, application security experts, industry players, and developers are all welcome at the Summit. Attendees come ready to work and produce deliverables that advance the state-of-the-art in application security.

Many of the working sessions were created "dynamically" by the attendees. Anyone can propose a new working session, sign up for a room and time slot, and meet to work with other interested parties. Many of the main sessions ended up spawning multiple dynamic sessions to accomplish particular goals.

Much of the work that goes on at the Summit is at meals, social events, or hallways. We live together, eat together, and play together. We work hard and play hard for a solid week focused on application security. Even the OWASP Band is free and open for anyone to participate.

SUMMIT QUOTES

- *"I never would have found myself in a meaningful dialog with Google had it not been for this conference." – Robert Hansen (RSnake)*

- *"I needed to discuss complex security problems that required input from a number of different people to solve it. At OWASP Summit we brought things together!" -- Tobias Gondrom, IETF*

- *"Seeing and meeting the world's best-known security professionals at one place! Great party!" – Achim Huffmann*

- *"The Summit had an intense feeling of activity, information exchange, and planning" – Chris Wysopal, Veracode*

- *"It was interesting to see how much work got done in less than a week!" – Vishal Garg, AppSecureLabs*

- *"I'd like to say that the Summit has been absolutely a great experience. It's the most useful security event that I've been to in the last few years. This most definitely was one of those events where things actually got done!" – Edward Bonver*

© Ofer Maor

- *"The Summit is THE place to come together and transform great ideas into reality" – Cecil Su, Grant Thornton*

- *"Browser Security Track has made great progress in terms of outreach, involvement, and cross-company collaboration. Other groups should replicate this behaviour."*

© Ofer Maor

- *"The system really works! The process is transparent and OWASPers are very committed in having a more secure world" – L. Gustavo C. Barbato - Dell*

- *"I saw the 'blossoming' of OWASP in Portugal's Spring. From an external viewpoint, OWASP has moved from niche to widely relevant, from localized to global, from pentesting to SDLC, from server to every component of the application's delivery and use, from infosec to business process relevance." – Colin Watson, Watson Hall*

- *"I enjoyed the sheer energy of the group"*

- *"I really liked the format of many sessions that were panel and open discussion around looking at problems and finding solutions"*

- *"It was a great summit and one of the best security event in the world" – Mohd Fazli Aaran – USDCMY*

- *“It worked democratically and made everyone give idea, complaint, planning, critic, and opinion” – Mohd Fazli Aaran – USDCMY*

- *“The small working groups got the conversation flowing between many people of different viewpoints” – Chris Wysopal, Veracode*

- *“It was so cool to get all these security experts under the same roof and you could pickup anybody’s brain about any security issue”*

- *“For those who missed the Summit: you missed out, try to make the next one”*

- *“It is a great way to meet and exchange experience with some of the most important IT professionals of the world” – Massimo Biagiotti – Business.E*

- *“The best thing was the exceptional discussions generated from the main topics and continued into the late evenings.” – Steve Schwartz, Stack and Liu*

- *“There were great discussions both inside and outside working sessions. I can’t wait to see the results of the seeds planted.” Juan Carlos Calderon, Softtek Mexico.*

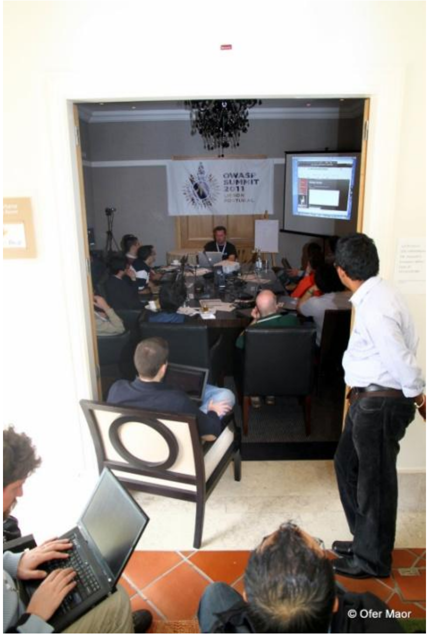
- *“The best was to see how ‘linking’ frameworks for education, government, and third-parties is taking shape and finally seems that it can materialize. It will be a huge enabler for OWASP mission.” Juan Carlos Calderon, Softtek Mexico.*

- *“Best part was being able to gather and talk with the best security minds in the world to solve difficult security problems.” – Abraham Kang*

- *“Attending the Summit was a unique experience because it was not about presentations, but actually having an active contribution to the discussions, knowing that all your contributions are going to make a difference to the future of OWASP.” – Vishal Garg, AppSecureLabs*

- *“The evening sessions are great. Highly productive, relaxed atmosphere, laughing, and beer.” –Bart De Win*

- *“The best experience was seeing so many companies like Microsoft, Google, Mozilla, etc… send large contingents to Portugal to participate in our Summit” – Dave Wichers, Aspect Security*


© Ofer Maor

- *"We arrived, we were impressed, and we were inspired!" – Cecil Su, Grant Thornton*

- *"The Summit is a place to work hard, play hard, and get things done." – Abraham Kang*

- *"Bringing together the best security experts and leaders from around the world and discussing solutions for the future of web application security" – Tobias Gondrom, IETF*

- *"Get to know and listen to the best of breed in app security in the world" – L.A. Vilares Da Silva, Open*

© Laurence Casey

COMPANIES PARTICIPATING IN OWASP SUMMIT

mozilla FOUNDATION
Microsoft
NOKIA
Google
Symantec.
McAfee SECURITY
PayPal
DELL
Minded security
SECURICON
Grant Thornton
springsource A division of vmware
ERNST & YOUNG Quality In Everything We Do
ASPECT SECURITY Application Security Experts
RUHR-UNIVERSITÄT BOCHUM
Security Innovation
ascure
WATSON HALL
MANDIANT
(ISC)2
SIC [V] sec
DENIM GROUP
GEORG-SIMON-OHM HOCHSCHULE NÜRNBERG
PervaSec
GOTHAM DIGITAL SCIENCE
PRAETORIAN
SYNTAX
fishnet SECURITY
FIS
VERACODE
COMPASS SECURITY
VerSprite Navigate Beyond Risk
SEC Consult
Trustwave SpiderLabs
Softtek
AUDITMARK
Rockwell Automation
cigital Software Confidence. Achieved.
AppSecure LABS
HACKTICS
armoredcode.com we make software you'll love to use
WUL4 WHAT YOU LOOK FOR
lusolabs mipe tecnologias de informação
armorize
CENZIC
sait zenitel
L7 Sécurité
osdc.my
dri
BUSINESSe drive your e-success

WORKING SESSIONS

The Working Sessions are how we actually produce results at the OWASP Summit. Each working session meets in a room where everyone participates to discuss, argue, collaborate, and most importantly produce a deliverable.

FIXED WORKING SESSIONS

Tuesday, February 8

XSS and the Frameworks
XSS - Awareness, Resources, and Partnerships
OWASP Training
OWASP Academies
WAF Mitigations for XSS
Virtual Patching Best Practices
OWASP Exams
University Outreach
Risk Metrics
Metrics and Labeling
Government Outreach
Counting & scoring application security defects
OWASP Secure Coding Practices Project
Enterprise Web Defense Roundtable
Threat Modeling

Wednesday , February 9

Protecting Information Stored Client-Side
Common structure and numbering for all guides
OWASP Common vulnerability list
Providing Access to Persisted Data
OWASP Testing Guide
Site Security Policy
OWASP Industry Outreach
Microsoft's SDL in 16 steps (and lessons learned)
OWASP Projects
DOM Sandboxing
Overhauling the OWASP Website

Thursday, February 10

Contextual Output Encoding
ESAPI-CORE
OWASP Board/Committee Governance
Board Structure
ESAPI for Ruby
Applying ESAPI Input Validation
Professionalize OWASP
OWASP funding and CEO discussion
EcmaScript 5 Security
OWASP Certification
HTML5 Security
What is an OWASP Leader?
Tracking OWASP Participation
Mobile Security
OWASP Licensing

DYNAMIC WORKING SESSIONS

Tuesday, February 8

OWASP vs Government vs Universities
Building the OWASP Brazilian Leaders Group
Common structure and numbering for all guides
OWASP Board/Committee Governance
XSS and the Frameworks
OWASP Academy Portal
Browser Security meet up

Wednesday, February 9

Formal Risk Assessment Methods
OWASP TOP 10 online training in Hacking-Lab
Defining AppSensor Detection Points
OWASP Asia/Pacific working group
Development Guide
Defining a minimal appsec program for universities, governments, and standards bodies
OWASP Portuguese Language Project
ASVS Project
Secure development guidelines for smartphone developers
Privacy - Personal Data/PII, Legislation and OWASP
Mobile Security
Should OWASP work directly with PCI-DSS?
OpenSAMM
Threat Modeling
Governance Part Two

Thursday , February 10

How can OWASP reach/talk/engage with auditors
Hackademic Challenges
OWASP Java Project
OWASP Exams
Industry - Healthcare
Industry - Banking/Finance
Developer Outreach
Scaling Web Application Security Testing
The future of OpenSAMM
Corporations at the Summit & funding opportunities
Conferences - Improving Conference Planner Support
OWASP College Chapter Program
Vulnerability Disclosure Policies
Global Conferences Committee Monthly Meeting
Planning South America/Central America AppSec Chapters
O2 Platform
ESAPI framework integration
Education

ATTENDEES

Adamski, Lucas
Agarwal, Anurag
Aguilera, Vicente
Agustini, Alexandre
Akhmad, Zaki
Alamri, Lorna
AlBasha, Talal
Angal, Rajeev
Aniceto, Alexandre
Aryavalli, Gandhi
Barbato, L. Gustavo C.
Barnett, Ryan
Baso, Sarah
Batista, Marco
Bergling,Mattias
Bernik, Joe
Biagiotti, Massimo
Bonver, Edward
Booth, Rex
Brennan, Tom
Brewer, Deb
Bristow, Mark
Brzozowski, Daniel
Buetler, Ivan
Calderon, Juan Carlos
Campbell, David
Casey, Larry
Causey, Brad
Chalmers, Matthew
Chandra, Pravir
Cheng, Steven
Clarke, Justin
Coates, Michael
Coimbra, Paulo
Cornell, Dan
Corry, Bil
Cruz, Dinis
Cruz, Sarah
Dawson,Isaac
De Win, Bart
Deleersnyder, Seba
DiPaola, Stefano
Donovan, Fred
Durkee, Ralph
Dworakowski, Wojciech
Elias, Wagner
Eng,Chris
Evans, Arian
Falkenberg, Andreas
Fazli Azran, Mohd
Fedon, Giorgio
Ferraz, Felipe
Ferreira, Lucas C.
Fette, Ian
Fitzgerald, Alexis
Fitzhugh, Justin
Flores, Mauro
Fontes, Antonio
Fort, Julio Cesar
Fortuna, Pedro
Frosch,Tilman
Galvao, Pedro
Gao, Helen
Garrancho, Bruno
Garg, Vishal
Gomes, Leandro
Gondrom, Tobias
Hansen, Robert
Hartmann, Kate
Heiderich, Mario
Heyes, Gareth
Hinojosa, Kuai
Hodges, Jeff
Hoff, Jerry
Hoffman, Achim
Hofmann, Chris
Hogben, Giles
Ichnowski, Jeff
Jorge, Eduardo
Jimenez, Juan Jose Rider
Kang, Abraham
Keary, Eoin
Knobloch, Martin
Kosturjak, Vlatko
Koussa, Sherif
Kuivenhoven, Marinus
Kumar, Nishi
Lacerda, Filipe
Lauritão, Rogério
Li, Jason
Lindsay, David
Long, Jeremy
Loureiro, Nuno
Luptak, Pavol
Lyon, Chris
Manico, Jim
Maor, Ofer
Mancini, Lucilla
Martinez, Mateo
Martorella, Christian
Matatall, Neil
Melo, Ricardo
Mendo, Tiago
Meucci, Matteo
Nagra, Jasvir
Neaves, Tom
Paiva, Sandra
Papapanagiotou,
Konstantinos (Kostas)
Pegorelli, Marta
Perego, Paolo
Potjes, Linda
Reinhart, Ralf
Richler, Heiko
Rohr, Mathias
Ross, David
Roth-Mandutz, Elke
Saario, Mikko
Samuel, Michael
Schmidt, Chris
Schuh, Justin
Schwartz, Stephen
Searle, Justin
Secker, Tanya
Serrao, Carlos
Stasinopoulos, Anastasios
Sterne, Brandon
Steven, John
Su, Cecil
Tasar, Vehbi
Taylor, Jason
Tesauro, Matt
Thomas, Mark
Tomhave, Benjamin
Turpin, Keith
Tusha, Ervis
UcedaVelez, Tony
Uhley, Peleus
van der Baan, Steven
Vasilopoulos, Kyprianos
Vela, Eduardo
Vilares Da Silva, Luis
Vlachos, Vasileios
Vroom, Ferdinand
Watson, Colin
Weston, David
Wichers, Dave
Wilander, John
Williams, Jeff
Wilson, Doug
Wuensch, Stefan
Wysopal, Chris
Yeo, John
Zusman, Mike