OWASP FOUNDATION PRESENTS

APPSEC USA

NOVEMBER 18 - 21

NY MARRIOTT MARQUIS, NYC

2013

CONFERENCE PROGRAM

Presented by OWASP Foundation | Host by the OWASP New York City Chapter

OWASP FOUNDATION PRESENTS

APPSEC USA 2013

NOVEMBER 18 - 21 | NEW YORK MARRIOTT MARQUIS, NYC

Welcome to New York City!

Thank you for attending AppSec USA and supporting the OWASP Foundation. This year's event is a product of the blood, sweat, and energy of our unpaid volunteers who have worked tirelessly alongside the paid Foundation employees to put on OWASP's biggest conference to date and raise money to support the OWASP mission around the world.

A few months ago, one of our community members told me he was worried about AppSec USA being TOO big this year. He said that what he and others value most about OWASP conferences is the opportunity to engage with the community – catching up with old friends as well as meeting new ones, and discussing the cause of software security. He pointed out that as a conference grows in size, the sense of community and feeling like more than a number diminishes for attendees.

This community member's concern struck a chord with me and I have thought about how to support a successful, profit-generating event, without losing the core of what makes OWASP conferences unique, its community. What the volunteers, staff, and I came up with is a conference with great value and educational content as well as an opportunity to engage and be a part of the OWASP "family." Our community activities include open mic sessions (utilizing community energy boards), the OWAS Project Summit, Chapter Leader Workshops, "The Great Bug Smash of 2013", and Lockpick Village. We also have 2 capture the flag competitions and OWASP Jeopardy. Finally, we have provided space for you to collaborate as builders, breakers, and defenders to discuss the state of software security AND be a part of the solution.

We are thrilled to be hosting this year's event in the heart of New York City. New York exerts a significant impact upon commerce, finance, media, art, fashion, research, education, entertainment, and technology. As the home for the United Nations Headquarters, NYC is an important center for international diplomacy and has been described as the cultural capital of the world.

What better place to host the 2013 OWASP Foundation's premier software security conference and gathering of community members from around the world? Are you as excited as we are?!?

During your time at AppSec USA we trust you will take the opportunity participate with the community and see the city. We have made every effort possible to accommodate our attendees by facilitation of events, activities, and collaboration sessions. Enjoy!

Sarah Baso
Executive Director
OWASP Foundation

OWASP FOUNDATION PRESENTS

APPSEC USA 2013

NOVEMBER 18 - 21 | NEW YORK MARRIOTT MARQUIS, NYC

TABLE OF CONTENTS

SCHED

Personalize Your Conference Experience!

Check out our customizable mobile-friendly schedule at

http://appsecusa2013.sched.org/mobile

twitter

@AppSecUSA
#AppSecUSA

UPCOMING EVENTS
Save the Date!

OWASP
Open Web Application Security Project

Presents:

AppSec California 2014 | Santa Monica

January 27-28

appseccalifornia.org

AppSec AsiaPac 2014 | Tokyo

March 17th - 20th

appsecapac.org

AppSec EU Research 2014 | Cambridge

June 23rd - 26th

appsec.eu

AppSec USA 2014 | Denver

September 16th - 19th

appsecusa.org

Hours of Operation

Conference Rooms

We have a full conference schedule this year and have events running on Wednesday, Nov 20th from 8:30 PM to 11:59 PM and on Thursday, Nov 21st from 9:00 AM to 5:00PM. We hope this will give you many opportunities to see talks, participate in activities, visit our sponsor booths, and network with other attendees.

Sponsor Expo Hall

We have asked sponsors to staff their booths during the following times:

Wednesday, Nov 20th from 9:30am to 5pm and Thursday Nov 21st from 10am to 5pm

OWASP Merchandise Store

OWASP is running a merchandise store in the Alvin Room with AppSec USA and general OWASP branded gear. You are welcome to redeem your red tokens here or pay cash/credit card for the items we have available. Hours of operation are:

Wednesday, Nov 20th and Thursday, Nov 21st 8:00 AM – 5:00 PM

Sponsor Passport Program

How to Play:

- Visit ALL 15 of the participating AppSec USA Sponsors listed on the Passport Card.
- Have your Passport Card stamped and submitted to the ballot box at the OWASP Information Desk in the Carnagie Room by 15:00 on Thursday, November 21.
- Prize Winners will be announced at the Conference Awards and Closing Ceremony starting at 16:00 on Thursday, November 21 in the 5th Floor Westside Ballroom. A list of prizes is included on the Passport Card!

Conference Currency: What do I do with the poker chips?

DRINK! Yellow chips can be redeemed for a beverage of your choice at our conference "bars" stationed on the 5th floor. When you run out of chips, these are cash bars as well.

DONATE OR GET OWASP SWAG! Blue chips have a $5 value and can be donated to an OWASP initiative or spent like "cash" at the store in the Alvin Room.

Conference Activities

This year we have quite a few different activities and participatory events going on throughout the conference. Please take time to engage in at least a few of them. Details on these activities are on our website under the "Activities" Tab! http://appsecusa.org/2013

- Capture the Flag x 2 – Do you like to hack websites? Do you like to solve puzzles? This year we are featuring 2 different CTF Competitions. Learn more at the CTF Headquarters in the 5th Floor Westside Ballroom Foyer.
- Career Fair & Wounded Warrior Project – Want to work for Mozilla, Twitter, ADP, BNY Mellon, GE Capital, or any of our security vendors in the expo hall? Visit their tables to find out about career opportunities and maybe even schedule an impromptu interview! We also are pleased to be working to benefit the Wounded Warrior Project. Learn more on page 14.
- Fight Hunger Campaign - We've set up a food drive campaign in conjunction with APPSEC USA Security Conference in NYC to support City Harvest, an organization that helps to feed hundreds of thousands each year in the NYC area.
- Open Mic Sessions– Details on p. 8
- Lockpick Village - Join OWASP and TOOOL (The Open Organisation Of Lockpickers) at our LockPick Village to learn how to circumvent locks. You'll have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised. Visit the Lockpick Village in the 5th Floor Westside Ballroom Foyer.
- OWASP Chapter Leader Workshops – Details on p. 13. Sessions will take place on Thursday, Nov 21st in the Booth Room.
- OWASP Jeopardy – Join our "moderator" Jerry Hoff for a fun interactive game of OWASP and AppSec Trivia. Wednesday 5:30-7:00 PM in the Belasco & Broadhurst Rooms. Want to be a contestant? Sign up Wednesday AM in Carnagie Room.
- OWASP Project Summit– Details on p. 11. Sessions taking place throughout the week in the 16th Floor Skyroom.
- OWASP Project Talks & Project Leader Workshop– Sessions taking place in the Edison Room, see the schedule for times.
- The Great OWASP Bug Smash of 2013– Join Bugcrowd and the OWASP team for the Great OWASP Bug Smash of 2013 where we will unite clans of hackers across the world, participating in the first ever Internet-wide bug smash on the public bug bounty programs. More info on p. 12.
- WASPY Awards – Learn more about the award nominees on p. 10 and join us for congratulating the winners Thursday, November 21th at 4:00 PM in the 5th Floor Westside Ballroom.
- Women in AppSec – Learn more about our Sponsorship Program and this year's sponsorship recipients on p. 9.
- 3k Run benefiting ScriptEd - Join us before the start of the second day of the Conference – Thursday November 21st – Meet up at 7:15AM in the 1st floor lobby of the Marriott to enjoy this "cool" event, please dress appropriately. Race "fee" is $40 and registration is required. Race proceeds will benefit ScriptEd (http://scripted.org/)

Conference Schedule: Wednesday, November 20, 2013

Customizable mobile schedule, speaker bios, and abstracts available online at: http://appsecusa2013.sched.org/

Location	SALON 1 5th Floor Ballroom	SALON 2 5th Floor Ballroom	SALON 3 5th Floor Ballroom	SALON 4 5th Floor Ballroom
Room Sponsor	hp	ongoing security.com	LIVEPERSON	MANDIANT
8:30AM – 9:00AM	Welcome to OWASP AppSec USA – Opening Remarks & Guide to the Conference			
9:00AM – 9:50AM	**Keynote: Bill Cheswick** Computer and Network Security: I Think We Can Win!			
10:00AM – 10:50AM	**Brandon Spruth** Automation Domination	**Bill Sempf** Hardening Windows 8 apps for the Windows Store	**PANEL:** Aim-Ready-Fire	**Robert Hansen** The Perilous Future of Browser Security
11:00AM – 11:50AM	**Amol Sarwate** Why is SCADA Security an Uphill Battle?	**Chris Eng** From the Trenches: Real-World Agile SDLC	**Tor Ekeland, Attorney** Computer Crime Laws	**John Dickson** Can AppSec Training Really Make a Smarter Developer?
12:00PM – 12:50PM	**Jason Haddix & Dawn Isabel** BASHing iOS Applications: dirty, s*xy, cmdline tools for mobile auditors	**Josh Corman & Nicholas Percoco** The Cavalry Is Us: Protecting the public good	**Daniel Peck** All the network is a stage, and the APKs merely players: Scripting Android Applications	**Yair Rovek** Case Study: 10 Steps to Agile Development without Compromising Enterprise Security
1:00PM – 1:50PM	**PANEL:** Privacy or Security: Can We Have Both?	**Johannes Ullrich** HTML5: Risky Business or Hidden Security Tool Chest?	**Tobias Gondrom & Marco Morana** 2013 AppSec Guide and CISO Survey: Making OWASP Visible to CISOs	**Greg Disney-Leugers** Mantra OS: Because The World is Cruel
2:00PM – 2:50PM	**PANEL:** Cybersecurity and Media: All the News That's Fit to Protect?	**Mary Ann Davidson** "What Could Possibly Go Wrong?" - Thinking Differently About Security	**Timothy Morgan** What You Didn't Know About XML External Entities Attacks	**Dan Kuykendall** Revenge of the Geeks: Hacking Fantasy Sports Sites
3:00PM – 3:50PM	**PANEL:** Mobile Security 2.0: Beyond BYOD	**Milton Smith** Making the Future Secure with Java	**Simon Bennetts** OWASP Zed Attack Proxy	**Brian Holyfield & Erik Larsson** Pushing CSP to PROD: Case Study of a Real-World Content-Security Policy Implementation
4:00PM – 4:50PM	**Ondrej Krehel** Forensic Investigations of Web Explotations	**Ory Segal & Tsvika Klain** Big Data Intelligence	**Robert Martin** Tagging Your Code with a Useful Assurance Label	**Jim Manico** OWASP Top Ten Proactive Controls
	JOIN US IN THE 5TH FLOOR BALLROOM FOYER FOR FOOD & BEVERAGES SPONSORED BY HP			
6:00PM – 7:00 PM	**Silk, Webservers, Exploits and RATz by M4v3r1ck**			
7:00PM – 9:00 PM	**LIVE MUSIC by Jam Underground**			
9:00PM – 12:00 AM	**The Great OWASP Bug Smash of 2013 -- Bug Bounty Group Hack**			

Conference Schedule: Wednesday, November 20, 2013

Customizable mobile schedule, speaker bios, and abstracts available online at: http://appsecusa2013.sched.org/

Location	Belasco & Broadhurst 5th Floor	Booth 5th Floor	Edison 5th Floor	Ballroom Foyer 5th Floor	Sky Lounge 16th Floor
	Conference Talks	OWASP Forums & Open Mic Sessions	OWASP Project Talks	Sponsors, CTF, Lockpick Village, Food & Beverages	OWASP Project Summit
8:30AM – 9:00AM					
9:00AM – 9:50AM					
10:00AM – 10:50AM	**Joseph Friedman** How To Stand Up an AppSec Program - Lessons from the Trenches		**Samantha Groves** OWASP Project Leader Workshop	**Food and Beverages available**	**Project Summit Activities:** **ESAPI Hackathon Session** **Writing and Documentation Review Session**
11:00AM – 11:50AM	**Warren Axelrod** Securing Cyber-Physical Application Software		**Chris Schmidt & Kevin Wall** OWASP Enterprise Security API Project		
12:00PM – 12:50PM	**Kenneth Lee** Build but don't break: Lessons in Implementing HTTP Security Headers	OWASP NIST NSTIC IDecosystem Initiative: Initial Discussion Meeting			
1:00PM – 1:50PM	**Parth Patel** A Framework for Android Security through Automation in Virtual Environments	**OPEN MIC**	**Seba Deleersnyder & Pravir Chandra** OWASP OpenSAMM Project	Visit our sponsors, participate in the CTF, and visit the lockpick village!	
2:00PM – 2:50PM	**Stefano Di Paola** Javascript libraries (in)security: A showcase of reckless uses and unwitting misuses.	**OPEN MIC**	**Kostas Papapapanagiotou & Martin Knobloch** The OWASP Education Projects		
3:00PM – 3:50PM	**Sreenarayan Ashokkumar** Advanced Mobile Application Code Review Techniques	**OPEN MIC**	**Dennis Groves** OWASP Security Principles Project		
4:00PM – 4:50PM	**Phu Phung** Sandboxing JavaScript via Libraries and Wrappers	**OPEN MIC**	**Amy Neustein & Judy Fincher** Healthcare Security Forum	**4:30-7:30** **Evening Reception Sponsored by HP**	
5:15PM – 7:00 PM	**OWASP Jeopardy**				
7:00PM – 9:00 PM					
9:00PM – 12:00 AM					

Conference Schedule: Thursday, November 21, 2013

Customizable mobile schedule, speaker bios, and abstracts available online at: http://appsecusa2013.sched.org/

Location	SALON 1 5th Floor Ballroom	SALON 2 5th Floor Ballroom	SALON 3 5th Floor Ballroom	SALON 4 5th Floor Ballroom
Room Sponsor	hp	ongoing security.com	LIVEPERSON	MANDIANT
9:00AM – 9:50AM	**Ron Gutierrez** Contain Yourself: Building Secure Containers for Mobile Devices	**Andrew Hoog** Mobile app analysis with Santoku Linux	**Jeff Williams** AppSec at DevOps Speed and Portfolio Scale	**Robert Salgado** ‘) UNION SELECT `This_Talk` AS (‘New Exploitation and Obfuscation Techniques’)%00
10:00AM – 10:50AM	**Gregg Ganley** iOS Application Defense - iMAS	**Kelly Fitzgerald** Accidental Abyss: Data Leakage on The Internet	**Mike Park** PiOSoned POS - A Case Study in iOS based Mobile Point-of-Sale gone wrong	**Bill Thompson, Aaron Weaver, David Ohsie** Leveraging OWASP in Open Source Projects - CAS AppSec Working Group
11:00AM – 11:50AM	**Simon Roses Femerling** Verify your software for security bugs	**Kostas Papapanagiotou** OWASP Hackademic: a practical environment for teaching application security	**Ryan Berg** An Introduction to the Newest Addition to the OWASP Top 10	**Jeremiah Grossman** The State Of Website Security And The Truth About Accountability and “Best-Practices”
12:00PM – 12:50PM	**PANEL:** Women in Information Security: Who Are We? Where Are We Going?	**Matt Konda** Insecure Expectations	**James Landis** OWASP Periodic Table of Elements	**Eoin Keary** Application Security: Everything we know is wrong
1:00PM – 1:50PM	**Jim St. Pierre and Matthew Scholl** NIST Information Technology Laboratory	**PANEL:** Threat Intelligence and Software Security: Opportunities for Improvement?	**Armando Romeo** Hack.me: a new way to learn web application security	**Bruno Oliveira** Hacking Web Server Apps for iOS
2:00PM – 2:50PM	**Jeff Williams & Ryan Berg** Go Fast AND Be Secure: Eliminating Application Risk in the Era of Modern, Component-Based Development	**Michele Orru** Buried by time, dust and BeEF	**Chuck Willis** OWASP Broken Web Applications (OWASP BWA): Beyond 1.0	**Pratik Guha Sarkar, Shawn Fitzgerald** Modern Attacks on SSL/TLS: Let the BEAST of CRIME and TIME be not so LUCKY
3:00PM – 3:50PM	**Vaagn Toukharian** HTTP Time Bandit	**Ari Elias-Bachrach** CSRF: not all defenses are created equal	**Dave Wichers** The 2013 OWASP Top 10	**Gursev Singh Kalra** Wassup MOM? Owning the Message Oriented Middleware
4:00PM – 4:50PM	**AppSec USA WASPY Awards & Closing Ceremony**			

SAVE THE DATE! Join us for AppSec USA 2014, September 16-19 in Denver, CO

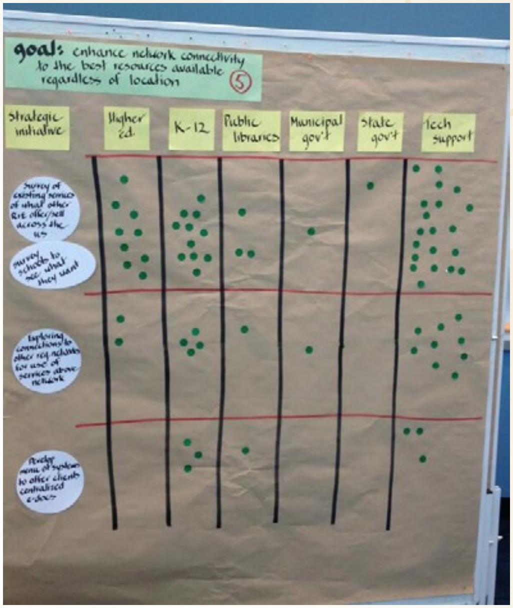
Conference Schedule: Thursday, November 21, 2013

Customizable mobile schedule, speaker bios, and abstracts available online at: http://appsecusa2013.sched.org/

Location	Belasco & Broadhurst 5th Floor	Booth 5th Floor	Edison 5th Floor	Ballroom Foyer 5th Floor	Sky Lounge 16th Floor
	Conference Talks & Open Mic Sessions	OWASP Chapter Workshops	OWASP Project Talks	Sponsors, CTF, Lockpick Village, Food & Beverages	OWASP Project Summit
9:00AM – 9:50AM	**Stephen Wolf** Defeating XSS and XSRF using JSF Based Frameworks	OWN THE CON: How we organized AppSecUSA - come learn how you can do it too			
10:00AM – 10:50AM	OPEN MIC	OWASP Chapter LIfecycle	**Dinis Cruz** Project Talk and Training: OWASP O2 Platform	Food and Beverages available	Project Summit Activities: ESAPI Hackathon Session ZAP Hackathon Session Open SAMM Session
11:00AM – 11:50AM	OPEN MIC	Chapter Handbook – 2013 Revisons		Food and Beverages available	
12:00PM – 12:50PM	OPEN MIC	Event Planning for Chapter Leaders	**Andrew Mueller** Project Talk: OWASP Testing Guide	Food and Beverages available	
1:00PM – 1:50PM	OPEN MIC	Promoting your OWASP Chapter	**Andrew Van Der Stock** Project Talk: OWASP Development Guide	Visit our sponsors, participate in the CTF, and visit the lockpick village!	
2:00PM – 2:50PM	OPEN MIC	OWASP Chapter – Vendor Relationships	**Dennis Groves** Project Talk: OWASP AppSensor	Last chance to complete your Sponsor Passport Card for prizes!	
3:00PM – 3:50PM	OPEN MIC	OWASP Chapters: The Invisible Chapter	**Larry Conklin** Project Talk: OWASP Code Review Guide	Food and Beverages available	
4:00PM – 4:50PM					

SAVE THE DATE! Join us for AppSec USA 2014, September 16-19 in Denver, CO

Open Mic Sessions


goal: enhance network connectivity to the best resources available regardless of location (5)
Strategic initiative
Higher ed.
K-12
Public libraries
Municipal gov't
State gov't
Tech support
Survey of existing services of what other R+E offer/sell across the US
Survey to schools to see what they want
Exploring connections to other reg. networks for use of services above network
Develop menu of system to other clients centralized e-docs

I noticed on the schedule there are "OPEN-MIC" sessions, what exactly are they and how do I present during those time slots?

During the morning hours of **Wednesday, Nov. 20 and Thursday, Nov. 21**, badge-holding conference attendees interested in presenting an AppSec related topic may sign up for the Open Mic slots. There will be large voting boards in **the Carnagie Room on the 5th Floor** where you can post your submission proposal (session title, mini abstract and name) on a post-it note. Depending on the amount of submissions, we may be hosting 2-3 "speed talks" during each Open Mic session.

All badge-holding conference attendees will use little sticky dots, included in their conference registration bag, to vote on the talks they'd be interested in attending. **Voting will be open until Noon on each day**, at that time the conference organizers will post the accepted submissions on the AppSec USA Schedule webpage.

Create your custom schedule now and earmark the Open Mic Sessions: http://appsecusa2013.sched.org/

OWASP FOUNDATION PRESENTS

2013 WOMEN IN APPSEC

The OWASP Foundation, in recognition of value to both organizations and society, is working to support and enhance programs that increase the participation of women in the field of application security. As part of this effort, OWASP sought funds to sponsor women from North America to attend OWASP AppSec USA, to be held in New York City in November of 2013.

Overall, the program had 36 women apply for the sponsorship. After careful consideration, the Women in AppSec selection team chose two winners this year. Please help me in congratulating our 2013 Women in AppSec Winners, Nancy Lorntson and Carrie Schaper.

Nancy Lorntson is the Security Program Manager at Infinite Campus, the largest American-owned Student Information System, managing 6 million students in 43 states. Previously, Nancy was a school district Information Services Manager and part-time trainer for Guidance Software. In her current role, Nancy is responsible for all things security at Infinite Campus, working between the application development organization and the support, network, business operations, and hosting teams to implement, grow and improve a world class security program.

Carrie Schaper is an Information Security Professional with over 12+ years of industry experience ranging from Penetration Testing Fortune 500 companies, the Banking Infrastructure, and Government to Incident Response and Continuous Monitoring. She has performed Threat-Mitigation against targeted attacks from domestic and foreign adversaries for both corporate and government environments.

SPONSORED BY:

iSECpartners
part of nccgroup

OWASP Boston Chapter

W
UNIVERSITY of WASHINGTON | BOTHELL
CYBER SECURITY ENGINEERING

OWASP Ireland Chapter

OWASP Long Island Chapter

OWASP Minneapolis St. Paul Chapter

OWASP would also like to give a special thank you to the very dedicated and hardworking 2013 Women in AppSec Selection Team. They diligently planned and sought out funding to ensure the success of the program this year. Thank you, Helen Gao, Bev Corwin, Jim Manico, Tom Ryan, Lucas Ferreira, and Samantha Groves.

2013 GLOBAL OWASP
WASPY AWARDS

Congratulations to all the 2013 WASPY Awards Nominees & Winners!

Best Chapter Leader

Tin Zaw, Richard Greenberg, Kelly FitzGerald, Stuart Schwartz, Edward Bonver (Los Angeles)

Nominees:

- Paul Scott (Houston)
- Jonathan Marcil (Montreal)
- Abbas Naderi (Iran)
- John Wilander (Sweden)
- Jack Mannino (Northern Virginia)
- Trenton Ivey (Milwaukee)
- David Hughes (Austin)
- Dhruv Soi (India)

Best Community Supporter

Fabio Cerullo

Nominees:

- Jason Montgomery
- John Wilander

Best Project Leader

Simon Bennetts (ZAP)

Nominees:

- Abbas Naderi (PHP Security Project)
- Andrew van der Stock (Developer Guide)
- Epsylon “psy” (XSSer)

Best Innovator

Abbas Naderi

Nominees:

- Tanoh Aka Marcellin

Best Mission Outreach

Martin Knobloch

Nomineees:

- Fabio Cerullo
- John Wilander

Thank you our 2013 Platinum Sponsor:

Learn more about the awards and the nominees at:
https://www.owasp.org/index.php/WASPY_Awards_2013

QUALYS®

OWASP FOUNDATION PRESENTS

2013 PROJECT SUMMIT

NOVEMBER 18 - 21 | NEW YORK MARRIOTT MARQUIS, NYC

The OWASP Project Summit is a smaller version of the much larger OWASP Summits. This year's summit aims to give our project leaders the opportunity to have attendees sit down and work on project related activities during AppSec USA. It is an excellent opportunity to engage with active OWASP Project Leaders if you are a conference attendee, and it gives project leaders the chance to move forward on their project milestones while meeting new potential volunteers that can assist with future milestones. Please note, additional sessions may have been added recently so please make sure to check the live schedules for more up-to-date session details. Below is our 2013 OWASP Project Summit Session Schedule.

SUMMIT LOCATION: Most sessions will be taking place in the **16th Floor Sky lobby, please check the live schedule on sched.org for the most up to date information! ALSO: https://www.owasp.org/index.php/Projects_Summit_2013**

Monday: Nov 18th

OWASP Projects Review Session

ESAPI Hackathon Session

Bug Bounty Hack Session

Tuesday: Nov. 19th

University Outreach, Education, and Training Session

Mobile Security Session

ESAPI Hackathon Session

Bug Bounty Hack Session

Wednesday: Nov. 20th

Writing and Documentation Review Session

ESAPI Hackathon Session

Bug Bounty Hack Session

Thursday: Nov. 21st

ZAP Hackathon Session

Open SAMM Session

ESAPI Hackathon Session

Bug Bounty Hack Session

OWASP FOUNDATION PRESENTS

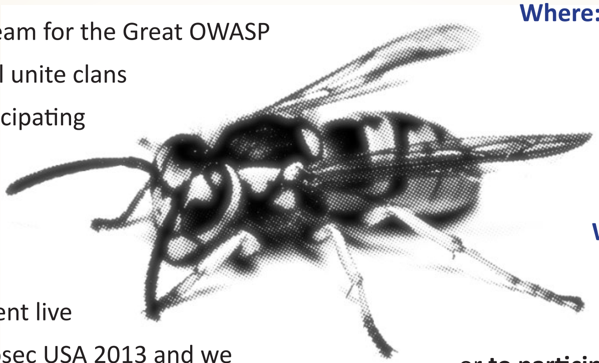
2013 PROJECT TALKS

The OWASP Project talks give Leaders an opportunity to showcase their project progress, and announce new project activity. This year, we have ten projects participating in the AppSec USA 2013 Project Talks. More information about each project talk can be found in talk abstract section of this program guide. **Project Talks will be taking place on Wednesday and Thursday in the Edison Room (5th Floor).**

The Great OWASP Bug Smash of 2013

Bug Bounty programs have been getting a lot of press lately, and for good reason. They work. Data shows that bug bounties lead to better feedback for organizations and overall, better application security.

Join Bugcrowd and the OWASP team for the Great OWASP Bug Smash of 2013 where we will unite clans of hackers across the world, participating in the first ever Internet-wide bug smash on the public bug bounty programs.



Bugcrowd will be running this event live from 8-12 every night during Appsec USA 2013 and we actively encourage OWASP members around the world to participate.

Just some of the targets to pick from:

https://bugcrowd.com/list-of-bug-bounty-programs/

To participate, join us at the event:

When: Monday & Tuesday Night 8pm – 11:59pm
Where: 16th Floor Sky lobby

When: Wednesday Night
9pm – 11:59pm
Where: 5th Floor Ballroom

or **to participate online:**

https://www.bugcrowd.com/owasp/

Coordinated by:

OWASP
Open Web Application
Security Project

bugcrowd™

OWASP CHAPTERS
global strategic group

Chapter Leader Workshop Sessions

OWASP Chapters are one of the core building blocks of the organization and many of the details of running a chapter are included in the Chapter Leader Handbook. These sessions are a place for discussion and clarity on some of the common problems and questions that arise in running a chapter. **Sessions will be taking place on Thursday in the Booth Room (5th Floor).**

OWASP Chapter Lifecycle

Do you want to start an OWASP Chapter? What about reenergize one that seems to be lacking some energy? Come learn about the lifecycle of a chapter and how to get involved at any stage.

Chapter Handbook - 2013 Revisions

Come suggest changes and updates that are needed to the OWASP Chapter Handbook. Let us know what is working for you and what isn't. Where could you use more guidance?

Event planning for Chapter Leaders

Unravel the mysteries of planning local chapter events. This session will focus on some of the common logistical questions that arise when chapter leaders want to increase the outreach in their region by stepping up their chapter meetings. Topics will include OCMS walkthrough, reimbursements and payments, contracts, registrations, venue and catering selections, budgets, and much more.

Chapter Promotion

How to promote your chapter and increase attendance. This session will review different methods of promotion for your chapter all aimed at increasing meeting attendance. Topics will include social media, mailing list management, speaker selections, networking ideas. Geared for the new or re energized chapter leader looking to expand their reach.

Vendor relationships

Vendors are not the bad guys. This session will include a lively discussion on vendor relationships within your chapter. Topics will include some benefits of vendor relationships, how to leverage neighboring companies, chapter fundraising, and Foundation guidelines on relationships with vendors/sponsors.

The Invisible Chapter

This session will focus on steps to take when there is a chapter that may be in need of some energy or starting a new chapter. As a community, we all share a responsibility to each other to build the OWASP community.

Activities Benefiting Charity

ScriptEd – Central Park Charity Run/Walk

We encourage you to participate in this fun event to benefit ScriptEd, a 501(c)(3) not for profit organization. ScriptEd teaches computer programming to students in low-income areas. This light 1.58 mile loop around a pretty lake will offer you a great view of the Manhattan skyline. Join us before the start of the second day of the Conference – Thursday November 21 **– Meet in the 1st floor lobby of the Marriott at 7:15AM** to enjoy this "cool" event, please dress appropriately. http://scripted.org/

To Benefit the Wounded Warrior Project

OWASP Foundation is facilitating technology providers and industry firms seeking candidates to fill opportunities worldwide during AppSec USA 2013. For all attendees, this is an opportunity to meet with prospective employers for opportunities and apply in person. For returning United States Veterans, this is an opportunity to meet those civilian employers that value proven leadership and discipline.

OWASP Foundation and the conference volunteers will be collecting $5 applicant donations at the career fair for the Wounded Warrior Project. 100% of collected donations will be presented to the Wounded Warrior Project from the OWASP Foundation at the conclusion of the event.

Fight Hunger Campaign

The OWASP community is a community that likes to give back and we do it in many ways. We've set up this food drive campaign in conjunction with APPSEC USA Security Conference in NYC to support The Salvation Army, **an organization that helps to feed hundreds of thousands each year in the NYC area.**

http://appsecusa.org/2013/activities/fight-hunger-campaign/

OWASP FOUNDATION PRESENTS

APPSEC USA 2013

NOVEMBER 18 - 21 | NEW YORK MARRIOTT MARQUIS, NYC

Thank you to our Speaker and Training Selection Committee!

Israel Bryski

Vice President at TD Securities

James Landis

Senior Manager at EBAY

Kevin Greene

Software Assurance Program Manager at DHS S&T

Robert Martin

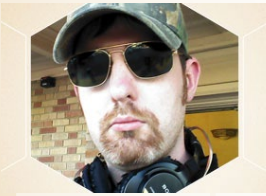
Principal Engineer at MITRE

Joan Goodchild

Executive Editor at CSO Magazine and Online

Pravir Chandra

Security Architect at Bloomberg



Matt Joyce

Cloud Operations Engineer at Cloudscaling

Hans Zaunere

Managing Member at Stackware

Ben Rothke

Manager at Wyndham Worldwide

Name Withheld

Technology Risk Management at Large Bank

2013 AppSec Guide and CISO Survey: Making OWASP Visible to CISOs

Marco Morana, Tobias Gondrom

As organization born from grass root ideals and volunteering efforts that stared 12 years ago from the visionaries of the like of Mark Curphey and the likes OWASP has grown in members. OWASP mission has been to make application security visible to application security stakeholders. Thanks to the OWASP corporate sponsors and volunteers working on sponsored projects, OWASP has delivered free tools and guides that helped software developers to build more secure web applications. Most notably, the OWASP Top Ten provided the benchmark for testing web application vulnerabilities for several organizations. Projects such as the development guide and testing guide provides pointed guidance to software developers on how to design and test web applications. Among the application security stakeholders that OWASP serve today, (CISOs) Chief Information Security Officers are often the ones that make decisions on rolling out application security programs and activities invest in new tools and set budget for application security resources. Recognizing the important role that the CISO has in managing application security processes within the organizations, OWASP sponsored a project in 2012 to develop guidance specifically for CISOs. The aim of the OWASP guide is to provide useful guidance to CISOs for effectively managing the risks of insecure web applications and software by planning the application security activities, investing in countermeasures to mitigate threats and considering the costs and the benefits for the organization. Recognizing that a CISO guide has first and for most capture the needs of CISO in managing application security from information security governance, risk and compliance perspectives a survey was developed in parallel with the draft of the CISO Guide. As the results of the 2013 CISO survey have become available, they have been used to tailor the guide to the specific CISOs needs. One of the most important aspects covered in the CISO guide are to making the business case for application security investments by helping CISOs in translating technical risks such as the OWASP top ten into business impacts, compliance with standards and regulations and risk management. Specifically the version of the guide that is presented at OWASP AppSec USA will be the first version that highlights the results of the CISO survey and seek to introduce CISOs to projects/resources that can help them in rolling out an application security program whose main goal is managing web application security risks.

A Framework for Android Security through Automation in Virtual Environments

Parth Patel

This session introduces a practical approach to securing Android applications through an automated framework. The framework uses a simple interface and automatically evaluates applications - even hundreds of them - harvesting behavioral data and run patterns, facilitating the vast

majority of evolving security tests. Citing research from using this framework, this session will also answer some of today's most pressing android security questions.

This presentation will address the limitations of real time security and fragmented security models for security evaluations of Android applications, and will demonstrate how to resolve this using an automated virtual environment that analyzes behavior of Android apps while providing a layer of transparency between Android apps and Android users.

Then it will present how I built an open source framework - the Android Security Evaluation Framework (ASEF) to help resolve security needs of a larger spectrum of Android users including researchers and developers. I will explain how to perform security evaluations on a bigger scale for app stores and large organizations by demonstrating scheduled automatic security evaluations that can be done remotely from an android device using ASEF and its agent.

Citing results from using ASEF, I will also recommend safe practices to follow by being proactive about security measures before installing an app, as well as tips for effective security management after android apps are installed. I will also discuss the importance of Behavioral Analysis and Vulnerability Management of android devices along with idea of integrating security tests in the plug and play framework of ASEF.

Lastly, I will discuss the future of Android security through the eyes of automation and what tactics can be used to achieve conclusive and comprehensive coverage of upcoming Android security needs.

Accidental Abyss: Data Leakage on The Internet

Kelly Fitzgerld

PII is personally identifiable information. In the information age, seemingly useless bits of PII can be found everywhere on the web from Facebook to Amazon to county records. Using purely legal methods and nothing more than artful searching I will show you the art of the low-tech, high-targeted recon. How much of your identity is scattered around on the internet? In this ambitious talk we will look at better hacking through television, how to combine crumbs to build thorough dossiers and learn some tricks on how to do some basic information reconnaissance. By the end of the talk you'll have some frightening statistics, something good to think about and some tools that will make you a more effective social engineer, an aware user and a more thoughtful security expert.

Advanced Mobile Application Code Review Techniques

Sreenarayan Ashokkumar

Learn how Mobile experts blend their techniques in order to accelerate code reviews. While reviewing Windows Phone 8, Hybrid or HTML 5 applications, you will love these handy tricks that help in detecting famous and a few not-so-famous flaws. Using demonstrations and code snippets, we will highlight the benefits of blended techniques in comparison with those of simple scanning or manual testing. You will also learn how to reduce the time taken for review and obtain a ready-to-use checklist.

Objectives:

- To give live demonstrations of the most common insecurities found in Windows Phone 8, HTML5 or Hybrid applications.
- To share tested and proven methods of discovering insecurities via code reviews.
- To learn how to efficiently conduct source code reviews for mobile applications.
- To develop a checklist for Mobile Code Reviews.

All the network is a stage, and the APKs merely players: Scripting Android Applications

Daniel Peck

The existance of open well defined APIs for many popular websites has been a boon to spammers, but as they have grown in popularity the operators have begun to care more about the integrity of the network. 3rd party access to these APIs is becoming increasingly restricted, while at the same time desires for a frictionless mobile experience have led to much looser restriction in their own applications.

We'll leverage this, along with the ability to load and execute Android APKs within JRuby sessions to create and control a social botnet.

Beginning with a brief overview of tools for disassembling, understanding, modifying, and rebuilding APKs. We will then move onto scripting portions of the application in a JRuby session, along the way covering key recovery, bypassing custom cryptographic routines, and general exploration of the code in a dynamic environment.

We'll conclude with leveraging what we've discovered to create and control thousands of accounts. Building on available information sources, such as the US census, and streams provided by the targetted network itself these accounts will have realistic characteristics and interact with the network in believable ways.

An Introduction to the Newest Addition to the OWASP Top 10. Experts Break-Down the New Guideline and Offer Provide Guidance on Good Component Practice

Ryan Berg

Experts in the field of application security and open source software development discuss the new OWASP A9 guidelines, offering session attendees unique intelligence on component vulnerabilities and how to deploy new approaches to application security and risk management that address security at the component level, while simultaneously eliminating risk in the modern software supply chain. Panelists to include: Sonatype, Aspect Security, Two Senior Security Executives from Fortune 500 Companies

Most development teams don't focus on security. The 2013 Open Source Software Development Survey, the largest survey of OSS users with more than 3,500 participants, found that more than half of the developers, architects and managers surveyed don't focus on security at all. Nearly 20% of this group shared they know application security is important but they don't have the time to spend on it, while almost one-third deferred responsibility to the security and risk management group entirely. As open source component use continues to skyrocket with applications

now more than 80% component-based, organizations continue to struggle with establishing policy to secure and govern component use. According to the survey, an alarming 65% of organizations have no component management policies in-place.

This lack of internal controls and a failure to address security vulnerabilities throughout the software development lifecycle threatens the integrity of the software supply chain and exposes organizations to unnecessary risk. Open source component vulnerabilities are exceedingly common, with more than 70% of applications containing components with vulnerabilities classified as severe or critical. Virtually every application has these issues because most development teams don't focus on ensuring their components stay up to date. In many cases, developers don't even know all the components they are using let alone the versions. In fact, the Open Source Software Development Survey shows only 35% of organizations maintain inventories of the components in their production applications.

This panel of industry experts will dissect the new OWASP A9 guidelines that look at the widespread use of insecure open source libraries in today's modern application development. Executives from Sonatype, will offer exclusive component usage data from the Central Repository – the industry's largest source of open-source components receiving 8 billion requests annually. With its deep history as leaders in open source development, Sonatype can also share with attendees its unmatched knowledge of open source development practices. Jeff Williams, CEO of Aspect Security and founding member of OWASP, will offer best practices and advice to organizations looking to revamp their software assurance policies. Lastly Jim Routh, the head of application and mobile security at Citibank will share with attendees the real-world challenges and resolutions faced by the financial institution in mitigating risk in agile, component-based development.

Together, the panel will address the following key points and offer attendees important takeaways to jumpstart A9 compliance, including:

- How software assurance is now largely incompatible with modern development and why new approaches to security must provide developers with immediate feedback on security context to act as the new frontline of defense;
- How to inform component choice throughout the development lifecycle, including how to pinpoint flaws early and how to deploy flexible remediation options for flawed components
- How to build-in component security and risk mitigation into the development process that can also be used by non-security experts; an
- How new security and risk mitigation approaches must be continuous to address ongoing threats in real-time and to ensure sustaining trust between development, risk management and the application end-user.

Application Security: Everything we know is wrong

Eoin Keary

The premise behind this talk is to challenge both the technical controls we recommend to developers and also our actual approach to testing and developing secure software. This talk is sure to challenge the status quo of web security today."Insanity is doing the same thing over and over and expecting different results." - Albert Einstein

We continue to rely on a &ldquo;pentest&rdquo; to secure our applications. Why do we think it is acceptable to perform a time-limited test of an application to help ensure security when a determined attacker may spend 10-100 times longer attempting to find a suitable vulnerability?

Our testing methodologies are non-consistent and rely on the individual and the tools they use; Some carpenters use glue and some use nails when building a wooden house.

Which is best and why do we accept poor inconsistent quality.

Fire and forget scanners won't solve security issues. Attackers take time and skill but our industry accepts the output of a software programme to help ensure security?

How can we expect developers to listen to security consultants when the consultant has never written a line of code?

Why don't we ask Experts in the field of application security and open source software development discuss the new OWASP A9 guidelines, offering session attendees unique intelligence on component vulnerabilities and how to deploy new approaches to application security and risk management that address security at the component level, while simultaneously eliminating risk in the modern software supply chain. Panelists to include: Sonatype, Aspect Security, Two Senior Security Executives from Fortune 500 Companies

Most development teams don't focus on security. The 2013 Open Source Software Development Survey, the largest survey of OSS users with more than 3,500 participants, found that more than half of the developers, architects and managers surveyed don't focus on security at all. Nearly 20% of this group shared they know application security is important but they don't have the time to spend on it, while almost one-third deferred responsibility to the security and risk management group entirely. As open source component use continues to skyrocket with applications now more than 80% component-based, organizations continue to struggle with establishing policy to secure and govern component use. According to the survey, an alarming 65% of organizations have no component management policies in-place.

This lack of internal controls and a failure to address security vulnerabilities throughout the software development lifecycle threatens the integrity of the software supply chain and exposes organizations to unnecessary risk. Open source component vulnerabilities are exceedingly common, with more than 70% of applications containing components with vulnerabilities classified as severe or critical. Virtually every application has these issues because most development teams don't focus on ensuring their components stay up to date. In many cases, developers don't even know all the components they are using let alone the versions. In fact, the Open Source Software Development Survey shows only 35% of organizations maintain inventories of the components in their production applications.

This panel of industry experts will dissect the new OWASP A9 guidelines that look at the widespread use of insecure open source libraries in today's modern application development. Executives from Sonatype, will offer exclusive component usage data from the Central Repository – the industry's largest source of open-source components receiving 8 billion requests annually. With its deep history as leaders in open source development, Sonatype can also share with attendees its unmatched knowledge of open source development practices. Jeff Williams, CEO of Aspect Security and founding member of OWASP, will offer best practices and advice to organizations looking to revamp their software assurance policies. Lastly Jim Routh, the head of application and mobile security at Citibank will share with attendees the real-world challenges and resolutions faced by the financial institution in mitigating risk in agile, component-based development.

Together, the panel will address the following key points and offer attendees important takeaways to jumpstart A9 compliance, including:

- How software assurance is now largely incompatible with modern development and why new approaches to security must provide developers with immediate feedback on security context to act as the new frontline of defense;
- How to inform component choice throughout the development lifecycle, including how to pinpoint flaws early and how to deploy flexible remediation options for flawed components
- How to build-in component security and risk mitigation into the development process that can also be used by non-security experts; an
- How new security and risk mitigation approaches must be continuous to address ongoing threats in real-time and to ensure sustaining trust between development, risk management and the application end-user.How much code development have you done, seen as you are assessing my code for security bugs?" Currently we treat vulnerabilities like XSS and SQLI as different issues but the root causes it the same. &ndash; it's all code injection theory!! Why do we do this and make security bugs over complex? Why are we still happy with &ldquo;Testing security out&rdquo; rather than the more superior &ldquo;building security in&rdquo;?

AppSec at DevOps Speed and Portfolio Scale

Jeff Williams

Software development is moving much faster than application security with new platforms, languages, frameworks, paradigms, and methodologies like Agile and Devops. Unfortunately, software assurance hasn't kept up with the times. For the most part, our security techniques were built to work with the way software was built in 2002. Here are some of the technologies and practices that today's best software assurance techniques *can't*handle: JavaScript, Ajax, inversion of control, aspect-oriented programming, frameworks, libraries, SOAP, REST, web services, XML, JSON, raw sockets, HTML5, Agile, DevOps, WebSocket, Cloud, and more. All of these rest pretty much at the core of modern software development. Although we're making progress in application security, the gains are much slower than the stunning advances in software development. After 10 years of getting further behind every day, software *assurance* is now largely incompatible with modern software *development*. It's not just security tools – application security processes are largely incompatible as well. And the result is that security has very little influence on the software trajectory at all. Unless the application security community figures out how to be a relevant part of software development, we will continue to lag behind and effect minimal change. In this talk, I will explore a radically different approach based on instrumenting an entire IT organization with passive sensors to collect realtime data that can be used to identify vulnerabilities, enhance security architecture, and (most importantly) enable application security to generate value. The goal is unprecedented real-time visibility into application security across an organization's entire application portfolio, allowingall the stakeholders in security to collaborate and finally become proactive.

Automation Domination

Brandon Spruth

Building your application security automation program as part of the Software Development Lifecycle (SDLC) with architects, developers, and QA has always been challenging. Automation Domination is the answer to that challenge, structuring a continuous integration framework around your portfolio of dynamic (DAST) and static (SAST) scanning products with integration into your software development stack. We will explore how to take theory into practice with a proven, scalable enterprise solution with OWASP Projects, continuous integration (CI), bug-tracking, and content creation products.

BASHing iOS Applications: dirty, s*xy, cmdline tools for mobile auditors

Jason Haddix, Dawn Isabel

The toolchain for (binary) iOS application assessment is weak BUT, like an island of misfit toys, there can be stregnthin numbers. Join us as we explore what actually needs to be done in a mobile assessment and how we can do it right from our SSH prompt on our iOS device. Our tool is simple yet effective and as you learn to do mobile assessments you'll also teach yourself the fundamentals of the OWASP Mobile Top 10. Topics explored will be binary analysis, app decryption, data storage, endpoint parsing, class inspection, file monitoring, and more! Heck we might even release some sort of ghetto BASH Obj-c source parser!

Big Data Intelligence (Harnessing Petabytes of WAF statistics to Analyze & Improve Web Protection in the Cloud)

Ory Segal, Tsvika Klein

As web application attacks turn into massive campaigns against large corporations across the globe, web application firewall data increases exponentially, leaving security experts with a big data mess to analyze. Pinpointing real attacks in a sea of security event noise becomes an almost impossible tedious task. In this presentation, we will unveil a unique platform for collecting, analyzing and distilling Petabytes of WAF security intelligence information. Using the collected data,we will discuss the OWASP ModSecurity Core Rule Set project's accuracy, and reveal common attack trends, as well as our impressions and suggestions for how to wisely make the best out of the CRS project.

Build but don't break: Lessons in Implementing HTTP Security Headers

Kenneth Lee

Content Security Policy is a new standard from the WC3 that aims to help stop a mainstay of the OWASP top 10, cross-site scripting (XSS). The problem faced by many major sites today is how to craft a working content security policy that works for already existing applications. We will discuss real world techniques to simplify policy generation and testing, as well as discuss what changes are coming in CSP version 1.1. I will also discussion additional security headers such as X-Frame-Options to stop clickjacking and HTTP Strict Transport Security to stop man-in-the-middle attacks.

Buried by time, dust and BeEF

Michele Orru

For those who do not listen Mayhem and black metal, the talk title might seem a bit weird, and I can’t blame you. You know the boundaries of the Same Origin Policy, you know SQL injection and time-delays, you know BeEF. You also know that when sending cross-domain XHRs you can still monitor the timing of the response: you might want to infer on 0 or 1 bits depending if the response was delayed or not. This means it’s possible to exploit every kind of SQL injection, blind or not blind, through an hooked browser, if you can inject a time-delay and monitor the response timing. This works flawlesslyin cross-domain situations, you don’t need a 0day or a particular SOP bypass to do this, and it works in every browser. The potential of being faster than a normal single-host multi-threaded SQLi dumper will be explored. Two experiments will be shown: WebWorkers as well as multiple synched hooked browsers, which split the workload communicating partial results to a central server. A pure JavaScript approach will be exlusively presented during this talk, including live demos. Such approach would work for both internet facing targets as well as applications available in the intranet of the hooked browser. The talk will finish discussing the implications of such an approach in terms of Incident Response and Forensics, showing evidence of a very small footprint.

Can AppSec Training Really Make a Smarter Developer?

John Dickson

Most application risk managers agree that training software developers to understand security concepts can be an important part of any software security program. Couple that with the Payment Card Industry, who mandate that developers should have training in secure coding techniques as laid out in their Data Security Standard. Yet others call developer training “compliance-ware,” a necessary evil and a tax on software development in the enterprise. This presentation shares the results of a yearlong survey of nearly 1,000 software developers that captures their knowledge of application security before and after formal training. The survey queries developers from various backgrounds and industries, to better understand their exposure to secure development concepts and to capture a baseline for post-training improvements. The session also includes the results of a “retest” of a subset of respondents, to identify how much security knowledge they retained after a specific length of time. The results were surprising, and include information every application risk manager should know, particularly those who rely on training as part of an application security strategy.

Case Study: 10 Steps to Agile Development without Compromising Enterprise Security

Yair Rovek

In an Agile, fast paced environment with frequent product releases, security code reviews &amp; testing is usually considered a delaying factor that conflicts with success. Is it possible to keep up with the high-end demands of continuous integration and deployment without abandoning security best practices? We started our journey seeking a way to reduce friction, risk and cost driven from identifying vulnerabilities too late, when already in Production. After a long way and many lessons learned, we have successfully added in-depth security coverage to more than 20 SCRUMS and up to 1M lines of code. We are happy to share our insights, tips and experience from that process. LivePerson is a provider of SaaS based technology for real-time interaction between customers and online businesses. Over 1.5 billion web visitors are monitored by the platform on a monthly basis. LivePerson's R&amp;D center consists of hundreds of developers who work in an Agile and Scrum based methods, closely tied with our Secure Software Development Lifecycle. In order to achieve best results and reduce friction, we have tailored the SSDLC to the standard SCRUM process and added security coverage (both operational + technical controls) for each phase starting with a mutual Security High Level Design post release planning with Software Architects, defining technical security controls and framework in sprint planning, implementation of ESAPI and Static Code Analysis at the CI, manual code reviews, Automated Security Tests during QA and a penetration test as part of the release. This session will include detailed information about the methodologies and operational cycles as well as measureable key success factors and tips related to implementation of tools and technologies in our use (e.g. ESAPI package, Static Code Analysis as a Maven Step, Vulnerability Scanning plugins) References: OWASP ESAPI https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API Writing Secure Code, Second Edition, Michael Howard and David LeBlanc, Microsoft Press The Burp Suite http://portswigger.net/burp/ OWASP Developer Guide http://ignum.dl.sourceforge.net/project/owasp/Guide/2.0.1/OWASPGuide2.0.1.pdf

Computer and Network Security: I Think We Can Win!

Bill Cheswick

Some think that computer and network security is a lost cause.I have spent forty years in the field, and it is discouraging that wehave made few advances, and lost a lot of ground: our current technologies and practices are clearly unable to keep attackers out of our business.Bob Morris said that security people are paid to think bad ideas,and I have had a lot of them. The threats are persistent, butnot really advanced in most cases. Iremain optimistic: it is still early in the game.These are our computers, our software, our network wiring. We have plenty of CPU cycles and storage and daunting cryptography. We ought to be able to win this battle---we have the home field advantage!Some things are pretty clear to me at this point: user education and strict edicts are an inadequate substitute for good engineering; a good scientific measure of security still eludes us and is probably an intractable problem; standards compliance and checklists don't solve the problem; and our industry has not improved over the decades.What does a cure look like? It is still early in the game, our software designs and userinterfaces are still at the level of the Ford Model T. I will try to describe some of thetechnology and scenarios that may be part of the solutions.

Computer Crime Laws - Tor Ekeland, Attorney

Tor Ekeland

The Computer Fraud and Abuse Act: An OverviewThe notorious Computer Fraud and Abuse Act (CFAA) is the most litigated federal computer misuse statute in existence. This presentation will cover the basics of the CFAA, starting with its origins, how Congress intended it to be used, and how the Department of Justice currently uses it today. After a brief discussion of the legislative origins of the CFAA in the Orwellian year of 1984, the presentation will sketch the main statutory components of the law, focusing specifically on the provisions that prohibit unauthorized access to obtain information and those that prohibit damage to a computer. Because the CFAA fails to define what it primarily seeks to prohibit &ndash; unauthorized access to a protected computer &ndash; the presentation will then cover the myriad of different interpretations of unauthorized access. Finally, the presentation will cover more recent CFAA cases invoking these different concepts that Tor has worked on as either lead or co-counsel, including United States v. Auernheimer, (aka weev's case) which is currently on appeal in front of the Third Circuit Court of Appeals. If there is time Tor will take questions.

Contain Yourself: Building Secure Containers for Mobile Devices

Ron Gutierrez

In today's world, everyone wants access to information from his or her personal mobile device. As a business, this includes your customers and/or employees. What if the information they want access to is highly sensitive? While it's tempting to resist these pressures for security reasons, providing mobile access can be a significant competitive advantage and most importantly keep your customers and employees happy and productive. The reality is that in order to survive in a connected world, we must provide a way to meet these demands without sacrificing security. Organizations have begun moving from "managed devices" to a Bring Your Own Device (BYOD) model where company resources can be accessed and stored on unmanaged devices. As you can imagine, there are some inherent risks with this approach due to the organizations inability to enforce policies on personal devices. There is currently a huge market for solutions that allowing enterprises protect their data on unmanaged devices. Enter "Secure Containers&rdquo; and &ldquo;Application Wrapping". The basic premise of these solutions is that it allows organizations enforce policies at the application layer rather than the device layer. For example, authentication, remote wipes, lockouts and data encryption can now be enforced on a per application basis. Application Wrapping is a technique, which allows the ability inject their own code into existing iOS applications. Once injected, existing iOS method implementations can be overwritten to enforce these policies. In a nutshell, you can have an existing application and have it wrapped so that it enforces various defined policies and secure it without developers having to manually implement it.We have performed security assessments of various commercial BYOD solutions and custom secure containers. Additionally, we have also provided guidance in the development and design of such solutions. We plan to share our experiences through various case studies showcasing the various security issues encountered and testing techniques used throughout these assessments. We expect to cover and provide the audience with newfound knowledge in the following topics:What is Application Wrapping and How It Is Implemented - Dynamic Library Injection - iOS Method SwizzlingWalkthrough of Common Designs for Secure Containers - Weak Crypto Key Storage and Generation - Common Crypto Implementation Flaws - Online and Offline Authentication DesignsLeveraging iOS Runtime Analysis for Reversing Implementations - Common iOS Reversing Techniques - Writing Mobile Substrate HooksCompleteness of the Implementation - Preventing Common Mobile Security Plaintext Storage Issues - Inadvertent Caching of Sensitive Data - Jailbreak Detection - Weaknesses in Policy Enforcement and Remote WipesAttendees will leave with an understanding of the advantages and disadvantages of using "secure container" solutions. The presentation will be delivered from the point of view of a security tester with experience in assessing various implementations. Organizations can leverage this knowledge in order to perform informed decisions when choosing or developing solutions. Security testers will leave with baseline checks and testing techniques for assessing secure container implementations.

CSRF: not all defenses are created equal

Ari Elias-Bachrach

CSRF is an often misunderstood vulnerability. The standard way to protect against it is by implementing the singleton token pattern. This is usually done in the framework and not by the individual developer. For example .net applications can use the antiforgerytoken (for MVC applications) or viewstateuserkey. Tomcat web server and F5 load balancers also now include CSRF prevention filters. OWASP of course has the CSRF guard. All of these solutions though are slightly different and can lead to different side effects, some of which are little understood and poorly documented. Some side effects have even caused worse security problems (namely revealing the session cookie) while trying to defend against CSRF. In this talk I will introduce CSRF and the basic defenses against it. Then I will go through all of the various major solutions mentioned above and describe how they implement the general solution and the positives and negatives of each implementation.

Defeating XSS and XSRF using JSF Based Frameworks

Stephen Wolf

During several recent code review engagements, I have discovered that developers sometimes gain a feeling of comfort when they read that frameworks protect them from certain attacks. This sometimes leads to the assumption that if you use this framework, you are protected. This presentation will focus on Frameworks built upon JSF API component of JEE and two specific vulnerabilities which frameworks commonly advertise built-in mitigation; cross site scripting and cross site request forgery. It is very common for a framework to provide ways to prevent XSS and XSRF so to begin the session, I will take a few minutes to describe at a high level what these frameworks are and what we assume their capabilities are regarding these two vulnerabilities. During the course of this presentation, I will demonstrate what happens when these frameworks are used out-of-the-box by exploiting a sample application. Since this code is open source, we will look at the framework code to confirm or deny that they have automatically protected you against these attacks. I will then proceed to give you a couple of options which will close these gaps and secure the application from these attacks. You should leave this presentation with an awareness of what these frameworks are capable of and how to take advantage of their features to help secure the application.

Forensic Investigations of Web Explotations

Ondrej Krehel

Investigation of hacking incidents often requires combine effort of different technologies. Evidence and forensics artifacts are often found in various forms and formats. Network Forensics is one of the components in the process of finding compromised hosts, capturing and reconstructing malicious sessions. Attacks on web vulnerabilities can be replayed and transmitted data uncovered. This session will cover open source tools used for investigation of web compromised hosts and network forensics. Variety of tools can produce quite significant supplement to electronic evidence, and in many cases also capture the malicious executables transmitted in the traffic, or ex-filtrated data. Various network protocols and their structure will be presented. Open source Network forensic tools will be used on the traffic captured from a hacked web server. Different tools will be introduced for specific tasks in the investigation process. Captured traffic will be analyzed and reconstructed, and various artifacts found in the investigation will be discussed.

From the Trenches: Real-World Agile SDLC

Chris Eng

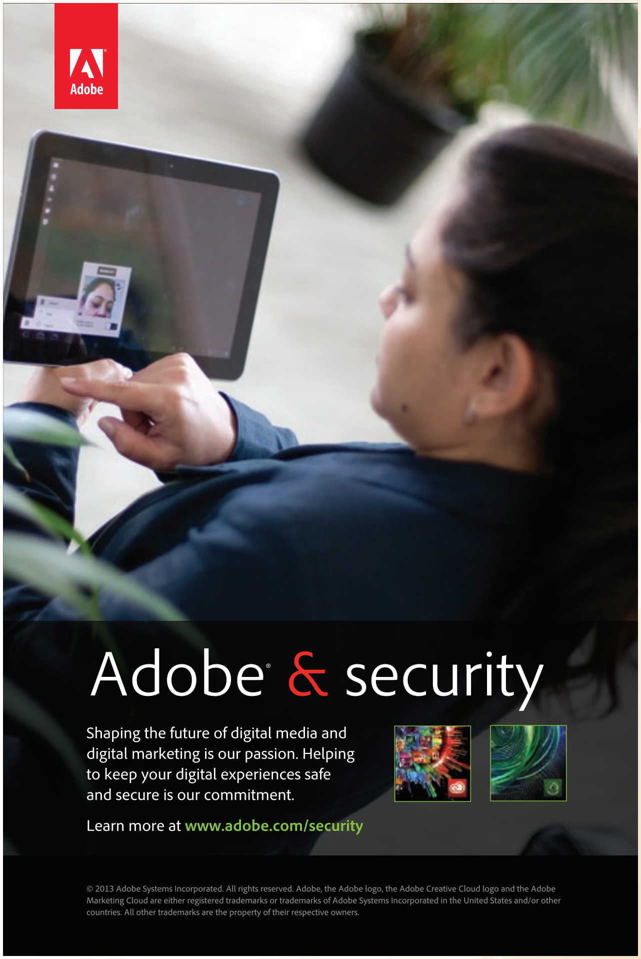
Ideally, all organizations would incorporate security into their Agile development processes; however, best-practices Agile SDL models typically assume a simplified, idealized model of how software is built. These models also impose impractical requirements without providing the necessary support or expertise. In reality, software development often involves multiple Agile teams working on various components of a larger product, and only the most well-resourced enterprises or ISVs have the bandwidth to execute on the ideal Agile SDL, while smaller organizations are forced to adapt and make tradeoffs. In this session, we'll discuss how Veracode has incorporated security into our own Agile development lifecycle for a product that involves anywhere from two to seven Scrum teams working in concert to ship monthly releases. We do this without designating any security experts full-time to the project. We'll explain how we've evolved our practices to optimize the way our security research team interacts with our engineering teams and accommodates their processes. We'll also talk about some of the lessons we've learned along the way, including things that haven't worked or wouldn't scale, and how other organizations can use our experience to integrate security practices into their own Agile development programs.

Go Fast AND Be Secure: Eliminating Application Risk in the Era of Modern, Component-Based Development

Jeff Williams, Ryan Berg

Organizations are exposed to significant risks caused by their increasing reliance on open-source components.

Component flaws are exceedingly common &ndash; 71 percent of applications contain components with known security flaws classified as severe or critical. Everything from Big Data, to cloud and mobile applications are exposed to unmanaged risk. The pressure to add more features and put applications into production quickly comes at a devastating tradeoff &ndash; to go fast or be secure. Using never-before-seen data from the Central Repository &ndash; the industry's primary source for open source components receiving 8 billion requests annually this presentation will examine how modern development is ushering in massive amounts of unmanaged risk demanding a new approach to mitigating the risk in modern, component-based applications &ndash; one that is significantly simpler to use, integrated throughout the software lifecycle and shows real, sustainable results. Like automobile manufacturers, today's software developers assemble applications using existing components or parts rather than writing applications from scratch. Open source component use has skyrocketed in recent years. In 2012, the Central Repository registered eight billion component downloads, doubling activity from 2011. 90% of a typical application today is now comprised of components, the bulk of these are open source, coming from dozens, if not hundreds, of individual suppliers. Yet, 71 percent of applications contain components with known security flaws classified as severe or critical, pointing to a major breakdown in application security. Unlike manufacturing, the software industry lacks the tools to manage the intricacy and risk associated with a complex and distributed software supply chain. When coupled with a trend toward agile development, enterprises are finding themselves with massive, unmanaged risk. Few organizations have the controls or processes to identify which components are in use, to govern their usage or to eradicate flawed components from applications. In the annual Open Source Development Survey &ndash; the largest study of its kind surveying more than 3,500 developers, architects and IT managers using open source &ndash; 76 percent of respondents shared that they have no control over what components are being used in software development projects and more than half cited a failure to maintain an inventory of components



used in production applications. Like operating systems or database, open-source components represent a rich attack vector for hackers to exploit given their commonality across organizations and applications. New to the OWASP Top 10 Guidelines is A9: Use of Insecure Libraries, acknowledging the widespread use of open source components in today's applications and the significant security risks that exists when organizations lack proper internal controls or fail to address security vulnerabilities throughout the software development lifecycle. Joint research from Aspect Security and Sonatype found the probability of having at least one vulnerability in an application due to a KNOWN insecure library is 95%. In this presentation, Ryan Berg, CSO of Sonatype and Jeff Williams, CEO of Aspect Security will examine why traditional approaches to application security can't protect today's applications. Using exclusive data from the Central Repository and sharing the findings of joint research, Berg and Williams will show why organizations must extend defense-in-depth to the application layer and how to deploy new approaches to software assurance that are simple, quick and continuous. Key topics and takeaways include: &bull;How to empower developers to become the new frontline of defense in today's cyber-security war &bull;Why securing the perimeter is not enough to protect the critical data housed in modern applications &bull;How to breakdown the traditional walls that exist between development teams and security and risk professionals &bull;Steps for introducing policy to govern component usage that will actually be adopted by developers &bull;How organizations can expedite development (go fast) and govern/manage (be secure) the entire application lifecycle to ensure the integrity of the software supply chain &bull;How to give developers the tools and authority to focus on security in real-time

Hack.me: a new way to learn web application security

Armando Romeo

The Hack.me (https://hack.me) project is a worldwide, FREE for all platform where to build, host and share simple and complex vulnerable web applications. It's completely online and doesn't require any software to be installed, just a web browser. Users will be able to run and practice offensive techniques against always new vulnerable web applications provided by the community. Users will be able to practice the OWASP Top 10, testing CMS vulnerabilities,verifying the latest exploits. The vulnerable web applications, referred as hackmes, are run in a sandboxed and user-isolated environment provided by the Coliseum Framework. We will show a typical use of the platform and some of the challenges, both technical and legal, faced by the project.

Hacking Web Server Apps for iOS

Bruno Oliveira

Since the iPhone has been released, people have been trying to figure out different ways to turn it into a common data storage device. Many applications have been released in the iTunes Store in order to add this capability, some using USB transport (via iTunes), others Bluetooth. However, another way found by most of these software vendors is to share the disk space in the cellphone using not only using

WiFi capabilities but also the data cellphone connections (GSM/CDMA). All of this by implementing a simple web server with file upload feature. Web file servers are now very common applications available in the iTunes Store with both free and paid versions that satisfies the users need to "share" the phone as being a file storage unit using the (... yes) HTTP protocol. Most (if not all) of these applications are not so well-designed with usually poor features. Yet, these apps are still very popular amongst those users that have no intention in jailbreaking their reliable mobile devices but really want file sharing capabilities. As previously mentioned, these apps are mainly developed using just HTML (which also brings some limitations to our testing) with no encryption (SSL) and mostly no authentication (and those supporting it are turned off by default??). This research covers these applications described above, both free and paid versions, how they work and what problems they bring to non-jailbroken devices, on top of describing the flaws, there will be a live demo on how risky these apps are. Despite of not being the highlight of the talk, it will be also demonstrated how worse things can be in jailbroken devices, once the sandbox security feature is lost. This talk will present current unpatched vulnerabilities that have been found while researching these applications, these range from medium to critical risks, and it will be shown how we can exploit these vulnerabilities and compromise the phone's file system with practical attacks. From a basic reflected XSS to an optimistic scenario: RCE, when the device is jailbroken and also has other app to support (web server with dynamic language for example), some of these exploitations will be presented to the public. And, all of the issues previously discussed can be magnified since the service (web server) is automatically advertised (and/or responds) to mDNS queries, making the device running that APP an easy target for anyone in the same wireless connection and watching these packets or simply running an mDNS browser.

Hardening Windows 8 apps for the Windows Store

Bill Sempf

Security and privacy in mobile development has been a topic in the iOS and Android world for a few years now. Microsoft is entering the fray with be their first significant push into the mobile space. Will your apps be the next ones on the front page of Ars Technica (for the wrong reasons)? Bill would like to help you make sure that won't happen. Learn the security considerations of HTML5, backend services, cloud computing and WinRT.

Healthcare Security Forum

Moderator(s): Amy Neustein, Judy Fincher

The Healthcare Security Discussion Forum is offered to provide security application developers an opportunity to discuss and share perspective on a vital industry sector where their work is gaining traction. The Healthcare Forum is an open discussion of activities underway to adopt secure applications (apps) and mobility in the Healthcare sector. It includes guidance from the Office of the National Coordinator (ONC) for Health Information Technology (HIT), from the Healthcare Committee of the National Strategy for Trusted Identities in Cyberspace (NSTIC),fromHealth Level Seven (HL7), and from the U.S. National Institute for

DENIM GROUP
Leading the Way for Secure Software Development
Application Vulnerability Management
Post-Testing Remediation
Deep Mobile & Web App Testing
Hybrid Developer Training
(210) 572-4400
www.denimgroup.com

Standards and Technology (NIST), such as Special Publication 800-53-4,"Recommended Security Controls for Federal Information Systems and Organization.&rdquo; All are welcome to participate in this open discussion oftrends, issues, and other topics of interest in the healthcare security sector. A bibliography will be provided to Forum participants.

How To Stand Up an AppSec Program - Lessons from the Trenches

Joseph Friedman

We all know the importance of building security into the development of a company's applications. Most of us know many of the steps needed for an effective Application Security Program. In this talk, we will discuss the best practices for implementing an AppSec Program, we'll list all the moving parts, and we'll talk about what worked and what didn't work in various organizations. Risk Management Metrics Training SDLC Requirements Design Review Development Testing Pre-Production Production Lessons Learned

HTML5: Risky Business or Hidden Security Tool Chest?

Johannes Ullrich

The term "HTML5" encompasses a number of new subsystems that are currently being implemented in browsers. Most of these were created with a focus on functionality, not security. But the impact of these features is not all negative for security. Quite the oposit. New abilities to store data on the client, or having access to hardware sensors like geolocation and tilt sensors have the ability to enhance session tracking and make authentication more secure and easier to use. This talk will select a number of examples to demonstrate the positive, as well as sometimes negative, impact of these features for web application security. Code samples for any demonstrations will be made available.

HTTP Time Bandit

Vaagn Toukharian

HTTP Time BanditWhile web applications have become richer to provide a higher level user experience, they run increasingly large amounts of code on both the server and client sides. A few of the pages on the web server may be performance bottlenecks. Identifying those pages gives both application owners as well as potential attackers the chance to be more efficient in performance or attack. We will discuss a tool created to identify weaknesses in the web application by submitting a series of regular requests to it. With some refinement and data normalizations performed on the gathered data, and then performing more testing based on the latter, it is possible to pinpoint the single most (CPU or DB) resource-consuming page of the application. Armed with this information, it is possible to perform more efficient DOS/DDOS attacks with very simple tools. The presentation will be accompanied by demos of the tool performing testing and attacking on various targets. The tool will be published for the interested researchers to play with.

Insecure Expectations

Matt Konda

Many developers rely on tests or specs (with expectations) to verify that our code is working properly. Few of us leverage the tests we are already writing to demonstrate security controls are properly applied. In this technical talk, we will walk through hands on examples of tests that demonstrate how to test for common security issues against an example Rails application (though the concept is not Rails specific). Although substantial testing is possible with existing tools, this talk will also present a new open source tool which provides developers with a simpler way to write security tests. The goals are twofold: &bull;To illustrate some common security issues. &bull;To give developers something concrete they can do about them. In addition to the technical portion of the talk, the speaker will spend a short time challenging the audience to help OWASP find ways to reach developers. The speaker has had success in a local community reaching developers through simple community organizing strategies, applied conscientiously over a long period of time.

iOS Application Defense - iMAS

Ganley, Gregg

iOS application security can be *much* stronger and easy for developers to find, understand and use. iMAS (iOS Mobile Application Security) - is a secure, open source iOS application framework research project focused on reducing iOS application vulnerabilities and information loss. Today, iOS meets the enterprise security needs of customers, however many security experts cite critical vulnerabilities and have demonstrated exploits, which in turn pushes enterprises to augment iOS deployments with commercial solutions. The iMAS intent is to protect iOS applications and data beyond the Apple provided security model and reduce the adversary's ability and efficiency to perform recon, exploitation, control and execution on iOS mobile applications. iMAS has released five security controls (researching many more) for developers to download and use within iOS applications. This talk will walk through various iOS application vulnerabilities, iMAS security controls, OWASP Mobile top10 and CWE vulnerabilities addressed, and demonstrate the iMAS App Password control integrated into an application.

Javascript libraries (in)security: A showcase of reckless uses and unwitting misuses.

Stefano Di Paola

Client side code is a growing part of the modern web and those common patterns or libraries, that are supposed to help developer's life, have the drawbacks to add complexity to the code exposing unexpected features with no or little warning. We will focus on the most popular JavaScript libraries such as jQuery, YUI etc and common design pattern, describing how happens that wrong assumptions can lead to unexpected, unsafe behavior. Several code example and live demos during the talk will try to clear both exploitation techniques and positive coding strategies. The presentation will also show some interesting case study, collected and identified during two years of real world applications analysis.

NIST Information Technology Laboratory

Matthew Scholl

Founded in 1901 and now part of the U.S. Department of Commerce, NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major handicap to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of England, Germany, and other economic rivals. Today, NIST measurements support the smallest of technologies—nanoscale devices—to the largest and most complex of human-made creations, from earthquake-resistant skyscrapers to wide-body jetliners to global communication networks.

In this session the NIST and ITL missions and impacts to US industry, economy and citizens will be presented. Attendees can learn about the current Programs, Projects and Research and Development activities in the US Governments premier scientific institutions.

Leveraging OWASP in Open Source Projects - CAS AppSec Working Group

Bill Thompson, Aaron Weaver, David Ohsie

The CAS AppSec Working Group is a diverse volunteer team of builders, breakers, and defenders that is working to improve the security of Jasig CAS, an open source WebSSO project. This presentation will show how the team is leveraging OWASP resources to improve security, provide security artifacts for potential adopters, and implementing policy and processes for vulnerability analysis and notification. The story is significant in that it directly addresses OWASP A9 "Using components with Known Vulnerabilities / Secure Coding", and points towards a model that other open source projects could adopt.

Making the Future Secure with Java

Milton Smith

The world is not the same place it was when Java started. It's 2013, and attackers are intensely motivated, sophisticated, and well organized. Java security is a significant concern across many organizations as well as for individuals. Attend to learn more about Oracle's progress on Java platform security and some our plans for the future.

Mantra OS: Because The World is Cruel

Greg Disney-Leugers

OWASP Mantra OS was developed under the mantra of &ldquo;OWASP because the world is cruel&rdquo;; The reason this mantra is used for a underlying principle for the development of Mantra OS is because simply it is better for the pen tester to find the exploit then the hacker. The tool-set of Mantra OS v13 contains the same tools many hackers use to exploit web applications such ddos, SQL injection, man in the middle attacks, and poisoning attacks. The purpose of this presentation is to show practical testing methodologies using Mantra OS and how to run these test in a controlled environment. In this talk we will discuss and demo: &bull; Demo of tool-set of Mantra OS &bull; Maltego and Intelligence collection. &bull; DDoS using LOIC, Slow HTTP poisoning and ping of death with scampy.

&bull; SQL injection with burp and sqlmap. &bull; Man in the Middle with SSL stripping. &bull; Arp Poisoning, ICMP poisoning and Smurf attacks. &bull; How to deploy these attacks in controlled environment. In addition we will discuss why and how hackers use these tools, methods of mitigation these style attacks by hackers, and how to turn pen testing into a risk mitigation plan.

Mobile app analysis with Santoku Linux

Andrew Hoog

Did you think there were a lot of mobile devices and platforms out there? Check out the hundreds of mobile tools being developed. We calculated it would take more time to install, test and maintain the various mobile tools than to actually fuzz the hell out all existing mobile operating systems. So, we created Santoku Linux, a F/OSS, bootable Linux distro to make life easier for mobile hackers. We pre-install not only the mobile platforms but promising tools in development. Santoku covers mobile forensics, mobile malware analysis and mobile security testing. The distribution is based on Lubuntu 12.04 x86_64 and we recently moved to .deb support for simplified upgrades. The Santoku website contains useful information on Santoku, notable:

- Tools: https://santoku-linux.com/features
- HOWTOs: https://santoku-linux.com/howtos
- Changelog: https://santoku-linux.com/download/changelog

This talk will introduce Santoku and provide live demos of 1) how to forensically acquire and analyze Android and iOS devices, 2) several tools to perform security audits of mobile devices and apps, and 3) how to analyze mobile malware analysis. All demos will leverage tools preinstalled on Santoku Linux and will cover both the iOS and Android platforms.

Modern Attacks on SSL/TLS: Let the BEAST of CRIME and TIME be not so LUCKY

Pratik Guha Sarkar, Shawn Fitzgerald

SSL/TLSis the core component for providing confidentiality and authentication in modern web communications. Recent vulnerabilities have undermined this and left much of web based communication vulnerable. This talk will survey recent attacks such as BEAST, TIME, CRIME, LUCKY 13 and RC4 biases, highlighting the conditions required for exploitation as well as the current state of mitigations. Comprehensive recommendations will be provided highlighting the real world risks and mitigations taking all attacks into account instead of providing conflicting solutions to mitigate these attacks individually. Finally, long term recommendations will be made as we move to a post TLS 1.0 world without overhauling the basic structure and operational infrastructure of modern web communication.

OWASP Broken Web Applications (OWASP BWA): Beyond 1.0

Chuck Willis

The OWASP Broken Web Applications (OWASP BWA) Project produces a free and open source virtual machine (VM) loaded with more than twenty-five web applications with a variety of

security vulnerabilities. The project VM is well suited for use as a learning and training environment or as a standard target for testing tools and techniques. After two years of betas, the project released version 1.0 of the VM in 2012. With that milestone behind us, this talk will focus on the project's future, though it will include some background on the project and demonstrate key features in the current release.

OWASP Hackademic: a practical environment for teaching application security

Konstantinos Papapanagiotou

Teachers of Application Security in higher education institutions and universities are presented with some unique challenges, especially when compared to other scientific or even computer science fields. This is mainly because students have to learn how to design, implement and protect applications against both known and unknown attacks. Moreover, the so far established stereotypes present the potential intruders as being ingenious and able to penetrate almost every system. The OWASP Hackademic Challenges Project introduces the "attacker's perspective" in higher education by implementing realistic scenarios with known vulnerabilities in a safe, controllable environment. Students can attempt to discover and exploit these vulnerabilities in order to learn important concepts of information security through the attacker's perspective. Its main difference from other projects that implement vulnerable applications for educational purposes, is that it is has been created mainly for use in a classroom environment, while most other solutions take a more self-learning approach. The OWASP Hackademic Challenges are currently used by more than a dozen universities around the world and are also part of the "Hacking Lab" and "OWASP University Challenge". In addition, we have received contributions to the project by several researchers, including the New Jersey Institute of Technology. The OWASP Hackademic Challenges simulate real-world scenarios that application security consultants and penetration testers encounter during their day-to-day engagements, combined with the academic requirements of a related module. These exercises can be used to complement the respective theoretical lectures. Statistical analysis of the feedback we received from students through questionnaires, shows that the students embraced this approach and have benefited significantly from going through these exercises. In practice, the OWASP Hackademic Challenges help students become more enthusiastic about application security by gaining a realistic, hands-on experience on some real-world vulnerabilities. In this presentation we will give an overview of the Hackademic Challenges and analyze its scientific background. In addition, we will present new features introduced to the interface that was developed during the Google Summer of Code 2012 and more importantly security improvements that were made possible by using OWASP ESAPI. The new interface introduces significant capabilities and features mainly for teachers and administrators. Moreover, as the project is still under development, we expect a bunch of new features to be ready by the conference dates. For example we are expanding the use cases of Hackademic in order for it to be used in a corporate environment to either train, assess or raise awareness among employees. Moreover, we will introduce a new scoring mechanism. CTF-type challenges usually follow a binary scoring system (solved/not solved), which is not sufficient for university classes. We have implemented a much more complex scoring system, that takes into account various parameters in order to depict how easy it was for the student to solve the challenge and how much time was required. Using this system, students can be graded according to their performance. Furthermore, we have introduced a randomization algorithm that produces slightly different answers for each try. Thus, it is much more difficult for students to cheat. A demo of the new Hackademic portal and challenges will also be delivered, emphasizing on how it can be used in a real classroom and giving the chance to attendees to get their hands on it.

OWASP Jeopardy

Moderator(s): Jerry Hoff

This interactive activity will be a fun filled event where top security professionals will get a chance to sit on a panel and answer a wide ranging set of questions relating to the world of OWASP. Unanswered questions will be presented to the audience, giving everyone a chance to participate and have fun. Questions and answers will be also synchronized through twitter to add to the participation. Join us for a night of special guest appearances, prizes, fun and drinks. Bring your squeeze balls!

OWASP NIST NSTIC IDecosystem Initiative: Initial Discussion Meeting

Moderator(s): Bev Corwin

BevCorwin, Member Representative for the OWASP IDESG Identity Ecosystem initiative is holding a first meeting discussion forum at AppSec USA to elaborate on the foundation's involvement with the NSTIC Identity Ecosystem Steering Committee.

OWASP Periodic Table of Elements

James Landis

After 25 years of software engineering since the first Internet worm was written to exploit a buffer overflow vulnerability, web developers are still building insecure software. It is time for a new approach. The vast majority of software bug classes can be eliminated by building protections into perimeter technologies, platform infrastructures, and application frameworks before a developer even writes a single line of custom code. By allowing developers to focus on just a small subset of bug classes, training and standards programs can be more targeted and effective so developers can write secure code much more efficiently. Vulnerabilities and weaknesses from industry-recognized indexes including OWASP Top 10, WASC TCv2, and CWE-25 are analyzed to determine which of the protection options are ideal for solving the software security problem. Where changes to internet standards and protocols are required, alternatives in perimeter, framework, or custom code solutions are also provided until the internet-scale solutions

are in place. If a solution can be completely implemented in perimeter or infrastructure technologies, only that solution is provided. Similarly, if any part of the solution can be provided in standard or custom frameworks, that solution is not recommended to be implemented in custom code. The guiding principle is essentially: "implement security controls as far from custom code as possible." Only if there is no other way to solve a particular security problem is a custom code solution recommended.

OWASP Top Ten Proactive Controls

Jim Manico

You cannot hack your way secure! The OWASP Proactive Controls is a "Top 10 like document" aimed to help developers build secure applications. This project is phrased and built in a positive, testable manner that describes the Top 10 software control categories that architects and developers should absolutely, positively include 100% of the time in every software project. This talk will cover the fundamental controls in critical software categories such as Authentication, Access Control, Validation, Encoding, Query Parameterization, Data Protection, Secure Requirements, Secure Architecture and Secure Design.

OWASP Zed Attack Proxy

Simon Bennetts

The Zed Attack Proxy (ZAP) is now one of the most popular OWASP projects. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing as well as being a useful addition to an experienced pen tester's toolbox. This talk will focus on the latest changes to ZAP and the plans for it's future. Due to the growing number of people working on ZAP, and the fact that it is very likely to be involved in the Google Summer of Code 2013, the content of the talk will be announced closer to the conference date.

PANEL: Aim-Ready-Fire

Moderator(s): Wendy Nather

Ajoy Kumar, Thien La, Pravir Chandra, Elliot Glazer, Suprotik Ghose, Jason Rothhaupt, Ramin Safai

Software assurance in the past 5 - 6 years has emerged as the key focus area for information security professionals. The C - suite has recognized software assurance to be more than a hygiene problem as the application security breaches have started making impact to the bottom line of the companies. The international regulators are demanding systems that are more resilient. The number and complexity of cyber breaches keeps on increasing, there is no relief in sight... lets learn what is working and what is not.

PANEL: Cybersecurity and Media: All the News That's Fit to Protect?

Moderator(s): Dylan Tweney

Rajiv Pant, Gordon Platt, Michael Carbone, Nico Sell

It's no longer possible to be in the news media without being security savvy.

Edward Snowden's NSA leaks, FBI subpoenas of reporters' phone records, and frequent hack attacks directed against news organizations -- all of these prove that we're living in a time when journalists need cybersecurity skills.

Whether to protect the sacred bond between reporters and sources or to protect the credibility and availability of a major news website, those in the media must know what security tools are available and how to use them. And the security industry must know what journalists need, and how existing tools fall short.Cybersecurity and Media: All the News That's Fit to Protect?

In this panel, reporters and IT pros will describe how security issues have affected them. We'll discuss leading-edge software and best practices to protect the newsroom. And we'll create a wishlist for the software and services needed to protect journalism's role as the 24/7, real-time, global clearinghouse of the information economy.

PANEL: Privacy or Security: Can We Have Both?

Moderator(s): Jeff Fox

Jim Manico, James Elste, Jack Radigan, Amy Neustein, Joseph Concannon

Often confused with each other, security and privacy are both interdependent (privacy generally requires robust security) and sometimes at odds with each other (security may require sacrificing privacy). While the public's online privacy has taken a big hit in the past decade, it is at least defended by an army of public-interest groups and legal experts. Meanwhile, to many, the public's online security often remains shrouded in technical jargon and barely present in public policy discussions.This panel will explore issues such as these: -When do security measures go &ldquo;over the line&rdquo; and begin encroaching on individual privacy? -What privacy rights is the public (or should it be) willing to trade for more security?- Online anonymity gets a lot of lip service. Has it outlived its usefulness? Political dissidents aside, is it now doing more harm than good by shielding criminals while hardly protecting the average user?- Major private and public institutions often fall down on the job of ensuring either cybersecurity or cyberprivacy. What combination of self-regulation, government oversight, and market accountability (in the form of cyber insurance, auditing, and litigation) would most effectively push them to better meet their responsibility to the public and shareholders? Moderator: Jeff Fox, Technology Editor, Consumer Reports and ConsumerReports.org

PANEL: Mobile Security 2.0: Beyond BYOD

Moderator(s): Stephen Wellman

Devindra Hardawar, Daniel Miessler, Jason Rouse

Abstract: BYOD has moved quickly from technology concept to business reality. Today's workers bring the mobile devices they want into their organizations, freely accessing data and working from the most convenient network connections. While all this mobility has unleashed greater productivity for today's companies, it has introduced a new level of complexity for IT. IT professionals today need to move their mobility strategies from BYOD 1.0 -- the introduction of different devices and network connections into the enterprise -- to BYOD 2.0 -- a comprehensive framework that helps IT better monitor and secure data and networks without compromising the productivity of workers. This panel will tackle the issues IT now faces it evolves from the early era of BYOD into a more complex work world of multiple devices, social media, apps, and more

PANEL: Threat Intelligence and Software Security: Opportunities for Improvement?

Moderator(s): Mark Miller

Josh Corman, Chris Eng, Space Rogue, Joe Sechman

The symbiosis between threat intelligence and software security is onlygoing to strengthen as adversaries become more fluent in waging attacks byany means necessary to achieve the desired impact of their actions. Byencouraging more open discussion amongst threat intelligence researchers,software security professionals and penetration testers, the means by whichan adversary can exploit these weaknesses diminishes. This panel willdiscuss ways in which the threat intelligence and software securitycommunity can increase collaboration in order to defend today's evolvingthreat landscape.

PANEL: Women in Information Security: Who Are We? Where Are We Going? (Salon 1 & 2)

Moderator(s): Joan Goodchild

Dawn-Marie Hutchinson, Valene Skerpac, Carrie Schaper, Gary Phillips

NPR reports that 80% of computer programmers are men. As an engaged group that believes in the benefits of gender diversity, OWASP wants to know what we can do to close that gap. In this session, we have invited women from different stages of their Information Security careers to share experiences and offer suggestion about what can be done to improve the situation. We will also hear from a stakeholder in the corporate community who offers best practices to manage diversity within organizations large and small. Moderator: Joan Goodchild, Editor, CSO Online.

PiOSoned POS - A Case Study in iOS based Mobile Point-of-Sale gone wrong

Mike Park

Mobile Point of Sale (POS) are becoming more and more common in a wide variety of retail outlets. And why not, it adds speed and convenience to shopping and can increase a retailers ability to sell. But POS and Mobile are hard to get right and secure. What happens when you try to combine the two on trendy iOS devices and rush your solution out the door? Based on multiple mobile tests conducted by Trustwave SpiderLabs' application security, Mike Park will walk through the typical mobile POS apps for iOS and show how and why they can be attacked, often with no sign an attack is going on. Mike will cover technological shortcomings, coding mistakes and the common misunderstanding of the underlying platform that almost always occur and result in an insecure application. This will include some hardware card reader devices that default to allowing almost no security. Outline 1. Introduction 2. Why Mobile POS? 3. Why iOS? 4. The Problem Poorly written apps Speed of jailbreaking Ability to hide the jailbreak The Card Reader 5. A walk through of the PiOSon POS demo app What the app does How the app reads CHD How the app processes and send the data to the backend How typical is this 6. Hacking the POS - Demo Jailbreak Intro to Method Swizzling Setting up the device Adding the reader Installing the malware Capture the Track data 7. How to improve this Understand the underlying platform Understand the way your card reader works Why is this so insecure? View a safer version of the app – AntidOte POS 8. What to do Coding best practices Choosing a card reader Outside the device – MDM? 9.Conclusion

Project Summit Working Sessions

Samantha Groves

The OWASP Project Summit is a smaller version of the much larger OWASP Summits. This event activity gives our project leaders the opportunity to showcase their project progress, and have attendees sit down and work on project tasks during the event. It is an excellent opportunity to engage the event attendees, and it gives project leaders the chance to move forward on their project milestones while meeting new potential volunteers that can assist with future milestones. Join us for 4 full days of OWASP Project working sessions. Firm session schedule will be up soon.

Project Talk and Training: OWASP O2 Platform

Dinis Cruz

The O2 platform represents a new paradigm for how to perform, document and distribute Web Application security reviews. O2 is designed to Automate Application Security Knowledge and Workflows and to Allow non-security experts to access and consume Security Knowledge Project Leader, Dinis Cruz, will be giving a talk along with a training session on how to use the platform.

Project Talk: OWASP AppSensor

Dennis Groves

The AppSensor project defines a conceptual framework and methodology that offers prescriptive guidance to implement intrusion detection and automated response into an existing application. Current efforts are underway to create the AppSensor tool which can be utilized by any existing application interested in adding detection and response capabilities. Learn more about OWASP AppSensor Project by attending this talk by OWASP Co-Founder, Dennis Groves.

Project Talk: OWASP Code Review Guide

larry conklin

The Code Review Guide focuses on secure code reviews and tools that aim to support the developer community. Such an activity is very powerful as it gives the developer community a place to start regarding secure application development. Project Leader, Larry Conklin, will be giving a talk about the project, and what the current state of Version 2.0 is.

Project Talk: OWASP Development Guide

Andrew van der Stock

The Development Guide is aimed at architects, developers, consultants and auditors and is a comprehensive manual for designing, developing and deploying secure Web Applications and Web Services. The OWASP Developer Guide 2013 aims to focus the content from countermeasures and weaknesses to secure software engineering. Learn more about the OWASP Development Guide by attending this project talk. Project Leader, Andrew van der Stock, will be speaking.

Project Talk: OWASP Enterprise Security API Project

Chris Schmidt, Kevin Wall

ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library that makes it easier for programmers to write lower-risk applications. The ESAPI libraries are designed to make it easier for programmers to retrofit security into existing applications. Learn more about the OWASP ESAPI Project from Project Leaders, Chris Schmidt and Kevin Wall.

Project Talk: OWASP OpenSAMM Project

Seba Deleersnyder, Pravir Chandra

The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. The resources provided by SAMM will aid in:

- Evaluating an organization's existing software security practices
- Building a balanced software security programin well-defined iterations
- Demonstrating concrete improvementsto a security assurance program
- Defining and measuring security-related activitieswithin an organization

SAMM was defined with flexibility in mind such that it can be utilized by small, medium, and large organizations using any style of development. Additionally, this model can be applied organization-wide, for a single line-of-business, or even for an individual project.Project Leader, Sebastien Deleersnyder, will be speaking about the project in depth in this talk.

Project Talk: OWASP Security Principles Project

Dennis Groves

The OWASP Security Principles Project aims to distill the fundamentals of security into a set of concise principles that must be present in any system through out the requirements, architecture, development, testing, and implementation of a system. OWASP Co-Founder and Project Leader, Dennis Groves, will be giving a talk about the future of the project.

Project Talk: OWASP Testing Guide

Andrew Mueller

This project's goal is to create a &ldquo;best practices&rdquo; web application penetration testing framework which users can implement in their own organizations. Contributors of this project are currently writing Version 4 of the guide, and are actively seeking authors.Learn more about the OWASP Testing Guide here by attending this talk by Project Leader, Andrew Muller.

Project Talk: Project Leader Workshop

Samantha Groves

The Project Leader Workshop is a 45 minute event activity that brings together current and potential OWASP project leaders to discuss project related issues and topics. The Project Leader Workshop is an optional event activity for our leaders that takes on a presentation and discussion format. It is an interactive tool used to bring together project leaders from across the globe in an effort to have participants share valuable insights and recommendations with their fellow members.

Leaders can expect to learn more about the OWASP Projects Infrastructure, the benefits of having an OWASP Project, and how they can leverage the infrastructure to help promote their project to the community and beyond. OWASP Project Manager, Samantha Groves, will lead the session.

Project Talk: The OWASP Education Projects

Konstantinos Papapanagiotou, Martin Knobloch

The OWASP Education project is meant to centralize all educational initiatives of OWASP. The project will not deliver education material as such, but define standards and guidelines on education material. Furthermore, this project aims to create an easy entrance towards understanding application security and usage of the OWASP tooling. By creating education documentation papers, screen scrape video courses, and setting up an OWASP Boot camp, a controlled education process of a standardized quality can be created continuously.

Initiatives of the OWASP Education Project are:

- OWASP Training
- OWASP Boot camp
- OWASP Training events
- OWASP Academies
- OWASP Academy Portal
- OWASP University Outreach
- OWASP Student Chapter

Project Leaders, Martin Knobloch and Konstantinos Papapanagiotou, will be giving a talk on the various education projects within the OWASP Projects Inventory. Attend this talk for an excellent overview of each initiative.

Pushing CSP to PROD: Case Study of a Real-World Content-Security Policy Implementation

Brian Holyfield, Erik Larsson

Widespread adoption of Content Security Policy (CSP) by most modern browsers has led many organizations to consider implementing CSP to thwart Cross-Site Scripting attacks in their web applications. In this session we will walk you through our experience successfully implementing CSP on our customer-facing web application, SendSafely.com, which relies heavily on JavaScript and HTML5. Our story will arm you with the knowledge you'll want should you decide to go down the same path. When we initially decided to implement CSP, the BETA version of our website was already live. Like many sites, our platform grew from something we initially started as a pet project. Admittedly, building CSP into our site from day one would have been much easier...but not nearly as challenging or fun. We'll start by walking you through our Content Security Policy, discuss the basic nuances between how each major browser implements CSP, and outline techniques for how we deal these nuances at runtime. Next, we'll discuss the basic techniques we used for converting all of our classic &ldquo;in-line&rdquo; JavaScript to comply with the strict CSP that we developed. We'll also talk about the not-so-easy task of getting third-party JavaScript to play nicely with CSP (cough, ReCaptcha, cough) and cover some edge cases we ran into related to the newer HTML5 APIs we rely on for certain tasks. Lastly, we'll discuss what we learned from implementing a notification mechanism to report violations of our CSP at runtime. Needless to say we were surprised by what was reported, and we'll share the results. Our hope is that by telling our story to the world, we'll either save the rainforest or make your life a little easier should you decide to implement CSP (worst case scenario we'll save you the trouble and dissuade you from even trying).

Revenge of the Geeks: Hacking Fantasy Sports Sites

Dan Kuykendall

In this talk, I'll show how all my IT security geek friends in the OWASP community can win the Super Bowl! I'll walk through the anatomy of a hack against popular Fantasy Football and Baseball mobile applications showing every "sneak play" required to control the application. The tools and techniques used in this hack can be applied against any mobile application. These applications leverage rich new formats like JSON and REST to deliver a rich user experience, and are not surprisingly exposing the same familiar vulnerabilities like SQL and command injection, yet are not being effectively tested. In this particular application, mistakes with the application's session management enable me to break down the nested communication formats and finally inject targeted payloads to manipulate both team lineups, to make sure my players were on top and to cause my opponents to lose. I also found that I could post false comments on the message board from the victims account. After we walk through the sack, I mean hack, we'll abstract these techniques, tie them directly to OWASP best practices, and apply them to other mobile applications so participants will walk away with specific tools and techniques to better understand mobile back-end hacking. Are you ready for some football? This presentation will: --Provide overview and details about each of the various formats (JSON, REST, SOAP, GWTk, and AMF) in popular use today --Provide clear examples of basic mobile app insecurityRevenge of the Geeks: Hacking Fantasy Sports Sites In this talk, I'll show how all my IT security geek friends in the OWASP community can win the Super Bowl! I'll walk through the anatomy of a hack against popular Fantasy Football and Baseball mobile applications showing every “sneak play” required to control the application. The tools and techniques used in this hack can be applied against any mobile application. These applications leverage rich new formats like JSON and REST to deliver a rich user experience, and are not surprisingly exposing the same familiar vulnerabilities like SQL and command injection, yet are not being effectively tested. In this particular application, mistakes with the application’s session management enable me to break down the nested communication formats and finally inject targeted payloads to manipulate both team lineups, to make sure my players were on top and to cause my opponents to lose. I also found that I could post false comments on the message board from the victims account. After we walk through the sack, I mean hack, we’ll abstract these techniques, tie them directly to OWASP best practices, and apply them to other mobile applications so participants will walk away with specific tools and techniques to better understand mobile back-end hacking. Are you ready for some football? This presentation will: --Provide overview and details about each of the various formats (JSON, REST, SOAP, GWTk, and AMF) in popular use today --Provide clear examples of basic mobile app insecurity --Demonstrate how to setup an environment to start watching mobile traffic, including how to leverage Wifi Pineapple hardware to set up a local access point --Demonstrate how to inject malicious characters into these services to find vulnerabilities --Discuss what tools are available to automate this process and make it a little easier --Show examples of real vulnerabilities in mobile apps in use today Attendees will be given a whitepaper with the details of the complete setup demonstrated in the talk.

Sandboxing JavaScript via Libraries and Wrappers

Phu H Phung

The large majority of websites nowadays embeds third-party JavaScript into their pages, coming from external partners. Ideally, these scripts are benign and come from trusted sources, but over time, these third-party scripts can start to misbehave, or to come under control of an attacker. Unfortunately, the state-of-practice integration techniques for third- party scripts do not impose restrictions on the execution of JavaScript code, allowing such an attacker to perform unwanted actions on behalf of the website owner and/or website visitor. In this paper, we present a two-tier sandbox architecture to enable a website owner to enforce modular fine- grained security policies for potential untrusted third-party JavaScript code. The architecture contains an outer sand- box that provides strong baseline isolation guarantees with generic, coarse-grained policies and an inner sandbox that enables fine-grained, stateful policy enforcement specific to a particular untrusted application. The two-tier approach ensures that the application-specific policies and untrusted code are by default confined to a basic security policy, with- out imposing restrictions on the expressiveness of the policies. Our proposed architecture improves upon the state-of-the- art as it does not depend on browser modification nor pre-processing or transformation of untrusted code, and allows the secure enforcement of fine-grained, stateful access control policies. We have developed a prototype implementation on top of a open-source sandbox library in the ECMAScript 5 specification, and validated it with several real-world JavaScript applications such as Google Analytics, Google Maps, and jQuery UI.

Securing Cyber-Physical Application Software

Warren Axelrod

Researchers and practitioners have not historically addressed sufficiently the fact that software engineers responsible for IT systems have very different approaches from those who design and build industrial control systems. When Web-facing and distributed information systems are interconnected with legacyindustrial control systems, which usually do not include effective security requirements, two major issues arise: one is the possibility of someone gaining access to control systems via Web applications and public networks, and the other is the potential for the transfer of fallacious information from the control systems to the information systems, as ostensibly occurred with Stuxnet. In this presentation we take a new approach to processes and technologies for mitigating the threats and hazards that impinge on, or result from, systems such as the smart grid. The presentation is based in part on the author's book Engineering Safe and Secure Software Systems (Artech House, 2012).

Silk, Webservers, Exploits and RATz by M4v3r1ck

Yuri

Disclaimer: If you have trigger issues -- please do not attend this talk.Now that the statute or limitations has run out on walk with me as I discuss the industry, the people and the events.From warelords, to the conference that was meant to be a one-time party to say good-bye to BBSs OG. Todays web applications still provide the perfect place for logic bombs. We will talk about current news events including carderprofit.cc and the newest threat to turning a profit. Face it.. the computer security industry is a JOKE, Vă veţi bucura acest talk.pssssss buddy you want to buy a shell... what'ca want what'ca need?

Tagging Your Code with a Useful Assurance Label

Robert Martin

With so many ways for software to be vulnerable, businesses needs a way to focus their assurance efforts on those potential vulnerabilities that are most dangerous to them and their software. This talk will offer a new way to focus and organize your software vulnerability assessment and assurance efforts across the entire life-cycle of a project so that you target the most impactful weaknesses when they are most visible. The approach can be done consistently across your enterprise and will have you looking for specific weaknesses at the point where you can gain the most assurance that you have dealt with them successfully. Matched to the activities of your development effort, this approach will have your team looking for those security weaknesses (CWEs) that are most discernable/findable in each of the different stages of a software development effort. For example, when you have a live exemplar system available you should look for the weaknesses in design, configuration, code, or architecture that are findable through dynamic analysis, pen testing, or red teaming of that living system. Similarly, in the coding phase you want the emphasis to be looking for weaknesses that are findable by static analysis tools. The follow-on step to this approach is to use what you found and what you did to create "An Assurance Tag for Binaries", basically an assurance "food label" for the code of that project. This talk will conclude with a discussion of what such a tag could look like, what it could capture, how the information could be obtained, whom would/could create them, and how they could be represented for humans and machines to use.

The 2013 OWASP Top 10

Dave Wichers

The OWASP Top 10 has become the defacto standard for web application security and is referenced by numerous important standards and guidelines around the world, including the Payment Card Industry (PCI) standard, as just one example. This presentation will explain how the OWASP Top 10 for 2013 changed from the previous version and why. It will then briefly go through each item in the OWASP Top 10 for 2013, explaining the risks each issue introduces to an enterprise, how attackers can exploit them, and what your organization can do to eliminate or avoid such risks in your application portfolio.

The Cavalry Is Us: Protecting the public good

Josh Corman, Nicholas J. Percoco

In the Internet of Things, security issues have grown well beyond our day jobs. Our dependence on software is growing faster than our ability to secure it. In our efforts to find the grown-ups who are paying attention to these risks, one painful truth has become clear: The Cavalry Isn't Coming. Our fate falls to us or to no one. At BSidesLV and DEF CON21, a call was made and many of you have answered. At DerbyCon, we begin the work of shaping our futures. Here at AppSec, we have the opportunity to level-up and reframe our role in all of this. As the initiated, we face a clear and present danger in the criminalization of research, to our liberties, and (with our increased dependence on indefensible IT) even to human safety and human life. What was once our hobby became our professionand (when we weren't looking) now permeates every aspect of our personal lives, our families, our safety&Scaron; Now that security issues are mainstream, security illiteracy has lead to very dangerous precedents as many of us are watching our own demise. It is time for some uncomfortable experimentation.

This session will both frame the plans to engage in Legislative, Judicial, Professional, and Media (hearts & minds) channels and to organize and initiate our 'constitutional congress' working sessions. The time is now. It will not be easy, but it is necessary, and we are up for the challenge.

It's high time we make our dent in the universe. For background, please watch the video of the launch of @iamthecavalry : http://bit.ly/16YbpC1 Join the conversations also at: google group: https://groups.google.com/d/forum/iamthecavalry

The Perilous Future of Browser Security

Robert Hansen

The tradeoffs required to make a secure browser are often largely poorly understood even amongst the best of security people. It makes sense since so few people actually work on browsers. There is little knowledge about what it requires to make a browser safe enough to use when viewing hostile websites - against all known adversaries. In this presentation Mr. Hansen will cover how browsers are critically insecure, how they can be made to be secure, and what consumers forfeit in order to gain that extra level of security. Lastly, the presentation will cover how to think about tradeoffs and what customers can live without.

The State Of Website Security And The Truth About Accountability and "Best-Practices"

Jeremiah Grossman

Whether you read the Verizon Data Breach Incidents Report, the Trustwave Global Security Report, the Symantec Internet Security Threat Report, or essentially all other reports throughout the industry, the story is the same -- websites and Web applications are one of, if not the leading target of, cyber-attack. This has been the case for years. Website breaches lead directly to financial fraud, identity theft, regulatory fines, brand damage, lawsuits, downtime, malware propagation, and loss of customers. Given modern society's ever-increasing reliance on the Web, the impact of a breach and the associated costs are going up, and fast. At WhiteHat Security we asked customers to answer roughly a dozen very specific survey questions about their SDLC and application security program. Questions such as:

- How often do you preform security tests on your code during QA?
- What is your typical rate of production code change?
- Do you perform static code analysis?
- Have you deployed a Web Application Firewall?
- Who in your organization is accountable in the event of a breach?
- We even asked: has your website been breached?

We received responses to this survey from 76 organizations, and then correlated those responses with WhiteHat Sentinel website vulnerability data. The results were both stunning and counter-intuitive. The connections from various software security controls and SDLC behaviors to vulnerability outcomes and breaches are far more complicated than we ever imagined. This is exactly the kind of research the application security industry must gather in order to advance the state-of-the-art. To cost-effectively make applications and websites measurably more secure.

') UNION SELECT `This_Talk` AS ('New Exploitation and Obfuscation Techniques')%00

Roberto Salgado

This talk will present some of the newest and most advanced optimization and obfuscation techniques available in the field of SQL Injections. These techniques can be used to bypass web application firewalls and intrusion detection systems at an alarming speed. This talk will also present the ALPHA version of an open-source framework called Leapfrog which Roberto is developing; Leapfrog is designed to assist security professionals, IT administrators, firewall vendors and companies in testing their firewall rules and implementation to determine if they are an adequate enough defense measure to stop a real cyber-attack.

Verify your software for security bugs

Simon Roses Femerling

Verification is an important phase of developing secure software that is not always addressed in depth that includes dynamic analysis and fuzzing testing. This step allows checking that security has been built in the implementation phase: secure coding and using compilers mitigations correctly. This presentation will cover the current state of verification technologies that developers can use to check the lack of security mitigations (ASLR, DEP, SafeSEH, Stack Guard, PIE, etc.) and vulnerabilities (Missing Code Signing, Insecure API, DLL planting, poor coding, etc.) and how to implement a battery of tests in their organization to verify their products are safe before releasing as required by an Application Assurance process. A new tool will be presented, BinSecSweeper, that performs security binary analysis, is open source and cross platform (Windows and Linux) and can scan PE &amp; ELF file formats for x86-64 that can be used by developers to check their software includes security mitigations and is compliance with Application Assurance best practices or by IT pros to identify insecure applications in their networks. This technology was sponsored by DARPA Cyber Fast Track (CFT). If you develop software or work in AppSec this is your talk!

Wassup MOM? Owning the Message Oriented Middleware

Gursev Singh Kalra

Message Oriented Middleware (MOM) allows disparate applications to communicate with each other by exchanging information in the form of messages. A MOM and its clients create an enterprise messaging application that forms the transactional backbone of several large organizations worldwide. Security is therefore an important aspect of these applications. This research analyzes enterprise messaging security from three different perspectives:

1. The first perspective derives from the fact that most of the enterprise messaging products support the vendor-agnostic Java Messaging Service (JMS) API and therefore focuses on the offensive uses of the JMS API to attack an enterprise messaging application.
2. The second perspective revolves around a JMS compliant message broker (or MOM) as message brokers form the core of the enterprise messaging. I chose ActiveMQ for my research as it is open source and among the most popular message brokers that support JMS API. I will discuss a few ActiveMQ 0days vulnerabilities, potential flaws in its various authentication schemes and its configuration defaults that can make it vulnerable to attacks.
3. The third perspective focuses on a new tool JMSDigger that can be leveraged to engage and assess enterprise messaging applications. Several live demonstrations will show attacks such as authentication bypass, JMS destination dumps, 0day vulnerabilities and JMSDigger etc...

“What Could Possibly Go Wrong?” - Thinking Differently About Security

Mary Ann Davidson

Almost all security professionals have one or more headshaking security stories caused by everything from sloppy design to execrable coding to insanely asymmetric risk assumption. Technical acumen is not enough if we want to improve actual security (instead of improving our job security): we need to think about, and talk about, security differently. This means absorbing the language, constructs and lessons of other disciplines from economics (systemic risk) to military history and tactics (force multipliers). It means understanding the limits of technology, that there are “unknown unknowns” and that humans are all too fallible (and there’s no upgrade coming). Lastly, it requires the techno-proficient among us to learn to de-geek our speak so that we can express security concerns in terms that decision makers and policy makers can understand: “barbarians are at the gate” is so much more understandable and actionable than “there’s a manifestation of a theoretic weakness in the Visigoth detection protocol.”

What You Didn’t Know About XML External Entities Attacks

Timothy Morgan

The eXtensible Markup Language (XML) is an extremely pervasive technology used in countless software projects. Certain features built into the design of XML, namely inline schemas and document type definitions (DTDs) are a well-known source of potential security problems. Despite being a publicly discussed for more than a decade, a significant percentage of software using XML remains vulnerable to malicious schemas and DTDs. This talk will describe a collection of techniques for exploiting XML external entities (XXE) vulnerabilities, some of which we believe are novel. These techniques can allow for more convenient file content theft, sending of arbitrary data to arbitrary internal TCP services, uploads of arbitrary files to known locations on a vulnerable system, as well as several possible denial of service attacks. We hope this talk will raise awareness about the overall risk associated with XXE attacks and will provide recommendations that developers and XML library implementors can use to help prevent these attacks.

Why is SCADA Security an Uphill Battle?

Amol Sarwate

This talk will present technical security challenges faced by organizations that have SCADA, critical infrastructure or control systems installations. It will provide examples of attacks and examples of security controls that orginizations can implement to protect against these attacks. It will focus on how OWASP and SCADA are getting knit closely together. The talk will also introduce an updated version of an open-source tool to help identify and inventory SCADA systems. The presentation will begin by introducing SCADA systems under the hood including RTU, IED, PLC, FEP, PCS, DCS, HMI, sensors, data historians and other SCADA components. The presenter will categories these components into distinct groups based on the functionality that each component provides. We will review the security implications on each of these groups and identify where most of the threats lie. We will take a packet level dive into SCADA protocols and study their security implications. The presentation will give example of attacks that can be carried out against each group and component. The presenter will release an updated version of an open-source tool to identify and inventory SCADA systems using the protocols discussed in this presentation. It will then focus on real world examples of successful and not-so-successful implementations of security controls with SCADA systems which will include examples of what some large organizations have done. We will conclude with guidance on how control system owners can start implementing additional measures to get to an acceptable security. Attendees who are in charge of control system infrastructure will get insight on what worked and what did not for other organizations. Engineers who are in-charge of security for control systems will get a better technical insight of SCADA protocols and components and can use the open source tool that is introduced. Attendees who are new to control systems will get an excellent overview of security complexities of control systems.

Sponsors

THANK YOU TO ALL OF THE APPSEC USA SPONSORS & SUPPORTERS!

Diamond Sponsor

HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. The world's largest technology company, HP brings together a portfolio that spans printing, personal computing, software, services and IT infrastructure to solve customer problems. More information about HP (NYSE: HPQ) is available at http://www.hp.com.

Platinum Sponsors

Adobe is changing the world through digital experiences. Our tools and services allow our customers to create groundbreaking digital content, deploy it across media and devices, measure and optimize it over time, and achieve greater business success. We help our customers make, manage, measure, and monetize their content across every channel and screen.

Aspect Security is a founding OWASP member and a leader in the application security community. We offer industry-leading penetration testing, code review, instructor-led training, eLearning, mobile security, and SDLC consulting services. Please stop by our booth to see Contrast™, our revolutionary application security technology.

Gold Sponsors

Akamai is the leading cloud platform for helping enterprises provide secure, high-performing user experiences on any devise, anywhere. Our Intelligent Platform™ removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud – Akamai accelerates innovation in our hyperconnected world.

Arxan provides software security solutions that protect the App Economy from hacker attacks with the world's strongest and most deployed application integrity protection products. Our self-defending and tamper-resistant technology secures mobile apps against tampering, reverse engineering, fraud, unauthorized use, malware exploits, piracy, intellectual property theft and brand compromise. www.arxan.com.

Gold Sponsors (continued)

ASTECH consulting

AsTech Consulting designs solutions to optimize every phase of a Secure Development Lifecycle. By understanding our clients' unique risk appetites and business objectives, our engineers bring strategic focus to application security initiatives. AsTech provides source code security assessments, grey-box testing, vulnerability remediation, secure development training, SDLC consulting, process automation and integration services.

eLearnSecurity
Forging security professionals

Based in Pisa, Italy and with offices in San Jose, California and Dubai, eLearnSecurity is a leading provider of IT security and Penetration Testing training for IT professionals. eLearnSecurity has innovated the field of practical security training by creating the most sophisticated virtual labs on Web Application and Network Security.

f5

F5 secures access to applications and data from anywhere while protecting the applications wherever they reside. Delivering an intelligent services platform deployed at strategic points in the network, F5 helps businesses protect critical resources and minimize interruptions. These highly scalable and extensible solutions create simplicity by integrating market-leading application delivery, monitoring, and context-based policy enforcement.

KPMG
cutting through complexity

KPMG's high-performing professionals use experience and insight to cut through complexity and deliver informed perspectives and clear methodologies that our clients value. Client focus, commitment to excellence, global mind-set, and consistent delivery build trusted relationships - core to our business and reputation. In essence, our competitive advantage is high-performing people cutting through complexity.

netSPI

Using its consulting team's deep security knowledge and its CorrelatedVM vulnerability management & reporting solution, NetSPI acts as a trusted advisor to large enterprises by providing penetration testing, assessment, and advisory services designed to analyze and mitigate risks and ensure compliance with relevant regulations and industry standards. More information is available at www.netspi.com.

PARASOFT®

Parasoft's innovative application quality and security solutions have been helping businesses achieve compliance with OWASP and other standards for over 25 years. Our comprehensive array of capabilities include static analysis, unit testing, functional/load testing, test environment management, and complete end-to-end traceability.

QUALYS®
CONTINUOUS SECURITY

Qualys (www.qualys.com) is a pioneer and leading provider of cloud security and compliance solutions with over 6,000 customers in more than 100 countries. The QualysGuard Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance, delivering critical security intelligence on demand.

Gold Sponsors (continued)

Quotium Seeker

Quotium is a leading software provider delivering innovative application security software solutions.

Seeker® Runtime Code & Data Security Analysis is the new generation of application security testing, delivering accuracy, clarity and simplicity. Seeker secures your applications easily and efficiently through seamless integration with existing software development and testing processes.

Sonatype

Sonatype protects enterprise software from security/compliance/licensing threats from component-based development, while reducing development/deployment time. Today 80% of the typical enterprise application is assembled with components, like OSS libraries/frameworks. Stop by to learn how to address the new OWASP Top Ten risk – "Using components with known vulnerabilities." FREE risk assessment/component inventory

WhiteHat SECURITY

Whitehat Security is in the website risk management business. Our flagship offering, WhiteHat Sentinel is a software as a service platform for conducting continuous website vulnerability assessment services. What that provides for the customer is a near-real time look at what their security posture is on their website so they can improve over time and fend off the attacks.

Silver Sponsors

acunetix

Acunetix Web Vulnerability Scanner is a must-have tool for the security of websites and web applications. Features include comprehensive SQL Injection and XSS vulnerabilities, advanced penetration testing tools, full HTML5 support, in-depth scanning of SPAs and JavaScript-based websites, mobile website support, plus detection of Blind XSS and DOM XSS vulnerabilities.

CHECKMARX

Checkmarx- Source Code Analysis Made Easy

Checkmarx (www.checkmarx.com) is the developer of next generation Static Code Analysis solutions which identify security vulnerabilities within an application's source code. Checkmarx provides the best way for organizations to introduce security into their Software Development Lifecycle (SDLC) which systematically eliminates software risk.

cigital

Cigital is the world's leading software security services and solutions company, specializing in helping organizations design, build, and maintain secure software. Our unique expertise, technologies, and training courses are the result of over twenty years of cutting-edge research and thousands of successful software security consulting engagements at leading public and private organizations.

CIPHERTECHS

CipherTechs, Inc. is a privately held information security services provider. We focus on delivering security solutions for businesses harnessing the power of Internet communications. We audit, design and implement information security solutions in areas of IP networking, firewalls, applications security, risk assessment, traffic monitoring, encryption, redundancy and strong authentication.

Silver Sponsors (continued)

CodeDx
A PRODUCT OF SECURE DECISIONS

Code Dx is an easy and affordable way to run your code through a variety of static source code analysis tools. It automatically runs the tools for you, consolidates and normalizes their results, and presents interactive visual analytics to help triage and prioritize your software's vulnerabilities for efficient and timely remediation.

coverity®

Coverity, the development testing leader, is the trusted standard for companies that need to protect their brands and bottom lines from software failures. Over 1,100 customers utilize Coverity's deep code intelligence to improve their overall software quality and security and to improve the efficiency and effectiveness of their automated testing.

DENIM GROUP

Denim Group, the market leading secure software development services and products firm, specializes in application security services, including application-centric penetration tests, source code reviews, software remediation and training. Denim Group recently released ThreadFix, a software vulnerability aggregation and management system that provides a centralized view of software defects across development projects.

fishnet SECURITY

FishNet Security - the leading provider of information security solutions that combine technology, services, support and training - enables clients to manage risk, meet compliance requirements and reduce costs while maximizing security effectiveness and operational efficiency. FishNet Security is committed to information security excellence and has a track record of delivering quality solutions to thousands of clients worldwide.

GOTHAM DIGITAL•SCIENCE

Gotham Digital Science (GDS) is an information security consulting firm that works with clients to provide flexible and customized solutions to identify, prevent, and manage security risks. With offices in both New York and London, GDS specializes in security testing, software security and helping our clients build more secure software.

iAppSecure
Innovative Intelligence

iAppSecure Solutions is a company started with a vision to create scientifically advanced technologies for application security analysis. The technologies that we build enable smarter and deeper application security analysis. Fusion Lite is one such innovative next generation technology from iAppSecure which radically changes the way applications are assessed.

IMPERVA®

Imperva protects high-value applications and data assets in physical and virtual data centers. We provide the third pillar of enterprise security. Endpoint and network security were never designed to protect against modern threats. Others can't offer a comprehensive, integrated data center security platform or the innovation that results from singular focus.

klocwork®

Klocwork® helps developers create more secure and reliable software. Our tools analyze source code on-the-fly, simplify peer code reviews and extend the life of complex software. Over 1000 customers in the mobile device, consumer electronics, medical technologies, telecom, military and aerospace sectors rely on our development tools.

L.J.KUSHNER
& Associates, L.L.C.

LJ Kushner and Associates is an executive recruitment firm dedicated to the Information Security industry and its professionals. Since 1999, the firm has provided industry specific recruitment services to clients that include the Fortune 2000, consulting firms, information security software vendors and service providers. The firm recruits management, technical, and sales professionals.

Security Innovation®
THE SOFTWARE SECURITY COMPANY

Security Innovation offers solutions based on the three pillars of a secure Software Development Lifecycle (SDLC): standards, education and assessment (application & SDLC). Our flagship training products include TeamProfessor, the industry's largest library of application security eLearning courses, and TeamMentor, "out of the box" secure development standards and vulnerability remediation guidance.

THANK YOU TO ALL OF THE APPSEC USA SPONSORS & SUPPORTERS!

Silver Sponsors (continued)

Trustwave®
Smart security on demand

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. Trustwave has helped hundreds of thousands of organization manage compliance and secure their network infrastructures, data communications and critical information assets. For more information, visit https://www.trustwave.com.

VERACODE

Veracode secures the world's software. We help the world's largest corporations, software providers and governments address the threat posed by hackers targeting software to gain access to critical data. Veracode provides automated, policy-driven, risk management solutions to secure mobile, web and third-party applications across the software supply chain. For more information, visit http://www.veracode.com

wwpass®

WWPass® authentication and access solutions safeguard identity and data for people and organizations. For the first time, authentication is completely secure and convenient, data is isolated and users are anonymous. Organizations shield corporate data from all unsanctioned access, easing compliance and minimizing risk, and people protect their digital identity.

Other Sponsors

brinqa

PALAMIDA™
Application Security for Open Source Software

FALLING ROCK
NETWORKS

RAPID7

Security Compass

LIVEPERSON

VerSprite
Navigate Beyond Risk

MANDIANT®

nVisium
SECURITY

VIRTUE
SECURITY

ongoingsecurity.com

Association Partners

Internet Society™
US New York Chapter

ISSA
Information Systems Security Association

(ISC)²®

NEW YORK PHP

Association Partners (continued)

RSA CONFERENCE 2014 FEBRUARY 24 – 28 SAN FRANCISCO, USA

Le Conseil de la CyberSécurité
Council on CyberSecurity

Media Partners

Information Security buzz The Latest News from the World of Information Security Visit us online

PenTest magazine

Hakin9 IT SECURITY MAGAZINE

Slashdot

Career Fair

ADP

mozilla

GE Capital

About OWASP

OWASP
Open Web Application
Security Project

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

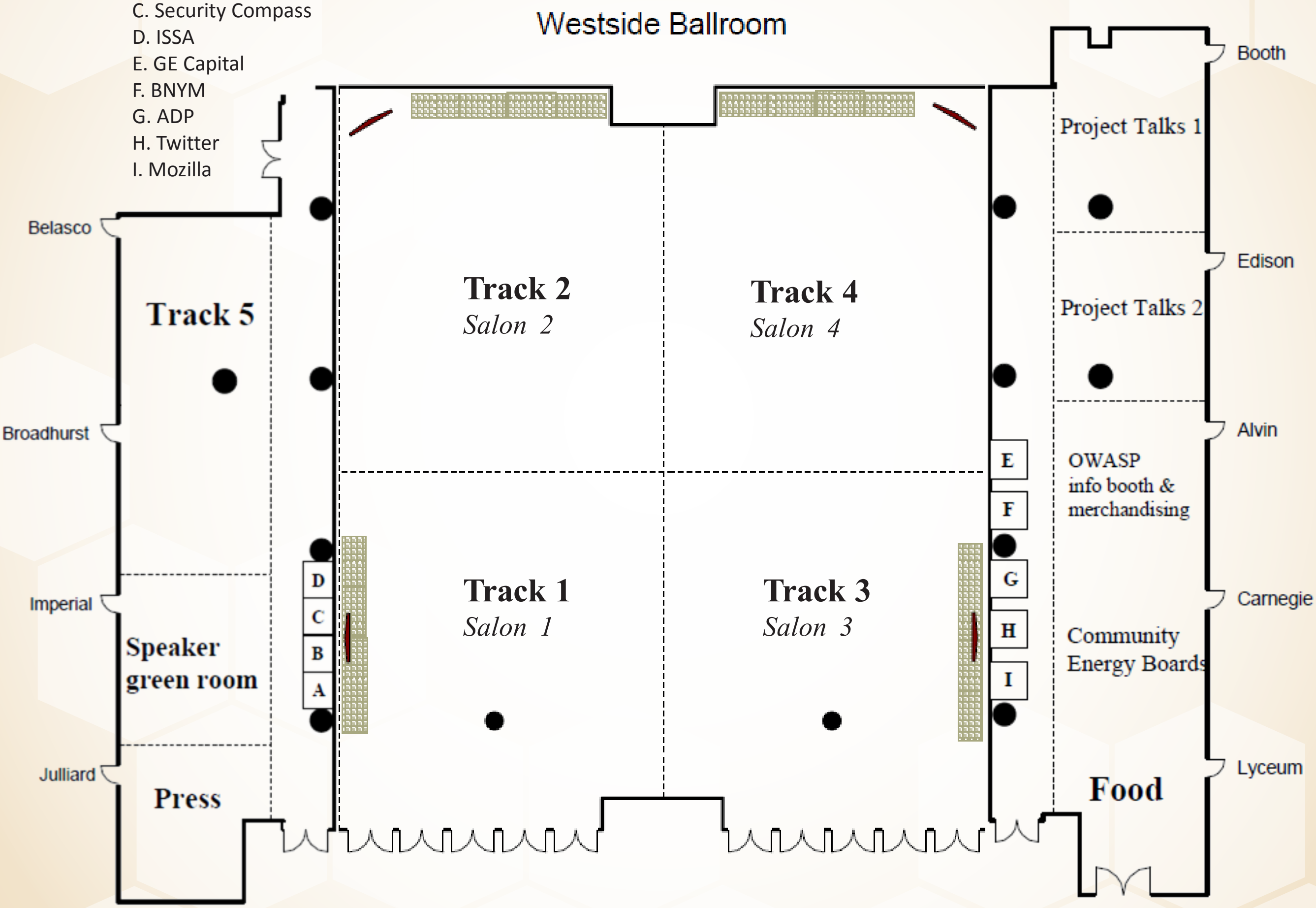
Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. OWASP does not endorse or recommend commercial products or services, allowing our community to remain vendor neutral with the collective wisdom of the best minds in software security worldwide.

There are thousands of active wiki users around the globe who review the changes to our website (https://www.owasp.org) to help ensure quality. If you're new, the best way to get started is just to jump in – the left hand navigation bar on the wiki should take you to the main chapters, projects, conferences, and volunteer pages. As a global group of volunteers with over 40,000 participants, we ask that you send questions or comments to one of our many mailing lists or email us at support@owasp.org.

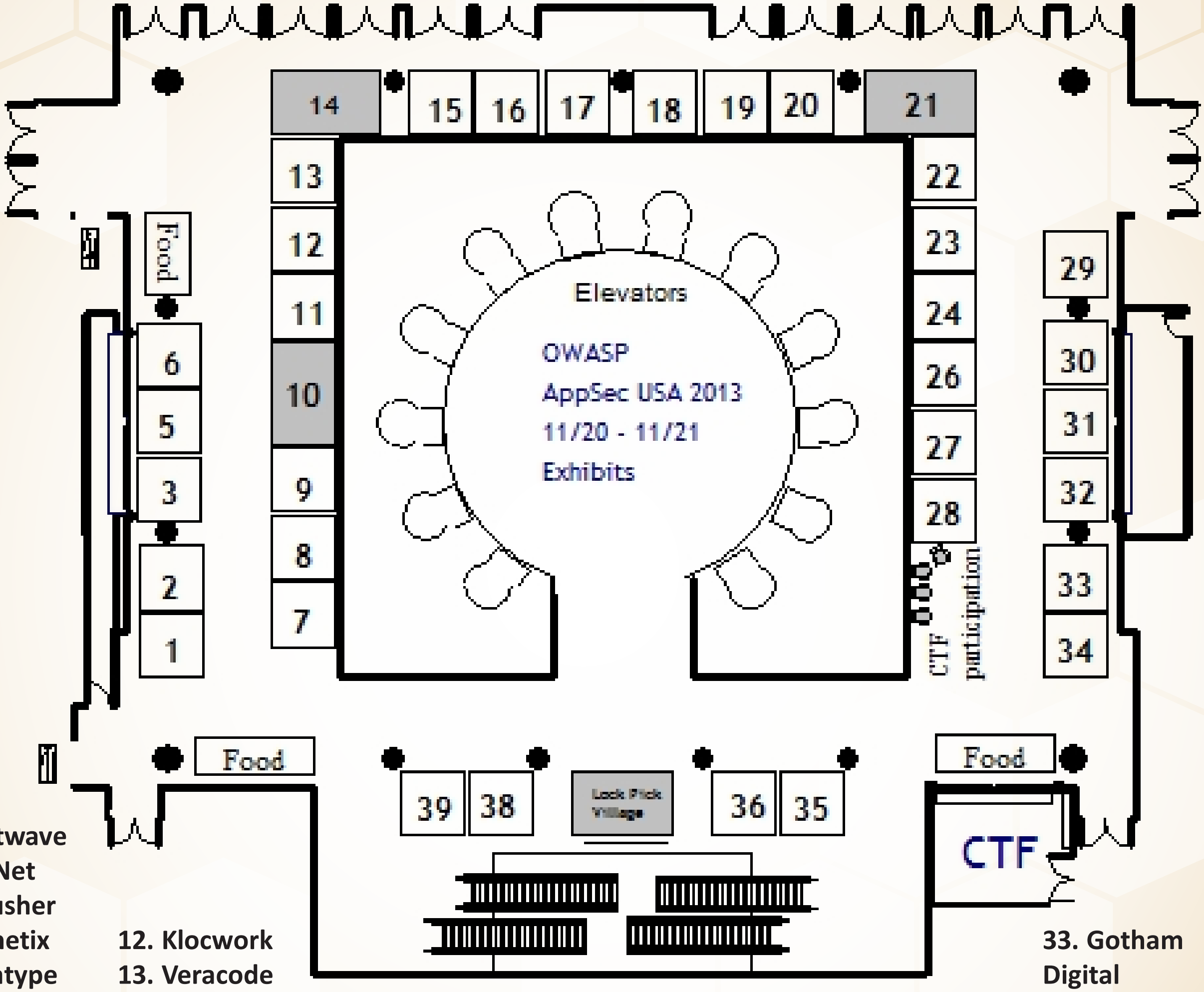
Floorplan

New York Marriott Marquis 5th Floor

A. Slashdot
B. Falling Rock
C. Security Compass
D. ISSA
E. GE Capital
F. BNYM
G. ADP
H. Twitter
I. Mozilla



5th Floor Foyer



1. Trustwave
2. FishNet
3. LJ Kusher
5. Acunetix
6. Sonatype
7. Coverity
8. Rapid7
9. Palamida
10. Adobe
11. Akamai

12. Klocwork
13. Veracode
14. Aspect Security
15. NetSPI
16. Checkmarx
17. F5
18. Whitehat
19.eLearn Security

20. AsTech consulting
21. HP
22. Imperva
23. Cigital
24. KPMG
26. Brinqa

27. iApp Secure
28. Code DX
29. Parasoft
30. CipherTechs
31. ISC (2)
32. Security Innovation

33. Gotham Digital
34. WWPass
35. Arxan
36. Qualys
38. Quotium
39. Denim Group

Notes:

Notes:

Notes:

THANK YOU!

Thank you to our amazing team of volunteers, paid staff, and contractors that have worked tirelessly over the past year to put this event together. If you know any of them (or see them around the conference - probably wearing a **yellow "EVENT STAFF" shirt**) please take a minute to thank them for their contributions!

A Special Thanks to our Local Volunteer Chairs:

Tom Brennan (General Conference Chair)**, I**s**rael Bryski (**Speaker & Trainer Selection Chair), **Pete Dean (**Budget & Sponsorship Chair)

Conference Volunteer Support Team:

Ali Chettih
Allen Lum
Alvin Fong
Ann Alfano
Anthony Martini
Anypriya Dutta
Bakul Singhal
Bev Corwin
Bojan Simic
Brian Johnson
Carlos Hoyos
Carlos Manzueta
Celestine Daniels
Charles Sanson
Chia-Ling Lee
Chris Elsmore
Chris Howell
Danny Chrastil
Venkat Kodur**i**

Darwin Yip
Dashmesh A. Singh
David Kadow
Donald Gooden
Doug Shin
Frank Aviles
Geet Chadda
Grisha Kumar
Helen Gao
Israel Bryski
Izabela Pelszynska
James Johnson
Jamie Strain
Jay Ball
Jean-Pierre Beltran
Jeet Damania
Jesus Ayala
Jim Blotterman

Jim Abercromby
Joanne De Vito De Palma
Jonathan Freeland
Jonathan Ruf
Karl Fosaaen
Kees Leune
Kelly Fitzgerld
Kington Chan
Leonard Bogdonoff
Lokesh Pidewekar
Lucas Duffey
Lucas Ferreira
Madhu Cheriyedath
Marina Khainson
Monika Chakraborty
Mordecai "Mo" Kraushar
Nakeishia Simic
Nebrass Lamouchi

Nneka O'Reilly-Smoot
Patrick Adam
Kevin Reiter
Peter Stern
Philip Derasmo
Praveen Nallasamy
Rachel Anderson
Reed Kelly
Ric Longenecker
Robert Shullich
Rolando Azpura
Richard Van Horn
Ryan Townsend
Samir Malaviya
Kevin Reiter
Peter Dean
Peter Stern
Philip Derasmo

Praveen Nallasamy
Rachel Anderson
Reed Kelly
Ric Longenecker
Robert Shullich
Rolando Azpura
Richard Van Horn
Ryan Townsend
Samir Malaviya
Srinivas (Sri) Lakhanigam
Stefan Edwards
Steven van der Baan
Ted Amor
Ted Henderson
Tom Ryan
Troy Bailey
Yang Li
Vinay Prabhushankar

OWASP Paid Staff and Contractors:

Sarah Baso, Executive Director
Kate Hartman, Operations Director
Samantha Groves, Projects Manager
Kelly Santalucia, Membership & Business Liaison
Laura Grau, Conference Manager

Alison Shrader, Bookkeeper
Matt Tesauro, IT Support (Contractor)
Jasmine Beg, NYC Support & Logistics (Contractor)
Nguyet Vuong, New Way Design (Contractor)
Bill Lessard, PR with Brains (Contractor