OWASP

Call for Training Application

Please forward to all interested practitioners and colleagues.

YOU MUST SUBMIT ALL OF THE FOLLOWING (Submission Deadline: DATE)

Please return this speaker form by fax to: NAME

Trainer Name:	Dave Wichers with Dan Amodio
Company/Employer:	Aspect Security, Inc.
Telephone:	301-604-4882
E-mail:	Shannon.ross@aspectsecurity.com

Proposed Training Title:

Securing Mobile Devices and Applications

Anticipated Audio/Visual Requirements:

☐ Laptop ☒ LCD Projector ☐ Overhead ☐ Other _____

Training Summary: (Be concise)

This two-day, hands-on course enables students to understand how easily mobile devices and applications can be successfully attacked. They will learn how to identify, avoid and remediate common vulnerabilities by walking through a threat analysis and learning critical security areas such as those identified in the OWASP Top Ten Mobile Risks and Controls. Using state-of-the-art testing tools, students will learn how to secure mobile devices across the enterprise.

Audience

☐ Management ☒ Technical ☐ Operations ☐ Other _____

Skill Level required of Attendees

☐ Basic ☒ Intermediate ☐ Advanced ☐ Other _____

Duration of Training

☐ 4 Hour ☐ 1 Day ☒ 2 days ☐ Other _____

Special Needs (e.g., will include labs, software needed, internet access, wireless setup, required reading, etc)

Will include hands on labs, students will need a machine that has the following capabilities:

- Mac OSx 10.6 or newer with xCode for iOS installed
  OR
  Windows 7
- Need VMWare player on windows or VMWare Fusion on Mac (for Android Labs)

Instructor will need internet access.

Please list any other publications or conferences where this material has been or will be presented/submitted.
This course has been presented at OWASP AppSec Research 2012**.**

Explain (in 3 sentences or less) reasons why you feel this material is innovative/significant for the OWASP event.
With over 5 billion mobile devices being used hackers can easily use mobile devices to gain access to company's confidential data. Therefore, it is essential that we stay ahead of them and secure our devices. OWASP is at the cutting edge of application security and OWASP members are asking for mobile security training.

Attendee takeaways and key learning objectives: *(Please list three learning objectives)*

- Understand how mobile devices and applications can be easily attacked.
- Identify; common vulnerabilities.
- Be able to use state-of-the-art mobile application security testing tools.
- Secure mobile devices across the enterprise.
- Think like an attacker so that students can be pre-emptive

Trainer Bio: Briefly describe your professional experience or areas of expertise related to this presentation. You should include education/certification information in this section.

1. **Experience of the Trainer**

Dave Wichers is a cofounder and the Chief Operating Officer (COO) of Aspect Security, a company that specializes in application security services. He is also a long time contributor to OWASP including being a member of the OWASP Board since it was formed in 2003. Dave has over 20 years of experience in the information security field, and has focused exclusively on application security since 1998. At Aspect, in addition to his COO duties, he is Aspect's application security courseware lead, one of their chief instructors, and provides a wide variety of application security consulting services to Aspect's clients. Prior to starting Aspect, he ran the Application Security Services Group at Exodus Communications. Dave has a Bachelors and Master's degree in Computer Science, is a CISSP, and a CISM.

2. **Training History (please indicate place and duration)**
   a. **OWASP related**

Dave Wichers – Many OWASP conference trainings over the years. The most recent was at OWASP AppSec Research in Athens Greece.
Dan Amodio – Has not trained at an OWASP event. He has recently joined Aspect and is one of the authors of the Mobile Security course. He has recently given and presentation at OWASP AppSec US 2012.

   b. **For organizations other than OWASP**

Dave Wichers – Has been delivering Aspect Training courses to our clients for over 10 years and is the primary author of our curriculum.

3. **Published Materials (News releases, Papers, Whitepapers, Research)**

Some of **Dave Wicher's** OWASP contributions:

- Project lead and coauthor of the OWASP Top 10,
- Coauthor of the OWASP Application Security Verification Standard,
- Contributor to the OWASP Enterprise Security API (ESAPI) project,
- Lead of the OWASP Prevention Cheat Sheet Series and primary author of the SQL Injection Prevention Cheat Sheet.

Dan Amodio is the OWASP ESAPI C Project leader and contributor to the OWASP ESAPI C++ project.

Outline (Topic and Sub-Topics; 2 levels) – Please attach samples if available

Outline

Mobile Devices and Applications

Section Overview: Introduction to Mobile Devices, their capabilities, and how to emulate mobile apps and use mobile testing tools.

1) Device Types and Capabilities
2) Mobile App Emulators / IDEs
3) Running the Class Apps
4) Using a Testing Proxy: Burp
5) How to get Proxying to work

Mobile Application Architectures and Threat Model

Section Overview: An explanation of high-level threats, attack techniques and the impacts associated with mobile computing and how different architectures affect these.

1) Different Mobile Architectures
2) OWASP Mobile Security Resources
3) Mobile Threat Model
4) Top 10 Mobile Controls
5) Risk Management
6) Mobile Threats and Attacks on Users, Devices, and Apps
7) Consequences
8) AppStore Security / Malware Threats
9) Hands On: Hacking Mobile URLs (iOS), or Intents (Android)

Mobile Application Architectures Deeper Dive

Section Overview: Different styles of computing in the mobile space, the core technologies involved, and how applications are built.

1) Device Protections built into Android and iPhone
2) Data Protection
3) Encryption
4) Client Only Architecture and Recommended Controls
5) Client-Server Architecture and Recommended Controls
6) Recommendation: Standard Security Controls
7) Mobile Web Applications and Recommended Controls
8) HTML 5 Risks
9) JavaScript Framework Risks
10) Same Origin Policy

Securing the Device

Section Overview: We demonstrate how to harden mobile devices against attack and the issues related to managing security across an enterprise. We show students how to secure employee-owned devices**.**

1) Mobile Device Management (MDM) Applications
2) Password Requirements
3) Data Protection
4) Enterprise Security Management (ESM)

Securing Communications

Section Overview: What are all the different communications technologies used by mobile devices and what security threats do they pose?

1) Threat: Unsafe wireless access points, sniffing, tampering
2) Review mobile protocols and platforms
3) How to use SSL Securely

Mobile Authentication

Section Overview: We explain how the user proves their identity to the phone, how server-side applications can authenticate the user, and how the phone can authenticate the services used.

1) Threats: lost/stolen phone, remember me, sniffing
2) Strong Authentication vs. User Usability
3) Communicating credentials safely
4) Storing credentials safely

Mobile Registration

Section Overview: How to register a device to a person and explain the need for mobile channel authentication.

1) Threats: lost/stolen device, remember me, lost/stolen credentials
2) Benefits of Registering the Device
3) Methods for Authenticating the Device
4) Avoiding use of UDID

Mobile Data Protection

Section Overview: All of the different places that sensitive data can be stored on phones, and how it can be protected.

1) Identifying sensitive data
2) Where and how is data stored on devices
3) Hashing and encryption
4) Storing keys
5) Browser Caching
6) Mobile specific 'accidental' data storage areas
7) Where NOT to store your data on the device
8) HTML5 local storage

Mobile Forensics

Section Overview: Where application data and configuration information typically gets stored on the mobile device.

1) Forensics tools for Android and iPhone
2) Exploring the file system (Android / iPhone)
3) Jailbreaking grants more access
4) Interesting areas of the file system (Android / iPhone)
5) Application configuration files
6) Autocomplete records / iPhone app screen shots
7) Dumping Android Intents
8) Scrounging in Backups

Mobile Access Control

Section Overview: The code-access security models to use in mobile apps.

1) Threat: user attacks server
2) Example attacks
3) Documenting your access control policy
4) Mapping enforcement to server side controls
5) Presentation Layer Access Control
6) Environmental Access Control
7) Business Logic
8) Data Protection
9) Hands On: Access Other Peoples Accounts, Steal Funds

How to Protect Against Cross Site Scripting (XSS)

Section Overview: The threat of XSS in mobile applications is real based on heavy usage of Webkit

1) Understand XSS
2) Learn how to execute XSS
3) Be able to identify XSS flaws in code
4) XSS real world examples
5) Practical Defenses: Primarily Output Encoding

Protecting A User's Privacy

Section Overview: How the phone can be used to undermine user privacy without their knowledge

1) Using location services (GPS, cell triangulation, compass, hardware device key)
2) Accessing contacts, photos, maps, and other personal data
3) Accessing calls, SMS, browser, cell usage history
4) Using camera, microphone safely

Secure Mobile Development Process

Section Overview: We explain how developers can ensure that their application doesn't have security holes.

1) Defining your goals, process, and risk management mechanisms.
2) Building security in to each phase of the development lifecycle
3) Mobile security analysis techniques
4) Defect tracking and process improvement

Responding to Vulnerabilities

Section Overview: What to do if your application gets hacked.

1) Create security@yourdomain.com
2) Publish security information
3) Acknowledge incidents and vulnerabilities
4) Engage with researchers immediately

Hack It and Bring It!

Section Overview: A hands-on challenge for students to demonstrate what they have learned.

Wrap Up, Close and Thank You