

FOR IMMEDIATE RELEASE:

## **OWASP AppSec USA 2013, NYC November 18-21, Announces Call for Papers, Call for Trainers**

***Application security practitioners invited to submit speaker and trainer proposals to premier Security Conference; Deadline: April 30, 2013***

NEW YORK, NY April 2, 2013—AppSec USA 2013 ([www.appsecusa.org](http://www.appsecusa.org)), the premier software security conference for Builders, Breakers and Defenders, invites all practitioners of application security and those who work or interact with all facets of application security to submit speaker and trainer proposals for AppSec USA 2013. Now in its ninth year, AppSec USA brings together leading global experts in software security for four days of discussion, training, exhibition and competition, November 18-21 at the Marriott Marquis, in Times Square, New York City.

Established in 2004, AppSec USA is the marquee North American conference from the OWASP Foundation Inc., a global, free and open non-profit community focused on improving the security of application software. As in previous years, AppSec USA 2013 will include a hands-on hacking capture-the-flag competition, along with extensive hands-on training and an exhibition hall featuring the most exciting companies in the software security industry.

The AppSecUSA 2013 Speaker Committee is seeking presentations and training sessions in the following subject areas:

- Web Application Security - OWASP Projects that include everything from language talks to exploits
- Hardware - Including but not limited to: application bypass, hardware hacking basics, and defeating "secure" hardware
- Physical Security - Including but not limited to: badging applications, lock-picking, physical access control, physical lock forensics and long range key duplication involving software
- Forensics - Including but not limited to: application, physical memory forensics, solid state disk forensics and network forensics
- Infrastructure - Including but not limited to: SCADA, routing, satellite and GSM.
- Android/iPhone/Windows Mobile research
- Reverse Engineering Malware and Malware Analysis
- Rootkit Detection, Techniques, and Defenses
- Exploitation Tactics
- Cloud Security / Assessing Cloud Security
- Legal Issues around EULA and related topics
- Industry Panels

### **Who Should Apply?**

- Practitioners of application security
- Those who work or interact with all facets of application security

Past participants of AppSec USA have included representatives from Adobe, Akamai, Amazon, Bank of New York Mellon, Cisco, Cox Communications, Electronic Arts, Exxon Mobile, Facebook, Goldman Sachs, JP Morgan, Square, Twitter, Morgan Stanley, Lockheed

Martin, Oracle, UBS, Unilever, Visa, Medco, Pfizer, Roche, Cushman & Wakefield, Wells Fargo.

### **Industry Testimonials:**

"... the best security conference I attend every year. I have met senior security officers from Goldman Sachs, UBS, Morgan Stanley and other leading firms, along with representatives of the Federal Government."

- Stephan DeBelle, Security Analyst, Unilever

"OWASP is an organization that professionals in the software security field should consider joining ... a great organization for networking."

- Joe Bernik, Head of Global Technology Risk Management, The Bank of New York Mellon

### **Deadline & Schedule\*:**

CFP/CFT Open: April 1st

**CFP/CFT Closes: April 30th**

Acceptance Notification: May 31st

Conference Schedule Publication: June 14th

\*Note: Training sessions will be held 11/18 & 11/19; three conference tracks, including one for research, 11/20 and 11/21.

**APPLY NOW (Deadline April 30): [www.appsecusa.org](http://www.appsecusa.org)**

AppSec is supported by Aspect Security, Checkmarx, Gotham Digital Science, iAppSecure Solutions Pvt. Ltd., NetSpi, nVisium Security, Qualys, Whitehat Security. For more information, including sponsorship, exhibition and early-bird discounts, visit: [www.appsecusa.org](http://www.appsecusa.org).

### **About OWASP Foundation**

The Open Web Application Security Project (OWASP) is dedicated to making application security visible by empowering individuals and organizations to make informed decisions about true software security risks. As a 501(c)(3) not-for-profit worldwide charitable organization, **OWASP does not endorse or recommend commercial products or services**. Instead, we allow our community to remain vendor-neutral with the collective wisdom of the best individual minds in software security worldwide. For more information, visit: [www.owasp.org](http://www.owasp.org).

### **MEDIA CONTACT:**

Bill Lessard  
PRwithBrains  
[wlessard@prwithbrains.com](mailto:wlessard@prwithbrains.com)  
(o) 914.476.6089

# # #