

Direction—From Points North:

Take I-91 South to Exit 21 (Rt. 372).
At the end of the exit, proceed straight onto Industrial Park Rd.
For approx. 1/2 mile and follow the signs to Aetna

Direction—From Points South:

Take I-91 North to Exit 21 (Rt. 372).
At the end of the exit, take a right.
At the next light, take a left onto Industrial Park Rd.
Proceed straight approx. 1/2 mile and follow the signs to Aetna.

Direction—From Points West:

Take I-84 East to I-91 South to Exit 21 (Rt. 372).
At the end of the exit, proceed straight onto Industrial Park Rd.
For approx. 1/2 mile and follow the signs to Aetna

Direction—From Points East:

Take I-84 West to Exit 57 (exit on left) CT 15 /NYCity/Charter Oak Bridge
Take Exit 86 for I-91 South
Take exit 21 for CT -372 Berlin / Cromwell
At the end of the exit, proceed straight onto Industrial Park Rd.
For approx. 1/2 mile and follow the signs to Aetna



For further details contact:
William Schreyer Steve Ryan, CSQA
President—QAAC Director Membership
914.333.6299 Phone 860-749-2337
914.333.6200 Main
wmschryer@snet.net Membership@QAAC.org



*A full-day conference on
Friday September 18, 2009*

Security Testing; How, When and Where

Location:

**Aetna Inc. (Lecture Hall)
Middletown, CT.**

8:00 A.M – 4:30 P.M

Registration: 7:30 – 8:00 A.M.

Fee: \$100.00 (includes lunch)



Program Agenda & Speakers

8:25 – 9:45 “Software Security Requirements” by **Paco Hope** – Cigital Inc.

Security is one of those non-functional properties of software that is difficult to specify well in requirements or traditional use cases. To come full circle with software security, we must leverage the skills and processes in our QA department. In this engaging presentation, Paco discusses misuse/abuse cases, security best practices, architectural risk analysis, and attack patterns as techniques for exploring the security needs.

10:15 – 11:45 “The Top 25 Software Security Vulnerabilities” by **Chris Wysopal** - Veracode

In this presentation, Chris takes the QA test perspective on finding the top 25 application security vulnerabilities that are most likely to be exploited by attackers by combining static, dynamic and manual test techniques. By putting security vulnerabilities into context with other security issues, he will show what testing techniques are best suited for each category. The strengths and weaknesses of automated static and dynamic analysis and manual methods are examined.

1:45 – 3:45 “Integrating Security Tools into the QA Test Process” by **Danny Allen** - IBM

An estimated 75 percent of applications are released with security vulnerabilities due largely to the absence of security processes in the quality assurance and development cycles. Compounding the problem is the difficulty of the coordination of security testing across multiple departments when QA is used as a hub. This presentation will expose some of the most common Web application security vulnerabilities and provide techniques and best practices to build application security testing into existing QA processes. In this presentation, you'll learn how to: 1) Understand common application vulnerabilities; 2) Select the most effective test tool for each type of vulnerability; 3) Address application security defects through dynamic and static analysis.



Paco Hope is a Technical Manager with Cigital, Inc. and has 12 years of experience in the security of gaming systems, web applications, operating systems, and embedded devices. Paco leads Cigital's efforts in online gaming security, including random number generator (RNG) certification and the SafeBet™ online gaming security certification. Paco is a frequent speaker at conferences like STAR East, the Better Software Conference, and also a prior co-chair of VERIFY, an international conference on software testing.



Chris Wysopal co-founder and chief technology officer of Veracode, is responsible for the security analysis capabilities of Veracode technology. Mr. Wysopal is recognized as an expert and a well known speaker in the information security field and has led a world class team of security researchers tackling the problem of automating the process for finding and disclosing security vulnerabilities in software. He has given keynotes at computer security events such as Defense Information Systems Agency (DISA) and has testified on Capitol Hill on the subjects of government computer security and how vulnerabilities are discovered in software.



Danny Allen is director of security research with IBM Rational. He has a background in web application security and compliance and brings with him more than seven years of business and security technology-related experience including penetration testing and internal system remediation. Danny has published several whitepapers and articles and participates in industry working groups and has also spoken at security events across the globe.

Event sponsored by

