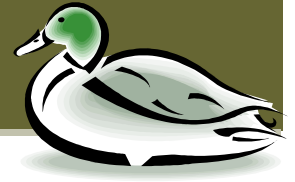


QAAC NEWSLETTER



Newsletter of the Quality Assurance Association of Connecticut, Inc.
www.qaac.org

Call For Speakers

As we begin the new year for QAAC there is a need for speakers. Last year speakers covered topics such as using metrics to manage projects, developing testing strategies and CMMI. There are several openings in the upcoming year.

Speaking at a QAAC meeting is a good way to earn CPU's toward your recertification. If you have, or need, an idea for a topic, please review the CBOK that interests you. To review the skill categories go to www.softwarecertifications.org/. The next step is easy. Contact Randy Cole (rcole1025@sbcglobal.net) Director of Education, and schedule a time to speak.

Even if you are not interested in speaking, but have recently seen a speaker who may be willing to present to QAAC, contact Randy with the speaker's name and contact information.

All topics should be educational, and cannot be given for the purpose of promoting or selling a product.



INSIDE THIS ISSUE

| | |
|---|---|
| Message from the President | 1 |
| 2009 - 2010 Board of Directors | 1 |
| Conference: Security Testing; How, When & Where | 2 |
| Book Review: "How to Break Software Security" | 3 |

2009 -2010 Board Members

Each fall QAAC elects a new board. Positions include president, vice-president, secretary, treasurer, membership, education, programs & logistics, communications, charter and one member-at-large.

Several board members are returning again this year, but some are transitioning off. If you are interested in a position, please contact Bill Schreyer, current president, via the QAAC website for additional details.

Don't feel like making the commitment of being a board member? There is always a need for helping hands, so consider volunteering for a committee.

And don't forget, QAAC board members receive additional certification hours.

Security Testing; How, When & Where

A full-day conference hosted by QAAC

Friday, September 18th, 2009

Register for this one-day seminar at <http://www.qaac.org>. Cost is \$100 per person and includes lunch that day. There are a limited number of seats, so don't wait and get shut out.

“Software Security Requirements” Security is one of those non-functional properties of software that is difficult to specify well in requirements or traditional use cases. If we're going 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 of a product.

Paco Hope is a Technical Manager with Cigital, Inc. & has 12 years of experience in the security of gaming systems, web applications, operating systems, & 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, & also a prior co-chair of VERIFY, an international conference on software testing.

“The Top 25 Software Security Vulnerabilities” 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 & 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 & weakness of automated static & dynamic analysis as well as manual methods are examined.

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.

“Integrating Security Tools into the QA Test Process” 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 & static analysis.

Danny Allan 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.

Book Review: "How to Break Software Security"

By Cheryl Klein, CSTE

I found this book to be easy to read, unlike many of the textbook variety books you can find related to testing that are out there. It skips the anecdotal stories and dives right into the meat of the topic. There is little extra or fluff included with this book. It won't waste your time.

Whittaker & Thompson spell out the various users and directions that can be used for accessing security and then dives right into doing that. Each section comes with exercises that the reader can try. The one down side to the book is it focuses on the Holodeck tool for many of the exercises. While a CD is included with the tool, it would have been nice to see other suggestions or a looser approach since this may not run on all systems or be feasible in all cases. In terms of planning, understanding and executing the attack it is a sufficient tool.

Where I work, security is not an "A-list" item in development, so I found this very interesting and while I won't have the time or

ability to incorporate all I've learned in this book, it has given me some ideas on a few tests that I can work into the regular testing to try and assure some of the bigger holes are at least secure.

If you test in security, or are just interested, I would recommend this book. It doesn't bore you with lofty theories and text; it gets right to the issue and takes you through quickly and concisely, respecting your time and need to get back to testing.

"How to Break Software Security"

Written by: James Whittaker &
Herbert H. Thompson

ISBN 0-321-19433-0

Newsletter Submissions

Have you read an interesting book lately? Or maybe attended an interesting training session? Or how about that new tool you picked up and love/loathe and want to let everyone know about? Here is your chance - submit an article to the QAAC Newsletter! Not sure you can write an article by yourself? That's okay... we can help!

If you are interested in contributing to the August QAAC newsletter, please send your submission to Cheryl Klein @ Ch_K_Klein@comcast.net.

QAAC is a tax-exempt, non-profit educational organization, independent but affiliated with the QAI Global Institute as a local chapter of its Federation of Associations.

QAAC is exempt from federal (and state) income taxes (and state corporate taxes) under section 501(a) of the Internal Revenue Code as an organization described in section 501(c)(3). We handle money only to pay our expenses. We do not pay our officers or board members. We have no employees. We collect dues from our members to cover our operating expenses. We are permitted to accept donations to further our goals, and they are tax deductible.