

You're logged in as: Meranda Powers Edit your Profile | Log-out

ADVERTISEMENT

Microsoft SQL Server 2008 R2

Help your revenue...

TEST/QA	SOA	EBIZQ	JAVA	.NET	AJAX	ALM EVENT
---------	-----	-------	------	------	------	-----------

SearchSoftwareQuality.com  
Helping you develop, deploy and manage quality software.

NEWS    WHITE PAPERS    MULTIMEDIA    TIPS  
BLOGS    DOWNLOADS    EXPERTS    RSS

MODELS/METHODOLOGIES    REQUIREMENTS    TESTING AND QA    PROJECT MANAGEMENT    MAINTENANCE

  Powered by 

[Site Index](#)

ADVERTISEMENT [Check out latest OSGi news and learn more about getting started with OSGi in this tutorial from SearchSOA.com.](#)

[Home](#) > [Software Quality Tips](#) > [Application Security Strategies](#) > The role of quality assurance (QA) pros in software security

## Software Quality Tips:

[EMAIL THIS](#)

### TIPS & NEWSLETTERS TOPICS

#### APPLICATION SECURITY STRATEGIES

### The role of quality assurance (QA) pros in software security

Kevin Beaver, CISSP

04.10.2009

Rating: -3.60- (out of 5)

[Software quality news and advice](#)

[Digg This!](#) [StumbleUpon](#) [Del.icio.us](#) [Google™](#)



Kevin Beaver

In a forthcoming tip I'll cover what developers can and should be doing to get on board with security. In this tip I'll share what quality assurance (QA) analysts, engineers and testers can do to reduce business risks in this capacity.

As with developers, security managers and IT auditors, QA professionals have a very important role in the information security process. As an aspect of overall quality, it's part of your responsibility to ensure that code is secure before it goes into production. This fact alone validates that your role is arguably the most important among everyone involved. No pressure.

The biggest driver of secure software is that people pretty much expect it these days. Sure, the languages your applications are written in (e.g., Java and C#) can help take some of the security burden off your shoulders. But unfortunately that's a relatively small part of software security. There are still more advanced input validation concerns that have to be looked at. There are SSL and session management issues to check. Even bigger, you have to look at application logic, authentication and access control components, and more -- all things that need to be looked at using manual analysis and good tools.

Beyond these basics, how exactly are you expected to contribute to software security as a QA professional? Every situation is different and there's no best

answer. That said, if you're going to make a difference beyond the basics, you're going to have to step up your game several notches. This means getting more involved in the design phase of new applications. It also means collaborating more openly with developers about the issues you're seeing on the back end that can and should be fixed up front.

One of the most profound changes you can make is to seek out and utilize a good commercial static analysis tool such as [Klocwork](#), [Checkmarx](#) or [QAInspect](#). These tools are essential for rooting out software vulnerabilities that would otherwise be next to impossible to find. If management is not supplying you with the budget you need, there are free tools such as [FxCop](#) and [FindBugs](#) that can certainly help fill the void, but they may not be as extensive as what you need. Based on my experience, you need to do everything you can to get management on your side and provide you with the budget for a commercial product, because in most cases you get what you pay for.

#### More application security tips from Kevin Beaver

Common [software security risks](#) and oversights

[Cloud computing and application security](#): Issues and risks

Using the Firefox Web Developer extension to [find security flaws](#)

Another essential element of integrating security with QA is for you to learn how the bad guys work. Understanding their motivations (financial and self-esteem), insights (technical knowledge and understanding of breaking software) and techniques (manually exploiting application logic and using penetration testing tools to their advantage) will allow you to look at your software with a malicious mindset and fine-tune your misuse cases to uncover security issues you never knew existed.

To learn and keep up with the latest in this area I suggest reading [2600](#) and [Hakin9](#) magazines as well as the numerous books on the subject such as [Exploiting Software: How to Break Code](#) and [19 Deadly Sins of Software Security](#). I also cover the malicious approach to testing your systems and applications in my book [Hacking For Dummies](#). Books such as [Hacking Exposed Web Applications](#) and [Hacking Exposed Web 2.0](#) are good resources as well.

I highly recommend you get to know -- possibly get involved with -- the [Open Web Application Security Project \(OWASP\) and its Top 10](#) Project. OWASP is a great community of like-minded software and security professionals who work together to find better ways to produce higher-quality software. The recently released [Top 25 Most Dangerous Programming Errors](#) is a great resource for understanding what's being exploited -- and thus, what you should focus on. A final resource you can't afford to overlook are the [Hacme](#) and [WebGoat](#) tools. They're *invaluable* for learning the ins and outs of software hacks -- both the technical details and the manual analysis required -- that no QA professional should be without.

Arguably the biggest responsibility of all is for you to understand the security standards and regulations your organization is up against. If you learn the ins and outs of [ISO/IEC 27002](#), the [Payment Card Industry Data Security Standard](#) (PCI DSS) and so on you'll definitely be at an advantage. I'm not saying you need to understand them at the level of an IT auditor or a security consultant. But familiarizing yourself with their software security components and staying current by reading about [how compliance is affecting others](#) will do wonders. The key is to expose yourself to information security concepts in every way possible.

So what's the next step? Again, generally secure code is expected as a baseline these days. You're going to have to go beyond that in order to really contribute to security and start effecting change that will help minimize business risks. This is going to take a good bit of initiative and leadership on your part. Rather than waiting for someone to tell you the security requirements, why not start blazing your own trail? It will require you to learn more about security concepts as I mentioned above and will also force you to get more involved with security inside your organization. From attending security committee meetings to assisting with ongoing security assessments, there's a lot you can do.

Sure, secure software is only a component of the overall information security equation, but it's one of the most important ones, and it will make or break your business. You, as the QA professional, play a critical role in minimizing business risk. Learning the ins and outs of software security will put you in a great position to contribute in a positive and visible way. Focus on establishing yourself as an enabler of information security. Becoming a person of value will not only help your organization, it will also help make your job more fulfilling and even help your career moving forward.

---

**About the author:** Kevin Beaver, CISSP, is an independent information security consultant, keynote speaker and expert witness with Atlanta-based [Principle Logic LLC](#), where he specializes in performing independent security assessments and information security career counseling for up-and-coming IT pros. Kevin has authored or co-authored seven books on information security, including [Hacking For Dummies](#) and [Hacking Wireless Networks For Dummies](#) (Wiley). He's also the creator of the [Security On Wheels](#) information security audio books and [blog](#), providing security learning for IT professionals on the go. Kevin can be reached at [kbeaver \[at\] principlelogic.com](mailto:kbeaver@principlelogic.com).

Rate this Tip

(BAD)  1  2  3  4  5 (EXCELLENT)

[Submit a Tip](#)



#### SOFTWARE QUALITY RELATED LINKS

##### Ads by Google

###### [Ottawa Agile Training](#)

Maximize the return on your IT investments. Get Agile training now  
[www.WestboroSystems.com](http://www.WestboroSystems.com)

###### [QA Software Testing Trg](#)

Quality Assurance Software Testing Best in Toronto Mississauga GTA  
[www.iibs.ca](http://www.iibs.ca)

###### [Manage Software Project](#)

Reduce costs associated w/ changes while improving application quality  
[Serena.com/ReleaseMgmt](http://Serena.com/ReleaseMgmt)

###### [Software Testing Courses](#)

100% Online Testing Courses Request More Information Today!  
[www.VillanovaU.com](http://www.VillanovaU.com)

#### RELATED CONTENT

##### ■ [Application Security Strategies](#)

[Beefing up SSL to ensure your applications are locked down](#)  
[Security best practices for today's Web 2.0 applications](#)  
[Application security checklist: Ways to beat cross-site request forgery](#)

Software Design & Testing - [Project Management](#)

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Site Index](#) | [RSS](#)

SEARCH  SEARCH

TechTarget provides technology professionals with the information they need to perform their jobs - from developing strategy, to making cost-effective purchase decisions and managing their organizations' technology projects - with its network of [technology-specific websites, events and online magazines](#).

[TechTarget Corporate Web Site](#) | [Media Kits](#) | [Reprints](#) | [Site Map](#)

All Rights Reserved, [Copyright 2006 - 2010](#), TechTarget | [Read our Privacy Policy](#)

