



Source Code Security Audit

Securing Your Applications

Is your company building a new web portal or application? Many companies today are choosing to build custom applications in-house. Doing this ensures support for all of the necessary features in a solution, but it also carries with it a number of pitfalls. Most developers do not focus on security auditing early in the development of a product. The result is a large amount of money spent over the lifetime of the solution resolving vulnerabilities, bugs and providing patch maintenance.

In addition to overall cost reduction, federal regulations and control frameworks, including PCI DSS requirements 6.5 and 6.6, SOX, FISMA, COBIT and COSO, mandate that organizations incorporate software security assurance and auditing into the software development lifecycle. The reason for this is most web portals and Internet applications can provide an indirect path into systems containing confidential or private data.

Why Tevora?

Our skilled senior consultants have a vast array of knowledge of both zero-day and legacy vulnerabilities and hold industry leading certifications including CISSP, CEH and PCI QSA. Our audit methodology combines extensive manual code review augmented with several industry leading automated code analysis tools to ensure you are provided a complete assessment. We work directly with your development teams to resolve the identified issues as well as provide them with education and best practices for creating code.

Tevora offers code security reviews for both web-based applications and traditional host-based applications. Our methodology is based upon industry leading standards. For web-based applications we have incorporated DHS and OWASP's Top Ten methodology. Our host-based application methodology draws from CERT/CC, MITRE, Sun and NIST secure coding guidelines and standards.

Tevora's Code Review Services

Tevora's consultants are available to provide source code security audits for your organization in the following languages:

- .NET, VB, ASP, C#, AJAX
- Delphi
- Java / JSP
- C/C++
- Flex, BlazeDS, AMF
- Perl, PHP, Ruby, Python
- Fortran, COBOL

OWASP Top Ten vulnerabilities tested, including:

- Unsecure and unvalidated input or output
 - ◊ Cross-site scripting, SQL injection
- Broken or incomplete authentication controls
 - ◊ User ID manipulation
- Flawed session management
 - ◊ Session or Cookie hijacking
- Bounds checking
 - ◊ Buffer or Integer overflows
- Weak storage encryption
 - ◊ Broken or insecure encryption algorithms
- Insecure communication protocols
 - ◊ Clear-text and unauthenticated protocols
- Improper Exception Handling
 - ◊ Debugging and error messages

Please contact us for more information:
e: info@tevora.com
t: (888) 4 - TEVORA