Web Services Security Assessment

**BENEFITS**
- We find holes in production web services before the hackers do
- We perform security assurance as applications move into production
- We understand your risk and the potential impact on your business and use that for our risk calculation in addition to the industry recognized CVSS v2 scoring system
- Our proprietary and up to date testing process consists of over hundred checks which includes specific checks for XPATH Injection, Schema Poisoning, WSDL Scanning etc.
- Only 5% of testing is automated, rest is manual testing based on 15 years of industry experience for accuracy
- Our training program, comprehensive methodology and strict quality control ensures almost no false positives
- We place a strong emphasis on manual testing to discover critical business logic bypass and authorization issues that automated scanners overlook
- We actively transfer knowledge of testing techniques, issues, remediation to our customers

**DELIVERABLES**
Our deliverables include:
- Daily updates
- Preliminary Findings Report
- Web Services Security Assessment Technical Report
- Executive Summary Report
- Close Out Presentation

**RELATED FOUNDSTONE SERVICES**
Foundstone offers many related services and training classes.
- Web Application Penetration Testing (WAPT)
- Thick Client Assessment
- Mobile Application Assessment
- Security Code Review Assessment
- Application Threat Modeling
- Software Security Maturity Assurance

Web Services are poised to revolutionize application development and how IT organizations operate, much the same way that client-server and Web-based applications did in the past. They offer businesses a new, standardized way of integrating disparate applications and systems between suppliers, partners and customers.

Unfortunately, Web Services security is a major concern and can be a stumbling block. The existing traditional security infrastructure is inadequate to satisfy the security needs that XML and Web Services present. Foundstone Professional Services offers a comprehensive security assessment methodology to identify threats, vulnerabilities and risks associated with your organization's Web Services infrastructure. We assess the security aspects of design and implementation - confidentiality, integrity, trust relationships, and authentication using security standards like XML signatures, XML encryption, SAML and WS-Security. Foundstone has led the field of web services assessment since day one. As early as 2005, we published an open source framework – WSDigger¹, to automate web services testing. It helps identify data validation issues such as SQL injection and XPath injection etc.

**Methodology**
A significant part of Foundstone’s success is having developed a detailed methodical approach to web services assessment to ensure we are effective, efficient, and repeatable. The methodology looks for XML content-based attacks, next generation web services attacks, and application infrastructure attacks like SQL injection and denial of service (DoS). Our customized methodology allows the process to be consistent across testers, while allowing them to be creative and leverage their "Hacking" skills. Our detailed methodology spans across different security categories:
- Discovery
- Configuration Management
- Authentication
- Authorization
- User & Session management
- Data validation
- Error handling and Exception Management
- Data Protection

**Reporting and Deliverables**
Findings are communicated on a daily basis. We pay special attention to the quality of the findings. Our findings include:
- Detailed description of the vulnerability
- Steps to reproduce the finding
- Affected Functionality/Parameter/URL/Application
- List of tools used and where to download them

DISCOUNTED RETESTING

Foundstone partners with your organization in attaining its strategic security goals. At the conclusion of this engagement, Foundstone will list all discovered vulnerabilities based upon a ranking of high, medium, and low. At a discounted rate, Foundstone will perform a retest of each of the discovered vulnerabilities within three months of the completion of your engagement. This will allow you to validate that your security remediation efforts resolved all vulnerabilities discovered by Foundstone.

“When I was asked why I chose Foundstone, I thought, would I want to hire a company that runs the tools and reads the books, or should I hire the company that writes the tools and writes the books? The choice was simple”

– Foundstone client

The technical report is provided in multiple formats such as Word, CSV and PDF as requested by the client. Report goes through several levels of review process such as peer review, engagement manager’s review and director’s review before it is finalized and shared with the client. The report consists of:

- Executive Summary
- Summary of Strengths
- Benchmark Data upon request
- Testing Notes
- Report Card
- Strategic Recommendations: People, Process and Technical
- Findings & Recommendation

You can request a copy of our sample findings and technical report by emailing us at consulting@foundstone.com.

The Foundstone Difference

All Foundstone projects are managed using Foundstone’s proven Security Engagement Process (SEP) for project management. This process ensures continual communication with your organization to ensure the success of all Foundstone consulting engagements. Reports are communicated securely using agreed upon methods e.g. PGP encryption.

Foundstone staff are certified in their areas of expertise including: CISSP, CEH, CISM, PCI QSA, GIAC etc. All Foundstone employees have full background investigations performed prior to offers being extended. They go through rigorous interview and hiring process and are put on the internal training program until they are qualified to meet our standards. Our testers are thorough, efficient and have a great track record of beating competition on bake-off and comparative tests.