Security Source Code Review

**Benefits**

Foundstone's capability in security source code review extends from our SASS consultants, who have performed source code audits on numerous client applications as well as their own software. Our SASS consultants have all worked as development practitioners on commercial enterprise software systems and understand the software development process as well as why and how security bugs are introduced. Our experience combined with advanced automated tools using contextual analysis enable us to look at more code faster, more accurately, and more effectively than other security consulting services.

**Deliverables**

Our deliverables include:

- Daily updates
- Preliminary Findings Report
- Technical Report for the SCR Assessment
- Executive Summary Report
- Close Out Presentation

**Related Foundstone Services**

Foundstone offers many related services and training classes.

- Web Application Penetration Testing (WAPT)
- Web Services Security Assessment
- Thick Client Assessment
- Mobile Application Assessment
- Application Threat Modeling
- Writing Secure Code Training (Java, .Net, C/C++)
- Secure Coding Policies and Standards
- Software Security Maturity Assurance (SSMA) Assessment/ S-SDLC Gap Analysis

**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.

Research has shown that fixing security problems early in the Software Development Life-Cycle (SDLC) is more efficient and cost effective than the traditional penetrate-and-patch model. Foundstone consultants use rigorous and efficient source code inspection to identify detrimental software security problems at the onset of the SDLC. We use commercial static source code analysis tools to help us automate the process. Foundstone experts manually validate every issue to eliminate false positives and inspect code to overcome the limitations of automated tools and techniques that are ineffective. For example, these tools are not good at finding authorization or application logic bypass issues as they do not understand the business context. Our consultants find policy or best practice violations such as inappropriate cryptography algorithms and common semantic language constructs that lead to vulnerabilities.

We have expertise in C, C++, C#, VB.Net, ASP.Net, Java, LUA, CFML, Classic ASP, Android, Objective C and PHP, working within development frameworks such as J2EE and .NET.

**Methodology**

Foundstone's methodology is broken down into four steps: Threat modeling/Code Walkthrough, Scanning, Triaging and Manual Code Review. When examining any sizeable application, we start by building a threat model in conjunction with the development team. This threat model helps us understand the applications functionality, technical design, and existing security threats and counter-measures. Threat models help us manage the size of the code base we need to examine down to a much smaller scope (typically 60 percent of the code). Armed with the threat model and a complete understanding of the applications architecture we use automated static analysis tools to assess the code for semantic and language security bugs. The automated scans have the advantage of identifying code hotspots, instances of poor coding practices and identifying “low hanging fruit”. Triaging the results involve validating the results from automated tools and eliminating any false positives. However, the bulk of the code review engagement is performing manual review of the code. This review is performed using Foundstone's internal checklists and test plans that are based on the Foundstone Software Security Framework described below, as well as the coding language, underlying technology, and the application or system type (e.g., web application, service or daemon, thick client, kernel mode device driver, API, etc.).

In general, we are looking for two types of issues: design flaws and implementation bugs. Design flaws include poor design ideas that have been implemented, such as choosing an inappropriate source of randomness for cryptographic key generation. Implementation bugs are typically syntactical or semantic language constructs that lead to security vulnerabilities.

Software Magazine has published our work and methodology for code assessments in multiple articles.
“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

Software Security Framework

To ensure quality and consistency of results, Foundstone consultants use a standard framework for code reviews. The framework is designed to allow flexibility in testing methods and the specific tests that are performed to allow consultants to apply their expertise to the application being tested, but its comprehensive nature ensures all potential weaknesses in the application are properly assessed. A summary of Foundstone’s software security framework is shown below.

- Configuration Management
- Data Protection in Storage & Transit
- Authentication
- Authorization
- User & Session Management
- Data Validation
- Error Handling & Exception Management
- Logging & Auditing

Reporting and Deliverables

Our detailed reports provide specific vulnerability information including line, file locations, the issue itself, and suggested solutions. We also provide an overview, including statistics for code sections such as the number of vulnerabilities in specific areas (per 1,000 lines of code) and suggested strategic remediation such as the creation of re-useable components or security libraries.

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 deliver assessments that meet our standards.