CALIBRE

Assured Software and Website Security

HIGHLIGHTS

- >> *CALIBRE works with our customers to determine the benefits of static source code analysis and dynamic application vulnerability analysis.*
- >> *CALIBRE developed a robust tool kit of multiple static and dynamic analysis tools to provide comprehensive security assessment.*
- >> *Our static and dynamic analysis tools are on the Defense Information System Agency (DISA) approved list and are on the Software Assurance Metrics and Tool Evaluation (SAMATE) and Open Web Application Security Project (OWASP) recommended list of tools.*

In today's world a comprehensive approach to verifying the quality and security of a software product is paramount for maintaining a secure posture. To improve the quality of your software, teams should adopt a security development lifecycle (SDL) approach, which aims to reduce the number of security-related coding defects.

CALIBRE uses multiple static code analysis tools to optimize the identification of vulnerabilities and increase the true positive rate of detection, as recommended by the National Security Agency's (NSA) Center for Assured Software (CAS).

CALIBRE provides a cost-effective process for an independent assessment of software security quality. Our process uses multiple mainstream static and dynamic code analysis tools to optimize the identification of vulnerabilities while limiting the number of false positive findings.

>> *WhWhat are CALIBRE's static and dynamic analysis?*

Static source code analysis, or white-box testing, reviews software in a non-runtime environment, revealing code patterns that violate defined coding rules, bugs, and coding errors. These scanners identify potential weaknesses or reliability issues within your code. Dynamic analysis occurs when software is operational. Unlike its static counterpart, dynamic analysis does not test at the code level, and instead detects exploits by performing or duplicating attacks. Through automation, dynamic analysis tools search for a range of vulnerabilities including input/output validation configuration errors and application issues. This allows organizations to detect vulnerabilities in released software in ways similar to malicious attackers by comparing actual results with the established baseline of expected results.

>> *Why perform static and dynamic analysis?*

Software security is a critical component to successful software deployment. Identifying potential security vulnerabilities in systems before they are placed in a production environment should be part of every organization's security program. The key is to quickly identify software weaknesses without spending time wading through reams of false positives (issues that are reported but are not really defects). CALIBRE's processes more accurately identify true positives and prioritize the impact of vulnerabilities.

The use of static and dynamic analysis tools through the entire software development lifecycle will help lower the cost of fixing defects and help you develop a higher quality product. CALIBRE's approach for software assurance and website security is based on the National Security Agency's Center for Assured Software (CAS) studies regarding the use of static source code security analyzers for the C/C++ and Java programming languages. The report, ”CAS Static Analysis Tool Study-Methodology” 2011 emphasizes that to be most effective, static source code security analysis should use multiple tools from multiple vendors. The study states that three different tools used in tandem provide a better true positive rate than using only one tool. The report can be found at: *http://samate.nist.gov/docs/CAS%20 2011%20Static%20Analysis%20Tool%20 Study%20Methodology.pdf*

>> *CALIBRE's approach*

CALIBRE's toolbox includes tools from the Defense Information Systems Agency (DISA) approved buy list, the Department of Homeland Security (DHS), and the National Institute of Standards and Technology's (NIST) Software Assurance Metrics and Tool Evaluation project.

CALIBRE's toolbox uses the best static and dynamic analysis tools in the industry, including HP Fortify, Parasoft C++ Test and JTest, Coverity Static Analysis, DMS Source Code Search Engine, WebInspect, and AppDetective Pro. This comprehensive list of industry leading tools, used in combination, increases code coverage, and is capable of identifying serious security issues that may reside in your website.

These vulnerabilities include SQL injection, cross-site scripting, and buffer overflows as well as many others found in the Common Weakness Enumeration (CWE) list.

>> *Past experience*

CALIBRE has worked with several customers providing in-depth software security risk review. We have performed extensive analysis of commercial voting systems, Department of Defense (DoD) systems, and law enforcement systems. Through our efforts we have been able to expedite the identification, prioritization, and mitigation of security vulnerabilities in both large and small applications.

The Federal Voting Assistance Program (FVAP) commissioned CALIBRE to perform analysis on three different internet voting systems using the three static analyzers theory presented in the CAS report. The purpose of the study was to determine the usefulness of static and dynamic analysis tools for internet voting system manufacturers.

The analysis will also help the Election Assistance Commission determine if static code analysis may be useful in internet voting system certification. CALIBRE is a leader in performing such an analysis for the voting industry.

>> *CALIBRE services*

Source code analysis uses multiple best-in-industry tools to ensure:

- Dynamic application vulnerability analysis
- Determination of software vulnerabilities and poor coding practices
- Possible mitigation for vulnerabilities
- Accurate identification of false positives

CALIBRE provides expert static and dynamic analysis of your source code and websites, using a suite of best in class tools.

ABOUT CALIBRE

CALIBRE Systems, Inc. is an employee-owned management consulting and information technology solutions company supporting government and industry. CALIBRE is committed to the success of our clients and delivers enduring solutions that solve management, technology, and program challenges.

For more info contact us at info@calibresys.com