VOLUME 2

State of Software Security Report

The Intractable Problem of Insecure Software

Executive Summary

September 22, 2010

VERACODE

Executive Summary

The following are some of the most significant findings in the State of Software Security Volume 2, representing 2,922 applications assessed in the last 18 months by Veracode SecurityReview®, a cloud-based application risk management services platform.

1. More than half of all software failed to meet an acceptable level of security and 8 out of 10 web applications failed to comply with the OWASP Top 10
2. Cross-site Scripting remains the most prevalent of all vulnerabilities
3. Third-party applications were found to have the lowest security quality
4. Developers repaired security vulnerabilities quickly
5. Suppliers of Cloud/Web applications were the most requested third-party assessments
6. No single method of application security testing is adequate by itself
7. The security quality of applications from Banks, Insurance, and Financial Services industries was not commensurate with their business criticality

Key Findings

1. More than half of all software failed to meet an acceptable level of security and 8 out of 10 web applications failed to comply with the OWASP Top 10

57% of all applications were found to have unacceptable application security quality on first submission, even when standards were adjusted for applications considered less business critical (Figure 3). Even more troublesome, more than 80% of internally developed and commercial web applications failed to comply with the OWASP Top 10 (Figure 5), an industry standard list of critical web application errors.

The level of risk in terms of repair costs, business continuity, and brand from so many business critical applications failing to meet an acceptable level of security on first submission is staggering. The potential exposure to brand reputation and loss of revenue from interruptions to business operations is significant.

Recommendation: Utilize industry standards such as OWASP Top 10 and CWE/SANS Top 25 list of most dangerous software errors as minimum thresholds and compliance policies to which applications need to adhere.

2. Cross-site Scripting remains the most prevalent of all vulnerabilities

Cross-site Scripting (XSS) remains the most prevalent vulnerability category, accounting for 51% of all vulnerabilities uncovered by Veracode's combined static binary, dynamic, and manual security testing methods (Figure 13). .NET applications, in particular, exhibited an abnormally high rate of Cross-site Scripting vulnerabilities, resulting from the use of .NET controls that do not automatically encode output (Table 4). While not as numerous, Cryptographic Issues—a category that includes unencrypted or inadequate encryption of data—appeared in the most applications, with 41% of all applications containing one or more vulnerabilities in this category (Figure 14). These statistics underscore the need for developers to become better educated and better equipped to avoid common vulnerabilities.

Recommendation: These flaws are easy to fix once found (Figure 4). Focusing on developer education and awareness is a cost-effective way to avoid introducing them.

3. Third-party applications were found to have the lowest security quality

Third-party code is getting more attention since Veracode first highlighted in Volume 1 of this report, that between 30% and 70% of software submitted as internally developed contained identifiable third-party components. Both Safecode.org[1] and a report from the research firm Secunia[2] have recently reinforced the elevated risks associated with third-party software in the supply chain. In Figure 3, Veracode shows that applications from all types of third-party suppliers were less secure than Internally Developed applications on first submission. Third-party suppliers failed to achieve acceptable levels of security 81% of the time. However, in Figure 2 it is also evident that third-party code is an essential part of the every organization's portfolio, comprising 29% of all applications submitted to Veracode. Furthermore, between 20% and 37% of very high or high criticality applications are sourced from third-parties.

Recommendation: Both internal and third-party components and applications must be subjected to the same level of security verification to ensure consistent security quality across the application portfolio. Procurement contracts for outsourced or commercial software vendors should insist upon the authority to perform independent security testing and specify minimum security acceptance criteria.

4. Developers repaired security vulnerabilities quickly

A common misperception is that it is easy to find defects and difficult to fix them. While this may often be true of functional defects in software it is less true for security defects. Observing a variance from functional specifications is relatively easy but determining the root cause can be hard. Conversely, determining that an application allows someone to do something it was never intended to do is actually quite difficult but relatively easy to fix once known (Figure 4). Among the most encouraging data in this report, the evidence that development teams using Veracode can fully remediate unacceptable levels of security quality in only 16 days and 1.1 resubmissions on average is among the best reasons to equip development teams with effective security testing and training—they can and did improve the state of software security quickly when properly informed.

Recommendation: Equip development teams with the appropriate application security resources and knowledge and plan for security verification and remediation in the project timeline from the outset.

5. Cloud/Web applications were the most requested third-party assessments

Assessments of third-party applications at the request of a purchasing organization have grown linearly over the past 6 quarters, reflecting the increased concern over the security of software in the supply chain and the availability of effective, new technologies such as cloud-based, static binary analysis that make third-party assessments possible without requiring source code or tools. In a new section of the report, Veracode explored the types of applications most often reviewed by request. As Figure 8 shows, suppliers of cloud and web applications made up nearly 60% of all third-party assessments requested, while integrators and commercial software providers made up most of the rest in equal parts. Since cloud-based applications are relatively new, their significant presence indicates the reasonable security concerns they raise and the criticality of the work they perform. Like other third-party software, these assessments resulted in low levels of acceptable security and rapid remediation.

Recommendation: Require Third-party Cloud/Web application and service providers to demonstrate verification of application security quality.

[1] www.safecode.org

[2] www.theregister.co.uk/2010/07/12/secunia_threat_report

6. No single method of application security testing is adequate by itself

Others have reported this year on the inadequacy of web application scanning.[3] Veracode's code-level analysis of vulnerabilities using multiple testing techniques on the same applications confirms that dynamic web application scanning tools are not sufficient as the sole testing method. Similarly, manual penetration testing, while necessary to fully comply with policies such as the OWASP Top 10 and the CWE/SANS Top 25, lacks consistency of coverage and will rarely detect all instances of commonly occurring vulnerabilities. However, while the evidence shows that static binary analysis provides the most consistent breadth and depth of coverage, it is also true that not all design and business logic vulnerabilities are discoverable with static methods alone.

Recommendation: CISOs and CIOs should view different testing techniques as operating controls that each play an important role in a comprehensive policy driven program. Multiple testing techniques should be adopted based on application business criticality and type of application. The use of multiple techniques is the only way to comply with industry standard security polices such as the OWASP Top 10 and the CWE/SANS Top 25 Most Dangerous Software Errors.

7. The security quality of applications from Banks, Insurance, and Financial Services industries was not commensurate with their business criticality

In a very interesting dichotomy, Financial Industry applications were found to have the best raw code-level security scores of any industry but only average levels of acceptability when the business criticality of an application was considered. This speaks to the high degree of awareness such firms have about code-level threats but also to the inadequate application risk management practices employed relative to the importance of these applications. Financial Services applications in particular demonstrated an exceptionally low prevalence of the most common vulnerabilities—less than half the rate of Cross-site Scripting errors as compared to Banks and Insurance (Table 7). The implication is that training, testing, and a high degree of focus on specific types of errors can make a significant difference. The net result is both encouraging because improvement is possible; and sobering because the most critical of applications remain too insecure.

Recommendation: Inventory and classify the application inventory based on business criticality. In the absence of this business context, an understanding of the code-level security quality is insufficient. What seems to be good code-level security quality may still not render the application fit for purpose when business criticality is taken into account.

[3] www.darkreading.com/vulnerability_management/security/app-security/showArticle.jhtml?articleID=222601207

VERACODE

www.veracode.com

ABOUT VERACODE

Veracode is the world's leader in cloud-based application risk management. Veracode SecurityReview is the industry's first solution to use patented binary code analysis, dynamic web assessments, and partner or Veracode delivered manual penetration testing, combined with developer e-learning and access to open source security ratings to independently assess and manage application risk across internally developed applications and third-party software without exposing a company's source code. Delivered as a cloud-based service, Veracode provides the simplest, most complete, and most accurate way to implement security best practices, reduce operational cost and comply with internal security policies or external standards such as OWASP Top 10, CWE/SANS Top 25 and PCI.

SSSR/0910