



VOLUME 3

State of Software Security Report

The Intractable Problem of Insecure Software

Executive Summary

April 19, 2011

VERACODE

Executive Summary

The following are some of the most significant findings in the Veracode State of Software Security Report, Volume 3, representing 4,835 applications assessed in the last 18 months by Veracode on our cloud-based application security platform.

1. When first tested, more than half of all applications fail to meet acceptable security quality, and more than 8 out of 10 web applications fail OWASP Top 10
2. Cross-site scripting prevalence remains constant over time, while SQL injection is trending slightly down
3. Finance and Software industries lead the charge on holding software suppliers accountable; Aerospace and Defense are following suit
4. Most developers are in dire need of additional application security training and knowledge
5. The software industry, including security products and services, have significant gaps in their security posture
6. While static analysis finds orders of magnitude more flaws than dynamic analysis, both techniques are required for comprehensive coverage
7. Building secure software or requiring it from your suppliers does not have to be time consuming

Key Findings

1. When first tested, more than half of all applications fail to meet acceptable security quality, and more than 8 out of 10 web applications fail OWASP Top 10

58% of all applications were deemed to have “unacceptable” security quality upon first submission (Figure 3). This remains essentially unchanged from the statistic that was reported in Volume 2¹ (57% unacceptable). Commercial acceptability dipped a small amount from 35% acceptable in Volume 2 to 32% in this Volume. When measured against the OWASP Top 10, an industry standard list of critical web application errors, more than 8 out of 10 web applications across internally developed and commercial supplier types fail to achieve compliance (Figure 10). OWASP Top 10 is one of the standards relied upon by the PCI council so this failure rate also gives one insight into the poor state of non-compliance with respect to regulations such as PCI. This poor state of security of applications on their first submission to Veracode is due to two possible factors; either security processes such as threat modeling or secure coding standards were not incorporated into the development lifecycle, or the security processes were incorporated but failed to reduce flaws significantly. When you consider these statistics in the context of the ever strengthening threat environment these application security weaknesses translate into real and present danger for the risk-free operation of your software infrastructure. The 2010 Verizon Data Breach Investigations Report estimates that 40% of breaches occur due to hacking (i.e. successful exploitation of a software vulnerability) and are responsible for 96% of the compromised records.²

Recommendation: More training and more testing. It is clear that there is room for significantly greater emphasis on training and awareness of common security vulnerabilities such as the OWASP Top 10 and CWE/SANS Top 25. The training should be reinforced with consistent testing for compliance with these benchmarks for both internally developed and third-party applications.

¹ <http://info.veracode.com/State-of-Software-Security-Volume-2.html>

² www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

2. Cross-site scripting prevalence remains constant over time, while SQL injection is trending slightly down

This report examined trends in Cross-site scripting (XSS) and SQL injection, the two most commonly discussed issues in web application security, by looking at the percent of applications affected, quarter over quarter since the beginning of 2009. We see XSS remaining nearly flat and SQL injection gradually decreasing by 2.4% per quarter, a statistically significant amount according to linear regression (Figure 20, Figure 21). On one hand, it's reassuring that the industry seems to be making progress at reducing SQL injection; on the other hand, it's disappointing that we're not seeing a steeper downward trend. This is particularly concerning given that XSS and SQL injection are hot-button issues in many enterprises and ones that most organizations are actively trying to reduce. This trend could indicate that testing and remediation efforts are just barely keeping pace with development of new applications. Perhaps the most alarming realization is that when you consider the threat environment, these vulnerabilities become more than just theoretical flaws in your code base. They are ticking time bombs waiting to be exploited in real world attacks. The 2010 Data Breach Investigations Report from Verizon reveals that 25% of attacks carried out via hacking techniques were attributable to SQL injection and 8% were attributable to XSS.³

Recommendation: SQL injection and XSS are repeatedly in the headlines as the initial attack vector for high-profile, targeted breaches. It is crucial to reduce their occurrence in software applications if we are to outpace attackers. Organizations are encouraged to double down on their efforts to train their development and security staff on how to avoid these errors in the first place or fix them quickly once they are found. Use automated testing techniques to expediently discover these vulnerabilities across your application portfolio and to verify that the development team is following the guidance learned from their training. There are even free services such as Veracode's free XSS detection service that can provide development teams a quick view into the XSS issues present in their web applications.⁴

3. Finance and Software industries lead the charge on holding software suppliers accountable; Aerospace and Defense are following suit

One of the fastest growing areas within application security is independent verification of third-party software. As organizations are breached because of vulnerabilities present in someone else's software, they are starting to hold their software suppliers more accountable. Organizations are demanding proof of independent security verification before proceeding with a commercial transaction. The two industry segments leading the charge in this movement are Finance and Software. Together they represent over 75% of the enterprises requesting formal verification of third-party suppliers (Figure 12). It was interesting to see Aerospace and Defense, an industry that prides itself in the rigor it brings to its manufacturing supply chain, starting to apply the same standards to its software supply chain. The results of these independent assessments are enlightening: 25% of third-party applications are found to be of acceptable security quality upon initial submission (Figure 15). While this marks a slight improvement from Volume 2 (19% acceptable) clearly most software suppliers have significant work to do to ensure they are complying with the security gate set by the purchasing enterprise.

Recommendation: Reliance on third-party software to perform critical business functions and collaboration amongst an organization's workforce is only going to increase with the adoption of cloud and mobile platforms. Not having visibility into the security of these third-party applications is leaving a blind spot in an organization's understanding of its risk posture while providing yet another attack point for malicious parties. Maintaining the status quo is simply not an option. Software purchasers should introduce independent security verification language into their legal contracts and require proof of independent testing as part of their procurement process. Software producers should participate in this process in a cooperative and transparent manner as it ultimately serves to elevate the security posture of their product. This in turn can be used as a competitive differentiator in the marketplace.

³ www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

⁴ www.veracode.com/freeservice

4. Most developers are in dire need of additional application security training and knowledge

Over 50% of users taking an application security fundamentals exam received a grade of C or lower. Over 30% received a failing grade of D or F (Figure 31). The exam covers knowledge of broad security concepts, including common threats, and may be taken by developers, managers, or QA testers. Considering these exam scores, it is no wonder that over 50% of applications fail to achieve acceptable security quality upon initial submission. Performance on other exams such as Secure coding for Java, Secure coding for .NET and Introduction to Cryptography didn't fare much better. Anywhere from 35% to 48% of users taking those courses received a grade of C or lower (Figure 31).

Recommendation: Application security training and education is not a formal part of most computer science curriculums and certainly not a consistent theme in the professional development opportunities made available to technology professionals in companies. Therefore the results obtained from these exams are no surprise. Organizations are strongly encouraged to institute developer training and education programs to ensure a high competency level on application security. Take advantage of eLearning platforms to provide this training in a cost-effective and scalable manner. Close the loop on training by allowing developers to test their code using automated analysis techniques.

5. The Software industry, including security products and services, have significant gaps in their security posture

Similar to our deeper analysis of the financial industry in Volume 2, we engaged in a deep dive on the software industry segment in this report. What we found was both surprising and disappointing. It also served to explain the recent breaches that have been carried out against prominent security vendors such as RSA, HB Gary and Comodo. Overall, 66% of software industry applications were found to be of unacceptable security quality upon initial submission (Figure 28), which is worse than the 58% unacceptable rate when applications from all industries are taken into account. When measured against Veracode's risk adjusted verification methodology the two worst performers within the software industry were the sub-categories of customer support (82% unacceptable) and most surprisingly security products and services (72% unacceptable) (Figure 28). The customer support category includes customer relationship management and web customer support applications. The security products and services category includes applications that are being used to perform a security function. The good news was that overall the software industry demonstrated the ability to meet acceptable security quality in a timely manner. Over 90% of all applications across the software industry achieved acceptable security quality within 1 month. The average for all applications in the security products and services sub-category was an impressive 3 days.

Recommendation: There are a few important lessons to be learned from this analysis. Security should not be assumed on the part of any industry segment even when it is those producing software for a living—including security software. A formal independent verification of security quality must be mandated in the procurement process as well as in the SDLC before pushing applications to production. Further, it should be noted that the verification process does not have to slow down the software acquisition or software deployment timeline. The data confirms that acceptable security policy can be achieved within reasonable timeframes. Compare the test results of different applications developed by staff with varying levels of security training to understand where training is working and to fill in gaps.

6. While static analysis finds orders of magnitude more flaws than dynamic analysis, both techniques are required for comprehensive coverage

Static analysis was able to find significantly more flaws as dynamic analysis in important categories such as XSS, CRLF injection and SQL injection (overall as much as 22 times more) (Table 5). One major contributing factor in the volumes of flaws found is that static analysis provides comprehensive coverage of the application whereas dynamic analysis only tests code paths that it can discover externally. Often, dynamic (and even manual) testing completely overlook portions of the application that are only reachable under certain circumstances (e.g. functionality that is gated behind a series of forms that trigger different behavior depending on how they are filled out). On the other hand, all the static findings will not necessarily be exploitable; dynamic and manual analysis are better at determining exploitability.

Recommendation: The lesson for CISOs and CIOs is that a robust application security program must incorporate multiple testing methods in order to ensure that applications are assessed with sufficient coverage, measured by both depth and breadth. Becoming overly dependent on too few analysis methodologies guarantees blind spots when assessing overall application risk. When you consider that prominent breaches such as Heartland Payment Systems, HB Gary, and the “Night Dragon” cyber attacks targeted at companies like Shell, Exxon Mobil and BP, had SQL injection as their root cause, it’s prudent to maximize your chances of finding as many instances of this issue in your code base as possible. Combining multiple testing techniques allows you to do exactly that. If your testing process is currently limited to automated dynamic and or manual testing adding static testing can greatly improve flaw identification.

7. Building secure software or requiring it from your suppliers does not have to be time consuming

Over 50% of commercial suppliers in our dataset resubmitted 90-100% of their applications and slightly under 40% of companies developing applications internally resubmitted 90-100% of their applications (Figure 4). When all applications were measured against Veracode’s risk adjusted verification methodology, it was found that more than 80% across all supplier types achieved an acceptable security quality within 1 month (Figure 7). What this tells us is that when developers and security professionals attempt to do the right thing (i.e. achieve the requisite security rating), they can do so quickly and efficiently. The trick is to have the right application security training, testing tools and accurate guidance on where the vulnerabilities are and how to fix them. No one intends to write insecure code, so when they are trained appropriately and made aware of the security weaknesses that exist in their work products, they can act on that information and strive to achieve acceptable security quality expediently.

Recommendation: CIOs and CISOs should take relief in the knowledge that when the right application security training, technologies for security verification and guidance on security weaknesses present in their applications are made available to their development staff they will take responsibility and pursue the appropriate corrective actions expediently. The same is true for an organization’s software suppliers. Arm your teams with the right training to avoid mistakes in the first place, but equally as important, implement a formal application security program for internally developed and third-party applications to improve the state of software security in your organization.



VERACODE

Veracode, Inc.
4 Van de Graaff Drive
Burlington, MA 01803

Tel +1.781.425.6040
Fax +1.781.425.6039

www.veracode.com

© 2011 Veracode, Inc.
All rights reserved.

SSSR/0411

ABOUT VERACODE

Veracode is the only independent provider of cloud-based application intelligence and security verification services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. By combining patented static, dynamic and manual testing, extensive eLearning capabilities, and advanced application analytics Veracode enables scalable, policy-driven application risk management programs. Veracode delivers unbiased proof of application security to stakeholders across the software supply chain while supporting independent audit and compliance requirements for all applications no matter how they are deployed, via the web, mobile or in the cloud. The company's more than 175 customers include Barclays PLC, California Public Employees' Retirement System (CalPERS), Computershare and the Federal Aviation Administration (FAA). For more information, visit www.veracode.com, follow on Twitter: @Veracode or read the ZeroDay Labs blog.