A GUIDE TO SOFTWARE SECURITY

ca technologies | VERACODE

Why Software Is Vulnerable

The innovations of the internet, software applications, and connected devices have launched a digital economy, enabling greater services and efficiencies. But at the same time, inherent vulnerabilities in computer networks, software, hardware, and end users have created a systemic risk to the economy and national security. Among these, software applications are the most vulnerable, and attacks on applications are the leading cause of confirmed breaches, according to the *Verizon Data Breach Investigation Report*.

There isn't a business today that doesn't produce or purchase applications in order to run more efficiently. Software powers everything from our critical infrastructure and healthcare to our commerce and financial systems. This growing dependence on software does improve efficiencies, but at a potential cost.

Despite the growing reliance on and risks related to software, vulnerabilities in applications still abound. Software vulnerabilities are the result of weaknesses in the code, which are introduced at the development stage. There are several causes of these weaknesses, including insecure coding practices, re-use of vulnerable third-party code, and inadequate policies and processes for updating software when new vulnerabilities are discovered.

CA Veracode has produced a series of research reports drawing on a wealth of data from code-level analysis of its customers' web and mobile applications. The *State of Software Security* (SOSS) report has plotted trends in application security over several years. Data in the 2017 SOSS report demonstrates that software is broadly vulnerable to attack, with less than one-third of applications passing basic security benchmarks when first tested. CA Veracode research also shows that systematic security testing yields positive results, and highlights which practices organizations can adopt to improve the security posture of the software they develop internally, buy, or assemble from third-party code.

This summary of CA Veracode's research offers policy makers and IT decision makers a basis for understanding the scope of the problem of insecure software, and provides recommendations for policies that can help reduce the vulnerabilities in software that threaten economic prosperity and the digital infrastructure of our society.

Definitions

- **Web application:** A piece of software accessible over the internet
- **Application security (AppSec):** The use of technologies and processes to secure software
- **Flaw:** A weakness in software code that is a potential security risk
- **Vulnerability:** A security hole caused by flaws that can be attacked to compromise software
- **Open source:** Third-party code that developers can use in their own applications for free
- **Component:** A library of open source or commercially-developed code that developers use to create software more efficiently
- **OWASP Top 10:** The 10 most critical application risks identified by the Open Web Application Security Project (OWASP)
- **Java:** A popular programming language used to create software
- **API:** An application program interface (API) is a protocol that enables two pieces of software to interact with each other
- **Static application security testing:** Scanning binary code for vulnerabilities in a static (non-runtime) environment
- **Dynamic application security testing:** Scanning applications for vulnerabilities in a runtime environment
- **Software development lifecycle:** The continuous process of developing and updating software
- **DevOps:** A software development process that unites development (creating applications) with operations (managing applications)
- **DevSecOps:** A development process that integrates security testing throughout the software development lifecycle

COMPONENTS: INCREASING SPEED AND RISK

To accelerate the delivery of digital innovations, it's now a common development process to incorporate reusable, pre-built software components, often obtained from open source projects. But while component usage speeds the delivery of software, it also increases risk. According to CA Veracode analysis, applications have an average of 24 vulnerabilities in their components. Even if developers are especially careful to only choose components that have no known vulnerabilities, new vulnerabilities are found and disclosed all the time.

It can be difficult for global enterprises with multiple code repositories to pinpoint all the applications where a risky component is used. This leaves countless web and mobile applications at risk. CA Veracode scan data found that 88% of applications written in Java have at least one flaw in a component.

Vulnerable components were exploited by attackers in several recent data breaches. A vulnerability discovered in March 2017 in a commonly used component was responsible for a major breach at the Canada Revenue Agency. The same component has been linked to the July 2017 Equifax breach that resulted in the theft of personal data of 145 million U.S. consumers and 15 million more in Great Britain, despite the availability of a security patch months earlier.

Fortunately, there are ways to decrease the risk of vulnerable components. Developers can keep an up-to-date inventory of the components they're using, and update those components when new vulnerabilities are discovered. Software composition analysis that scans applications for components makes it easier to inventory components and identify applications with vulnerable versions of components.

The Positive Impact of Application Security Testing

In the past 12 years, CA Veracode has scanned more than 6 trillion lines of code, across thousands of applications. According to analysis of these security tests, the majority of software is vulnerable: 77% of applications have at least one security flaw. Furthermore, surveys conducted by CA Veracode have found that more than one-third of organizations don't run any static application security tests, and 48% of organizations don't run any dynamic application security tests. It's difficult to estimate how much software does not undergo security testing, but it is not an insignificant number. Many CA Veracode customers scan only a small portion of their applications.

However, testing data shows that organizations that do scan their applications for vulnerabilities are making improvements in fixing the vulnerabilities they find. Additionally, organizations that implement comprehensive testing programs experience significant improvements in the performance of their applications against security benchmarks like the OWASP Top 10.

What This Means

Implementing an application testing program helps organizations chip away at software vulnerabilities. Organizations with a systematic approach to AppSec, including testing throughout the software development lifecycle, see measurable improvements.

Key Findings from the *State of Software Security 2017*

- The rate of applications passing OWASP Top 10 policy improves after the initial test by 13%.
- Organizations that have been CA Veracode customers for 10 years have a 35% higher OWASP Top 10 policy compliance rate than those testing for a year or less.

Best Practices for Improving Application Security

Based on CA Veracode's experience with thousands of customers over the past 12 years, the following are essential elements of high-performing application testing programs that drive results in reducing risk.

What a Good Application Security Program Looks Like

1 Test throughout the software development lifecycle with multiple technologies.

Different kinds of application security testing — static, dynamic, and manual penetration testing — find different types of vulnerabilities. The most effective AppSec programs use all three kinds of testing to find and fix vulnerabilities during development and once an application is live in production. Not all vulnerabilities are created equal, so effective programs also need to complement testing technologies with policies that describe what types of vulnerabilities make an application "fail" and require fixing.

2 Start small and build the program over time to secure the entire application landscape.

Organizations just starting out with security testing shouldn't try to fix every vulnerability in every application. Security teams need to triage the most critical applications and fix the most severe vulnerabilities first. Many CA Veracode customers are doing this — testing data shows that the fix rate for the most severe vulnerabilities is about twice that of the overall vulnerability fix rate.

As an AppSec program scales up into a more mature program, organizations will assess all of their software, not only applications developed internally, but also those purchased from third parties and those assembled with open source components. In addition, effective programs assess every application throughout its lifecycle — from development to quality assurance (QA) and production.

3 Use metrics to improve performance over time.

Advanced application security programs measure results through a set of metrics and key performance indicators (KPIs), such as compliance with policy (internal policy, OWASP policy, and industry regulations). Metrics allow organizations to quantify their risk. Metrics also enable AppSec managers to communicate areas for improvement to the security and development teams. These feedback loops are a key aspect of the development process known as DevOps, which brings development and operations teams together to meet joint goals of improving performance, functionality, and security.

4 Train developers to code securely, and enable them with the right tools.

As DevOps practices continue to take hold in IT departments today, security teams are increasingly filling the role of expert consultants and partners, rather than testers and compliance babysitters. This means developers are shouldering more responsibilities both during security testing and remediation. CA Veracode data shows that supporting developers with resources such as eLearning and remediation coaching by security experts can have a tremendous impact on the efficacy of developer teams in fixing security bugs.

Developers with eLearning fix, on average, 19% more flaws than those without eLearning, while developers who received security consulting fix 88% more flaws. Developers also benefit from testing tools that they can use directly within their development environments. Using APIs and plugins to connect AppSec testing with the DevOps toolchain enables more frequent testing. CA Veracode data shows that organizations who test more frequently, and early in the development process, fix 48% more flaws.

What This Means

Changing development practices in recent years have seen more development organizations adopting DevOps, which shifts the responsibility for quality assurance and security testing onto developers. When developers have training resources and tools at their disposal, the security of applications improves.

DevOps organizations are beginning to adopt new processes and technologies for incorporating security testing throughout the software development lifecycle. This shift from DevOps to so-called DevSecOps gives organizations the best posture for reducing the risk of software breaches.

Key Findings from the *State of Software Security 2017*

- 88% of Java applications have at least one high-severity flaw in a component.
- The fix rate for high severity vulnerabilities is about two times the overall fix rate.
- Organizations that scan applications more frequently during development have a 48% better fix rate.
- Organizations with eLearning programs have a 19% better fix rate.
- Organizations that provide developer consultations from third-party experts have an 88% better fix rate.

Recommendations for Policy Makers

The rising stakes for software security require an appropriate and urgent response from companies that produce software, the application security industry, and policy makers. Yet conventional wisdom in recent years has drifted away from prevention towards detection and response. A reactive approach is completely inadequate to stop today's destructive attacks, such as the viral strains of ransomware that recently crippled banks, governments, hospitals, shipping companies, and other businesses.

Securing the world's software requires a significantly increased focus on preventive approaches, by testing for coding flaws in software applications before they can be exploited by malicious actors. Over several years of collecting data from application scans, CA Veracode has identified areas where organizations are failing to secure their applications and has discovered best practices that help organizations reduce risk. CA Veracode offers the following guidance for policy makers.

1 Promote application security testing by organizations that sell software.

Many breaches come through third-party applications, which are outside the traditional security perimeter, and through commercial software, which many organizations, particularly smaller businesses, struggle to keep up to date with security patches. Promoting best practices and providing incentives for commercial software vendors to routinely scan their software for vulnerabilities will go a long way towards securing the software supply chain. This can potentially be applied in many different ways, including testing requirements for public procurement vendors, limits on liability for organizations that demonstrate adoption of application security practices, insurance premium support, and tax deductions.

2 Emphasize application security testing by critical infrastructure, financial, healthcare, and public sector institutions.

Not all software is equally attractive to attackers. Cybercriminals and nation-state attackers are far more likely to go after critical infrastructure, such as energy utilities, financial services institutions, governments, and healthcare organizations. An example of the consequences of attacks on critical institutions happened in May and June 2017, when viral strains of ransomware infected hundreds of thousands of systems, shutting down hospitals, banks, governments, and businesses. Reducing vulnerabilities in critical infrastructure and key industries, by testing critical applications and embedded software for security vulnerabilities, can help prevent a shutdown of the economy and industries vital to national security. Critical infrastructure sector-specific cybersecurity guidance should incorporate secure application development practices as key components in managing cybersecurity risk.

3 Update cybersecurity regulations to encourage adoption of application security best practices.

Policy makers can encourage organizations to adopt application security best practices through standards such as PCI, HIPAA, the Cybersecurity Framework, and other regulatory and voluntary frameworks. We've already seen the standards for electronic payments move in this direction.

Many organizations will need guidance on how to comply with application security regulations. Policy makers should seek input from organizations like PCI, OWASP, and security industry representatives to craft recommendations that will have the most positive impact on application security without undue burdens on organizations.

4 Provide incentives for primary and secondary education to train the next generation of developers and security professionals.

The shortage of cybersecurity professionals is on pace to reach 1.5 million vacant positions by 2020, according to Frost & Sullivan. And the growing demand for developers with security skills is also dangerously outpacing supply. One reason for the skills gap is a lack of formal cybersecurity education in computer science curricula.

As education institutions seek to increase the number of graduates in STEM disciplines, cybersecurity training should be encouraged in both primary education and at the university level. Grants for educational institutions to offer cybersecurity as part of computer science courses will help build the pipeline of well-trained employees. Private industry should also be incentivized to train developers on the job in order to increase their security skills.

Appendix

Industry Comparisons

CA Veracode scanning data offers a wealth of information about the performance of industries in key application security metrics. One such metric, the OWASP Top 10 pass rate, offers a glimpse into how industries are faring against the most commonly used and reliable application security benchmark. The data from the 2017 State of Software Security report shows an across-the-board decline in OWASP pass rates from the previous year.

INDUSTRY COMPARISON — OWASP PASS RATES 2017 VS. 2016

Industry	OWASP Pass Rate 2017 – First Scan	OWSAP Pass Rate 2016 – First Scan	Percent Change
Infrastructure	29.8%	N/A	N/A
Manufacturing	28.9%	38.7%	-25% ▼
Healthcare	27.6%	33.3%	-17% ▼
Retail & Hospitality	26.2%	37.6%	-30% ▼
Tech	25.4%	38.1%	-33% ▼
Financial Services	25.1%	39.1%	-35% ▼
Government	23.5%	25.1%	-6% ▼
Other	25.8%	40.7%	-37% ▼
Overall	30.2%	38.6%	-22% ▼

"Infrastructure" is a new category grouping that we created in 2017 to describe organizations in energy, transportation, and utilities. With just one year's worth of data, it's not possible to spot any trends, but infrastructure organizations had the highest OWASP pass rate on initial scan. Government organizations, including federal, state, local, and education organizations, had the lowest OWASP pass rates in 2016 and 2017.

INDUSTRY COMPARISON — FIRST AND LAST SCAN

Industry	OWASP Pass Rate 2017 – First Scan	OWASP Pass Rate 2017 – Last Scan	Percent Change
Infrastructure	29.8%	29.5%	-1% ▼
Manufacturing	28.9%	30.5%	6% ▲
Healthcare	27.6%	30.2%	9% ▲
Retail & Hospitality	26.2%	28.5%	9% ▲
Tech	25.4%	26.1%	3% ▲
Financial Services	25.1%	26.7%	6% ▲
Government	23.5%	24.7%	5% ▲
Other	25.8%	26.6%	3% ▲
Overall	30.2%	34.1%	13% ▲

We also examined the improvement in pass rates between the first scan of applications and the latest scan during our measurement period. We found that all industry groups, except infrastructure, improved their OWASP Top 10 policy pass rates in later scans.

INDUSTRY COMPARISON — MAJOR VULNERABILITY CATEGORIES

Percentage of Applications Affected

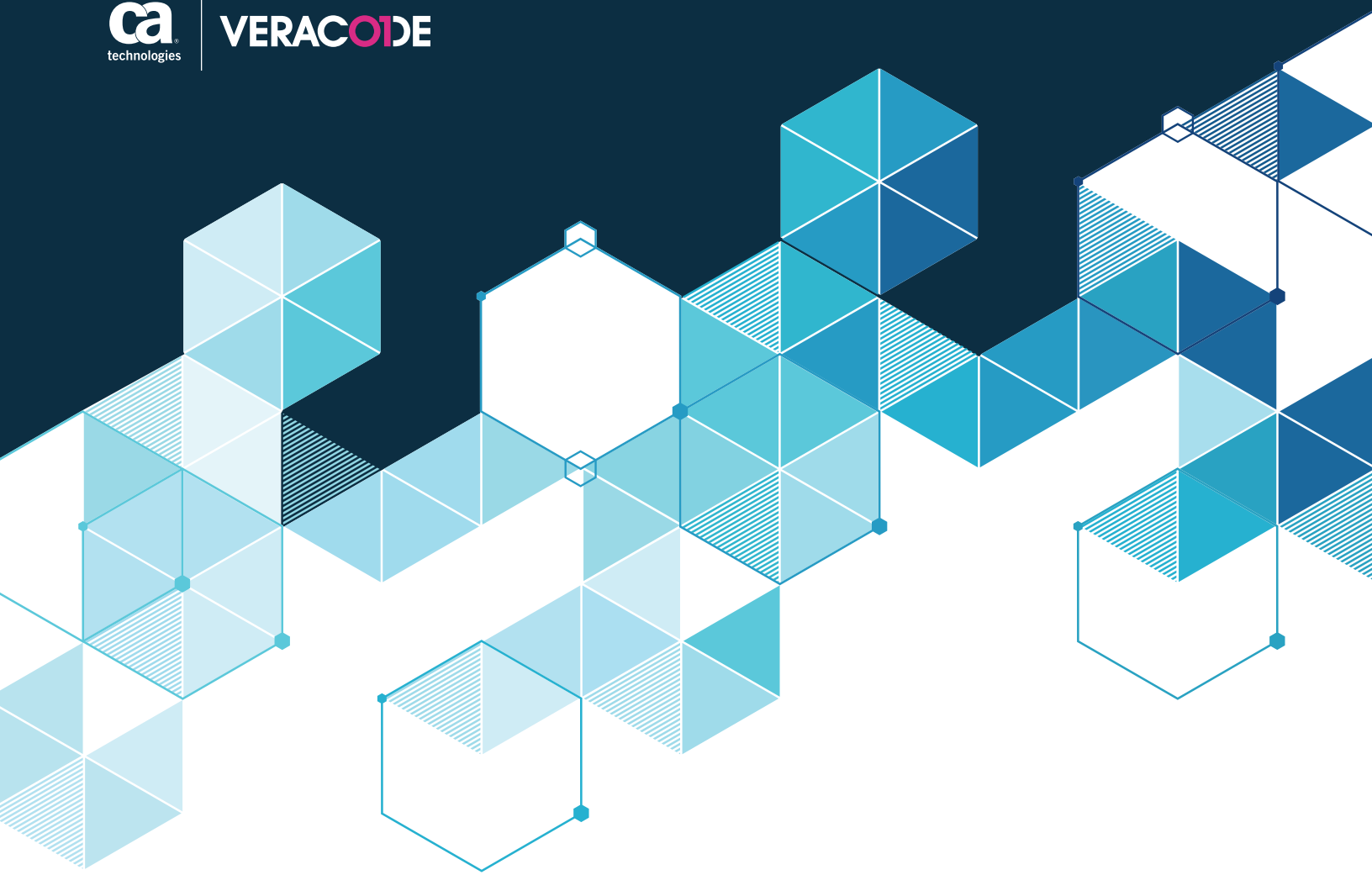
Industry	Cross-Site Scripting	SQL Injection	Credentials Management	Cryptographic Issues
Financial Services	29.0%	19.3%	28.4%	43.5%
Government	49.0%	31.5%	32.7%	48.3%
Healthcare	34.8%	25.4%	32.7%	51.5%
Infrastructure	21.4%	9.0%	21.4%	24.3%
Manufacturing	19.3%	9.9%	18.8%	30.2%
Retail & Hospitality	28.5%	19.3%	30.1%	44.6%
Tech	8.6%	6.6%	10.3%	16.0%
Other	12.8%	8.3%	13.7%	20.4%

For a finer-grained examination of industry performance, we looked at the prevalence of major vulnerability categories, such as SQL injection and cross-site scripting, both highly exploitable web vulnerabilities that are simple for attackers to execute. We also looked at vulnerabilities in credentials management and cryptographic vulnerabilities, which are essential methods for securing user accounts and data.

Key Findings from the *State of Software Security 2017*

- Most industry groups underperformed compared to overall OWASP pass rate benchmarks, with significant declines from a year ago.
- Government continues to underperform and had the highest prevalence of highly exploitable vulnerabilities.
- Retail/hospitality and healthcare showed the greatest improvement between first and latest scan.

ca technologies | VERACODE



STATE OF SOFTWARE SECURITY 2017

Read the Full Report
veracode.com/soss

Contact Us to Learn More

ABOUT CA VERACODE

Veracode, CA Technologies' application security business, is a leader in helping organizations secure the software that powers their world. Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development lifecycle, before they can be exploited by hackers. Our complete set of offerings help customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements, and cost effectively secure their software assets – whether that's software they make, buy or sell. Veracode serves over a thousand customers across a wide range of industries, including nearly one-third of the Fortune 100, three of the top four U.S. commercial banks and more than 20 of the Forbes 100 Most Valuable Brands. Learn more at veracode.com, on the Veracode Blog, and on Twitter.