VERACODE

VOLUME 11

The State of Software Security
Industry Snapshot: Financial Services

Veracode's State of Software Security (SOSS) Volume 11 focused on how developer actions can influence software security. It also looked at the impact that application attributes (their "nature") and the development environment (the "nurturing" of the app) can have on how quickly flaws are fixed. Our analysis uncovered key differences in software security between industries and found that these differences affect how quickly flaws were addressed, adding another dimension to our "nature vs. nurture" discussion. This infosheet provides a summary of factors that shape software security for the financial services sector.

Figure 1 describes how applications compare across industries in finding and fixing flaws. From left to right, the columns rank each industry by the proportion of applications with security flaws, the proportion of applications with high-severity flaws, the percentage of flaws that are fixed, and the median speed at which flaws are fixed. The financial services industry is often perceived as being on top of its security game, and this figure suggests the reputation is at least partially deserved.

The industry has the smallest proportion of applications with flaws, the second-lowest prevalence of severe flaws, and the best fix rate among all industries. Despite all of that, the time to remediation among financial services firms is surprisingly slow. This suggests that while financial services firms do a good job of not adding to the security debt, they take a bit longer to dig out of the hole.

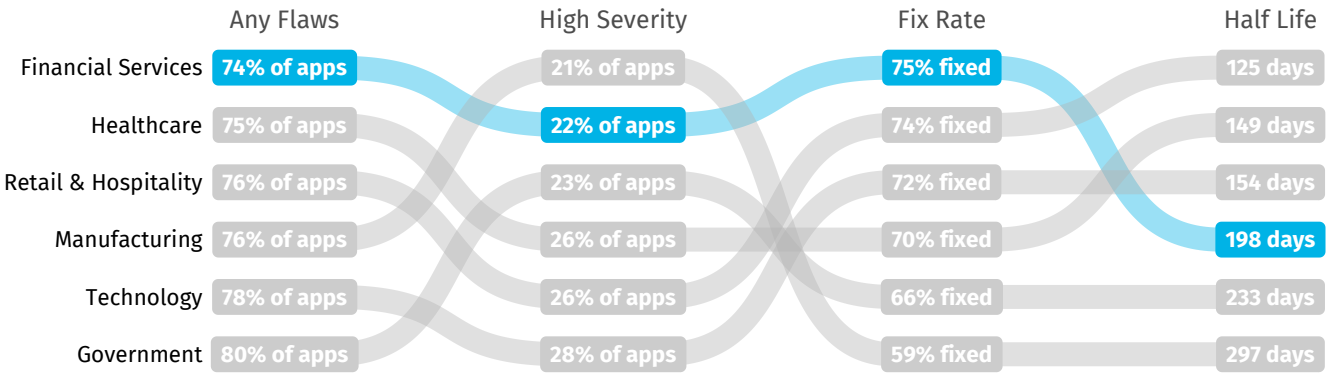

Figure 1: Values and rankings for key software security metrics by industry.

In Figure 2, we show a more detailed view of the types of flaws discovered in applications. The left axis shows the overall prevalence of each flaw category across all sectors, and the right axis shows the prevalence of the category for the financial services industry. The figure shows that the prevalence of these common flaw types tends to trend lower in this sector for all categories compared to the overall figures. Developers in the financial services industry appear to do a better job than others when dealing with issues related to cryptography, input validation, Cross-Site Scripting, and credentials management – all things related to protecting users of financial applications.

In this year's SOSS, we see strong evidence that certain developer behaviors associated with DevSecOps yield substantial benefits to software security. In Volume 10, we discovered that teams scanning applications most frequently carry five times less security debt than infrequent scanners. In this volume, we see other developer actions also make a difference in fixing flaws in software.

For example, we looked at the impact that application attributes and the development environment can have on how quickly flaws are fixed in software. There are some attributes that developers have no control over and others, such as best practices, that developers can influence.

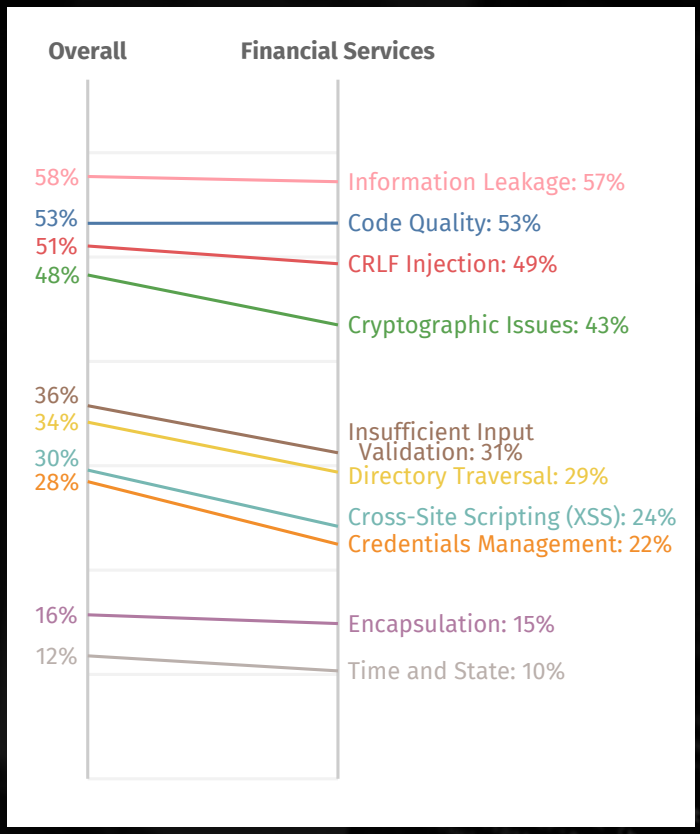

Figure 2: Prevalence of flaw categories in the financial sector

In Figure 3, we look at how financial service companies compare with companies in other industries in their development attributes (nature) and utilizing helpful developer behaviors (nurture). The data shows that financial services firms are all over the place for behaviors and attributes. The development environment is challenging for financial services firms, as their applications tend to be older than those in other industry sectors and the organizations are fairly large.

While applications tend to be smaller, the flaws are spread throughout the application (a middling ranking of flaw density). Behaviors are also haphazard, as financial services firms seem to be middle-of-the-road for scanning frequency and integrating security testing but are very consistent with the cadence of their scanning activities. They are not likely to be using dynamic analysis scanning technologies to uncover vulnerabilities but are the best at using software composition analysis (SCA) compared to other industry sectors. This suggests that for many financial services firms, developers face a challenging environment, with the adoption of additional DevSecOps practices showing the most opportunity for improvement.

In the most recent SOSS, we see that certain factors are likely to lead to flaws getting fixed faster, and others lead to slower fixes. Industry is something developers don't have control over, so how does being part of the financial services industry affect time to remediate flaws?

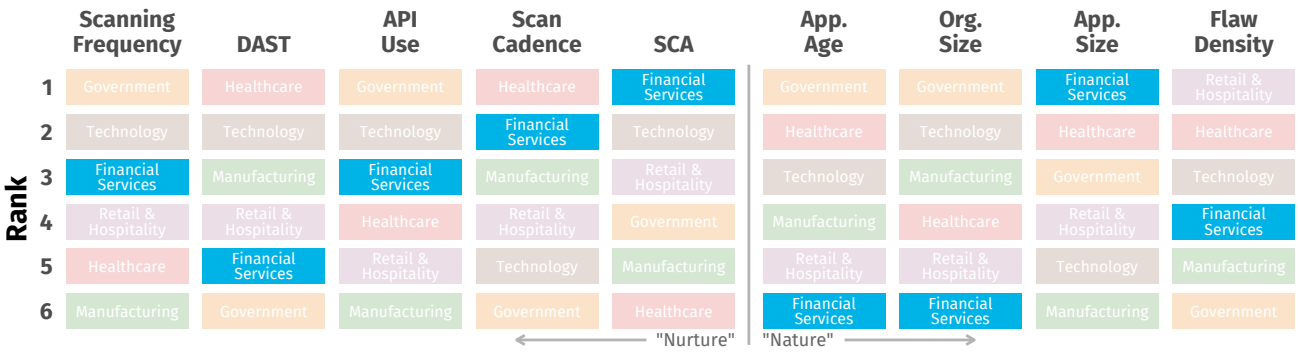

Figure 3: Relative ranking of the financial sector for attributes and actions associated with application security performance

Overall, remediation is slower for financial services firms. Figure 4 shows us that being in the financial services industry, all else being equal, means that a firm is more likely to be slow in remediating flaws. We saw in Figure 3 that developers in financial services are dealing with a challenging environment and are not consistently following DevSecOps practices compared to other industries.

The combined effects of nature and nurture indicate remediation efforts among financial services firms tend to result in flaw fixes being deployed more slowly than average. This may partially explain why the median time to remediation back in Figure 1 was so long, despite having a high fix rate compared to other sectors. It goes to show that when developers can't control their environment and don't adopt best practices for secure coding, there is a negative impact on software security.

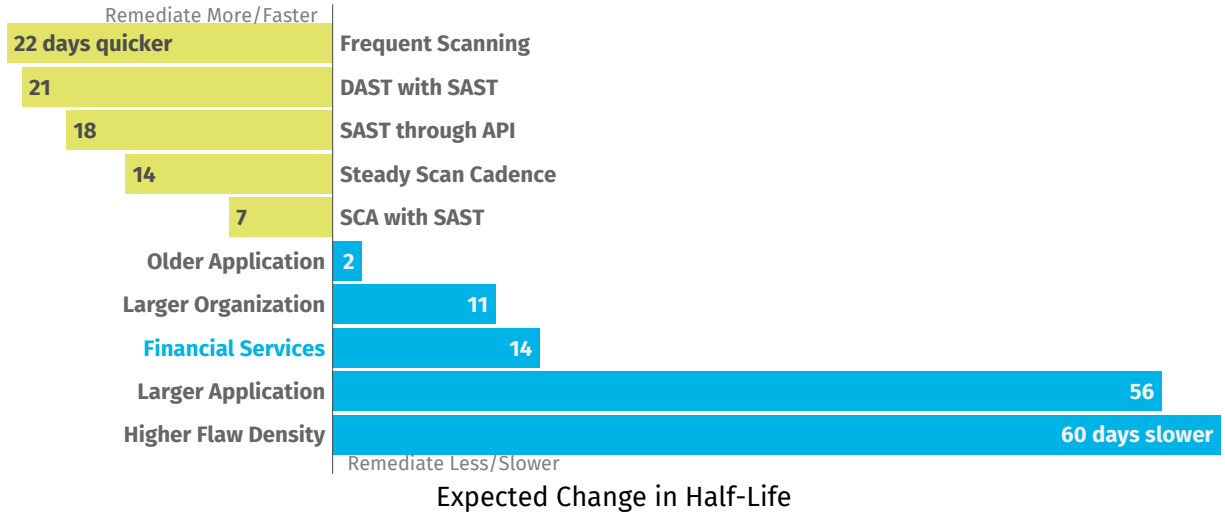

Figure 4: Remediation factors...

VERACODE

Veracode is the leading AppSec partner for creating secure software, reducing the risk of security breach and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities. Veracode serves more than 2,500 customers worldwide across a wide range of industries. The Veracode cloud platform has assessed more than 14 trillion lines of code and helped companies fix more than 46 million security flaws.

www.veracode.com **Veracode Blog** **Twitter**

Read the Full Report

TO LEARN MORE ABOUT SOFTWARE SECURITY, CONTACT US.