VERACODE

VOLUME 12

The State of Software Security Industry Snapshot: Retail

Veracode's State of Software Security (SOSS) Volume 12 examines historical trends shaping the software landscape and how security practices are evolving along with those trends. The data collected from 20 million scans across half a million applications suggests that we're making good progress toward the goal of producing more secure software.

This SOSS snapshot provides a view of software security in the retail sector. We hope it brings the findings a little closer to home so you can better refine your application security (AppSec) program based on the most relevant data. Let's start things off with Figure 1, which provides some core comparative metrics for the state of software security in the retail industry.

Starting on the left, retailers hold their own in terms of proportion of applications with any security issues as well as with high-severity flaws. The industry takes second place for the highest proportion of those flaws that are fixed, though the percentages are quite low across the board and show little variation. It appears that all organizations, retailers included, would benefit from efforts to address software flaws in a more comprehensive manner.

The rightmost columns rank industries according to how quickly they fix flaws once they're detected by three different types of scans. Retailers boast industry-leading fix times for flaws discovered by dynamic analysis (DAST) and land in the middle of the pack for static (SAST), and software composition analysis (SCA) scans. However, the number of days required to get to the halfway point for all scan types shows there's still ample room for continued improvement.

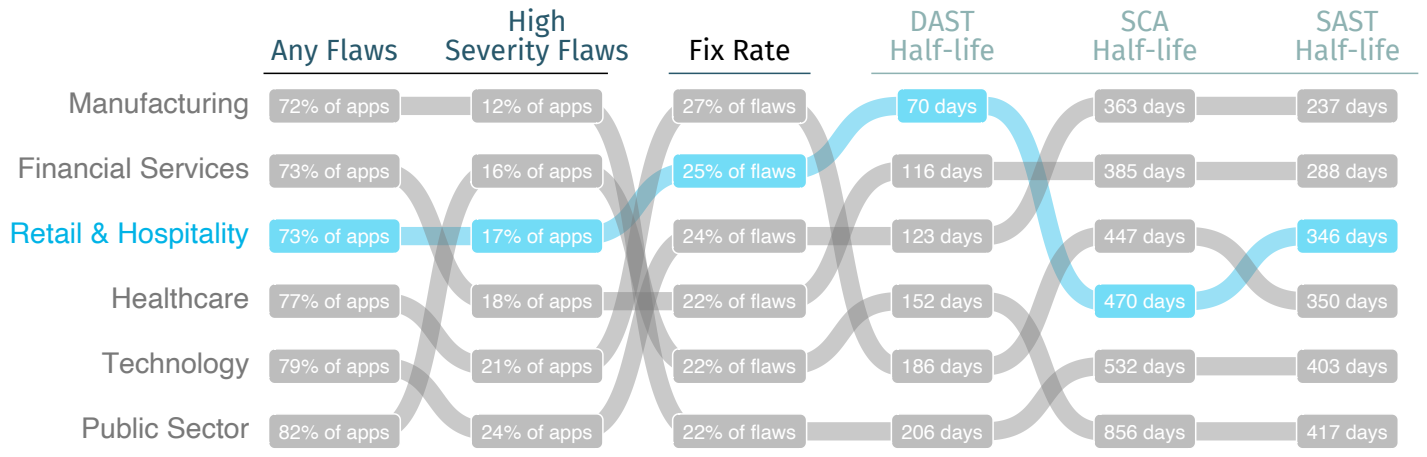

Figure 1: Values and rankings for key software security metrics by industry

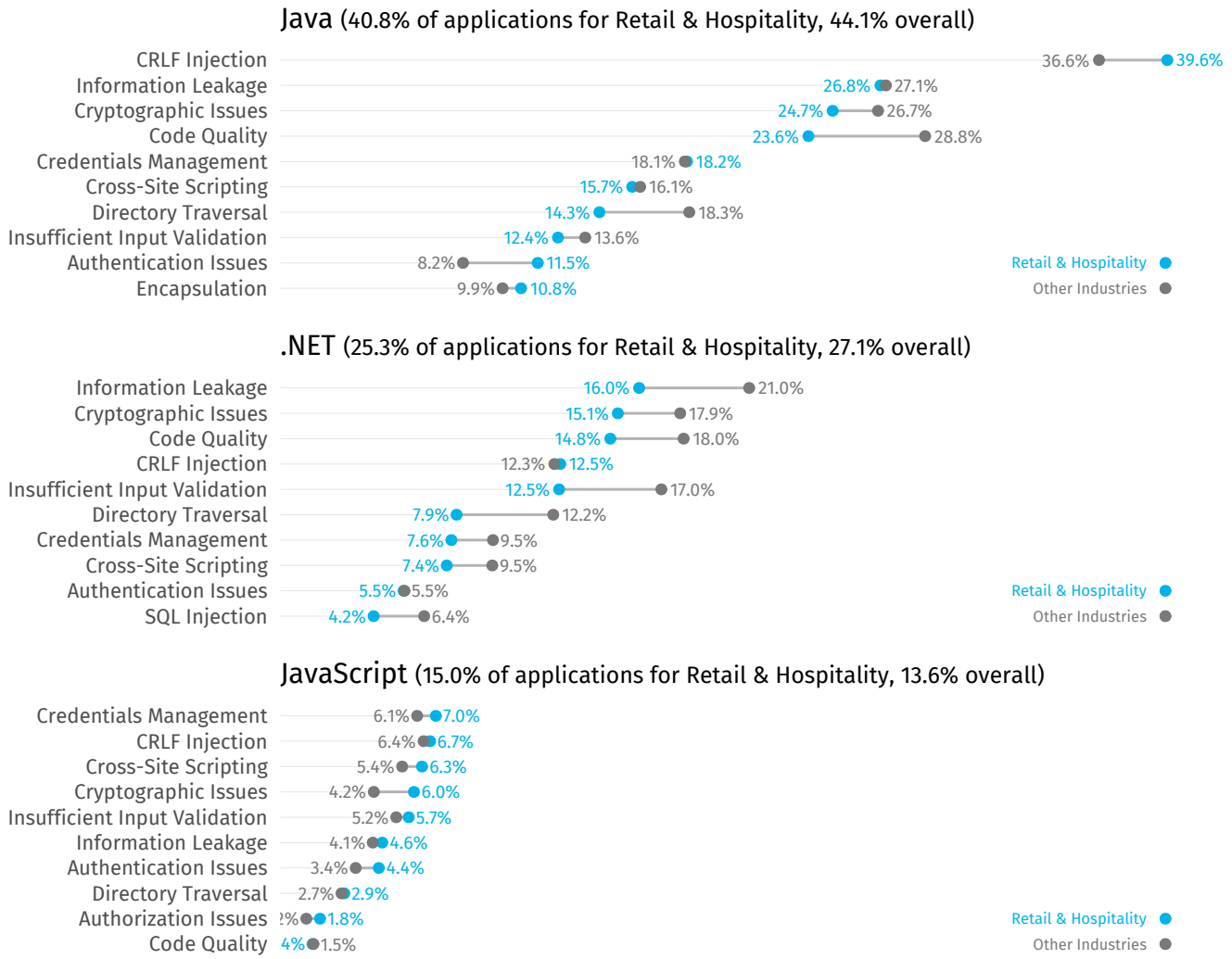

Figure 2: Most common flaws from static analysis in the retail sector.

Having compared overall flaw and fix rates, let's take a look at the most common types of flaws affecting applications. Because flaws found by SAST are very language-dependent, Figure 2 separates results by the top three programming languages used among applications in the retail sector. The chart makes it easy to determine whether retailers (in blue) have higher or lower rates than the overall average (in gray) for each type of flaw. Results for the retail sector are mixed for Java applications, better than par for .NET, and slightly subpar for JavaScript. There's a lot of information to digest here, so we'll leave you to develop your own takeaways.

Unlike SAST, DAST findings are largely consistent across languages, leading us to combine the findings into one chart. Retail follows a similar pattern to that of other industries in terms of which flaws are commonly vs. rarely identified by dynamic analysis. The percentages for the retail sector are higher for all categories save one (server configuration), perhaps due to greater functional complexity inherent to customer-facing and back office applications.

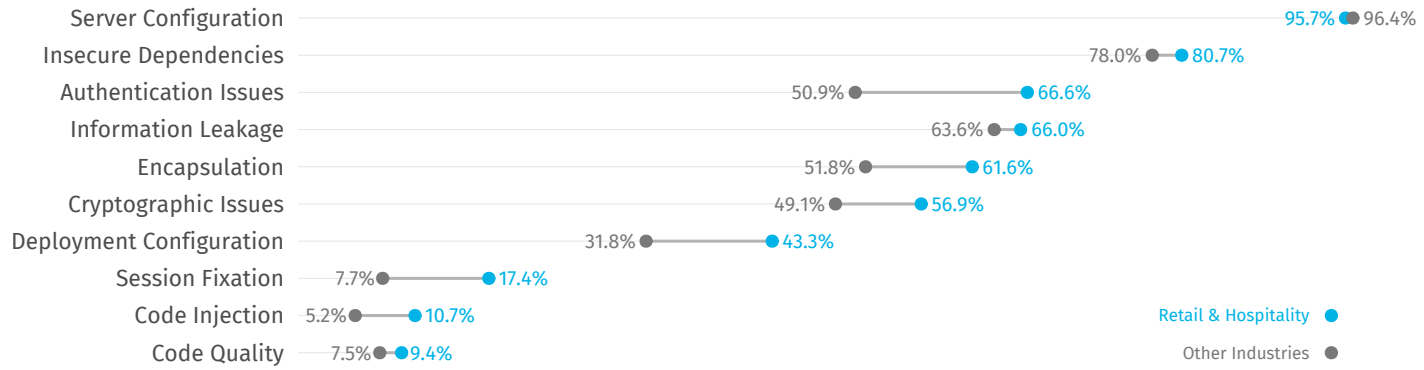

Figure 3: Most common flaws from dynamic analysis in the retail sector.

Next, we'll offer a few charts that expand on the half-life stats presented back in Figure 1. The number of days required to fix half the flaws in an application is a simple, benchmark-worthy stat, but what if you're curious about the comprehensive life-cycle of software security issues? Good news – Figure 4 enables exactly that using a method known as survival analysis!

Triangulating any point along the survival curve gives the percentage of flaws still "alive" after a period of time following discovery (e.g., ~55 percent still unresolved after one year). The retail sector is clearly experiencing challenges here, consistently lagging three months behind the overall average across the entire lifecycle of software flaws according to SAST. For DAST, retailers are faster out of the gate and hang onto that lead for the duration. That's something to be proud of.

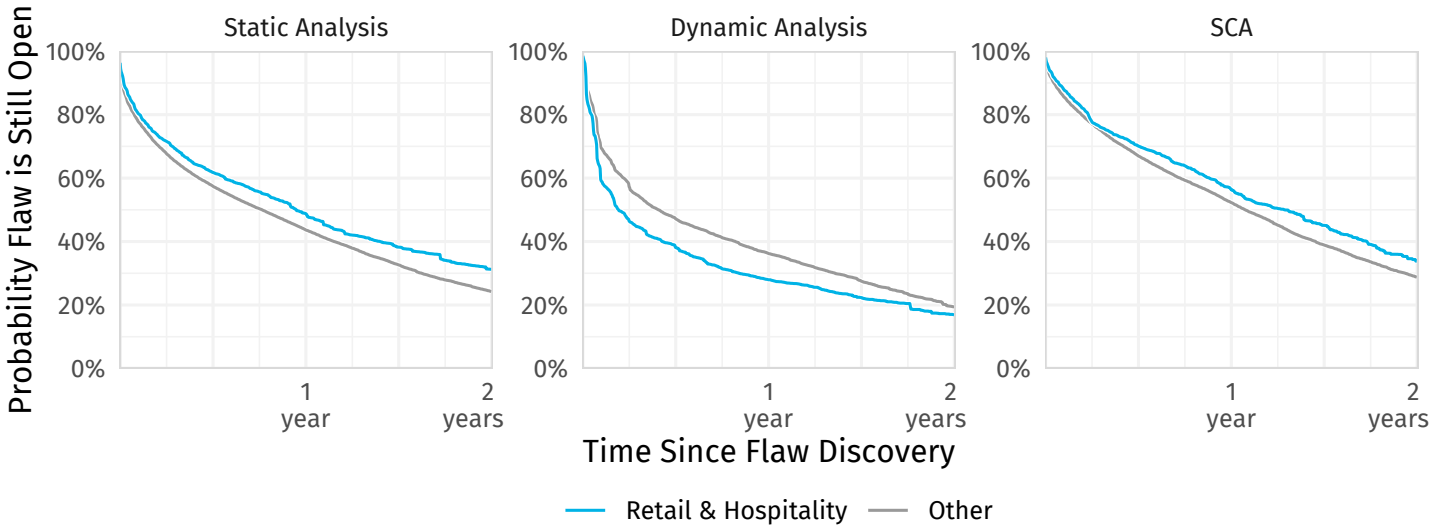

Figure 4: Two-year flaw survival rates for applications in the retail sector.

Flaws in third-party libraries found through SCA stick around longer for all industries, and even longer among retailers. Overall, about 30 percent of vulnerable libraries remain unresolved after two years. For the retail sector, that statistic rises slightly to 35 percent and lags the cross-industry average by over six months. Be assured that the gap is not so wide that it cannot be closed.

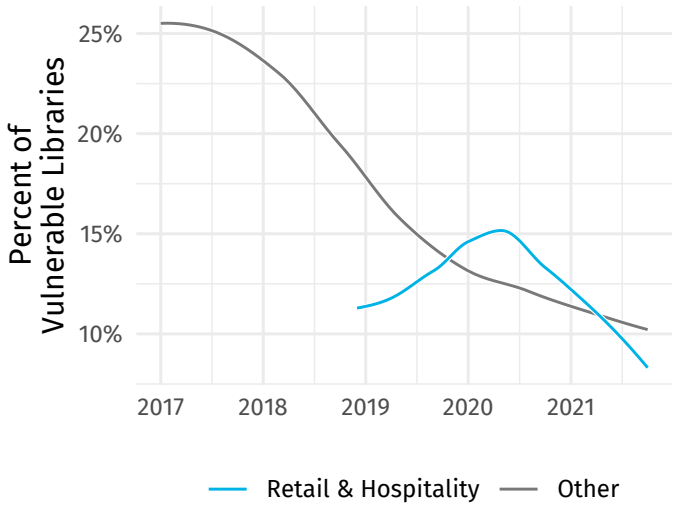

Figure 5: Proportion of vulnerable libraries used by applications in the retail sector.

Speaking of vulnerable libraries, you're probably aware that the software supply chain is kind of a big deal these days. This last chart shows the extent of flaws in third-party code discovered via SCA. The overall ratio trends down over time, with retailers experiencing a bit of a bump before driving rates down over the last year or so. It's nice to end on a good note, and we hope retailers see this as a welcome ray of sunshine amidst the all-too-often gloomy realm of software security. Here's to more clear skies in the years to come!

VERACODE

Veracode is a 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 process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Learn more at **www.veracode.com**, on the **Veracode blog**, on **LinkedIn**, and on **Twitter**.

Copyright © 2022 Veracode, Inc. All rights reserved. All other brand names, product names, or trademarks belong to their respective holders.

Read the Full Report