VERACODE

VOLUME 11

The State of Software Security

Industry Snapshot: Retail & Hospitality

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 retail & hospitality 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 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. Retailers and hospitality firms have an interesting story, as they are in the middle for the proportion of applications with flaws but have the second-largest proportion of applications with severe security flaws.

That isn't a good place to start, but the remediation side of the story is much better, as the fix rate for the retail and hospitality industry ranks second-best and median time to remediate is the best compared to other industries, with a half-life time of just 125 days. So, while they may start out with comparatively more security flaws, retailers and hospitality companies do much better digging out of the hole and closing flaws quickly. With the need to respond rapidly to consumer demands, the retail and hospitality sector seems to be emulating that nimbleness with fixes to their applications.

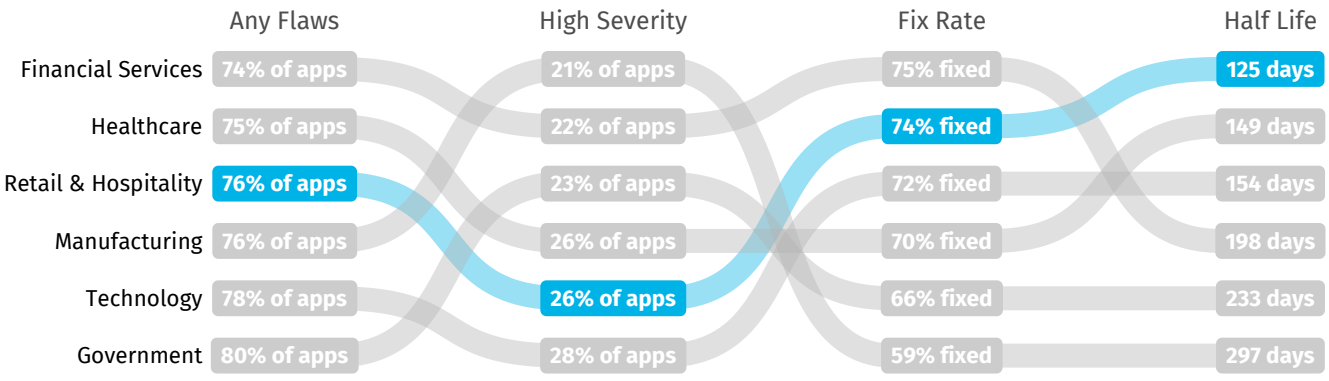

Figure 1: Values and rankings for key software security metrics by industry.

In Figure 2, we show a more detailed view of the flaw types 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 retail & hospitality 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 retail & hospitality sector appear to do a better job than others when dealing with issues related to information leakage and input validation (perhaps because of a strong focus on controls around shopping cart applications), but struggle significantly with encapsulation, SQL injection, and credential management issues.

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.

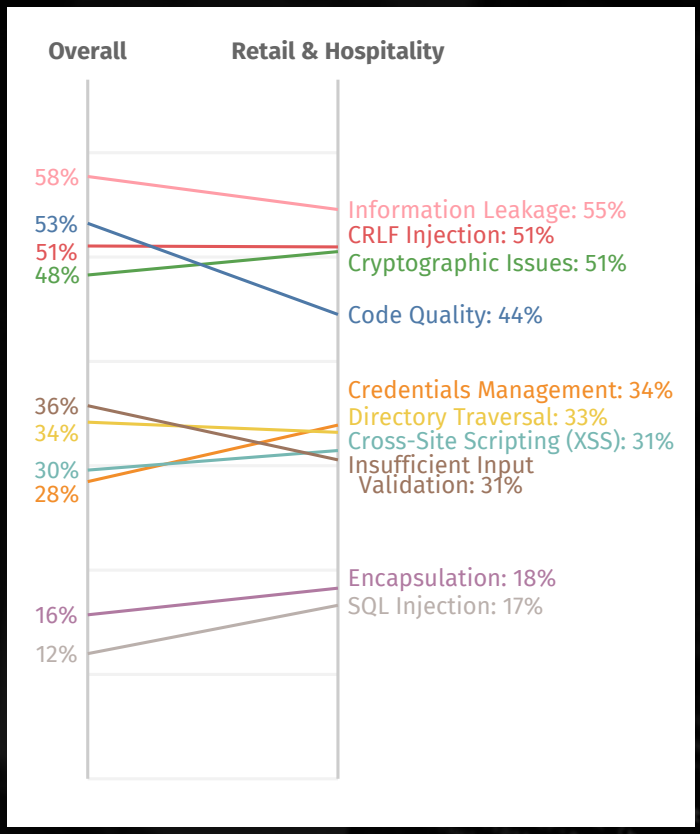

Figure 2: Prevalence of flaw categories in the retail & hospitality sector

In Figure 3, we look at how retail & hospitality companies compare with companies in other industries in their development attributes (nature) and utilizing helpful developer behaviors (nurture). The data shows that retail firms generally lag on both behaviors and attributes. The development environment is challenging for retail and hospitality firms, as their applications tend to be older than those in all other sectors save finance, with the overall size of the applications to be larger than many other sectors as well.

Despite these early concerns, the flaws found in retail and hospitality applications show a lower density than all other industries. Behaviors are very middle-of-the-road, with use of API-driven scanning being worse than average while software composition analysis (SCA) is slightly better than average compared to other sectors. This suggests that for many retail and hospitality 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 retail & hospitality industry affect time to remediate flaws?

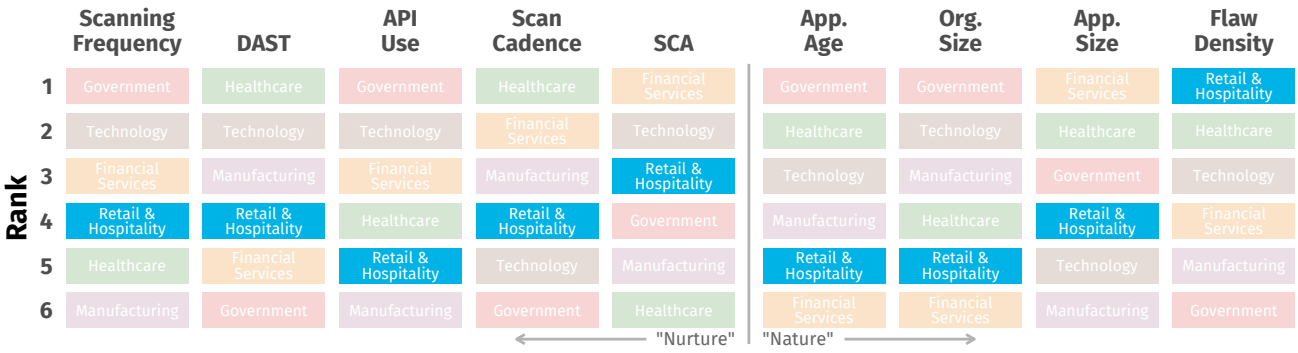

Figure 3: Relative ranking of the retail & hospitality sector for attributes and actions associated with application security performance

The picture for this sector is strikingly positive! Figure 4 shows us that being in the retail & hospitality sector means the organization is significantly faster than overall rates in remediating flaws. We see hints of this in Figure 1, with a median time to flaw remediation of 125 days, or approximately four months. Figure 4 suggests that even though developers in the retail & hospitality sector achieve a low flaw density relative to other sectors, applications with high security debt are still a hindrance to their efforts to quickly address buggy code. Retail & hospitality organizations were generally under par in Figure 3, in terms of which DevSecOps behaviors had been adopted, so there is plenty of room for improvement.

We clearly see the impact of erratic best practices on a fairly positive environment in Figure 4 as the data trends toward slower flaw remediation. It goes to show that when developers don't consistently utilize best practices for secure coding, there is a negative impact on software security even when the circumstances are somewhat in favor of the developers.

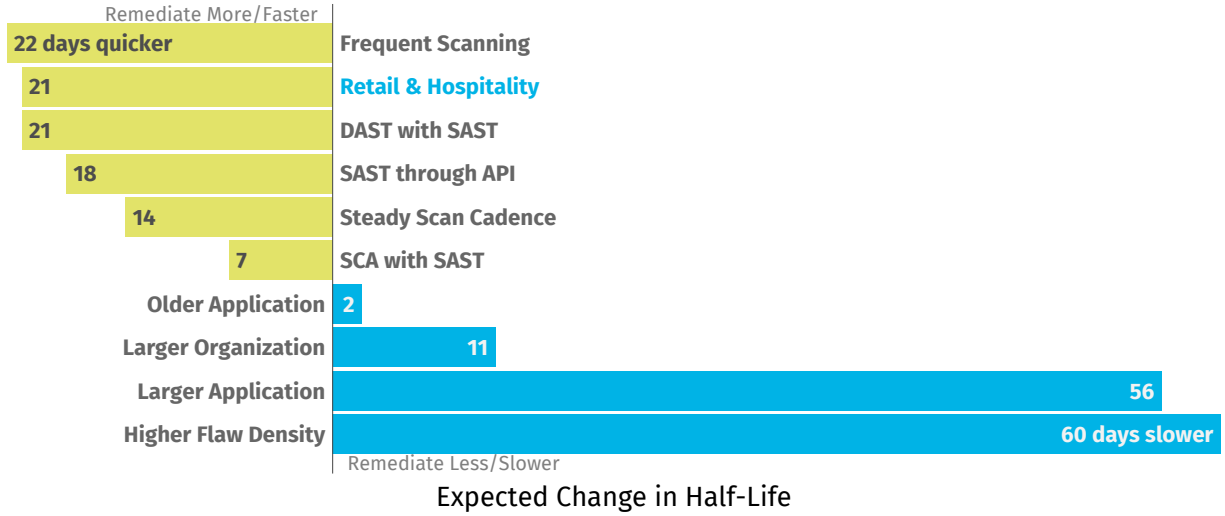

Figure 4: Remediation factors...