

SOSS VOLUME 10 INDUSTRY SNAPSHOT

Government and Education

Veracode's State of Software Security (SOSS) Volume 10 focused on the topic of security debt, defined as the amount of unaddressed flaws that accumulate in software over time. The report revealed about half of application teams added to their security debt, a little over a quarter paid it down, and a

quarter maintained a steady balance. As you might suspect, our analysis showed that debt profiles differed substantially among industries. This infosheet provides a summary of factors that shape the debt profile exhibited in the chart below for the Government and Education sectors.

Figure 1: Comparison of fix capacity and security debt by industry

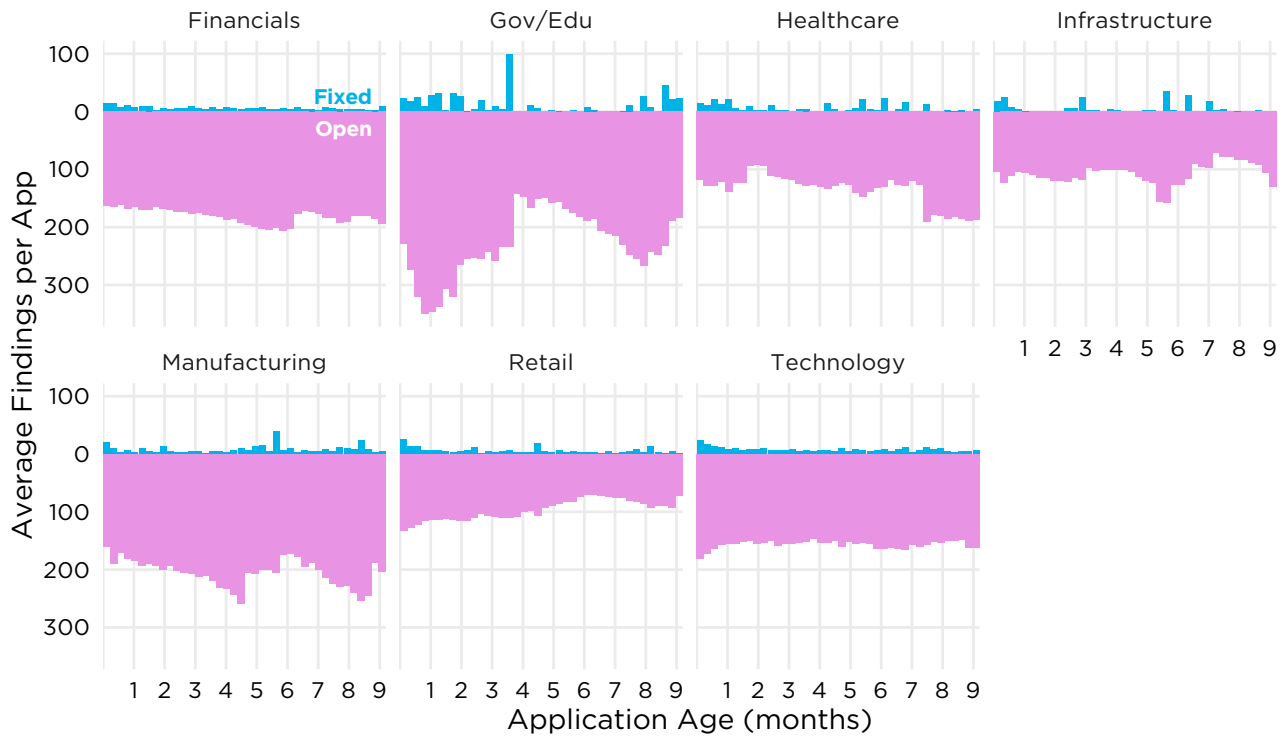
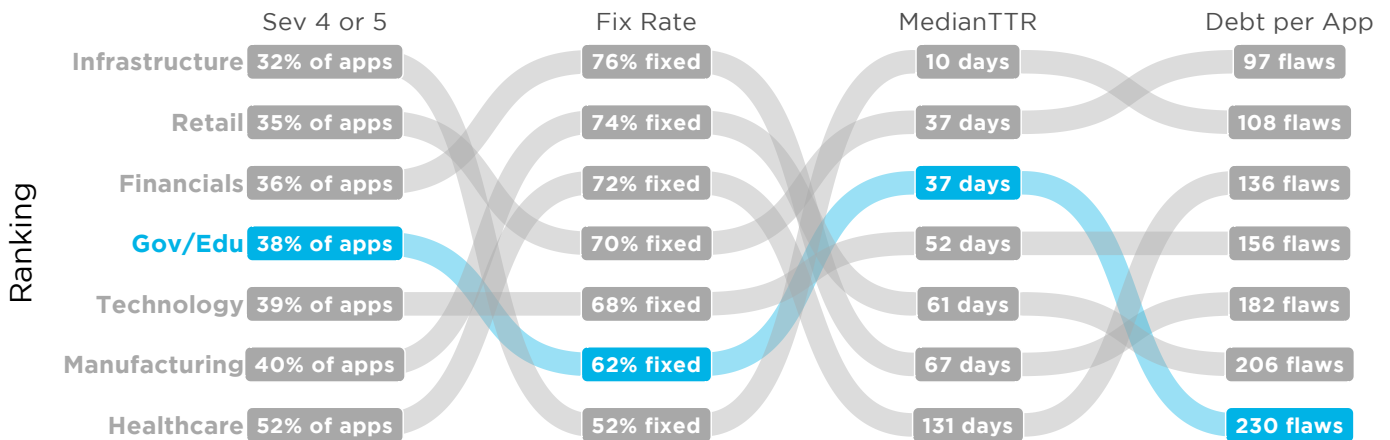


Figure 1 models the mechanics of security debt in a typical application. The dark blue bars on top correspond to weekly flaw closures. The pink area tallies the average number of unresolved flaws carried over each week. Per the figure, Gov/Edu exhibits the largest “iceberg” of debt lurking below the surface during the period. Let’s dig in and see what’s going on there.

Figure 2 ranks the Government and Education sector according to several key measures from our software security testing over the last year. Proceeding from left to right, the columns shed light on debt creation, starting with the proportion of applications with higher-severity (level 4 or 5) flaws, the percentage of those flaws that are fixed, the median speed at which those flaws are fixed, and the average amount of unfixd flaws (debt) per application.

Figure 2: Values and rankings for key software security testing metrics by industry

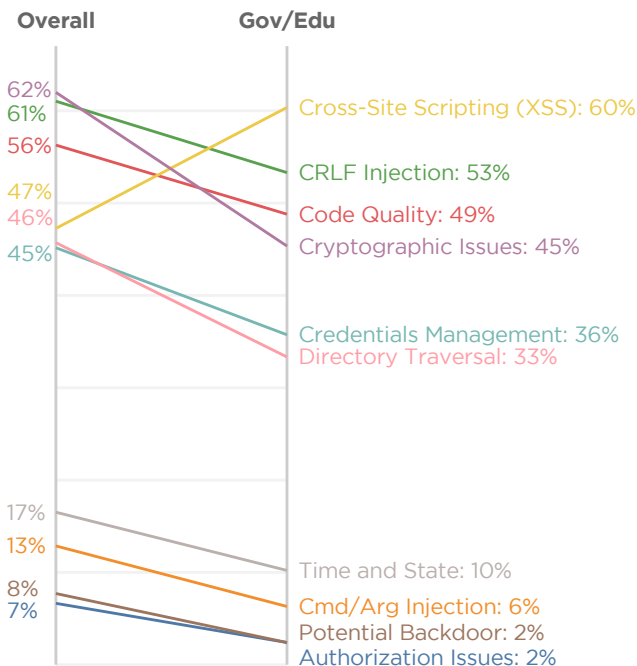


Source: Veracode SOSS Volume 10

Government and Education institutions fall in the middle of the pack for the prevalence of severe flaws and next to last in terms of fixing those flaws. The next two columns repeat that

pattern, with a mid-level ranking for typical remediation time frames and an industry-leading level of security debt that's an average 2.4X higher than that of the Infrastructure sector.

Figure 3: Prevalence of flaw categories in the Government/Education sector



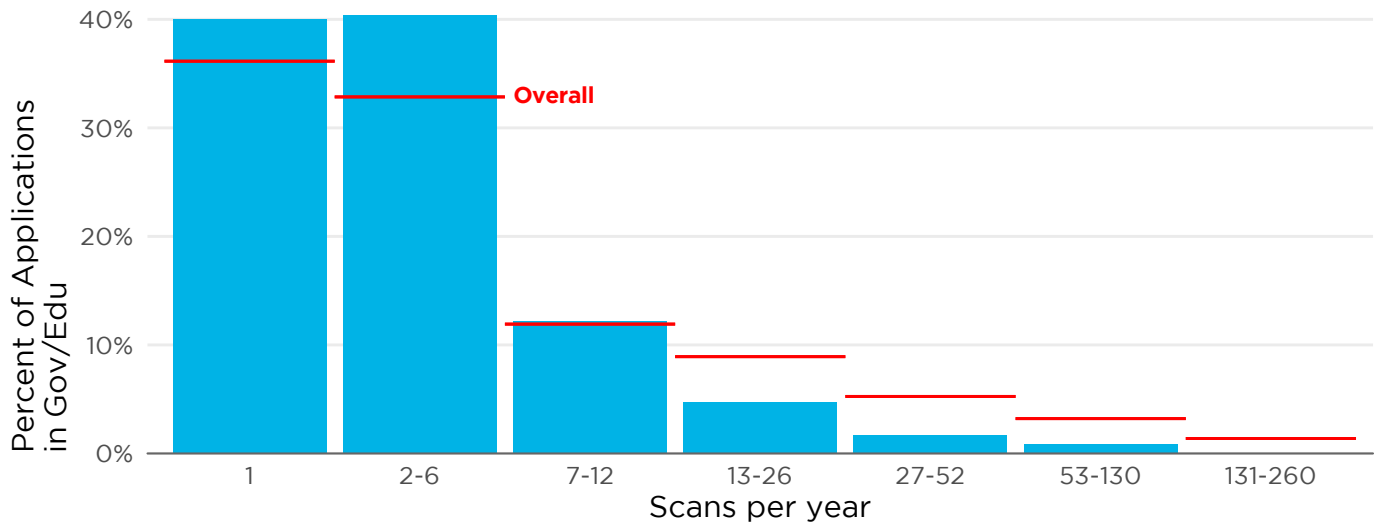
Source: Veracode SOSS Volume 10

A more detailed view of flaws discovered in Government and Education applications can be found in Figure 3. The left column marks the overall prevalence of each category across all sectors and the right traces the comparable statistic for Gov/Edu.

The categories toward the bottom of Figure 3 change in value but retain their ranking. The action takes place up top, where we see some crossing lines. The rate of XSS flaws jumps up significantly, and crypto issues make the biggest move in the opposite direction. Overall, nine of the top 10 flaws show a lower prevalence for Gov/Edu, which is perhaps counterintuitive given Figure 2.

The preceding figures give us an informative snapshot of how Government and Education performs in key software security measures, but they don't tell us much about what's driving those outcomes. Over the last two years, our research in the SOSS has uncovered strong evidence that practices in keeping with a DevSecOps approach yield substantial benefits to development teams that employ them. In Vol. 9, we discovered that the most active DevSecOps programs fix flaws more than 11.5x faster than the typical organization. The most recent SOSS found that teams scanning applications most frequently carry about 5X less security debt than infrequent scanners. So, how does Government and Education compare? Figure 4 has the answer.

Figure 4: Frequency of application security scanning in the Government/Education sector



Source: Veracode SOSS Volume 10

All industries show a skewed distribution for scanning frequency, with about 80 percent of applications scanned 12 times per year or less. That ratio is over 90 percent for the Government and Education sector, which helps explain why

that sector struggles to pay down security debt. Just like your personal credit card, it's hard to make a dent in the amount of debt if you only make a few payments per year.



READ THE FULL REPORT
[VERACODE.COM/SOSS](https://veracode.com/soss)

VERACODE

Veracode 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 life cycle, before they can be exploited by hackers. Our complete set of offerings helps 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 more than 1,400 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 Forbes' 100 Most Valuable Brands. Learn more at www.veracode.com, on the Veracode blog, on Twitter and in the Veracode Community.

Copyright © 2019 Veracode, Inc. All rights reserved. All other brand names, product names, or trademarks belong to their respective holders.