Contrast SECURITY

MARCH–APRIL 2021

Contrast Labs Application Security Intelligence Bimonthly Report

Table of contents

01 | Executive Summary

The Contrast Labs Application Security Intelligence Report for March–April 2021 is based on aggregate vulnerability and attack telemetry for custom code from customers whose applications are covered by Contrast Assess and Contrast Protect. Its purpose is to help application security and development teams to effectively prioritize their application security efforts by highlighting trends in both vulnerabilities and attacks.

As private- and public-sector organizations around the world recover from recent attacks such as those on SolarWinds Orion and Microsoft Exchange Server, application attacks and supply chain breaches continue unabated. Several social media networks were impacted in March and April, as were hospital systems and a technology company that holds the data of millions of airline travelers. In our data, things look slightly better overall when it comes to vulnerabilities, and somewhat worse regarding attacks.

Contrast RiskScore™. This objective measurement of the relative risk of different vulnerability types found that four of the five riskiest remained the same for March–April: broken access control, cross-site scripting (XSS), insecure configuration, and sensitive data exposure. The fifth-highest RiskScore for this bimonthly period is broken authentication, which pushed SQL injection out of the top five. Further down the list, insecure deserialization returned to the top 10 after being less risky than the top 15 vulnerabilities in January–February.

Top 5 Contrast Riskscores

BROKEN ACCESS CONTROL

CROSS-SITE SCRIPTING (XSS)

INSECURE CONFIGURATION

SENSITIVE DATA EXPOSURE

BROKEN AUTHENTICATION

Average RiskScore: 5.06,
down from 6.28 in July 2020

Vulnerability Trends. The percentage of applications containing at least one serious vulnerability decreased to 32% in March–April, but this number is still higher than in any month before November 2020. The percentage of applications with more than 20 serious vulnerabilities decreased to 6%, which is again close to long-standing averages. The percentage of overall vulnerabilities that were serious also declined slightly.

The data for March–April contains some good news for .NET users, who had seen significant increases in vulnerabilities for several months. For this bimonthly period, the percentage of .NET applications with at least one serious vulnerability declined from 28% to 23%. This number decreased from 39% to 37% for Java applications.

32%

of applications have at least one serious vulnerability, down from 34% in January–February

6%

of applications have 20+ serious vulnerabilities, down from 7% in January–February

38%

of overall vulnerabilities are serious, down from 39% in January–February

Attack Trends. The percentage of attacks that were viable—that is, attacks that hit an actual vulnerability in a piece of software—increased dramatically for Java applications after hitting a record low in January–February, when the percentage was at less than 0.5%. Fully 3 in 100 attacks on Java applications were viable in March–April, near the highest percentage observed by Contrast Labs.

Broken access control attacks impacted 86% of applications in this bimonthly period, and XSS attacks increased from impacting 29% of applications to 55%. These two attack types account for 82% of all attacks in March–April.

9%

average increase in percentage of applications impacted by specific attack types

3%

of attacks on Java applications were viable, up from less than 0.5%

90%

increase in percentage of applications impacted by XSS attacks

Takeaways. Our analysis of data from real applications reveals several interesting trends with both vulnerabilities and attacks. While vulnerability numbers are down somewhat, they remain too high. At the same time, all eyes are on application security after several massive attacks and a recent executive order from the White House. Everyone is in agreement that software security is a critical priority for national security and the economy.

The only way for organizations to improve their application security posture is to "shift left" and "shift right." Shifting left means discovering vulnerabilities in real time rather than days or weeks after they are introduced. This enables problems to be fixed as they occur and eliminates security-related delays to development. Shifting right involves focusing on attack visibility and exploit prevention in production. Security instrumentation is the best way to accomplish these simultaneous shifts, by embedding continuous security testing within the application itself.

02 | Software Security Breaches are Catalyst for New Standards

Contrast Labs' bimonthly Application Security Intelligence Reports aim to help development and security teams prioritize their application security efforts to deliver more secure applications for customers, partners, and co-workers. Every two months, we highlight trends in both software vulnerabilities and application attacks, based on telemetry data from applications using Contrast Assess during development and Contrast Protect in production. Contrast Labs' analysis helps readers understand the evolving risk posed by different kinds of vulnerabilities.

As IT and security leaders continued in March and April to deal with the aftermath of recent attacks on SolarWinds Orion and Microsoft Exchange Server, social media networks were hit with data-scraping attacks potentially impacting 533 million users on Facebook,[1] 500 million users on LinkedIn,[2] and 1.3 million users at social audio startup Clubhouse.[3] In each case, perpetrators posted some or all of the records publicly online, with the LinkedIn attackers posting 2 million samples and attempting to sell the remainder on the dark web.

The healthcare sector continued to face attacks, with Washington-based MultiCare Health System seeing 200,000 patient and employee records exposed through its supply chain, when a subcontractor's systems were infiltrated.[4] And the Cancer Treatment Centers of America notified more than 100,000 patients at its Midwestern Regional Medical Center that some protected health information (PHI) was contained in a compromised email account.[5]

As air travel resumes in earnest for millions of people, a breach at airline technology provider SITA enabled hackers to access passenger data from multiple airlines globally, possibly including users of mileage programs across the Star Alliance.[6]

These incidents serve as reminders that the threat landscape remains dire and may be getting worse. The impact of the SolarWinds attack on federal government operations—including national security and top-secret activities—prompted the White House to issue an executive order in May, with the aim of placing stringent new cybersecurity requirements on the software and hardware used by the federal government and its contractors.[7] Application security is prominent throughout the order, as is protection of the software supply chain. One can only hope that these new requirements will prompt software vendors to develop solutions for the private sector that meet these federal standards.

03 | Contrast Riskscore™ for March—April 2021

As described in a recent report,[8] the Contrast RiskScore is a numerical score that provides a dynamic ranking of application vulnerability types based on real-world data about vulnerability prevalence and attack rates. The underlying algorithm, developed by Contrast Labs, is regularly refined to improve its accuracy.

This report applies the RiskScore algorithm to the entire dataset from all Contrast customers, which can be useful to security and development teams as they prioritize their application security activities. For a more individualized view, Contrast Labs is developing an open-source version of RiskScore that will be available soon. This will enable a more precise measurement of risk—down to the organizational level or even for each application.

For March–April, the top four vulnerabilities by RiskScore remained in the same order—broken access control, cross-site scripting (XSS), insecure configuration, and sensitive data exposure (Figure 1). In the fifth position is broken authentication, which moved from sixth to fifth position despite its RiskScore remaining flat (Figure 2).

SQL injection, which had the fifth-highest RiskScore in January–February, has seen volatility in its RiskScore over the past year, with a sharp downward trend—down from 8.87 in July 2020 (the second-highest score that month) to 5.37 in April 2021. Its bimonthly score of 5.49 for March–April moves SQL injection to the sixth position by just 0.02 points. The decline in the RiskScore for SQL injection occurs because it is both less likely to exist in applications and slightly less likely to be attacked when it does occur.

FIGURE 1

Top 15 vulnerability categories by Contrast RiskScore, September 2020–April 2021.

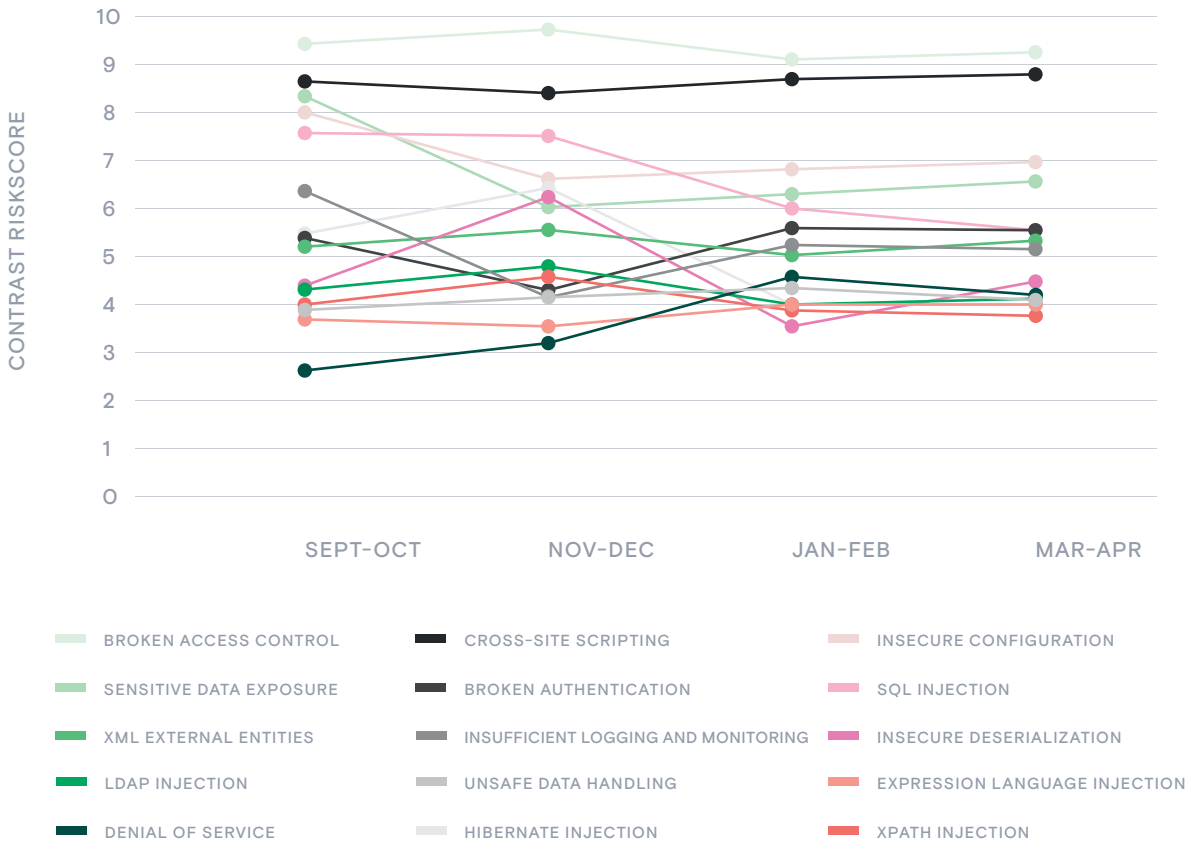
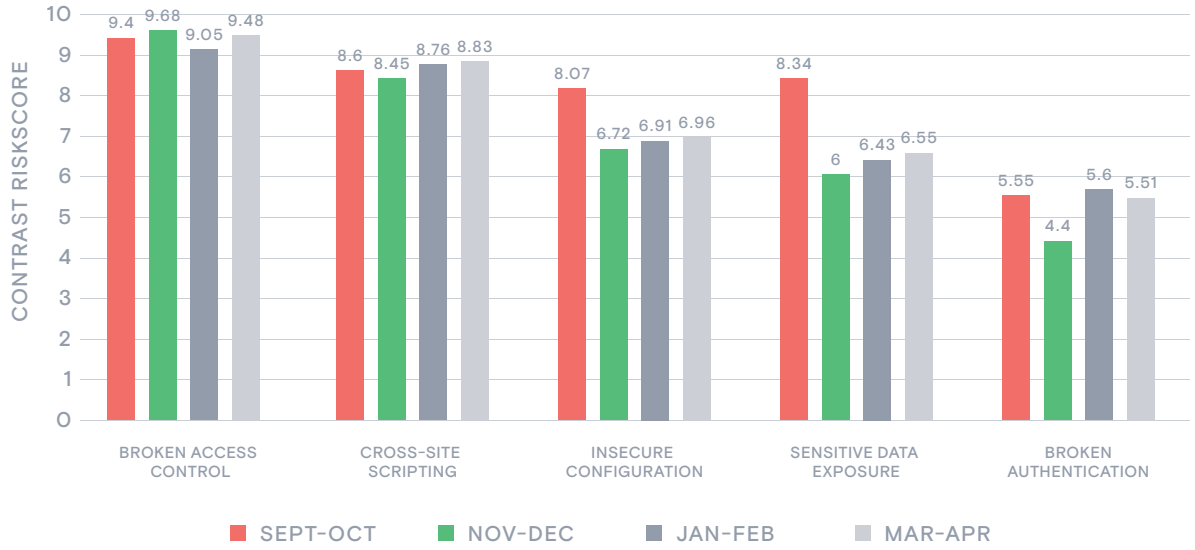


FIGURE 2

Top 5 vulnerability categories by Contrast RiskScore, September 2020–April 2021.



Further down the list, insecure deserialization returns to the top 10 with the ninth-highest score after its RiskScore increased by more than a point from the last bimonthly period, to 4.39. However, this is very much a reversion to the mean, as this vulnerability type has an average score of 4.96 during the eight months between July 2020 (when we first calculated RiskScores) and February 2021.

One long-standing trend continued in March–April: Overall RiskScores trended downward. The average RiskScore for all vulnerability types has declined from 6.28 in July 2020 to 5.06 in April 2021.

04 | Application Vulnerability Trends

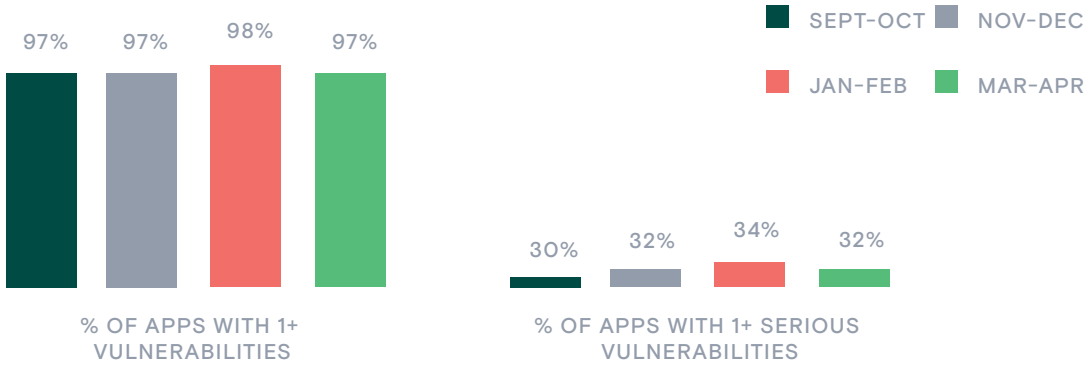
For custom code,[9] the overall vulnerability picture improved somewhat in March–April, perhaps because the Contrast customers in the dataset made headway in reducing their security debt. Contrast Labs noted the following application vulnerability trends during March–April 2021:

TREND: THE PERCENTAGE OF APPLICATIONS WITH SERIOUS VULNERABILITIES STABILIZED

At least one vulnerability occurred in 97% of applications, down from 98% in January–February but very close to the average over time (Figure 3). More importantly, at least one serious vulnerability—rated as High or Critical—was found in just 32% of applications in March–April, down from 34% in January–February, but still higher than any month prior to November 2020.

FIGURE 3

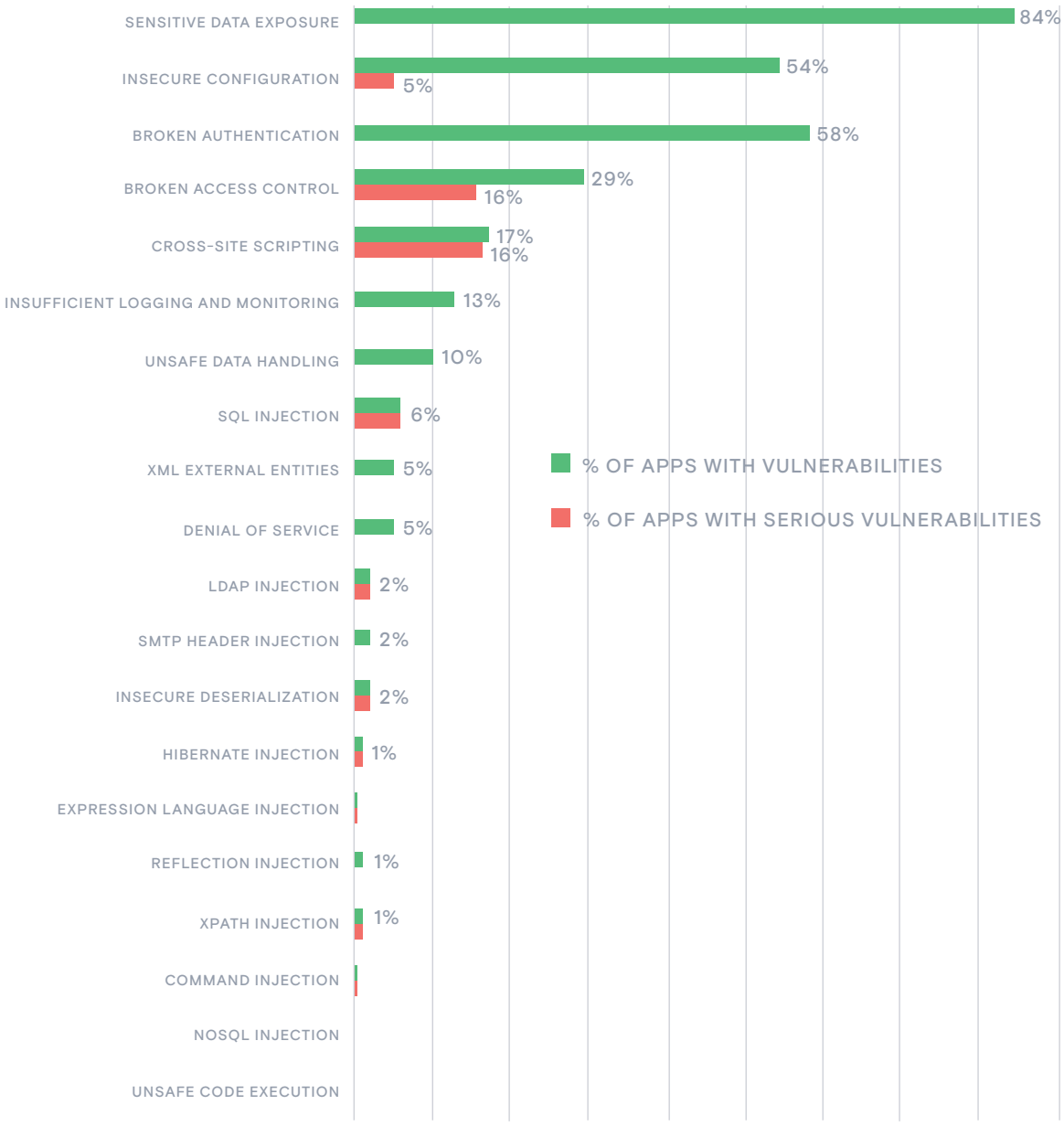
Percentage of applications containing at least one vulnerability and at least one serious vulnerability, four bimonthly periods.



Only two vulnerability types saw an increase in likelihood: insecure configuration and SMTP header injection (Figure 4). But the percentage of applications with serious insecure configuration vulnerabilities held steady at 5%, while no serious SMTP header injection vulnerabilities exist in the dataset. The top four vulnerability types all saw a decline in prevalence of one or two percentage points (Figure 5).

FIGURE 4

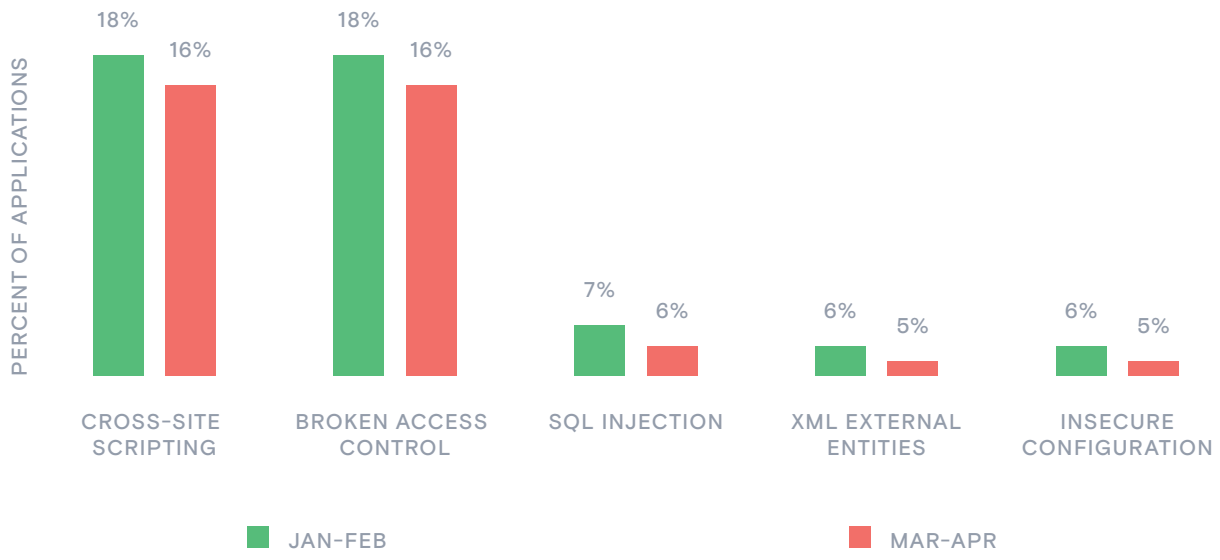
Percentage of applications with vulnerabilities and serious vulnerabilities, by category, March–April 2021.



Looking at all vulnerabilities in the dataset, the percentage that were serious declined from 39% in January–February to 38% in March–April (Figure 6), a small move back toward numbers in the high 20s and low 30s that were common in 2020.

FIGURE 5

Percentage of applications with serious vulnerabilities (top 5 most prevalent).

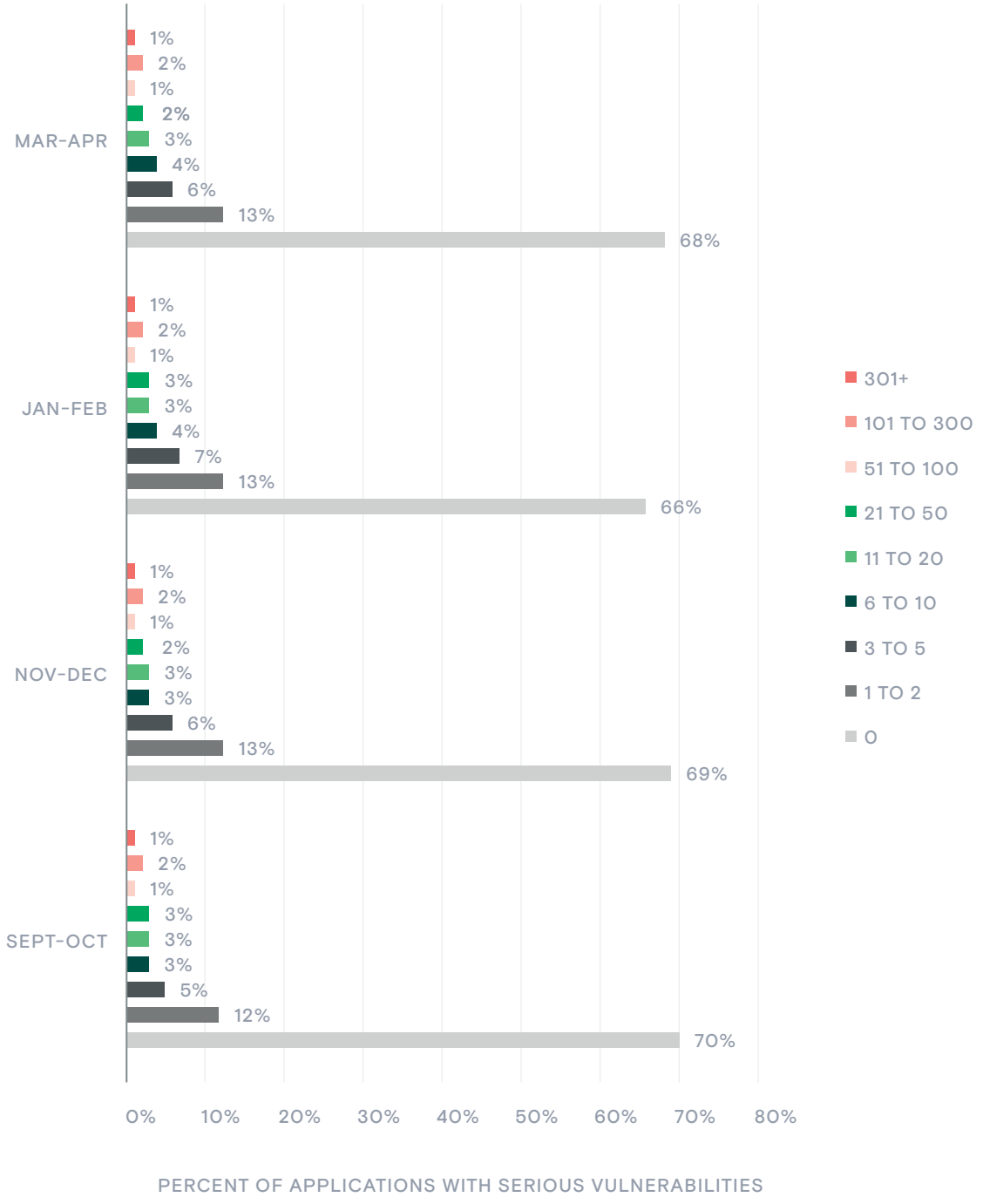


TREND: FEWER APPLICATIONS HAVE A LARGE NUMBER OF OVERALL VULNERABILITIES, BUT SERIOUS VULNERABILITIES HOLD STEADY

One consistent story that emerges from the data is that a relatively small subset of applications has a very large number of vulnerabilities—often well into the hundreds. Fortunately, the percentage of applications with more than 50 vulnerabilities declined from 11% to 9% compared with January–February (Figure 7). Similarly, the percentage of applications with more than 20 serious vulnerabilities declined from 7% to 6%.

FIGURE 6

Percentage of vulnerabilities that are critical or high, four bimonthly periods.



One result of this decline in applications with many vulnerabilities is that the average number of vulnerabilities found in a vulnerable application (that is, an application with at least one vulnerability) declined from 61 in January–February to 52 in March–April (Figure 8). Unfortunately, the same is not true of serious vulnerabilities. The number of serious vulnerabilities per vulnerable application actually increased from 58 to 59—a reversion to the mean.

FIGURE 7

Percentage of applications with different numbers of vulnerabilities, four bimonthly periods.

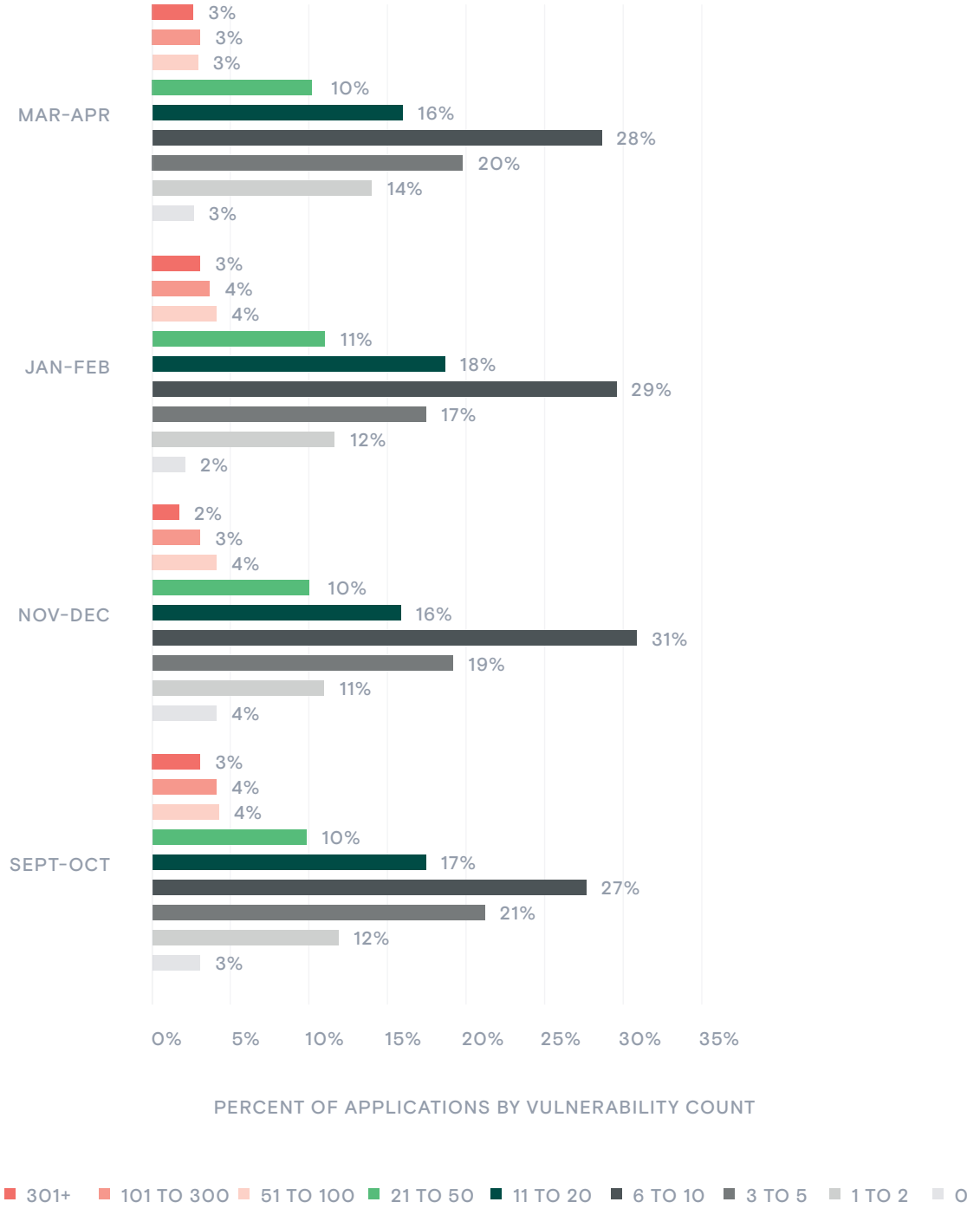
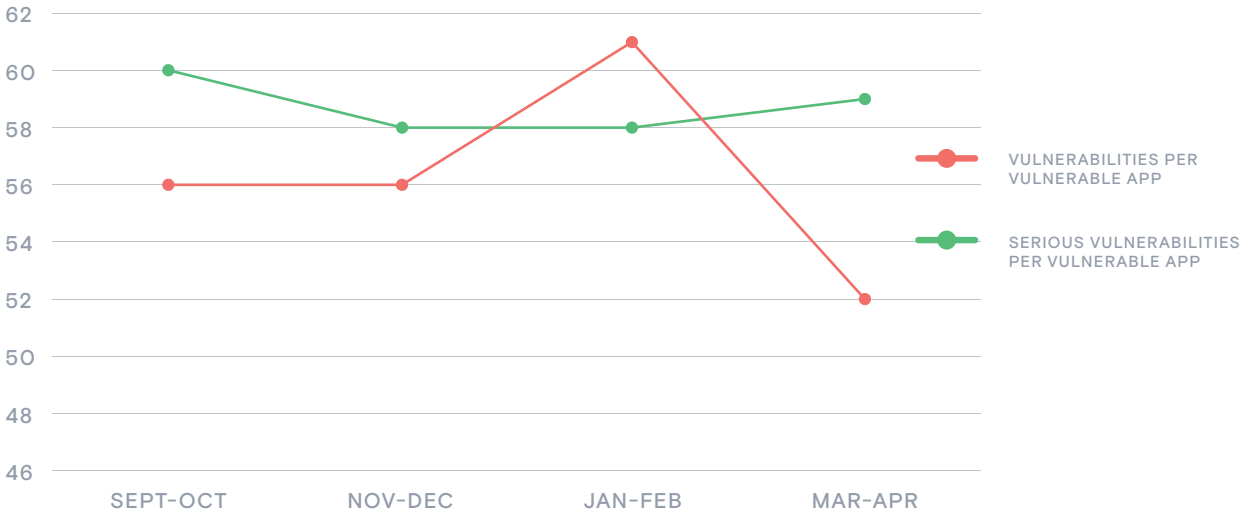


FIGURE 8

Vulnerabilities and serious vulnerabilities per vulnerable application, four bimonthly periods.

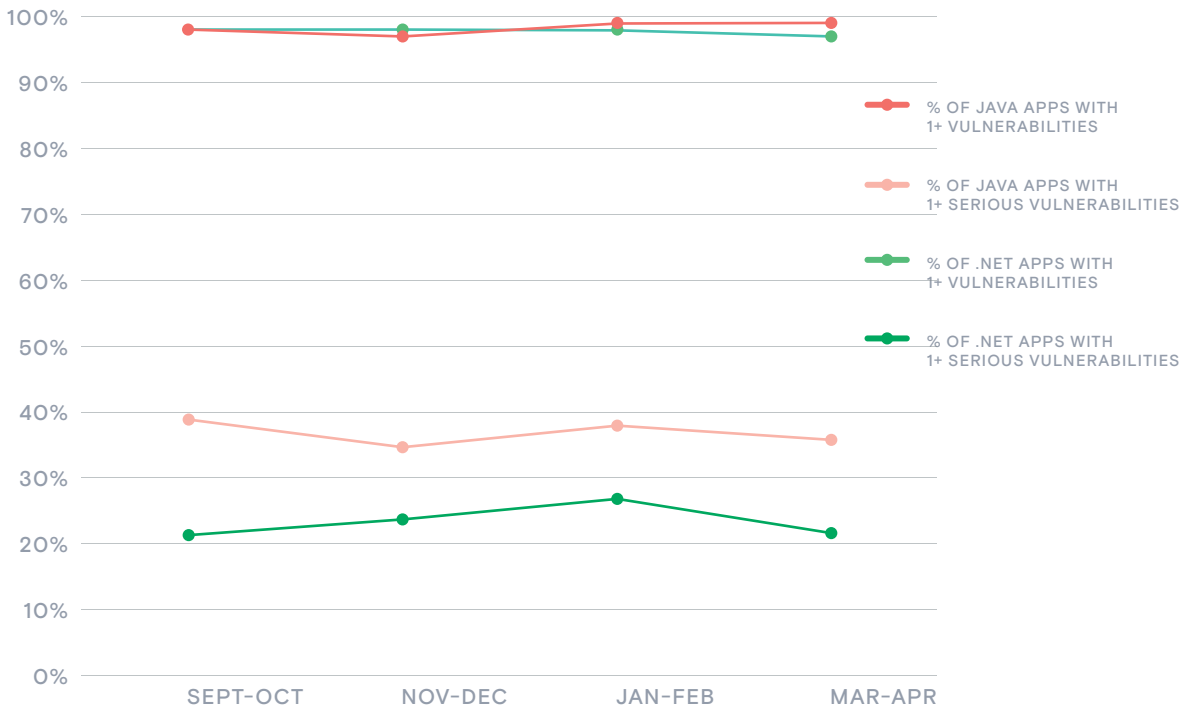


TREND: FEWER .NET APPLICATIONS HAD SERIOUS VULNERABILITIES

Looking at vulnerability data by programming language, an encouraging data point emerges with .NET applications, for which vulnerabilities had been trending upward for six months. For March–April, only 23% of .NET applications contained a serious vulnerability, down from 28% in the last bimonthly period (Figure 9). Specifically, the percentage of .NET applications with XSS and broken access control vulnerabilities declined by three and two percentage points, respectively.

FIGURE 9

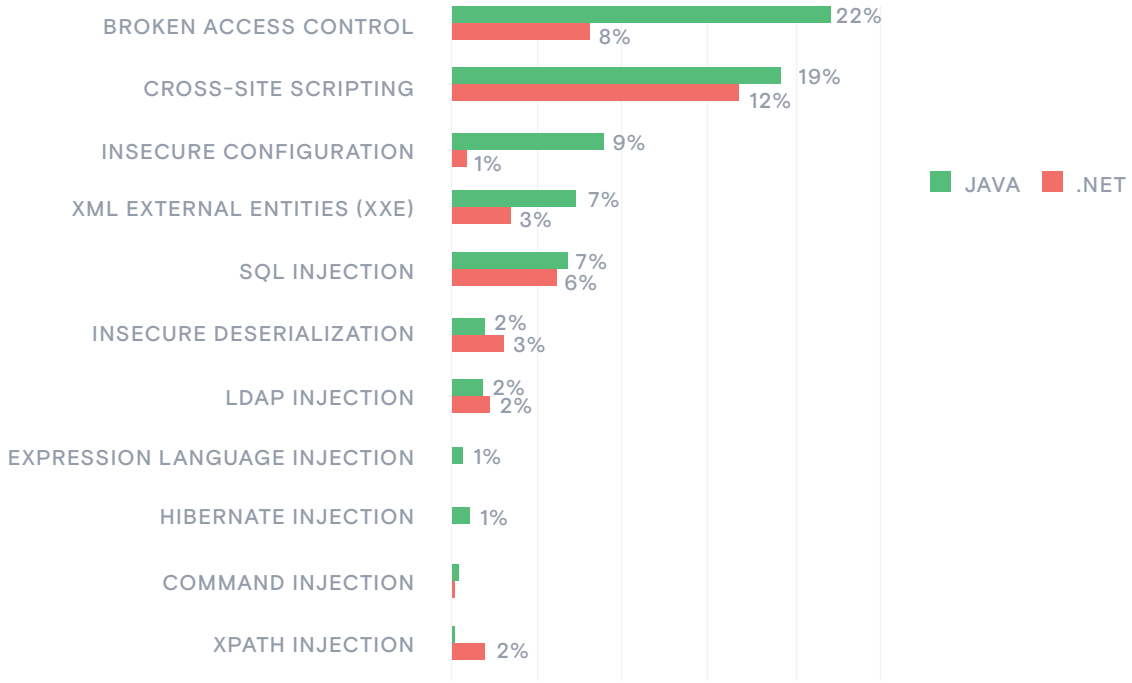
Overall vulnerabilities and serious vulnerabilities in Java and .NET applications, four bimonthly periods.



Serious vulnerabilities were also found in fewer Java applications—37% in March–April compared with 39% in January–February, again a reversion to the mean. Again, broken access control saw the biggest decline, impacting 22% of applications compared with 24% in the last bimonthly period.

FIGURE 10

Percentage of Java and .NET applications impacted by serious vulnerabilities, by category, March–April 2021.



05 | Attack Trends

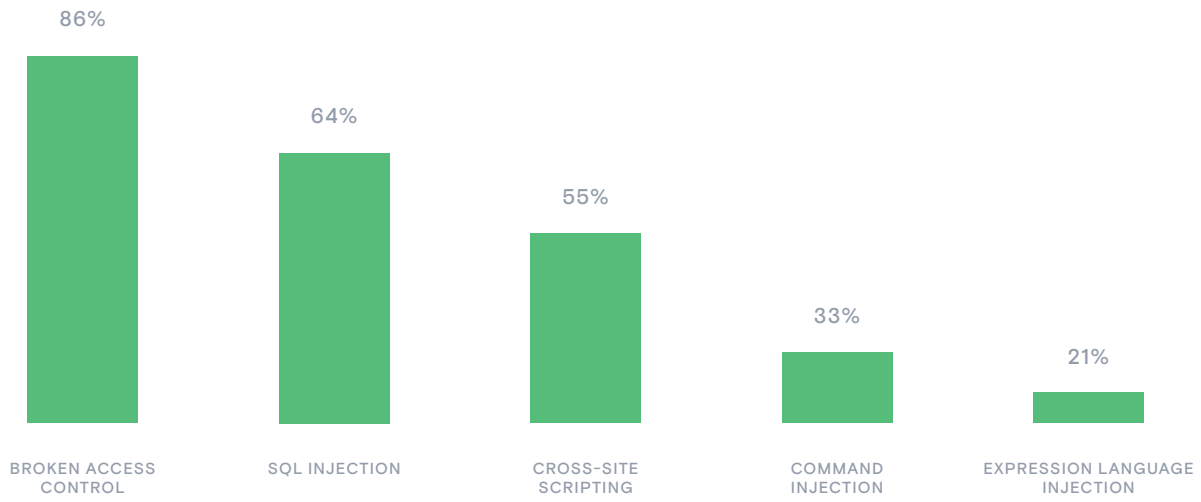
While many of the vulnerability trends were positive in March–April, attack trends were more concerning as a whole. Data from Contrast Protect during March–April reveals the following trends regarding application attacks on the custom code in applications:

TREND: VULNERABILITIES WERE ATTACKED MUCH MORE FREQUENTLY

Almost every attack type impacted a larger percentage of applications in March–April than in January–February, and the increases were dramatic for some. For example, XSS attacks impacted 55% of applications compared with 29% in the prior bimonthly period—a 90% increase (Figure 11). Similarly, the percentage of applications targeted by broken access control attacks increased by 79% and command injection by 74%. Overall, the average attack type impacted 9% more applications in March–April than in January–February.

FIGURE 11

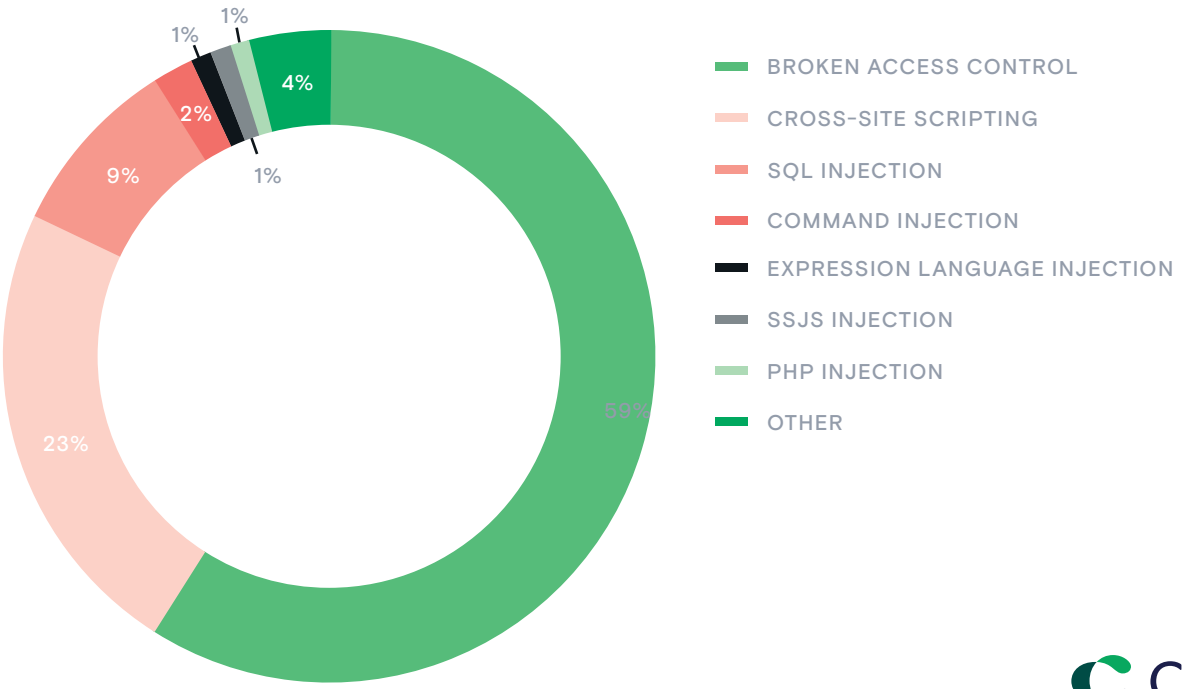
Rank of top 5 vulnerability types most likely to be targeted, March 2020–April 2021.



Broken access control regained the top spot in terms of percentage of applications impacted, at 86%. This is similar to the numbers seen during another spike in broken access control attacks in September–December 2020. The rest of the top five are the same as they have been since last fall—SQL injection, XSS, command injection, and expression language (EL) injection. But broken access control and XSS together accounted for 82% of all attacks in March–April (Figure 12).

FIGURE 12

Percentage of overall attacks by category, March–April 2021.



TREND: BAD ACTORS DELIVERED MORE VIABLE ATTACKS ON JAVA APPLICATIONS

In January–February, the viability of attacks hit an all-time low since Contrast has been measuring it, with less than 0.5% of attacks hitting an existing vulnerability in both Java and .NET applications. This meant that more than 99.5% of attacks were probes. That trend reversed itself in March–April for the Java language, in which fully 3% of attacks were viable (Figure 13). The last time we saw this rate was in May–June 2020, and it is near the highest percentage observed by Contrast Labs.

Despite that increased viability rate, most attack types impacted a somewhat lower percentage of Java applications than in January–February, with the percentage of applications hit with command injection attacks declining by 35% (Figure 14).

The viability rate with .NET remained below 0.5%, with the percentage of applications impacted by insecure deserialization, XSS, and EL injection attacks increasing by 25% or more.

FIGURE 13

Percentage of attacks viable, four bimonthly periods.

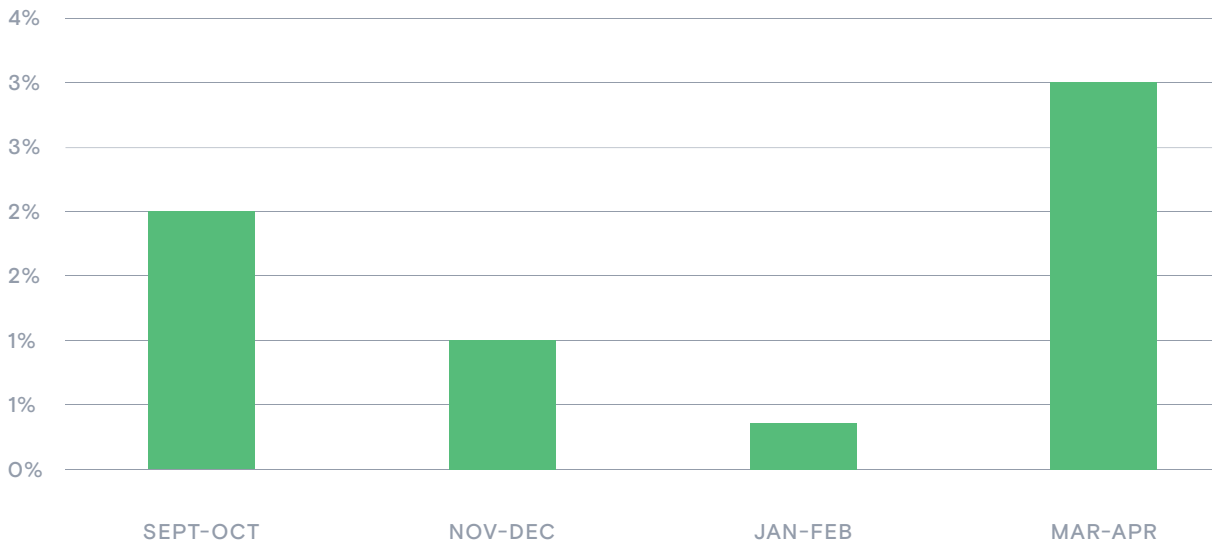
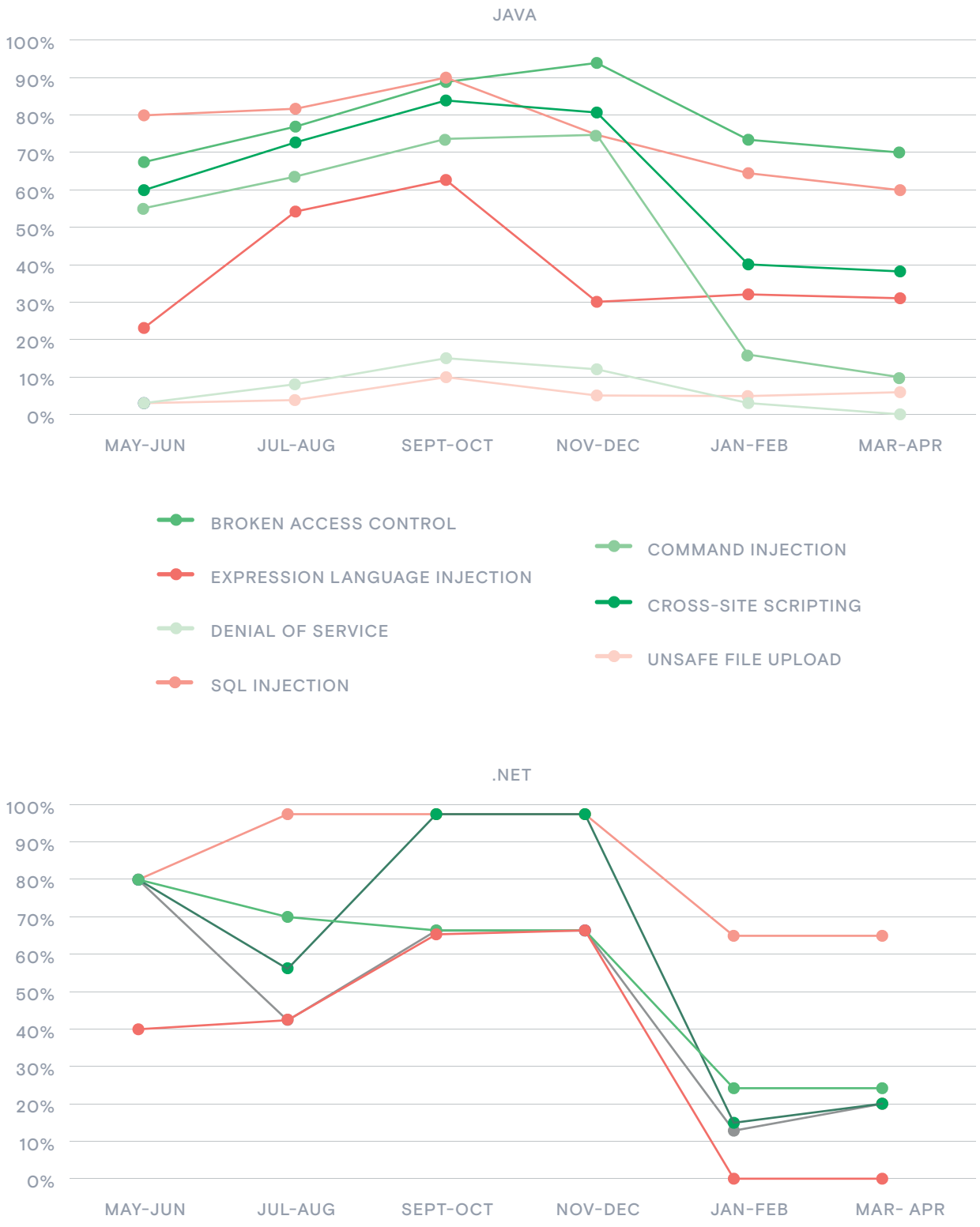


FIGURE 14

Java and .NET attacks by attack type, May 2020–April 2021.



06 | Conclusion

Telemetry from real-world software in March–April indicates an increase in the percentage of applications experiencing many attack types. What is more, the percentage of attacks that were viable increased more than sixfold over January–February to one of the highest percentages we have observed in more than two years of data collection. Buoyed by a series of massive and successful attacks, some bad actors may be attempting to ride the wave that those incidents created.

When such a large share of attacks actually hit an existing vulnerability in an application, it is clear that organizations need to work to reduce their security debt of unaddressed software vulnerabilities. And while vulnerability trends were somewhat more optimistic overall in March–April compared with recent months, applications continue to have far too many serious vulnerabilities. The data still shows 32% of applications containing at least one serious vulnerability and 7% having more than 20.

With all eyes focused on application security in the wake of the SolarWinds and Microsoft Exchange attacks—among others—the White House has recognized a need to create specific, stringent security standards for software. While the specific regulations have yet to be drawn up, some sort of security rating system for software may play a part in helping organizations understand the risk they are assuming when they deploy a certain application. If such a system is devised, it is especially important that it be based on actuarial data on both vulnerabilities and attacks, such as that contained in this report.

Contrast Labs hopes that this report will help readers prioritize their application security efforts—both short term and longer term. Security instrumentation places continuous security testing and runtime protection within applications themselves, enabling application security observability throughout the software development life cycle (SDLC). This runtime protection is often missing in organizations and leads to poor threat intelligence and exploits of vulnerabilities that are usually known weakness types that escape development into production, via either source code or open-source library. This gives organizations the ability to “shift left” by identifying and remediating vulnerabilities as they occur.[10] Instrumentation also enables entities to “shift right” to protect applications in production.[11] Shifting both left and right with application security is essential to preserving the integrity and speed of the development process. It also requires organizations to move beyond legacy tools and processes.

[1] Larry Dignan, "Facebook data on 533 million users posted online," ZDNet, April 4, 2021.
[2] "Scraped data of 500 million LinkedIn users being sold online, 2 million records leaked as proof," CyberNews, April 6, 2021.
[3] "Clubhouse data leak: 1.3 million scraped user records leaked online for free," CyberNews, April 10, 2021.
[4] Cody Miller, "Data hack exposed personal information of 200K MultiCare patients, workers, firms say," KOMO News, March 9, 2021.
[5] "Cancer Treatment Centers of America Announces 105,000-Record Data Breach," HIPAA Journal, March 26, 2021.
[6] Anthony Spadafora, "SITA data breach affects millions of airline passengers," TechRadar, March 8, 2021.
[7] "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021.
[8] "Prioritizing Application Security Risk Management With the Contrast RiskScore," Contrast Security, June 2021.
[9] See "2021 State of Open-source Security Report," Contrast Security, April 8, 2021, for similar analysis for third-party libraries and frameworks.
[10] Jakob Pennington, "Shifting Left: DevSecOps as an Approach to Building Secure Applications," Medium, July 18, 2019.
[11] Alan Shimel, "DevOps Chat: Shifting Security Left and Right, With Contrast Security," Security Boulevard, October 7, 2019

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com