Contrast SECURITY

MAY–JUNE 2021

Contrast Labs Application Security Intelligence Bimonthly Report

Table of contents

01 | Executive Summary

The Contrast Labs Application Security Intelligence Report for May–June 2021 is based on telemetry from real vulnerabilities and attacks in applications protected by the Contrast Application Security Platform. We hope it helps security and development teams to effectively prioritize their application security efforts by highlighting vulnerability and attack trends in custom code.

As spring moved toward summer in the northern hemisphere, high-profile attacks continued. Examples include ransomware attacks on Colonial Pipeline and JBS USA that disrupted U.S. supplies of gasoline and meat, respectively. Application-layer attacks hit organizations as diverse as Peloton and Electronic Arts as hackers look to replicate the damage done by attacks on SolarWinds Orion and Microsoft Exchange Server several months ago.

Contrast RiskScore™. This numerical score helps communicate the relative risk of different vulnerability types over time. For this bimonthly period, 16 of the 19 vulnerability types showed a lower RiskScore than in March–April, and this continues a longstanding trend. As applications gain tenure on the Contrast platform, the result is less risk over time.

Top 5 Contrast Riskscores

BROKEN ACCESS CONTROL

CROSS-SITE SCRIPTING (XSS)

INSECURE CONFIGURATION

SENSITIVE DATA EXPOSURE

BROKEN AUTHENTICATION

Average RiskScore: 4.96,
down from 5.06 in March–April

Vulnerability Trends. The percentage of applications with at least one serious vulnerability declined from 32% to 31% compared with the last bimonthly period, moving that number closer to historical averages.

But the percentage of overall vulnerabilities that are serious increased from 38% to 41%. The percentage of applications with serious vulnerabilities stabilized with an average of 59 serious vulnerabilities in the subset of applications that have at least one serious vulnerability. Only 2% of applications have more than 100 serious vulnerabilities, down from 3% in the last bimonthly period.

Looking at vulnerabilities by language, more Java applications continued to have serious vulnerabilities than .NET software. In May–June, 38% of Java applications and 24% of .NET applications had at least one serious vulnerability—a 1% increase in both instances.

31%

of applications have at least one serious vulnerability, down from 32% in March–April

2%

of applications have 100+ serious vulnerabilities, down from 3% in March–April

41%

of overall vulnerabilities are serious, up from 38% in March–April

Attack Trends. A record percentage of attacks were probes—that is, did not hit an existing vulnerability. In May–June, only 0.2% of attacks were viable—that is, not probes—compared with 3% in March–April.

Command injection attacks impacted far more applications than the last bimonthly period, but expression language (EL) injection and several other attack types declined significantly. In Java applications, the top four attack types (SQL injection, broken access control, XSS, and command injection) all impacted more than 75% of applications—a big jump from March–April.

0.7%

of attacks were viable, lowest percentage recorded and down from 3% in March–April

75%+

of Java applications impacted by these attacks:

SQL INJECTION
BROKEN ACCESS CONTROL
CROSS-SITE SCRIPTING
COMMAND INJECTION

Takeaways. Our analysis of data from real-world applications reveals a stable vulnerability landscape and interesting shifts in the actions of attackers. Slightly fewer applications had serious vulnerabilities, but the share of vulnerabilities that are serious rose by three percentage points.

Attackers sent a higher percentage of probes than ever before, with only 0.2% of attacks hitting an existing vulnerability. These probes provide information for attackers that can result in successful attacks later on. Java users in particular were hit more frequently with attacks on four common vulnerability types—big increases over March–April.

The only way for organizations to adequately improve their application security posture is to use security instrumentation to enable continuous security testing across the software development life cycle (SDLC). This enables full observability of the security of an application from the beginning of development to the retirement of the application.

02 | Massive Attacks Provide more Wake-Up Calls

As noted, the purpose of Contrast Labs' Bimonthly Application Security Intelligence Reports is to help organizations prioritize their efforts to deliver more secure applications for customers and co-workers.

Every two months, we highlight vulnerability and attack trends using telemetry data from applications using Contrast Assess in development and Contrast Protect in production. Contrast Labs' analysis helps security and development teams better understand the evolving risk posed by different kinds of vulnerabilities.

As the calendar year 2021 approached its halfway mark, high-profile attacks on large organizations showed no signs of slowing down. In mid-May, consumers in the eastern U.S. experienced gasoline shortages after a ransomware attack on Colonial Pipeline shut down America's largest fuel pipeline for several days.[1] The attack was described as a "wake-up call"—a term that has come to be overused in this context. Two weeks later, American and Australian consumers saw shortages of meat products following another ransomware attack that shut down slaughter operations at JBS USA—again for several days.[2] Across the Atlantic, a ransomware attack shut down the Irish Health Service for nearly a week.[3]

In an application-layer attack in June, hackers stole the source code to EA's popular soccer game FIFA 21 and are selling it on the black market.[4] The attackers also exfiltrated the code for the engine behind several games as well as other development tools. And a security researcher found that an application programming interface (API) belonging to trendy exercise brand Peloton had a vulnerability that enabled access to user account data.[5]

03 | Contrast Riskscore™ for May—June 2021

We begin by updating the Contrast RiskScore for this bimonthly period. RiskScore is a numerical score that ranks vulnerability types by the risk they pose at a specific time, based on data from real applications about vulnerability and attack prevalence.[6] While opportunities to use the RiskScore algorithm in narrower contexts will be available in the future, these scores reflect the aggregate data from all applications protected by Contrast Security.

The most notable shift with aggregate RiskScores is that they have been trending downward since the model was created a year ago. In May–June, 16 of the 19 vulnerability types we measure declined compared with March–April. And the average RiskScore for those 19 types was 4.96 in this bimonthly period, down from 5.06 in the prior period and the lowest average so far. The best explanation for this trend is that applications in the dataset, as a whole, are gaining tenure on the Contrast Application Security Platform, and that results in less risk over time.

Like in the previous bimonthly report, the four most dangerous vulnerability types remained the same in May–June—broken access control, cross-site scripting (XSS), insecure configuration, and sensitive data exposure (Figures 1 and 2). SQL injection and broken authentication have been trading places as the fifth-highest RiskScore for a few months, and the former moved into fifth place again for this bimonthly period.

Fluctuations further down the list can often be even more informative as organizations work to prioritize their activities in response to short- and long-term trends. In this bimonthly period, two vulnerability types saw big increases—NoSQL injection and denial of service. EL injection, on the other hand, saw its RiskScore more than cut in half compared with March–April.

NoSQL injection has been wildly fluctuating over the past year, from a high of 7.23 last August to 2.7 in April of this year. The move to 3.66 in May–June is something of a reversion to the mean. Denial of service, on the other hand, has been trending upward since September 2020.

FIGURE 1

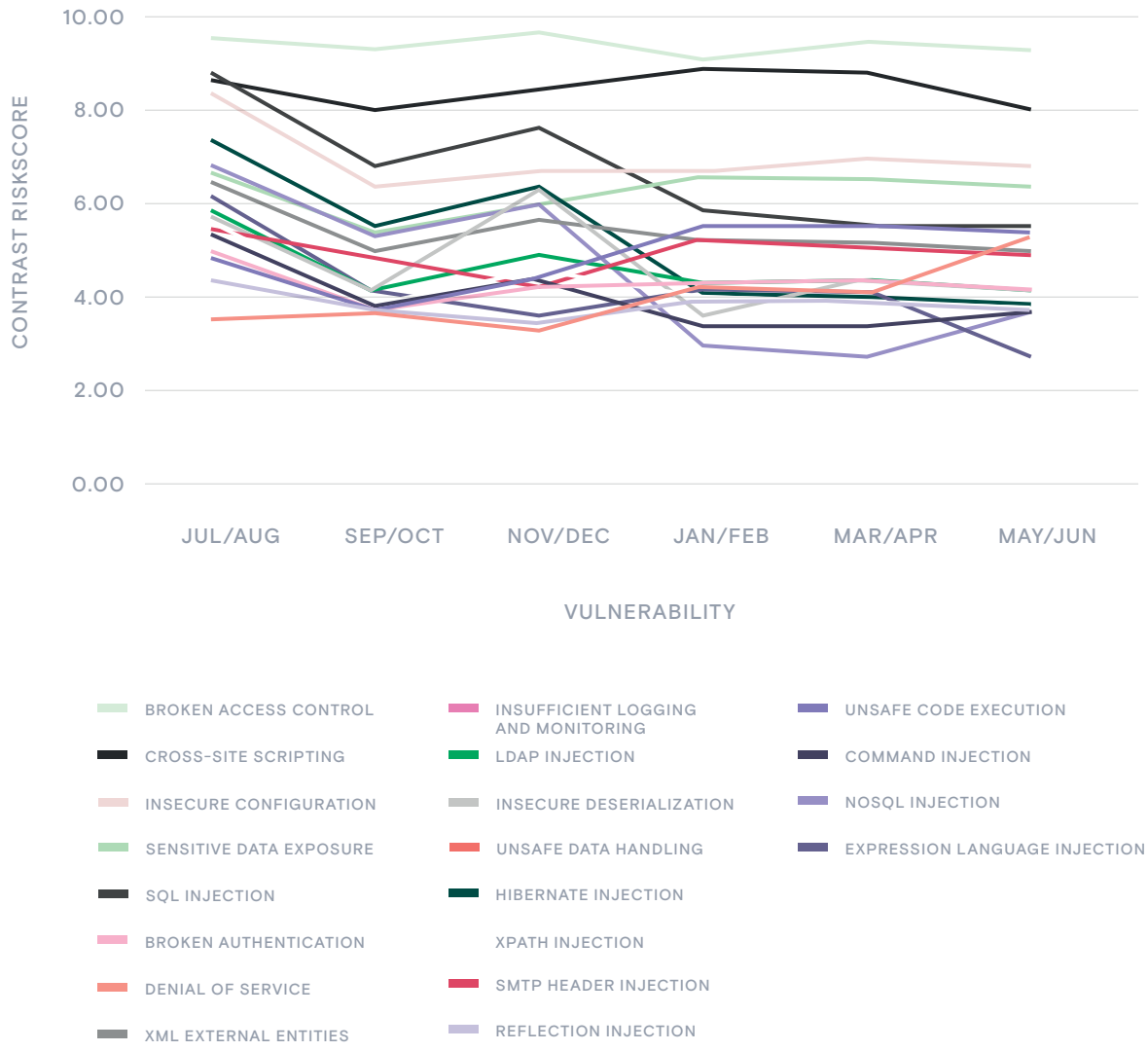
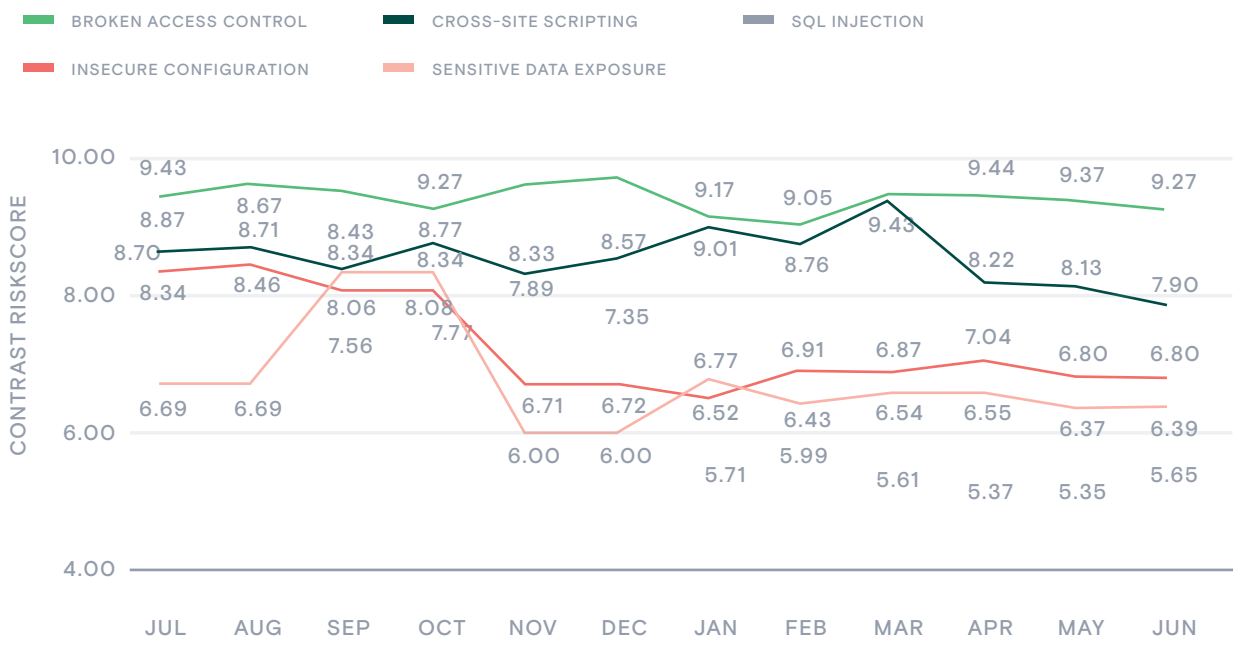


FIGURE 2


BROKEN ACCESS CONTROL
CROSS-SITE SCRIPTING
SQL INJECTION
INSECURE CONFIGURATION
SENSITIVE DATA EXPOSURE
CONTRAST RISKSCORE
10.00
8.00
6.00
4.00
9.43
8.67
9.27
9.17
9.05
9.44
9.37
9.27
8.87
8.71
8.43
8.77
8.57
9.43
8.70
8.34
8.34
8.33
9.01
8.76
8.22
8.13
7.90
8.34
8.46
8.06
8.08
7.35
7.56
7.77
6.77
6.91
6.87
7.04
6.80
6.80
6.69
6.69
6.71
6.72
6.52
6.43
6.54
6.55
6.37
6.39
6.00
6.00
5.71
5.99
5.61
5.37
5.35
5.65
JUL
AUG
SEP
OCT
NOV
DEC
JAN
FEB
MAR
APR
MAY
JUN

04 | Application Vulnerability Trends

For the Contrast customers in the dataset, vulnerability data for custom code[7] showed stability and perhaps modest improvement in May–June. Contrast Labs noted the following vulnerability trends:

TREND: SERIOUS VULNERABILITIES IMPACT FEWER APPLICATIONS, BUT A BIGGER SHARE OF VULNERABILITIES WERE SERIOUS

The vast majority of applications in the dataset continue to have at least one vulnerability—97% for May–June, which was unchanged from March–April (Figure 3). More significantly, the percentage of applications with at least one serious vulnerability decreased from 32% to 31% since the last bimonthly period—but a reversion to the mean. That number peaked at 36% in January, and the annual average for June 2020–May 2021 was 34%, up from 26% in the prior 12-month period.[8]

As in previous months, XSS and broken access control again impacted a far higher percentage of applications than any other type (Figure 4), with each type impacting 16% of applications in this bimonthly period.

FIGURE 3

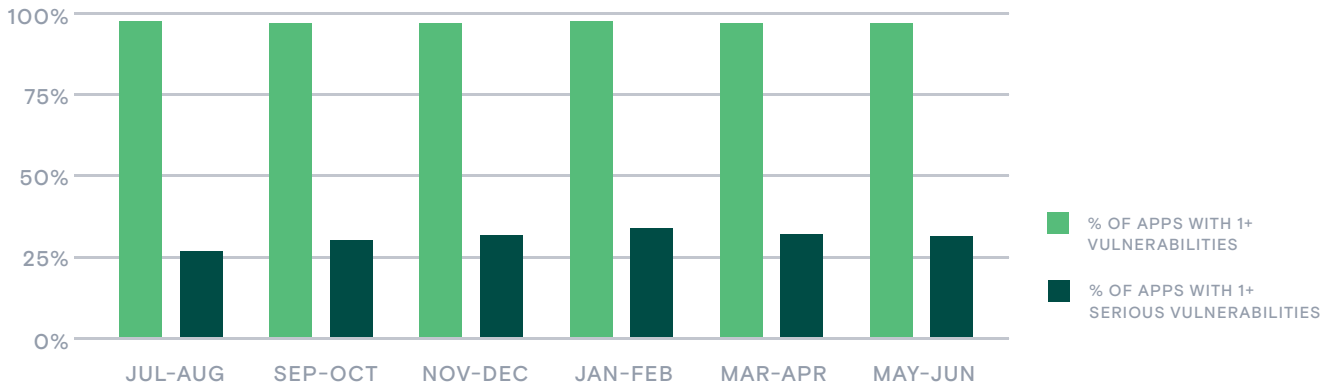
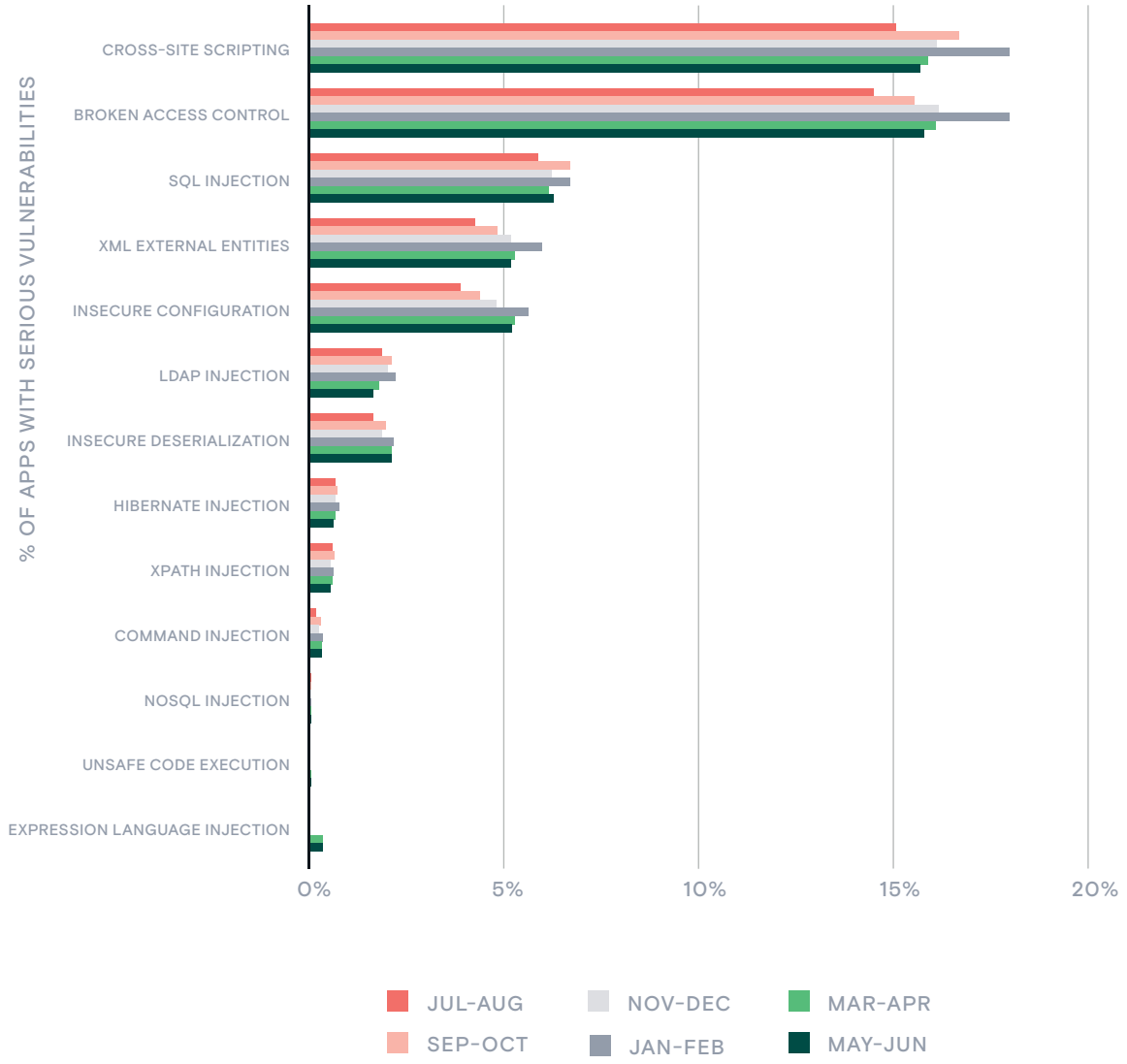
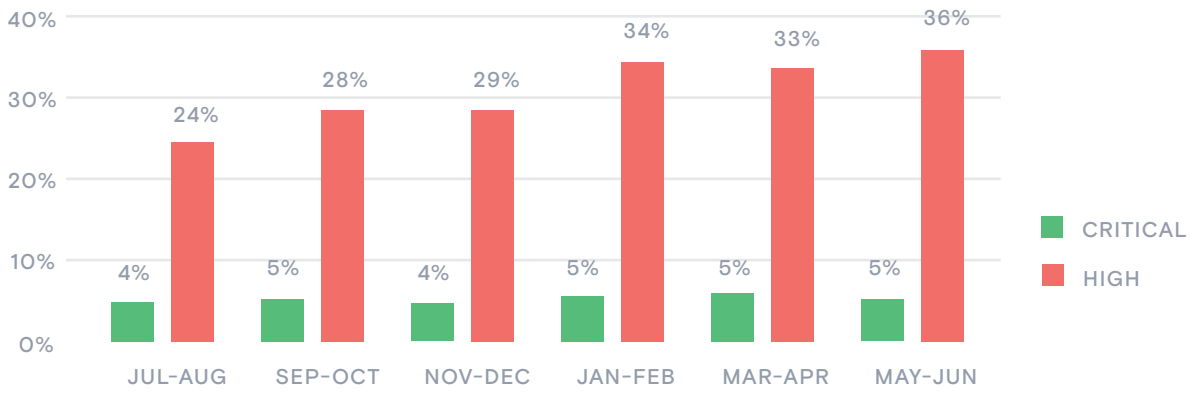


FIGURE 4


% OF APPS WITH SERIOUS VULNERABILITIES
CROSS-SITE SCRIPTING
BROKEN ACCESS CONTROL
SQL INJECTION
XML EXTERNAL ENTITIES
INSECURE CONFIGURATION
LDAP INJECTION
INSECURE DESERIALIZATION
HIBERNATE INJECTION
XPATH INJECTION
COMMAND INJECTION
NOSQL INJECTION
UNSAFE CODE EXECUTION
EXPRESSION LANGUAGE INJECTION
0%
5%
10%
15%
20%
JUL-AUG
SEP-OCT
NOV-DEC
JAN-FEB
MAR-APR
MAY-JUN

Despite the modest decline in the percentage of applications with serious vulnerabilities, a larger share of overall vulnerabilities was serious. Critical and High vulnerabilities made up 41% of all vulnerabilities in May–June, compared with 38% in March–April (Figure 5). This number has been steadily increasing from 28% in July–August 2020.

FIGURE 5

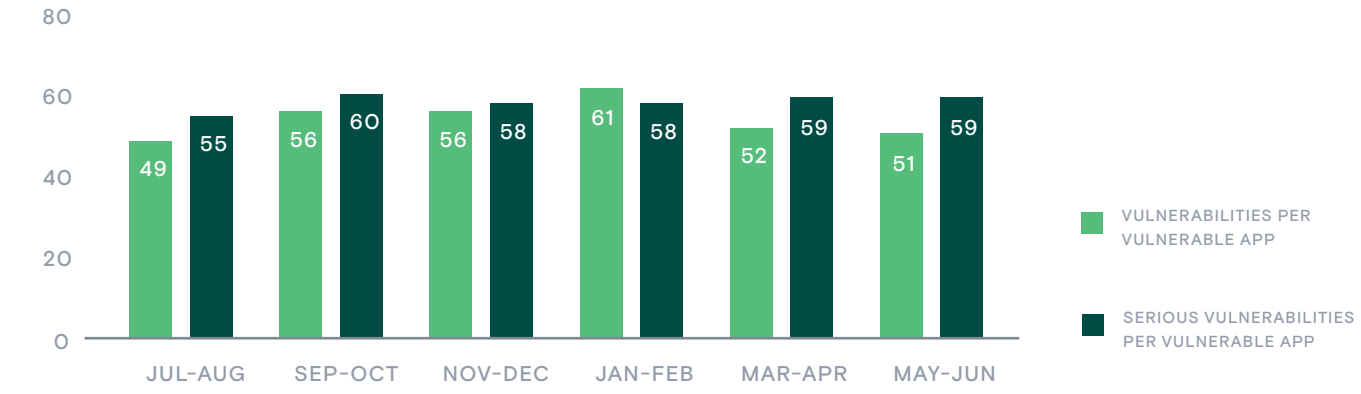


TREND: THE PERCENTAGE OF APPLICATIONS WITH MULTIPLE VULNERABILITIES STABILIZED

Applications that have vulnerabilities continue to have quite a few of them. Among applications with at least one vulnerability of any kind, the average has 51 vulnerabilities—a number that has stabilized after a spike earlier in the year. The average application with at least one serious vulnerability has 59 of them.

While the same percentage of applications had more than 20 serious vulnerabilities (6%) as the last bimonthly period, fewer applications had more than 100—2% versus 3% in March–April (Figure 7). This may be a result of organizations making headway in their security debt per application as reported in Contrast's 2021 Application Security Observability Report.[9]

FIGURE 6



TREND: SERIOUS VULNERABILITIES IMPACTED SLIGHTLY MORE JAVA AND .NET APPLICATIONS

As is always the case, serious vulnerabilities impact significantly more Java applications than .NET ones. In May–June, 38% of Java applications and 24% of .NET applications had at least one serious vulnerability (Figure 8). This is an increase of one percentage point in both cases, compared with March–April. Percentages of Java and .NET applications impacted by specific vulnerability types remained very stable (Figures 9 and 10).

FIGURE 7

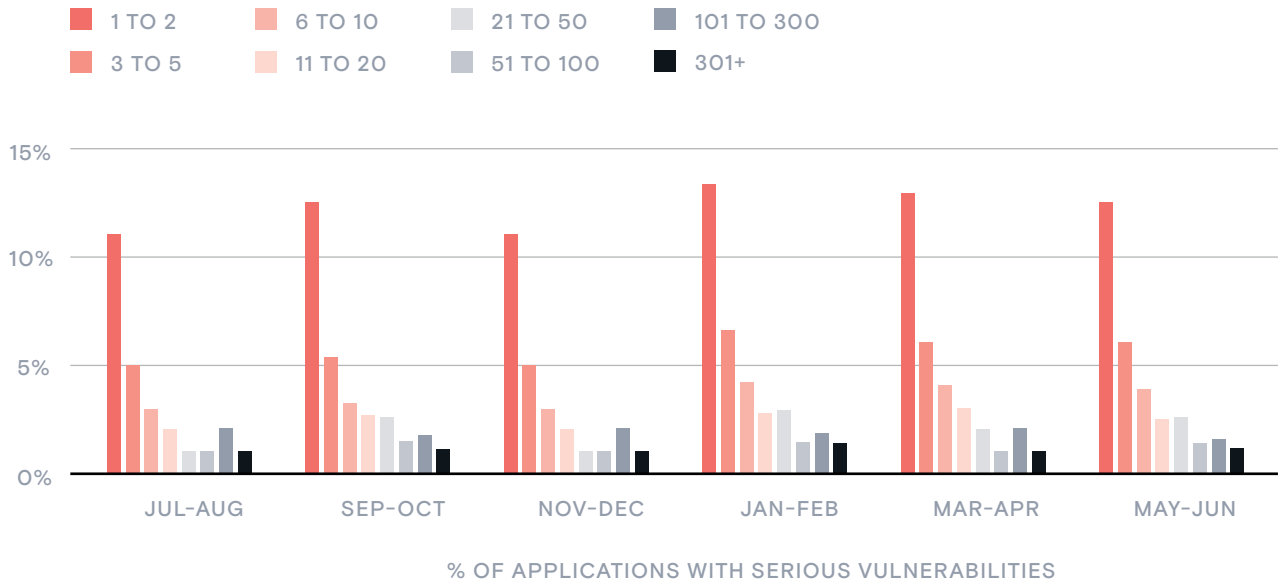


FIGURE 8

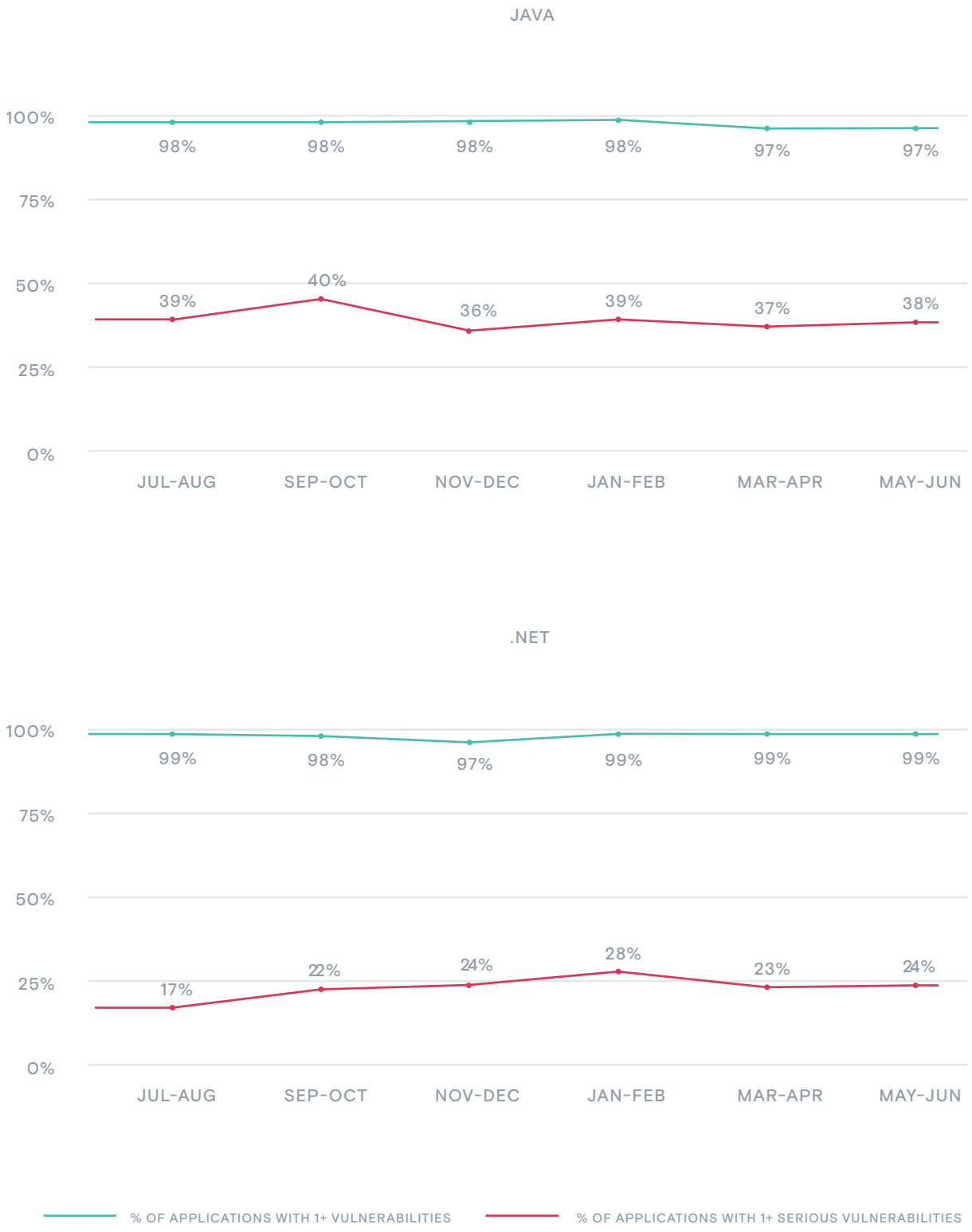
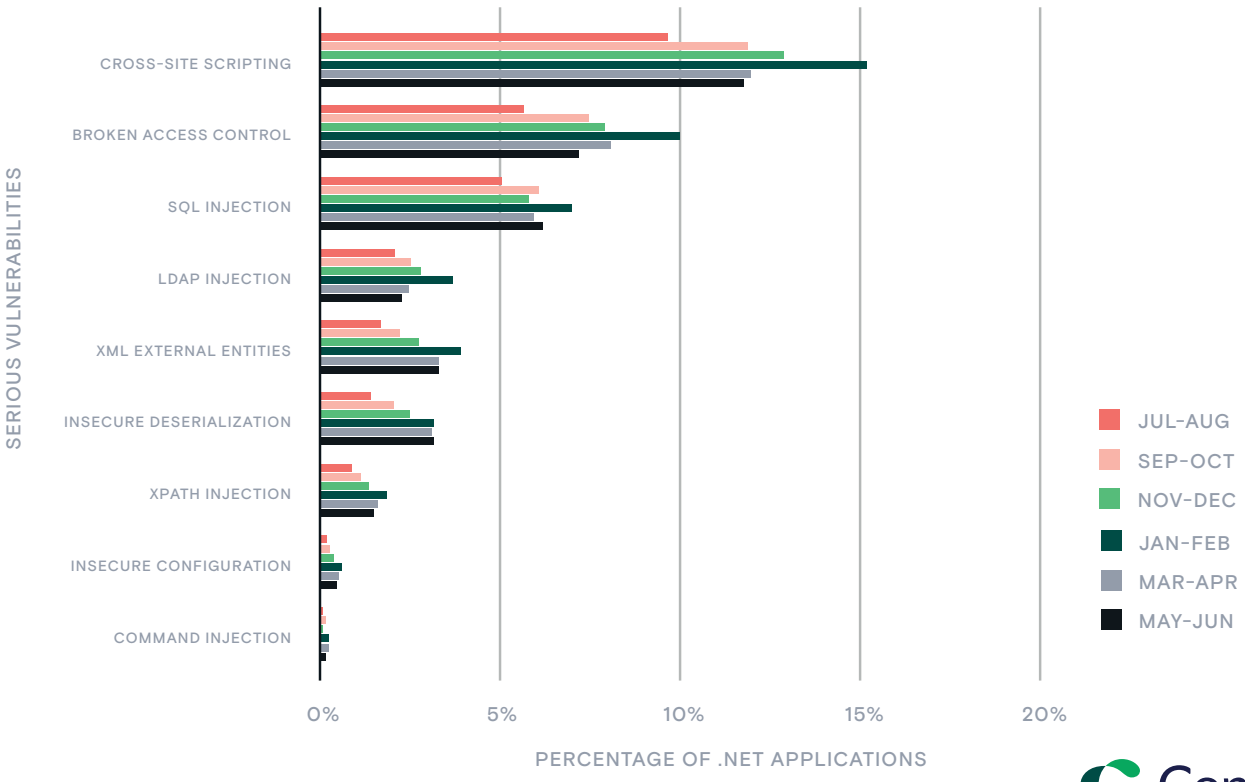

JAVA
100%
75%
50%
25%
0%
98%
98%
98%
98%
97%
97%
39%
40%
36%
39%
37%
38%
JUL-AUG
SEP-OCT
NOV-DEC
JAN-FEB
MAR-APR
MAY-JUN
.NET
100%
75%
50%
25%
0%
99%
98%
97%
99%
99%
99%
17%
22%
24%
28%
23%
24%
JUL-AUG
SEP-OCT
NOV-DEC
JAN-FEB
MAR-APR
MAY-JUN
% OF APPLICATIONS WITH 1+ VULNERABILITIES
% OF APPLICATIONS WITH 1+ SERIOUS VULNERABILITIES

FIGURE 9

FIGURE 10



Contrast SECURITY

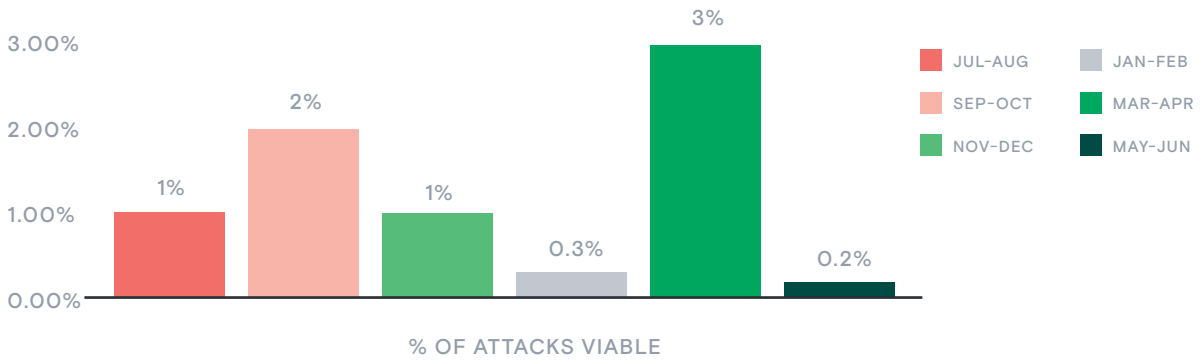
05 | Attack Trends

Data from Contrast Protect during May–June reveals the following trends regarding application attacks on the custom code in applications:

TREND: A RECORD PERCENTAGE OF ATTACKS WERE PROBES

The biggest trend in application attacks for May–June is the extremely low percentage that were viable—that is, hit an existing vulnerability in an application. That percentage was 0.2% this bimonthly period, the lowest figure observed since we have been tracking it (Figure 11). This is a big drop from the 3% observed in March–April but closer to the 0.3% seen in January–February.

FIGURE 11



Despite very low vulnerability rates, command injection attacks impacted far more applications—57% in May–June compared with 33% in March–April, a 73% increase (Figure 12). XSS attacks impacted 27% more applications than in the prior bimonthly period—70% in May–June compared with 55% in March–April. On the other hand, EL injection, remote file inclusion, and vulnerability scanner saw big declines on a percentage basis.

FIGURE 12

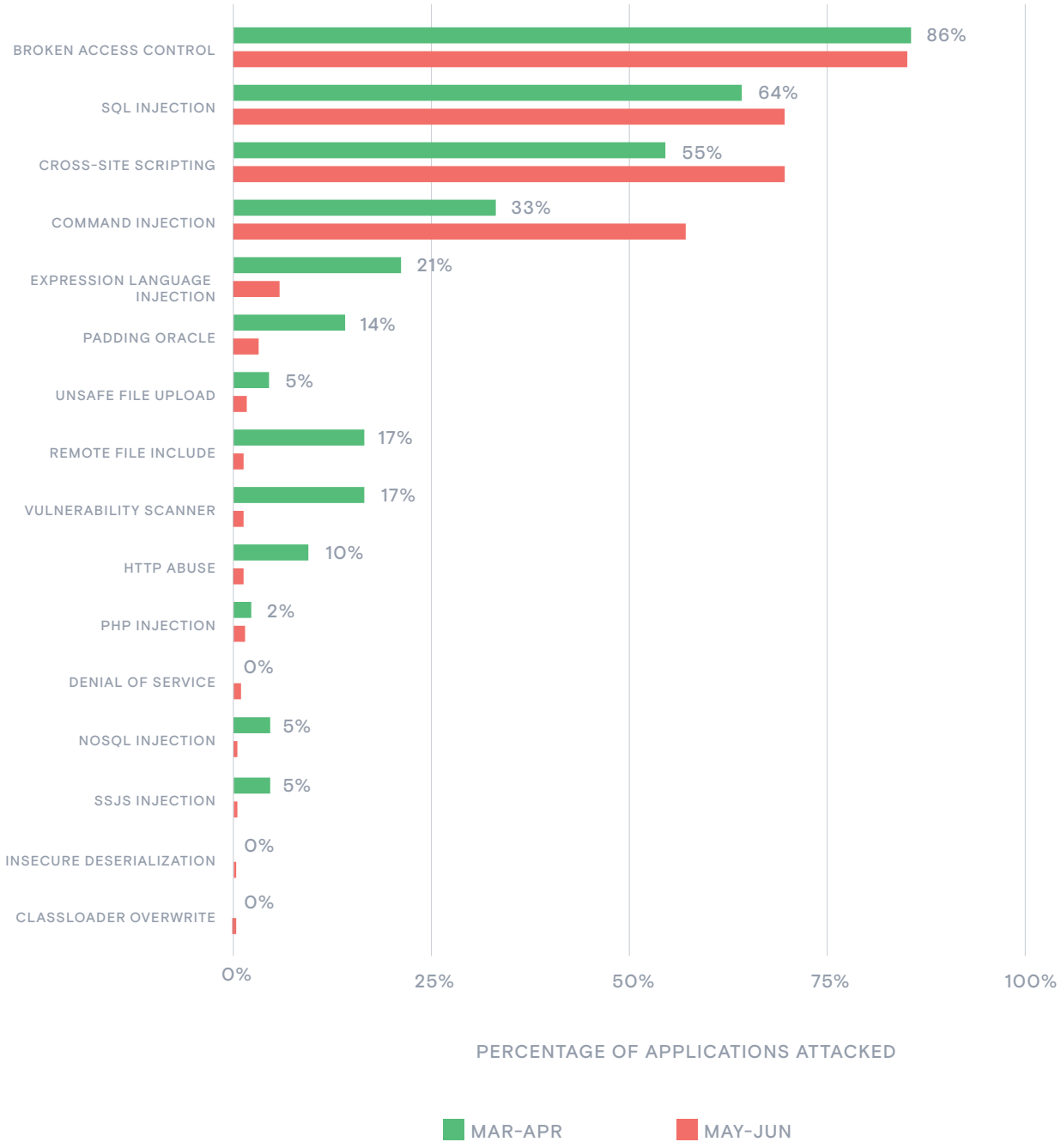
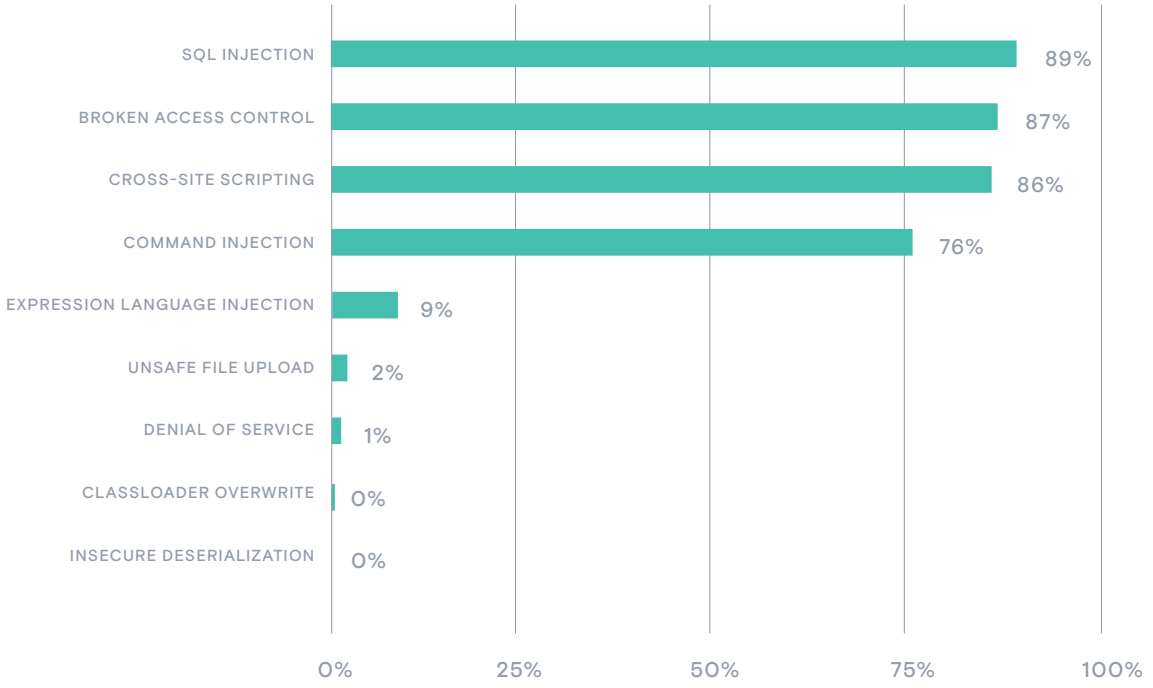


FIGURE 13



PERCENTAGE OF JAVA APPLICATIONS TARGETED, MAY–JUNE

TREND: THE TOP FOUR JAVA ATTACK CATEGORIES IMPACTED SIGNIFICANTLY MORE APPLICATIONS

In the Java language, SQL injection, broken access control, XSS, and command injection attacks all impacted more than 75% of applications—a number that increased by more than 25% in each case (Figure 13). Command injection went from 11% in March–April to 76% in May–June. EL injection, on the other hand, declined from 32% to 9%.

06 | Conclusion

Telemetry from actual applications in May–June shows a very stable landscape when it comes to vulnerability trends, after some of them spiked earlier in the year. The slight decrease in the percentage of applications with serious vulnerabilities—to 32%—is welcome news and a return to more "normal levels." But the increase in the share of overall vulnerabilities that are serious means that development and security teams need to be diligent about resolving those vulnerabilities and keeping security debt low.

Bad actors certainly aim to build upon the numerous high-profile application attacks of the past eight months, and our attack data shows significant volume. Attacks on Java applications were up in May–June, with four vulnerability types impacting 25% more applications than in the prior bimonthly period. Attackers also returned to an extremely high percentage of probes, with just 0.2% of attacks hitting an existing vulnerability. While this low viability rate is good news in the short term, probes can provide intelligence for attackers that help them launch successful attacks later.

With this report, Contrast Labs endeavors to help development, operations, and security teams as they prioritize their application security efforts—both short-term and longer-term. Security instrumentation is the key to understanding what to prioritize, as it provides continuous security testing and runtime protection within applications themselves. This enables full application security observability throughout the software development life cycle (SDLC)—including in production. Runtime protection provides not only protection against attacks but also threat intelligence that helps organizations to prepare for the next attack. Unfortunately, it is missing at many organizations. From the beginning of an application development project to the retirement of the software, immediate visibility and feedback through instrumentation keeps software safe and reduces organizational risk.

[1] Clare Duffy, "Colonial Pipeline attack: A 'wake up call' about the threat of ransomware," CNN, May 16, 2021.
[2] Tom Polansek and Jeff Mason, "U.S. says ransomware attack on meatpacker JBS likely from Russia," Reuters, June 1, 2021.
[3] Sylvia Hui, et al., "Irish health system struggling to recover from cyberattack," Associated Press, May 18, 2021.
[4] Mitchell Clark, "EA got hit by a data breach, and hackers are selling source code," The Verge, June 10, 2021.
[5] Anthony Spadafora, "Peloton security flaw would have let anyone access user data," TechRadar, May 5, 2021.
[6] "Prioritizing Application Security Risk Management With the Contrast RiskScore," Contrast Security, June 2021.
[7] See "2021 State of Open-source Security Report," Contrast Security, April 2021, for similar analysis for third-party libraries and frameworks.
[8] "2021 Application Security Observability Report," Contrast Security, August 2021.
[9] Ibid.

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