CONTRAST SECURITY

CONTRAST LABS APPLICATION SECURITY INTELLIGENCE BIMONTHLY REPORT

SEPTEMBER–OCTOBER 2020

TABLE OF CONTENTS

01 | EXECUTIVE SUMMARY

The Contrast Labs Application Security Intelligence Report for September–October 2020 provides analysis of aggregate data from Contrast Security customers to help readers understand vulnerability and attack trends and how application security efforts should be prioritized.

General findings for September–October include:

- **The percentage of applications that have at least one serious vulnerability increased** to 30%, up from 27% in July–August. The percentage of applications with 50 or more serious vulnerabilities also increased, from 9% to 11%.

- **Serious vulnerabilities in, and many types of attacks on, .NET applications continued to rise.** Serious vulnerabilities spiked from 17% to 22%, while more .NET applications were impacted by four of the top five attack types.

- **The percentage of attacks that were viable increased** from 1% to 2%, and more applications were impacted by four of the top five attack types.

These findings show that organizations continue to struggle to deliver secure applications in an efficient manner—and to protect them once they are in production. This is best accomplished by a comprehensive approach to application security that builds testing and protection into every step of the software development life cycle (SDLC).

KEY FINDINGS

30% of applications in development have 1+ serious vulnerabilities, up from 27% in July–August

11% of applications have 50+ serious vulnerabilities, up from 9% in July–August

33% of all vulnerabilities are serious, up from 32% in July–August and 28% in May–June

24% increase in prevalence of cross-site scripting vulnerabilities

22% of .NET applications have 1+ serious vulnerabilities, up from 16% in July–August

5% of the top five .NET vulnerability categories increased in prevalence by 20%+

2% of attacks were viable, up from 1% in July–August

300% increase in denial-of-service attacks over 6 months

30% increase in cross-site scripting attacks

02 | APPLICATIONS CRITICAL FOR COMPANIES' RECOVERY

Contrast Labs' bimonthly Application Security Intelligence Reports aim to help organizations prioritize their application security efforts by highlighting trends in both software vulnerabilities and attacks. The data comes from aggregated telemetry from applications using Contrast Assess during development and Contrast Protect in production. Contrast Labs analyzes this data regularly to provide updates on the overall prevalence of vulnerabilities and attacks, the level of risk they introduce for organizations, and which types are most common in protected applications.

In addition to making note of several vulnerability and attack trends for the past two months, the report updates the Contrast RiskScores for top vulnerability and attack categories. This provides an objective, at-a-glance visualization of the relative danger posed by different vulnerability types. While two-month fluctuations are often not large, publishing the reports on a regular basis helps readers to keep abreast of trends.

Many had envisioned a V-shaped economic recovery following the declines in the spring and early summer. But case counts for COVID-19 rose precipitously during September and October—both in the United States and in many European countries.[1] At the same time, different industries have experienced the economic recovery in different ways. This has resulted in a "K-shaped recovery," with industries like

technology and retail growing significantly from their low point while sectors like travel, entertainment, and food services continue to decline.[2]

Regardless of the leg of the "K" on which organizations find themselves, applications are key to helping companies weather the storm and enhance their position in the marketplace. Besides their clear benefits in streamlining operations, product development, and brand awareness, applications can often create new ways for organizations to generate revenue, at a time when that is an important short-term priority. As a result, software developers remain in high demand, even as corporate priorities undergo massive and frequent change.[3] Reflecting trends that Contrast Labs has reported on extensively, one increasingly sought-after skill for developers is cybersecurity.[4]

Not surprisingly, organizations continue to struggle with application security in this environment. In one recent survey, more than 7 in 10 respondents said that each security alert consumes more than an hour of time for application security professionals, and remediating and verifying each legitimate vulnerability takes more than four hours of developer time.[5] The same survey found that 61% of organizations experienced *three or more* successful exploitative attacks over 12 months—and only 5% saw none. To compound the problem, a major application security testing vendor found that time-consuming vulnerability scans must be run *every day* in order to keep the mean time to remediation (MTTR) below 60 days—and thus prevent security debt from growing.[6]

03 | APPLICATION VULNERABILITY TRENDS

FOR SEPTEMBER–OCTOBER 2020, CONTRAST LABS IDENTIFIED SEVERAL APPLICATION VULNERABILITY TRENDS FROM ANALYSIS OF ITS AGGREGATE DATA:

TREND: MORE APPLICATIONS HAVE SERIOUS VULNERABILITIES

As Contrast Labs has consistently reported for more than a year, nearly every application under development has at least one vulnerability. In September–October, aggregate telemetry from Contrast Assess customers reveals that 97% of applications are impacted (Figure 1). This number is down from 98% in July–August, but closer to the annual figure of 96% reported for the 12 months from June 2019 through May 2020.[7]

Figure 1: Percentage of applications containing at least one vulnerability and at least one serious vulnerability.

More important is the percentage of applications that have *serious* vulnerabilities, defined as high or critical. Unfortunately, this number was up in September–October. Three in 10 applications had at least one serious vulnerability in those two months, compared with 27% in July–August and 26% for June 2019–May 2020. This figure had spiked to 33% in May–June, when millions of workers were adjusting to a new work-from-home model. It is concerning that serious vulnerabilities are trending upward again.

Looking at vulnerabilities by category, sensitive data exposure vulnerabilities continued to be present in more applications than any other (Figure 2). But none of those vulnerabilities were serious. Among serious vulnerabilities, cross-site scripting (XSS) saw a 24% increase in the percentage of applications impacted—from 9% to 11%. On the flip side, insufficient logging and monitoring vulnerabilities are seeing a sustained decline, impacting 24% of applications in September–October after being present in 35% of applications in May–June and 26% in July–August.

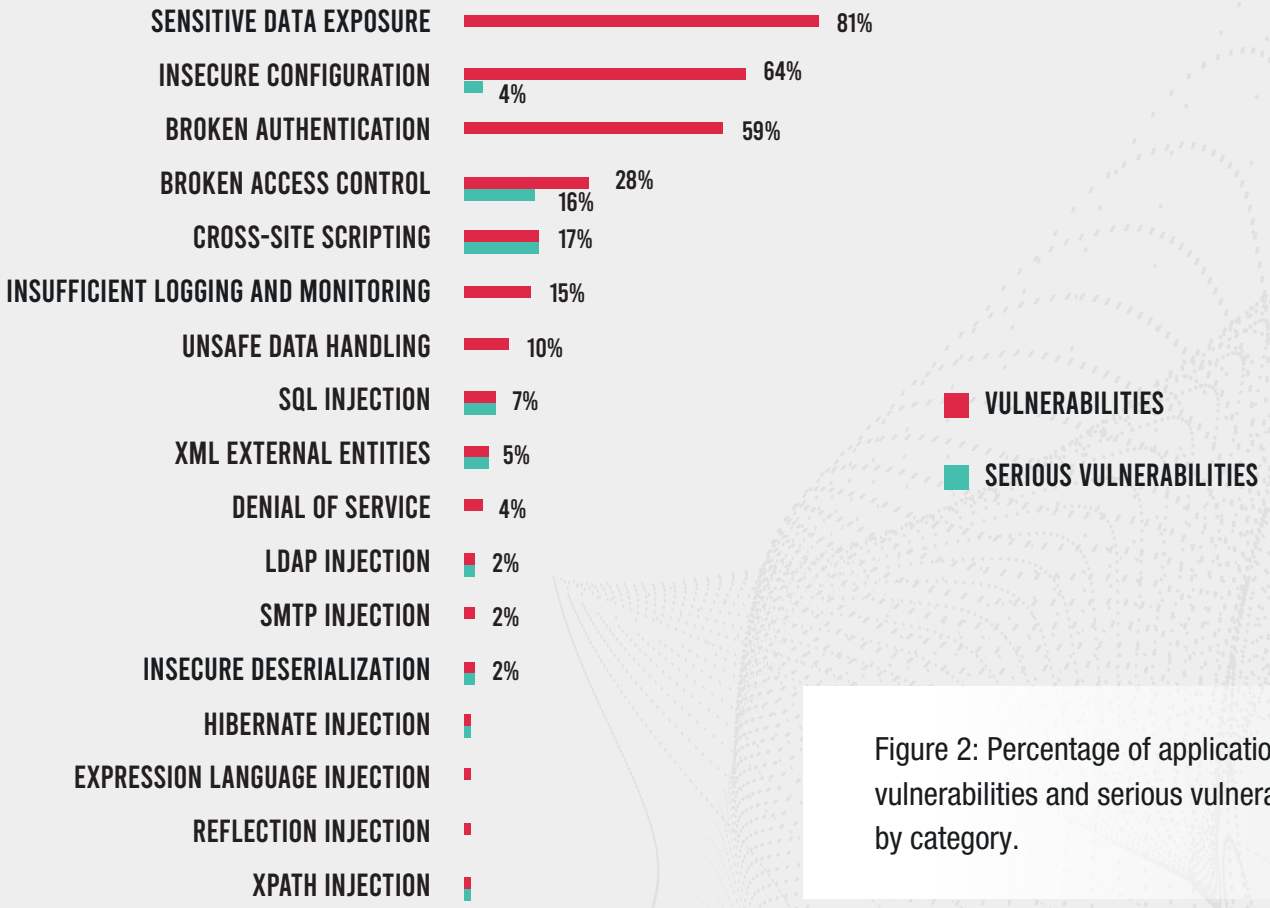


Figure 2: Percentage of applications with vulnerabilities and serious vulnerabilities, by category.

TREND: MORE APPLICATIONS HAVE 50+ VULNERABILITIES, AND THE PERCENTAGE OF VULNERABILITIES THAT ARE SERIOUS TRENDED UPWARD

A small but significant percentage of applications tend to have a large number of vulnerabilities. In September–October, the percentage of applications containing 50 or more vulnerabilities increased from 9% to 11% compared with July–August (Figure 3). This was a factor in the increase in the average (mean) number of vulnerabilities in applications with at least one vulnerability from 49 to 56 (Figure 4). While this trend is concerning, it is something of a reversion to the mean as this figure was 75 in March–April and 65 in May–June.

Drilling down to serious vulnerabilities, the percentage of applications with 20 or more such vulnerabilities grew from 5% to 7% between July–August and September–October. And the average number of serious vulnerabilities per vulnerable application rose to 60—a concerning increase after that number held steady at 55 for six months.

Figure 3: Percentage of applications with different numbers of vulnerabilities.

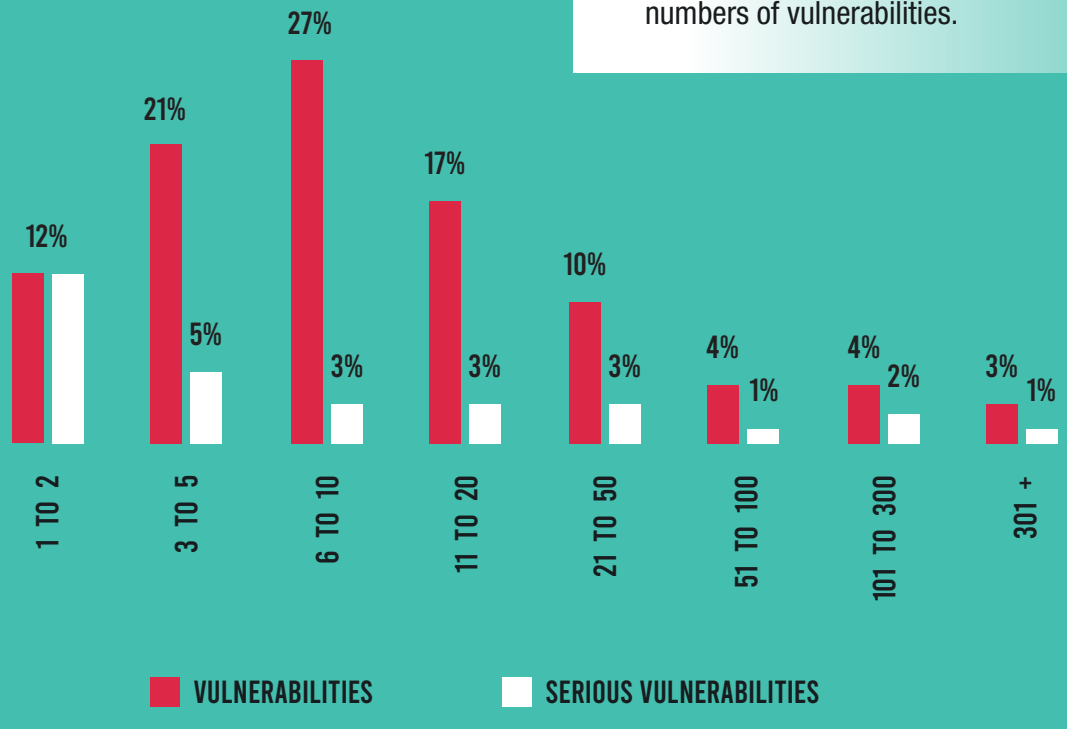


Figure 4: Vulnerabilities and serious vulnerabilities per vulnerable application.

While a great majority of vulnerabilities continue to be less serious, serious ones are growing as a share of all vulnerabilities. The percentage of all vulnerabilities that are serious increased from 32% to 33% between the last reporting period and this one, after being 28% in May–June (Figure 5).

Figure 5: Percentage of vulnerabilities by severity over six months.

TREND: THE PERCENTAGE OF .NET APPLICATIONS WITH SERIOUS VULNERABILITIES TRENDED BACK UPWARD

Looking at the data by programming language, Java applications continued to have much more prevalence of serious vulnerabilities than .NET ones. During September–October, Java vulnerability figures held relatively steady, with the percentage of applications with at least one serious vulnerability increasing to 40% from 39% in July–August (Figure 6). This increase moves this metric in a more typical direction, as the annual figure for the 12 months ending May 31 was 42%.

Unfortunately, the percentage of .NET applications with serious vulnerabilities trended back upward to 22% in September–October. Only 16% of .NET applications were impacted by such vulnerabilities during the 12-month period ending May 31, but that number spiked to 29% in the early months of the COVID-19 pandemic before settling back to a more normal 17% in July–August.

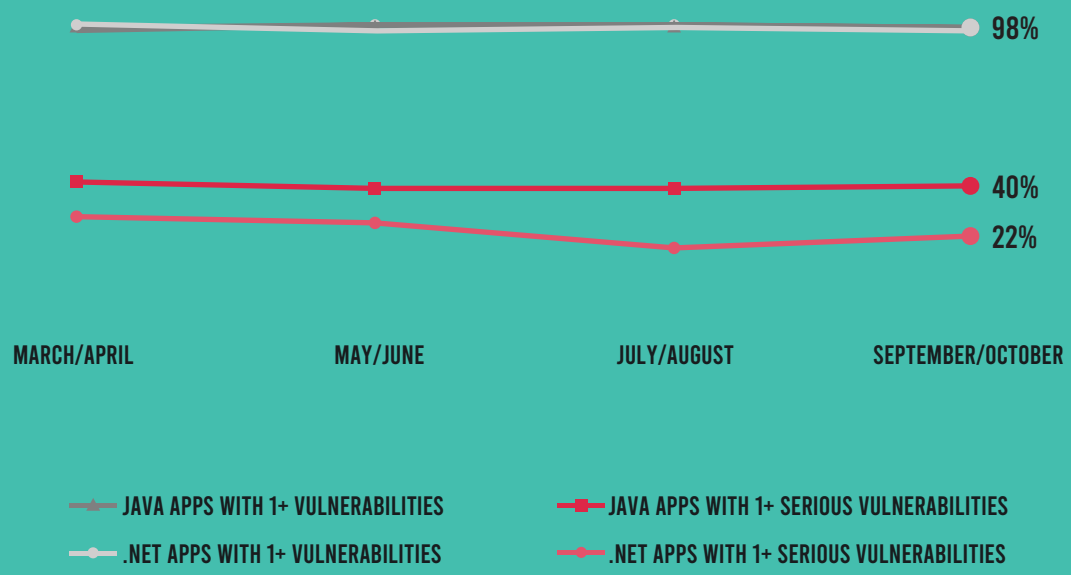


Figure 6: Overall vulnerabilities and serious vulnerabilities in Java and .NET applications, March–October 2020.

Drilling down to vulnerability categories by language, broken access control and cross-site scripting (XSS) continue to impact the highest percentage of Java applications (Figure 7). The numbers for all the categories have been quite level over the past several months.

The increase in the percentage of .NET applications impacted by serious vulnerabilities was also reflected in many of the vulnerability categories. All of the most common vulnerability categories increased in prevalence in applications by 20% or more. XSS continued to be present in more applications than any other category, increasing from 10% to 12% (a 23% increase) over the last bimonthly period. Broken access control increased by 31% (impacting 7% of applications in September–October versus 6% in July–August).

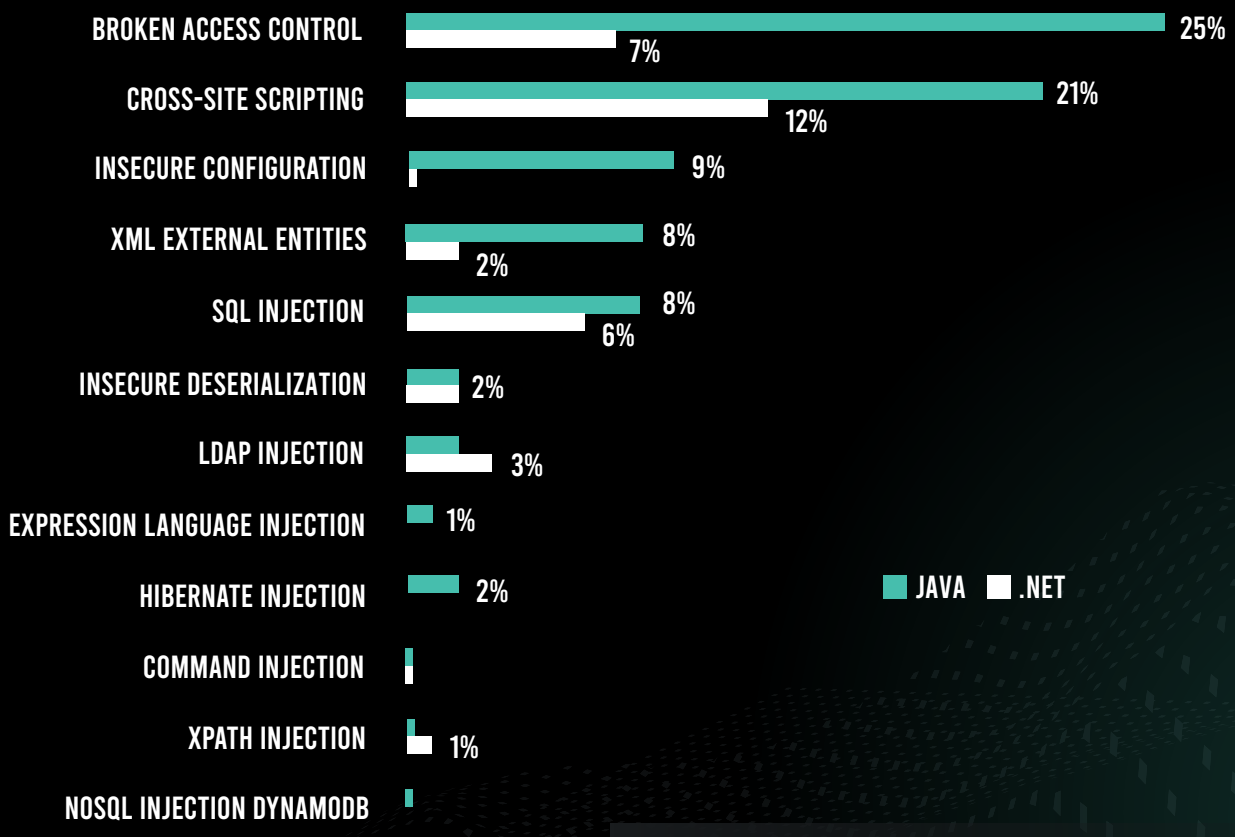


Figure 7: Percentage of Java and .NET applications impacted by serious vulnerabilities, by category.

04 | ATTACK TRENDS

DATA FROM CONTRAST PROTECT DURING SEPTEMBER–OCTOBER REVEALED A NUMBER OF TRENDS REGARDING APPLICATION ATTACKS:

TREND: MORE ATTACKS WERE VIABLE, AND MORE APPLICATIONS WERE IMPACTED BY SEVERAL ATTACK TYPES

September–October telemetry indicates that 2% of application attacks were viable—that is, hit an existing vulnerability (Figure 8). This is double the percentage found in July–August but a reversion to the 12-month average.

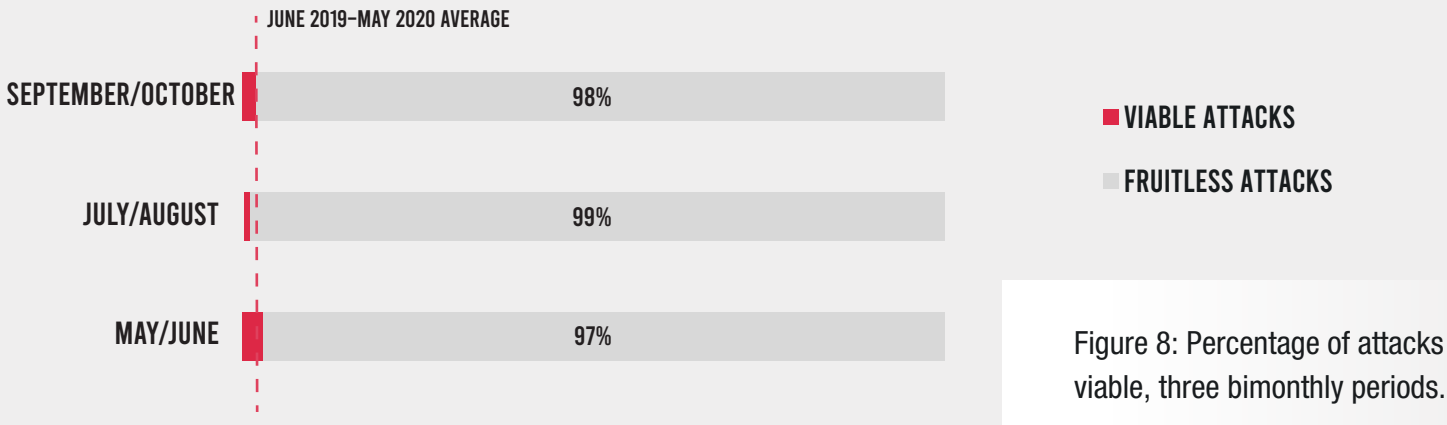


Figure 8: Percentage of attacks viable, three bimonthly periods.

Looking at attack categories, XSS attacks increased by 30%, impacting 76% of applications in September–October after affecting only 59% in July–August (Figure 9). Expression language (EL) injection and command injection hit 20% and 19% more applications than in the previous bimonthly period, respectively. One concerning thing to keep an eye on is the denial-of-service category, which has increased its impact from 3% to 6% to 9% of applications over the last three two-month periods. With distributed denial-of-service attacks up sharply in 2020,[8] this trend may continue.

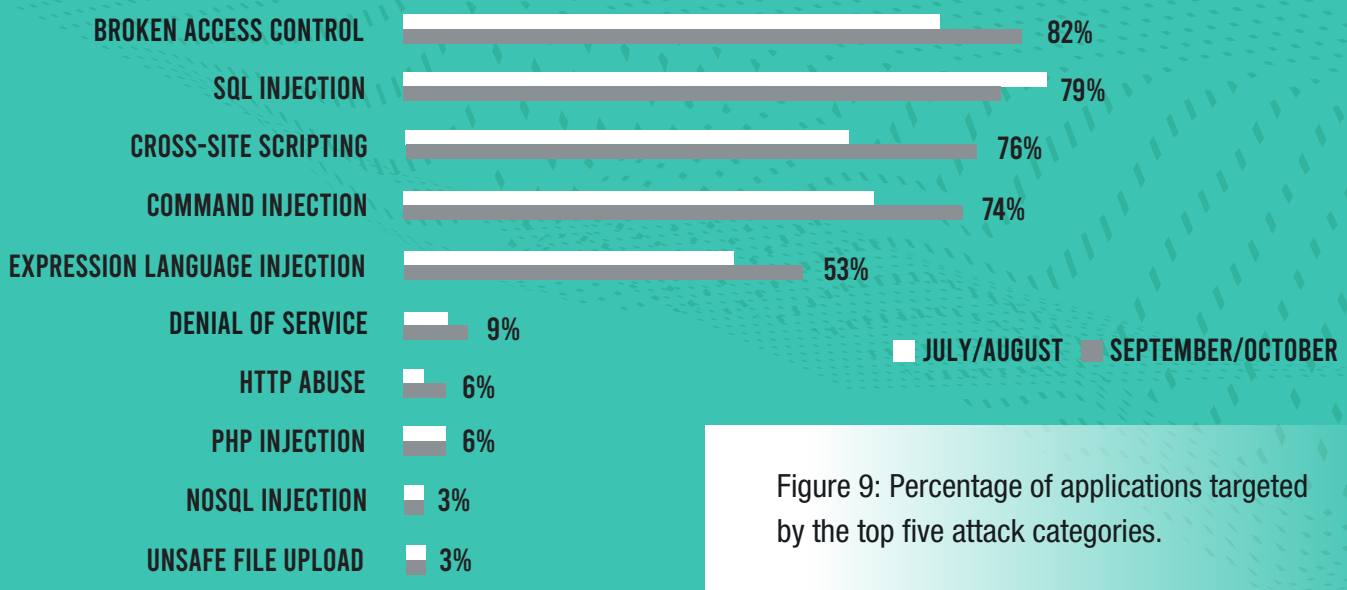


Figure 9: Percentage of applications targeted by the top five attack categories.

Looking at all attacks by attack type, 86% of attacks came from just two categories—SQL injection and command injection (Figure 10). This number is actually down from 96% in July–August, mainly due to a decrease in command injection attacks. But the current figure represents a reversion to a more "normal" percentage.

It is notable that XSS represented 9% of attacks in September–October, up from just 1% in July and August and 3% for the 12-month period ending May 31. This is reflected in the percentage of applications

affected by such attacks, as discussed above. If this trend continues, XSS will be an even more important consideration for those tasked with application security.

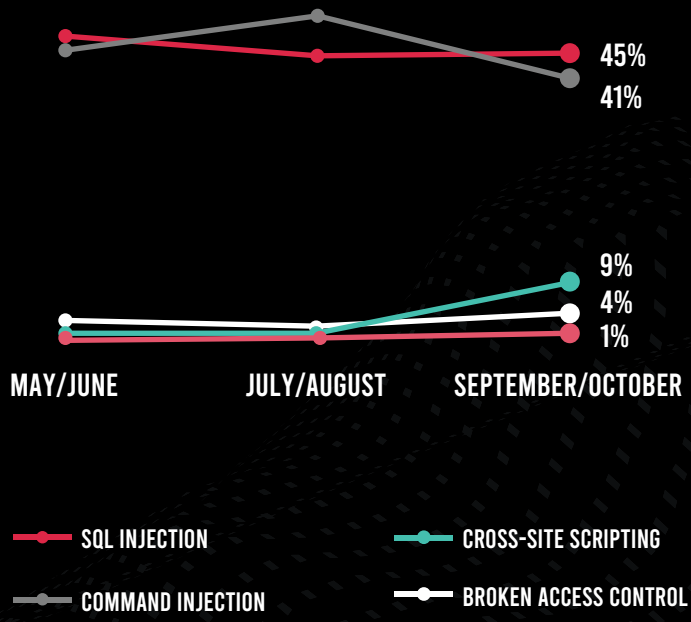
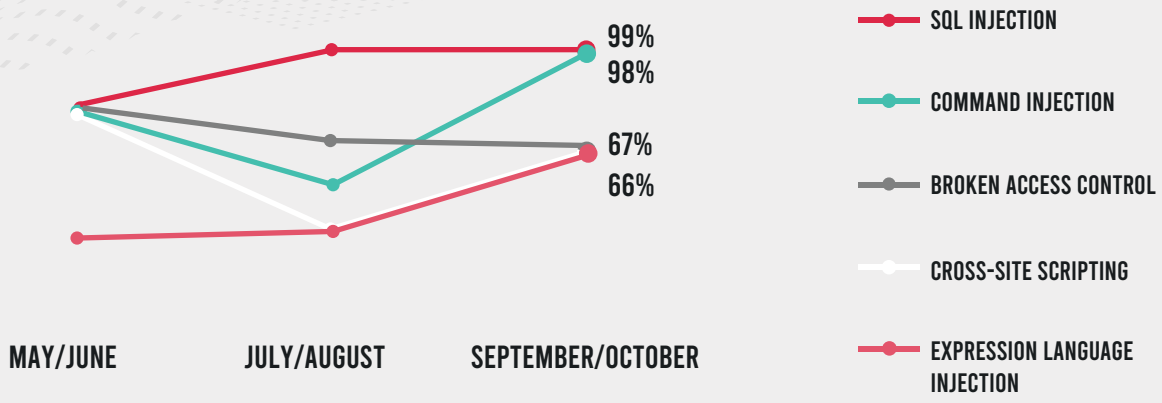


Figure 10: Percentage of attacks represented by the top five attack categories.

TREND: MANY ATTACK CATEGORIES IMPACTED .NET APPLICATIONS, WITH A BIG INCREASE IN COMMAND INJECTION

Looking at attacks by programming language, more .NET applications were impacted by a wide variety of attack types. Almost every .NET application experienced SQL injection and command injection attacks, with command injection increasing by 72% over July–August (Figure 11). XSS and command injections saw increases of more than 50% over the last bimonthly period. Overall, two-thirds or more of applications saw attacks in the five top categories in September–October.

Figure 11: Percentage of applications targeted, .NET.



For Java applications, the top five attack types all affected a higher percentage of applications in September–October than the previous two bimonthly periods (Figure 12), with increases of between 10% and 16%. Denial of service has also been spiking in terms of the percentage of Java applications affected. This attack category has gone from impacting 4% to 9% to 16% of applications over the past three bimonthly periods.

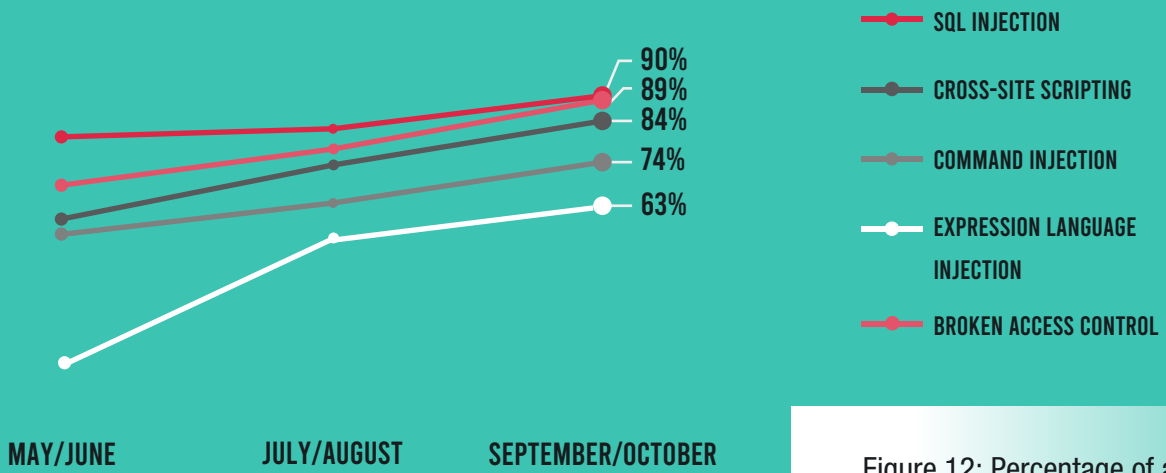


Figure 12: Percentage of applications targeted, Java.

05 | CONTRAST RISKSCORES FOR SEPTEMBER–OCTOBER 2020

The vulnerability and attack telemetry reflected in this report provides vital information for organizations trying to ensure secure applications. Contrast RiskScores provide an objective way to visualize the relative risk of different kinds of vulnerabilities over time—and adjust prioritization of remediation accordingly. Using its vulnerability and attack datasets, Contrast Labs continuously calculates the Contrast RiskScore based on the likelihood that a vulnerability type will occur compared with the likelihood that that specific vulnerability will be attacked. The rankings for September–October, along with past scores over a six-month period, are presented in Figure 13.

Given the increases in XSS seen throughout this report, especially the percentage of applications hit with such attacks, it is not surprising that the RiskScore for this category increased from 7.8 to 8.6. This moved XSS from fourth to second in the rankings behind broken access control. SQL injection, on the other hand, moved from second rank to fifth with a full point decrease in RiskScore to 7.7.

Further down the list, we see more significant increases and decreases. Hibernate injection declined almost two full points over the last bimonthly period, while insufficient logging and monitoring and XML external entities (XEE) injection increased by close to a point. In the biggest change for this report, NoSQL injection dropped from 6.8 to 4.6 after trending upward for several months.

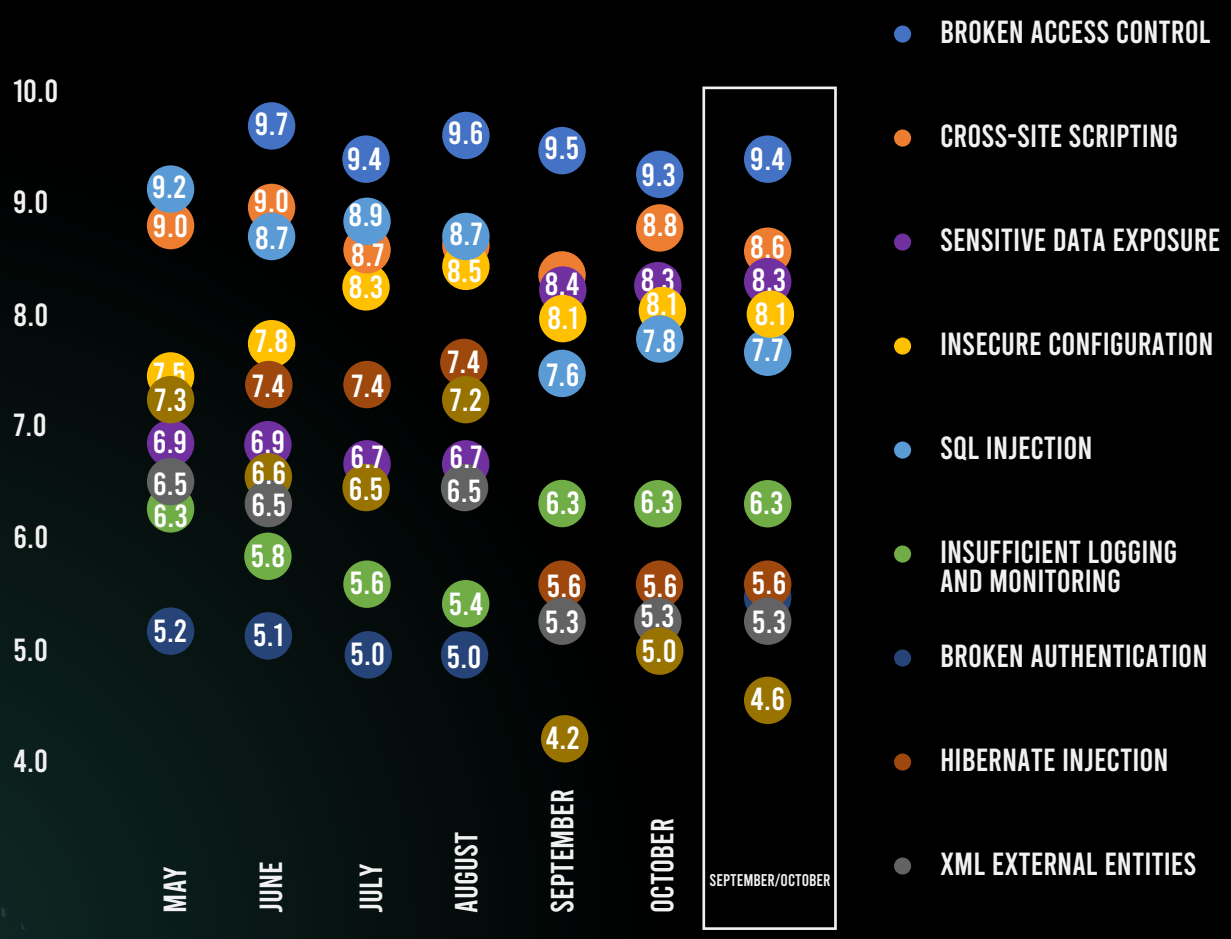


Figure 13: Top 10 vulnerability categories by Contrast RiskScore, May–October 2020.

06 | CONCLUSION

As different industries face differing economic prognoses in the near term, the importance of application development to the bottom line continues to increase almost universally. The uncertainty brought on by COVID-19 will weigh on organizations over the next several months, with many reluctant to make financial investments beyond those required to stay in business.

However, despite the opportunities it presents, the application security landscape continues to pose significant risk to organizations. Telemetry for September–October shows that more applications have serious vulnerabilities than in July–August, and more have 50 or more serious vulnerabilities. Those who use the .NET language should be concerned that both serious vulnerabilities and attacks were much more prevalent in September–October for that subset of applications.

Furthermore, a greater percentage of attacks by adversaries hit an existing vulnerability than in July–August. This could mean that some of the attack probes detected in the last bimonthly period identified vulnerabilities that could be exploited. And a significant spike in the percentage of applications impacted by SQL injection attacks is concerning. All in all, it is clear that many organizations need to take a more strategic approach to improving application security.

Contrast Labs hopes that the findings presented here will help readers prioritize their short-term application security efforts and refine their longer-term strategic plans. Security instrumentation embeds continuous security testing and runtime protection within the application itself. This enables application security observability throughout the SDLC. It also affords organizations the ability to discover and repair vulnerabilities in near real time, rather than identifying them later in the process. This "shift left" empowers developers to remediate problems on the fly and prevents coding delays.[9] Instrumentation also enables companies to "shift right" to protect applications in production as new vulnerabilities are identified.[10] This comprehensive and continuous protection helps organizations to move beyond legacy approaches to application security to methods that fit today's rapid development timelines and the increasingly complex threat landscape.

---

1 "Covid-19: U.S. Breaks Daily Record With Over 99,000 New Cases as Surge Quickens," The New York Times, October 31, 2020.

2 Chuck Jones, "Three Charts Show A K-Shaped Recovery," Forbes, October 24, 2020.

3 "Is COVID Changing the Job Market for Software Developers?" Decide Consulting, October 14, 2020.

4 Steve Ranger, "Software developer jobs are growing again. But the top skills companies want are changing," ZDNet, August 12, 2020.

5 "The State of DevSecOps Report," Contrast Security, December 2020.

6 "State of Software Security, Volume 11," Veracode, October 27, 2020.

7 "Contrast 2020 Application Security Observability Report," Contrast Security, July 2020.

8 Dan Raywood, "DDoS Attacks Hit 1 Tbps in 2020," Infosecurity Magazine, September 17, 2020.

9 Jakob Pennington, "Shifting Left: DevSecOps as an Approach to Building Secure Applications," Medium, July 18, 2019.

10 Alan Shimel, "DevOps Chat: Shifting Security Left and Right, With Contrast Security," Security Boulevard, October 7, 2019.

CONTRAST SECURITY

240 3rd Street
Los Altos, CA 94022
888.371.1333

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyberattacks, heralding the new era of self-protecting software. Contrast's patented deep security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncover vulnerabilities, prevent data breaches, and secure the entire enterprise from development, to operations, to production.