

PRIORITIZING APPLICATION SECURITY RISK MANAGEMENT WITH THE CONTRAST RISKSCORE

EXECUTIVE SUMMARY

Application security has become more and more important to organizations as digital transformation makes applications increasingly business critical. The proliferation of applications means an increase in vulnerabilities—and this translates into a backlog of unresolved ones at many organizations. To minimize risk exposure, organizations often need to prioritize which vulnerabilities must be fixed most urgently—and which risks should be prioritized for response for applications in production.

With no effective tools to measure the relative risks of application threats, Contrast Labs recently developed an algorithm to simply and precisely illustrate this risk. The Contrast RiskScore Index provides a numerical score that illustrates risk for a variety of vulnerability types. Later this year, the Contrast RiskScore Index will be released in an open-source version that will help organizations customize RiskScores to their individual risk profiles.

For this report, Contrast Labs calculated Contrast RiskScores retroactively for 12 months using the latest beta of the algorithm, to show how this measurement has changed over time. Overall, 14 vulnerability types (out of 19 total) registered one of the top 10 RiskScores in at least one month in 2020. And while the top three were remarkably consistent, nine entered the top six at some point during the year. Following the fluctuations in these “mid-tier” rankings can be especially helpful in prioritizing risk.

Now that there is a numerical score for each vulnerability type, organizations can prioritize vulnerabilities above a certain score based on bandwidth and risk tolerance. Such decisions should be a part of a larger application security strategy that emphasizes “shifting left” to discover and fix vulnerabilities earlier in the development process, and “shifting right” to provide continuous protection to applications in production.



As the global economy becomes more dependent on digital tools for everything from customer engagement to manufacturing operations, software applications—and the computing platforms they run on—have become increasingly critical to operations in every industry. At the same time, cybersecurity risk has become a bigger threat—and has now been a top concern for executives and board members for at least the last several years.¹

More recently, threats specifically targeting applications have become more pronounced. The 2020 Verizon Data Breach Investigations Report found that 43% of data breaches in the prior year were the result of a web application vulnerability—a figure that more than doubled over Verizon’s 2019 report.² Similarly, a recent Ponemon Institute study commissioned by IBM found that 42% of respondents whose company had suffered a breach attributed the cause to a known but unpatched security vulnerability.³

42% OF COMPANIES THAT SUFFERED A BREACH ATTRIBUTED THE CAUSE TO A KNOWN BUT UNPATCHED VULNERABILITY.⁴

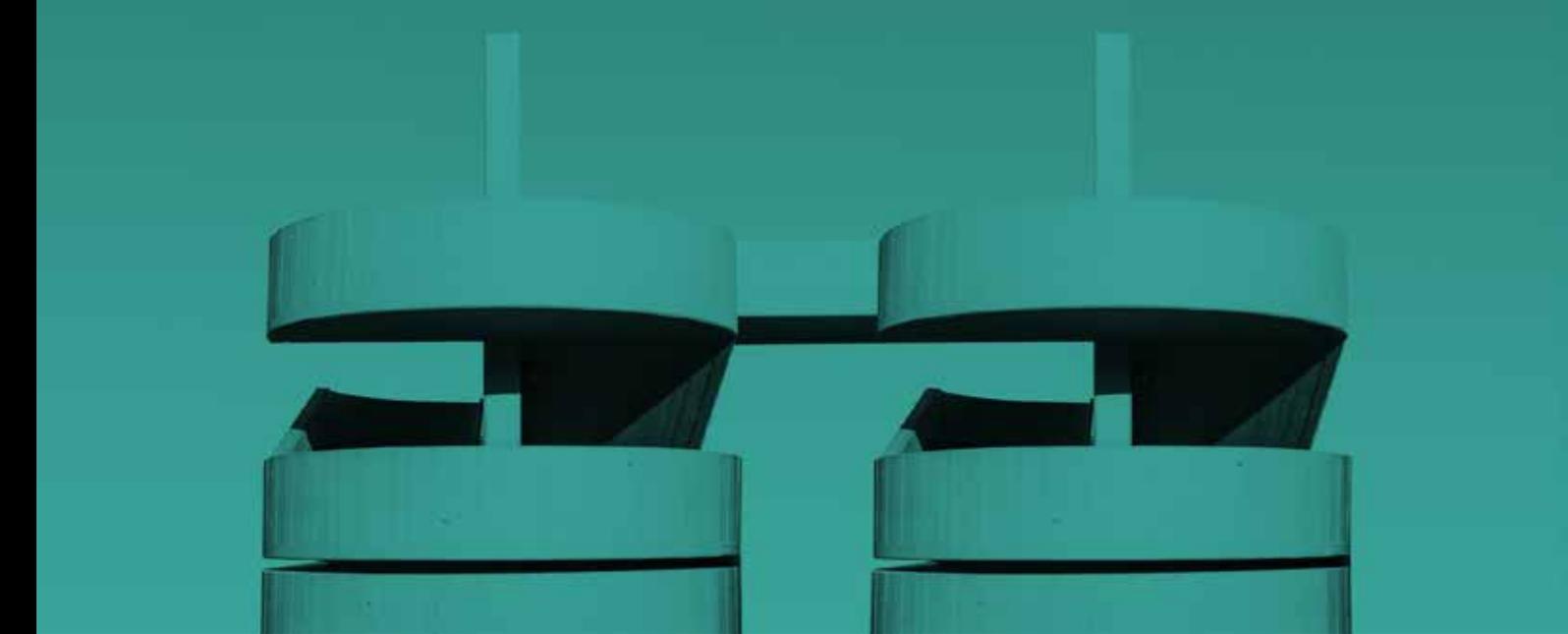
AVOIDING SECURITY DEBT

At first glance, it seems that the solution to this problem is relatively straightforward: Organizations should do a better job of remediating application vulnerabilities in a timely manner. But this is easier said than done. Recent research by Contrast Security found that at nearly three-quarters of organizations, detection, investigation, remediation, and verification of fixes consume five or more hours of time *per vulnerability* for the development and security teams.⁵ The sheer number of vulnerabilities identified—including a large number of false positives returned by legacy application security tools—means that many organizations simply do not have the bandwidth to remediate all of them.

The result at many organizations is a growing backlog of software vulnerabilities, known as security debt. This poses unacceptable risk to organizations: A recent study by the Ponemon Institute and IBM found that 42% of companies that suffered a data breach attributed the cause to a *known but unpatched* software vulnerability.⁶ This increases risk to organizations in both the shorter and longer terms.

Nearly every respondent to the above-referenced Contrast Security survey admitted that the average application *in production* where they work has four or more vulnerabilities, and 61% said they had sustained at least three attacks that successfully exploited vulnerabilities over 12 months.⁷ And over time, research based on application security telemetry by Contrast Labs finds that organizations with higher security debt see more vulnerabilities on an ongoing basis, increasing that debt further and making the problem even more insurmountable.⁸

61% OF ORGANIZATIONS SUSTAINED 3+ SUCCESSFUL ATTACKS ON VULNERABILITIES IN 12 MONTHS.⁹



THE NEED FOR DYNAMIC RISK SCORING

Given the volume of vulnerabilities, organizations clearly need a dynamic way to understand the relative risk presented by specific vulnerabilities so that remediation, threat hunting, investigation, detection, and response efforts can be prioritized. Unfortunately, this is, at best, a work in progress at many organizations. One study found that 57% of organizations have not taken the first steps to determine which vulnerabilities are the riskiest.¹⁰ And while actuarial data is used to evaluate many other areas of risk, telemetry data of vulnerabilities and attacks is seldom used to assess application security risk.

One problem is that tools simply do not exist to calculate the risk of a specific vulnerability to a specific organization at a specific time. Such a tool would need to be dynamic, enabling decision-making at the speed of DevOps. While exact precision is never possible, it would need to be reasonably accurate. Uncertainty factors should be built in and made transparent.

Existing tools simply do not meet these requirements. The oft-cited OWASP Top 10 from the Open Web Application Security Project provides a starting point by identifying 10 vulnerability types that need the most attention, but does little to help in prioritizing specific vulnerabilities. In addition, the OWASP Top 10 is only updated once every several years. The Common Weakness Scoring System (CWSS) is very accurate but too detailed, making it impractical to use in real-world settings. Similarly, Factor Analysis of Information Risk (FAIR) is too detailed in its measurement of broader risk to use with specific vulnerabilities.

One major weakness of all these models is that they fail to account for the likelihood that a vulnerability will be exploited by an attacker. In other words, threat intelligence and modeling from application attacks is not incorporated into the model. This is important because vulnerabilities targeted by active probes and attempted attacks present greater risk to an organization than vulnerabilities that are not targeted.

THE DEVELOPMENT OF RISKSCORE

To alleviate these problems and help organizations with these prioritization efforts, Contrast Labs tasked practitioners with many years of application security and risk management experience to develop a numerical score based on the current risk posed by each vulnerability type. Their goal was to create a scoring system that is simple to understand and use, dynamically adapts to real-world data, allows for uncertainty and missing data, and adaptively requires additional data when the risk is near an organization's risk threshold.

The Contrast Labs team developed and is continuously refining a robust algorithm that uses aggregate telemetry data on vulnerabilities and attacks from customers using Contrast Assess and Contrast Protect. The numerical score produced by the algorithm is dubbed the Contrast RiskScore Index, and scores were first included in Contrast Security's bimonthly Application Security Intelligence Report in July–August 2020. The Contrast RiskScore Index will be a part of every bimonthly Intelligence report going forward, as well as the annual Application Security Observability Report.

The ultimate goal is to provide an open-source tool that enables organizations to calculate their own RiskScores to quantify specific risk levels for vulnerabilities in their own applications against their own risk portfolio. Contrast Labs plans to release the open-source version of the RiskScore Index later this year.

DATA INPUTS

Contrast Labs uses several metrics to calculate its RiskScore:

- Vulnerability Prevalence

- The percentage of applications that have any instances of a *specific* vulnerability type
- The percentage of total vulnerabilities represented by a *specific* vulnerability type
- Vulnerability Severity
 - The percentage of applications that have any *serious* vulnerabilities of a specific type
 - The percentage of total *serious* vulnerabilities represented by a specific type
- Runtime Attack Likelihood
 - The percentage of overall attacks represented by a *specific* attack type
 - The percentage of overall *viable* attacks (i.e., attacks that hit an actual vulnerability in an application) represented by a *specific* attack type

The results of the three categories of data are multiplied, then weighted and normalized into a scale of zero to 10. After finalizing the current version of the formula, Contrast Labs retroactively calculated RiskScores going back 12 months to January 2020. This report is based on the Beta v.5 RiskScore Algorithm, on which the open-source algorithm will be launched.

BETA V.5 RISKSCORE ALGORITHM

Pre-release open-source algorithm (later in 2021) used to measure application risk at the level of individual applications, vulnerability types, and applications per language.

$$\left(\underset{\text{Vulnerability Prevalence}}{\text{VP}} \times \underset{\text{Vulnerability Severity}}{\text{VS}} \times \underset{\text{Viable Attack Prevalence/Likelihood to Exploit}}{\text{AP}} \right) \text{ Normalized and Weighted} = \text{RiskScore}$$

Vulnerability Prevalence (VP) is the percent of applications that have all or serious vulnerabilities

Vulnerability Severity (VS) is the percent of vulnerabilities represented by specific vulnerability type

Attack Prevalence & Likelihood to Exploit (AP) is percent of overall viable attacks represented by specific attack type and applications that received attacks of a specific type

Figure 1. Calculation of Contrast RiskScore Index.



RISKSCORE APPLIED: THE MOST DANGEROUS WEB APPLICATION AND API RISKS

On the RiskScore Index's 10-point scale, eight vulnerability types averaged above 6 for 2020, and three averaged above 8 (Figure 2). Looking at these annual averages can be informative for long-term planning, and a rolling 12-month average will be available in the open-sourced version of the RiskScore Index.

However, a more granular look at fluctuations in the RiskScore Index over time is helpful as well. Some threats, such as broken access control, cross-site scripting (XSS), and broken authentication, had only very narrow variations over the year (Figure 3). On the other hand, expression language (EL) injection, NoSQL injection, and XPath injection fluctuated by a full point or more on the scale. This could represent an increase or decrease in prevalence in a given month (because of prioritization—or lack thereof—by application owners) or an increase of attacks targeting the vulnerability.

Overall, a total of 14 vulnerability types appeared among the top 10 RiskScores during at least one month in 2020, nine threat types appeared in the top six, and four appeared in the top three (Figure 4).

BROKEN ACCESS CONTROL, SQL INJECTION, AND CROSS-SITE SCRIPTING TOPPED THE RANKINGS FOR 11 OUT OF 12 MONTHS.



Figure 2. Average RiskScores for January–December 2020.

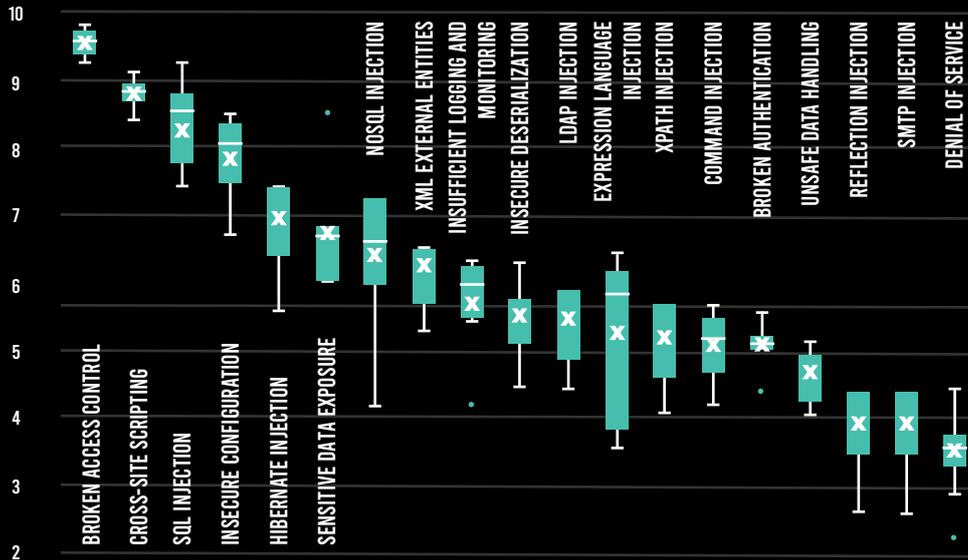


Figure 3. Minimum, 25th percentile, median, mean, 75th percentile, and maximum RiskScores for select vulnerability types, January–December 2020.

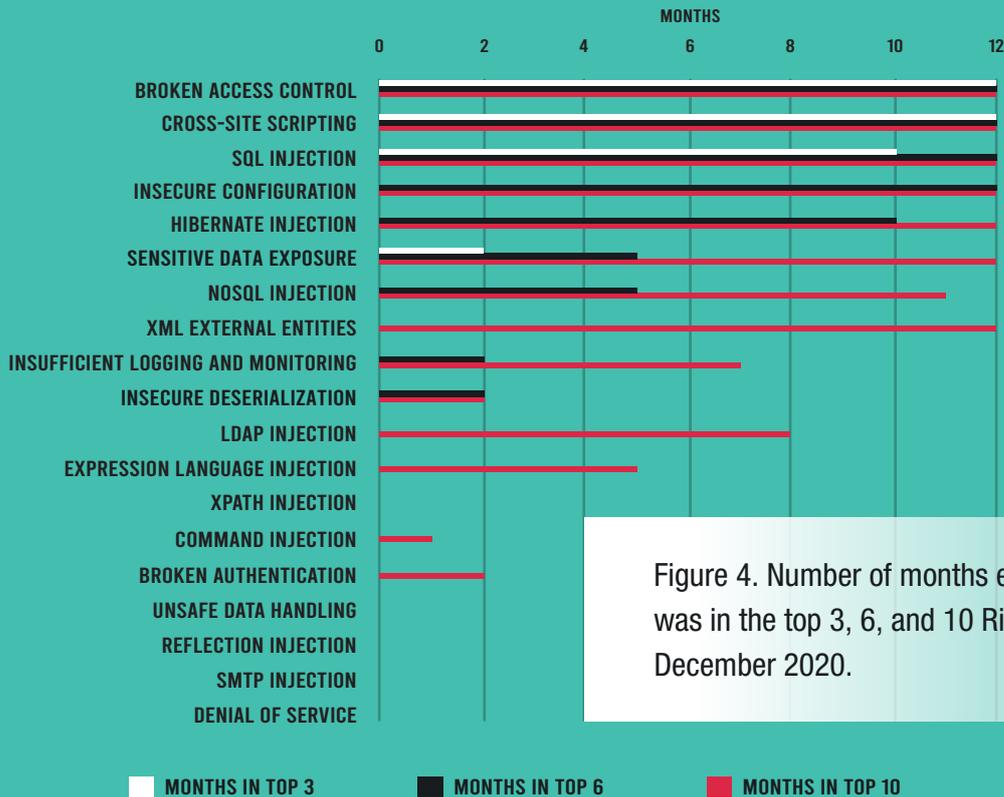


Figure 4. Number of months each vulnerability type was in the top 3, 6, and 10 RiskScores, January–December 2020.

BROKEN ACCESS CONTROL: CLEARLY THE BIGGEST RISK

Broken access control was indisputably the biggest threat for the year, with an average RiskScore for the year of 9.47, three-quarters of a point above any other category (Figure 2). It had the highest RiskScore for the entire year, except in May, when it was tied with SQL injection for the number one position (Figure 5). While the percentage of applications that had a serious vulnerability of this type hovered between just 13% and 16% over the year, attack likelihood was high. In fact, 85% of applications sustained a broken access control attack in the last two months of the year.

Considering that access control is a critical linchpin in any organization's cybersecurity architecture, and that many breaches and intrusions result from unauthorized access to various systems and applications, it is not surprising that this threat type consistently rated as the riskiest.

THE REST OF THE TOP FIVE: DECLINES LATE IN THE YEAR

Cross-site scripting (XSS) ranked second and SQL injection ranked third in the annual average, with average scores of 8.72 and 8.37, respectively (Figure 2). While the RiskScore for XSS threats remained relatively steady all year, the score for SQL injection declined in the latter part of the year (Figure 5). As a result, only broken access control and XSS were in the top three for every month of 2020.

Again, the high RiskScores for XSS and SQL injection are more attributable to attack volume rather than vulnerability prevalence, with close to three-quarters of applications on the receiving end of both attack types in the last half of the year. SQL injection has been used in several well-publicized data breaches in recent years, including a years-long crime spree in which Iranian hackers allegedly compromised data from consumers, companies, and the U.S. government.¹¹ On the other hand, some observers have noted that many XSS vulnerabilities present medium risk at worst.¹² Regardless, with RiskScores consistently above 8, XSS will remain a high priority in application security for the foreseeable future.

Insecure configuration and hibernate injection round out the top five in terms of the annual averages (Figure 2). However, both have seen a decline in their RiskScores in the last five months of 2020, pushing

both scores below 7. Despite this, they retained the fourth and fifth rankings in December 2020 after dropping out of the top five for a few months. Configuration errors have long been recognized as a major source of data breaches, and faulty configurations built into a piece of software can be replicated across an organization. Hibernate injection is related to SQL injection and targets one of the most commonly used database libraries used in Java applications.

RISKSCORE TRENDS FOR TOP VULNERABILITIES

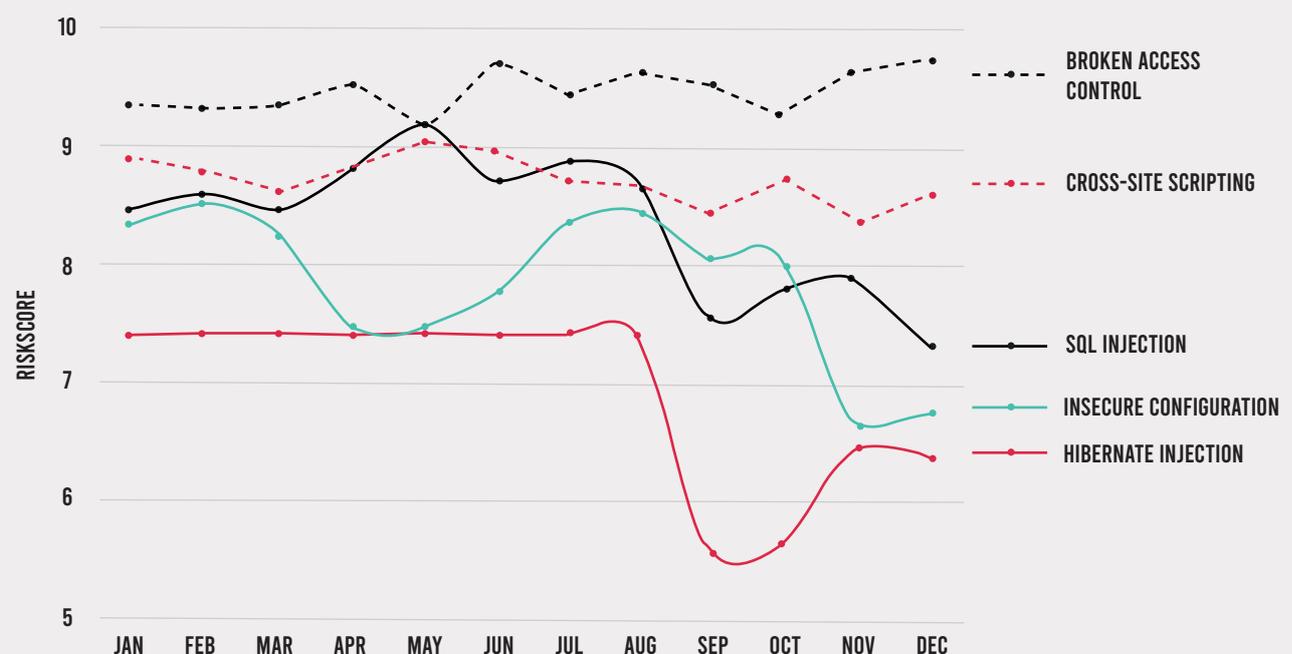


Figure 5. RiskScore trends for the five riskiest vulnerability types, January–December 2020.

MID-TIER RISKSCORES: FLUCTUATION CAN INFORM STRATEGY

As it turns out, five vulnerability types fluctuated into and out of the top six, but never cracked the top three (Figure 6). These “mid-tier” vulnerabilities often pose difficulties to organizations when it comes to vulnerability prioritization, and the truth is that their risk fluctuates as both vulnerability prevalence and

attack volumes change. Monitoring the evolving risk of these threats—and adjusting prioritizations accordingly—may be one of the biggest benefits of the Contrast RiskScore Index for organizations once the algorithm is available to the public.

Of the five, two have seen stable positions in the rankings. As discussed above, insecure configuration and hibernate injection held the fourth and fifth positions for almost the whole year. Others that moved into fifth and sixth position throughout the year include NoSQL injection, insecure deserialization, and insufficient logging and monitoring. The latter threat type has been trending higher in the rankings for most of the last half of the year.

9 VULNERABILITY TYPES APPEARED IN THE TOP 6 RISKSCORES FOR AT LEAST ONE MONTH IN 2020.

RISKSCORE TRENDS

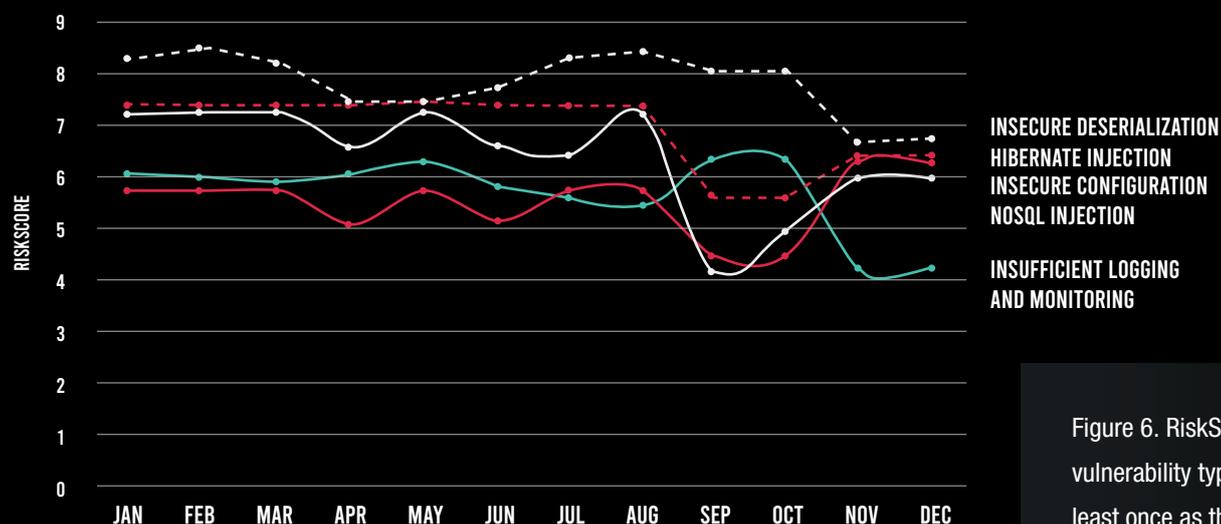


Figure 6. RiskScore trends for vulnerability types that appeared at least once as the 4th, 5th, or 6th riskiest, but never in the top 3 from January–December 2020.

12-MONTH RISKSORE TRENDS

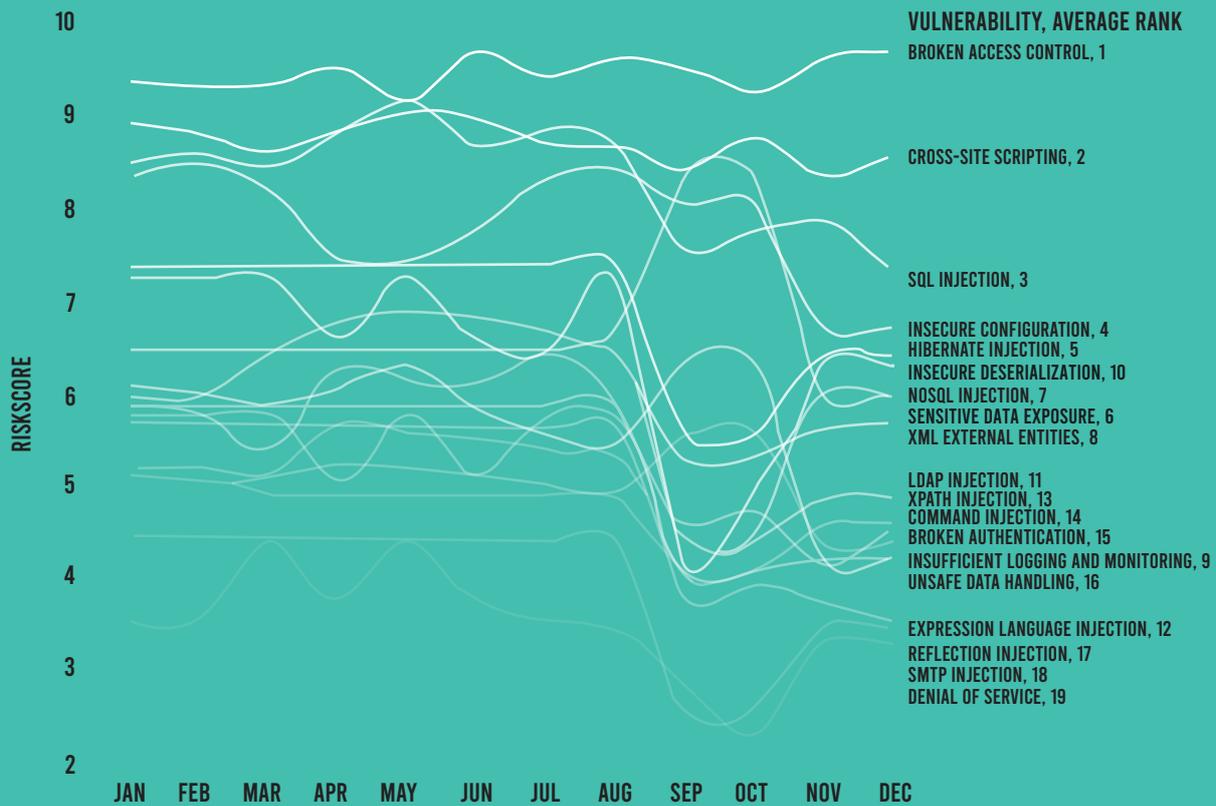
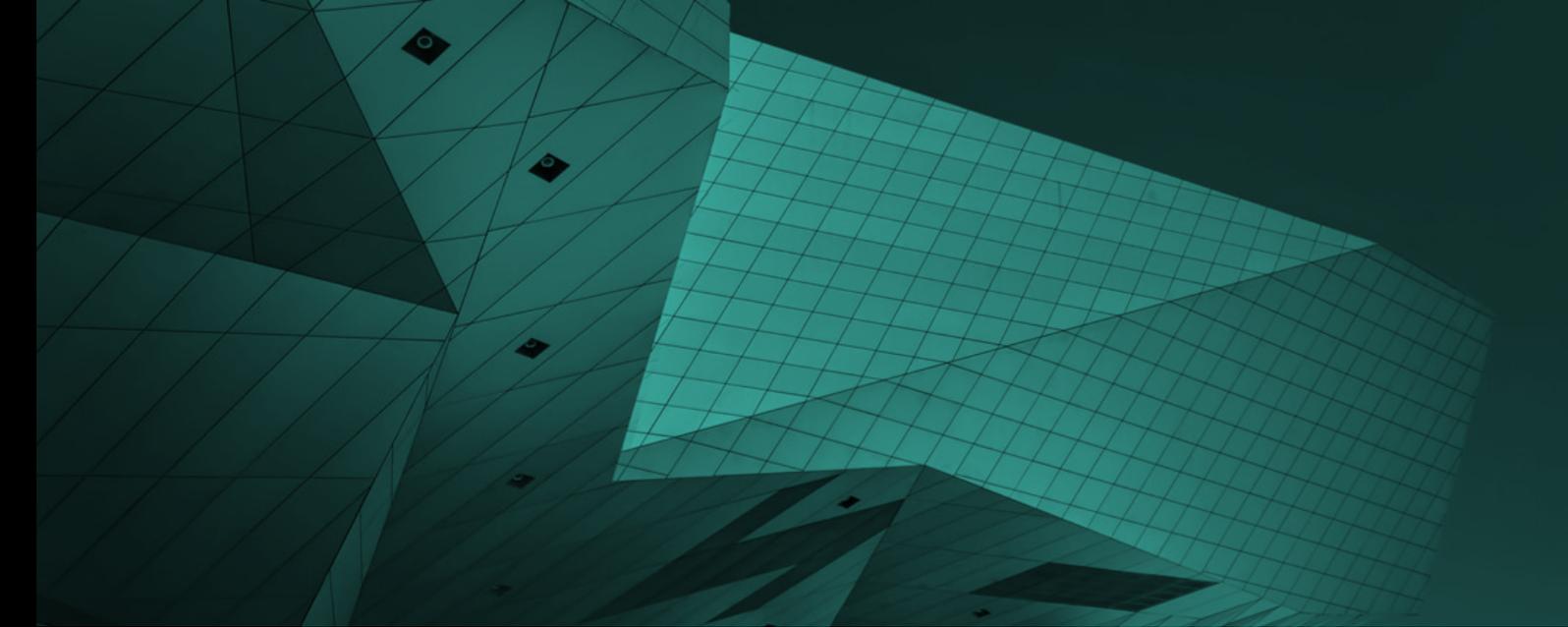


Figure 7. RiskScore trends for 19 common vulnerability types, January–December 2020.



TAKEAWAYS

The Contrast RiskScore Index uses actual data from real companies to help organizations prioritize their application security efforts. It will be a part of Contrast Labs' bimonthly Application Security Intelligence Reports going forward, along with analysis of trends and changes. The goal has been to create a model to help answer risk questions without getting overly complicated. Later in the year, the open-source version of the Contrast RiskScore Index will enable organizations to customize their scores with their own telemetry data and according to their own risk profile.

While much has happened in the past 12 months—including monumental changes in the ways that most companies do business—application security threats have remained remarkably steady. As a result, all organizations should have the goal of addressing all vulnerabilities within a short time frame, reducing the mean time to remediate (MTTR) and median time to remediate for all vulnerabilities, in order to eliminate security debt and minimize vulnerabilities in the future. However, some vulnerabilities present more risk than others. For example, vulnerabilities in open-source code that are not used by the application present zero risk. To determine which vulnerabilities matter and which ones present the highest risk, organizations can use the Contrast RiskScore as a tool to help prioritize those risks—both to reduce security debt in the short run and to manage risk over the long term.

Fluctuation in RiskScores from month to month can inform short-term decision-making by revealing short-term changes in risk. But for strategic planning, it is best to consider some sort of rolling average similar to the 12-month averages presented here.

Notwithstanding, the use of these insights is one part of a larger application security strategy. Vulnerabilities must be found and remediated much earlier in the software development life cycle (SDLC)—a process known as “shifting left.”¹³ This is enabled by security instrumentation, which helps developers to discover vulnerabilities in real time and remediate them on the fly, before they add time and expense to the development process. Instrumentation puts continuous security testing into the application itself, eliminating time-consuming scans and the false positives that they produce. At the same time, “shifting right” enables development teams to build self-protection into applications in production.¹⁴ This approach helps organizations eliminate security debt over time and provides comprehensive protection from a single platform throughout the SDLC.

¹ Cybersecurity was discussed at 89% of board meetings according to “NACD Director’s Handbook on Cyber-Risk Oversight,” National Association of Corporate Directors, February 25, 2020.

² “2020 Data Breach Investigations Report,” Verizon, April 2020.

³ “The State of Vulnerability Management in the Cloud and On-premises,” Ponemon Institute and IBM, August 2020.

⁴ Ibid.

⁵ “The State of DevSecOps Report,” Contrast Security, November 2020.

⁶ “The State of Vulnerability Management in the Cloud and On-premises,” Ponemon Institute and IBM, August 2020.

⁷ “The State of DevSecOps Report,” Contrast Security, November 2020.

⁸ “2020 Contrast Labs Application Security Observability Report,” Contrast Security, September 2020.

⁹ Ibid.

¹⁰ Lisa Morgan, “Focused on application vulnerabilities? You’re missing the bigger picture,” SD Times, March 2, 2020.

¹¹ John Leyden, “Iranian cybercrime duo charged with multiple US hacking offenses,” The Daily Swig, September 17, 2020.

¹² David Lindner, “Contrast Labs: Mapping Risk Profiles for Select OWASP Top 10 Vulnerabilities To Understand Their AppSec Risk,” Contrast Security, May 19, 2020.

¹³ Jakob Pennington, “Shifting Left: DevSecOps as an Approach to Building Secure Applications,” Medium, July 18, 2019.

¹⁴ 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 leader in modernizing application security, embedding code analysis and attack prevention directly into software. Contrast's patented deep security instrumentation completely disrupts traditional application security approaches with integrated, comprehensive security observability that delivers highly accurate assessment and continuous protection of an entire application portfolio. This eliminates the need for expensive infrastructure workloads and specialized security experts. The Contrast Application Security Platform accelerates development cycles, improves efficiencies and cost, and enables rapid scale while protecting applications from known and unknown threats.

