EBOOK

Contrast
SECURITY

How to Keep Up with the Rapidly Expanding Scope of the OWASP Top Ten

Using Out-of-the-Box Policy Management and Reporting in the Contrast Application Security Platform.

Executive Overview

The Open Web Application Security Project (OWASP) released the 2021 OWASP Top Ten, a ranking of the biggest application security risks facing organizations that develop and use software. The updated list is based on a massive study of telemetry data from more than 500,000 applications protected by tools from 13 different application security vendors. The study is significantly more comprehensive than all previous releases dating back to the initial release in 2003.

Three of the items in this edition of the OWASP Top Ten are new, attempts to identify emerging trends based on data analysis and a broad industry survey. Insecure Design debuts at number 4 and brings visibility to underlying architectural problems that can result in a host of vulnerabilities in an application. Its inclusion in the Top Ten highlights the need to design applications for security, even before the first line of code is written. Similarly, Software and Data Integrity Failures is a new category that addresses the need to ensure that applications and data are not tampered with by malicious third parties before being accessed by users. Finally, Server-Side Request Forgery (SSRF) is an emerging vulnerability that can give an attacker access to internal systems.

The other seven items in the Top Ten are continuations from the 2017 Top Ten, with some items combined and recategorized. In general, the Top Ten has evolved from focusing on individual vulnerabilities to covering broader security control areas. Items in the Top Ten include risks from the software supply chain, open-source libraries and frameworks, and common problems like broken access control and injection. In all, nearly 200 Common Vulnerabilities and Exposures (CVEs) are now included in the Top Ten.

Now is the time for organizations to start focusing on the new Top Ten—especially the three new items. They must ensure that adequate precautions are in place for each of its categories and underlying elements. The good news is that the Contrast Application Security Platform provides uniquely robust coverage for the OWASP Top Ten, including the changes made in 2021. The Contrast platform provides comprehensive coverage for custom and open-source code from development to production, policy management with rules for each Top Ten category and individual vulnerabilities, and automated reporting on OWASP Top Ten vulnerabilities. These key capabilities enable organizations to prompt development, security, and operations teams to collaborate effectively and execute on a true DevSecOps approach.

> “This installment of the top ten is more data-driven than ever but not blindly data-driven.
>
> OWASP Top Ten 2021, Draft for Peer Review

Table of contents

01

The Research: An Unprecedented Data Science Achievement

OWASP celebrated its 20th anniversary this year, and its work has become increasingly influential over time. The organization's most high-profile project is the OWASP Top Ten, a ranking of the biggest application security risks facing organizations. New versions of the Top Ten have been released, on average, once every three years. The latest release in September 2021 supersedes the 2017 OWASP Top Ten.

Many organizations now use the OWASP Top Ten to assess the completeness of their application security efforts. Thus, development and security teams need to know and understand the new Top Ten—and its implications for compliance and risk management.

THE LARGEST DATASET EVER

For the 2021 Top Ten, OWASP correlated telemetry data on more than 500,000 applications protected by solutions from 13 application security vendors. The number of applications analyzed almost tripled over the 2017 study, and the data is more complete. The organization also used data from a comprehensive survey that spanned many industries, company sizes, and geographies to glean insights on new and emerging threats.

The size of the dataset is a great achievement for OWASP. But there are downsides to the approach as well. One problem is that OWASP has no way to account for false positives in the dataset. In a recent survey by Contrast, 80% of respondents reported that at least half of alerts generated by their scanning tools are false positives, and 38% put that ratio above three-quarters.[1] With basically the entire application security industry providing data for the research, a similar percentage of the vulnerabilities identified in the data are likely false positives. Another drawback is that the OWASP study focuses only on vulnerabilities and does not include actuarial attack data. Contrast's 2021 Application Security Observability Report[2] is based on both vulnerability and attack data, and that data and the corresponding RiskScore Index™ are far more accurate than the industry average.

[1] "The State of DevSecOps Report," Contrast Security, November 2020.

[2] "2021 Application Security Observability Report," Contrast Security, August 2021.

Eight of the Top Ten were identified through the telemetry data, and seven of these represent elements that were a part of the 2017 Top Ten, albeit somewhat reorganized (Figure 1). One new element, Server-Side Request Forgery (SSRF), was added to the 2021 Top Ten based on both telemetry and survey data. Two new additions for 2021 were determined as emerging risks through the industry survey. A total of nearly 200 vulnerabilities from the Common Weakness Enumeration (CWE) database are a part of the 2021 Top Ten (Figure 2), categorized based on either their root cause or their impact. This number is up from 34 in 2017.

Since the OWASP Top Ten aims to be a fairly comprehensive list of the biggest application security risks, significant effort went into categorizing vulnerabilities in such a way that the vast majority of major risks fit into the arbitrary number of 10 bullets. The result is that each succeeding version of the list tends to contain more combinations of categories, and 2021 is no exception (Figure 1). This means that practitioners must be aware that many of the Top Ten have multiple subcategories that must be dealt with in unique ways.

> “
>
> OWASP’s approach necessarily sorts for applications that organizations are willing to pay to protect. As a result, this is a study of the most important applications out there.
>
> Jeff Williams, “The Forthcoming 2021 OWASP Top Ten Shows That Threat Modeling Is No Longer Optional,” Contrast Security AppSec Observer Blog, September 8, 2021.

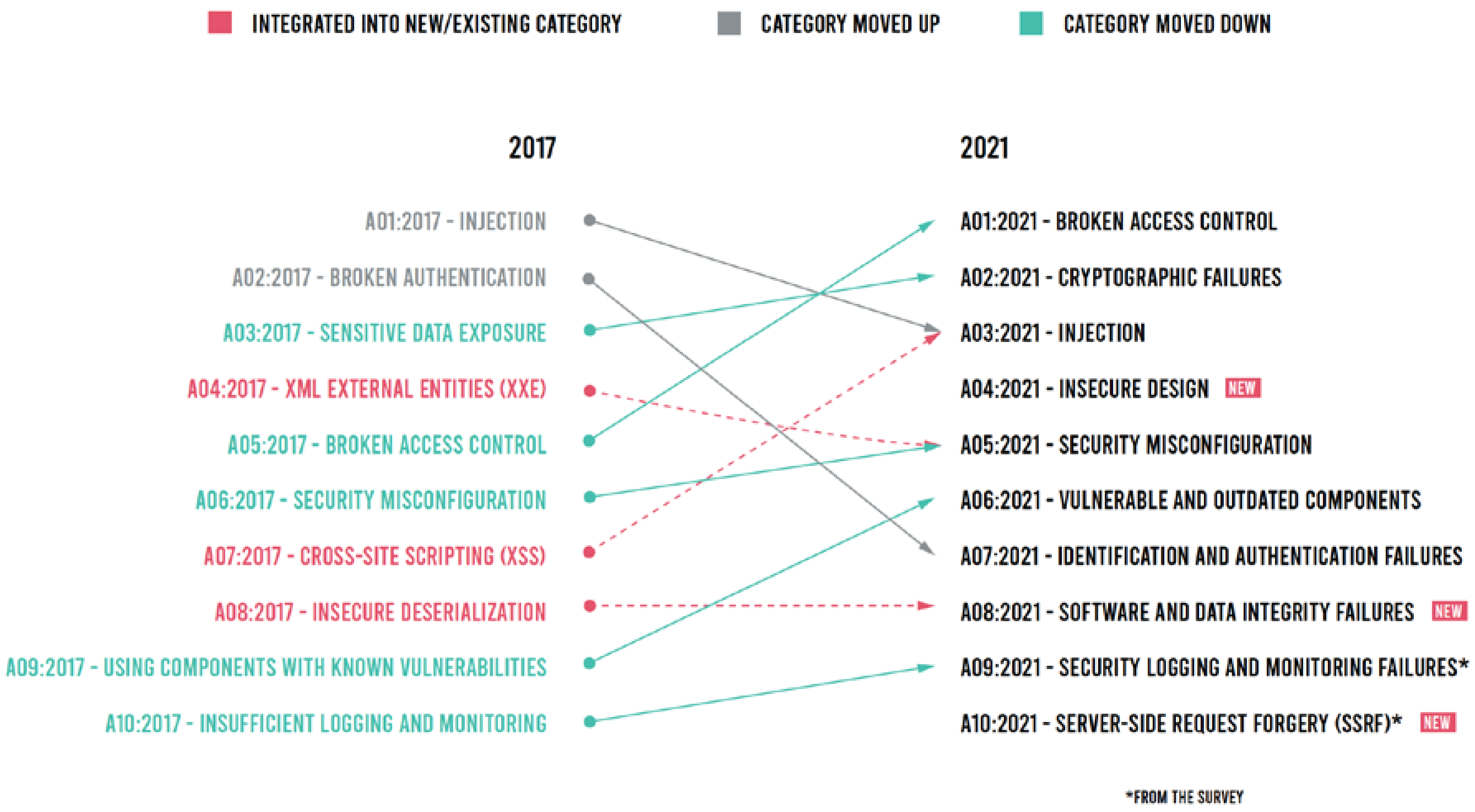

🟥 INTEGRATED INTO NEW/EXISTING CATEGORY
▨ CATEGORY MOVED UP
🟩 CATEGORY MOVED DOWN
2017
2021
A01:2017 - INJECTION
A02:2017 - BROKEN AUTHENTICATION
A03:2017 - SENSITIVE DATA EXPOSURE
A04:2017 - XML EXTERNAL ENTITIES (XXE)
A05:2017 - BROKEN ACCESS CONTROL
A06:2017 - SECURITY MISCONFIGURATION
A07:2017 - CROSS-SITE SCRIPTING (XSS)
A08:2017 - INSECURE DESERIALIZATION
A09:2017 - USING COMPONENTS WITH KNOWN VULNERABILITIES
A10:2017 - INSUFFICIENT LOGGING AND MONITORING
A01:2021 - BROKEN ACCESS CONTROL
A02:2021 - CRYPTOGRAPHIC FAILURES
A03:2021 - INJECTION
A04:2021 - INSECURE DESIGN NEW
A05:2021 - SECURITY MISCONFIGURATION
A06:2021 - VULNERABLE AND OUTDATED COMPONENTS
A07:2021 - IDENTIFICATION AND AUTHENTICATION FAILURES
A08:2021 - SOFTWARE AND DATA INTEGRITY FAILURES NEW
A09:2021 - SECURITY LOGGING AND MONITORING FAILURES*
A10:2021 - SERVER-SIDE REQUEST FORGERY (SSRF)* NEW
*FROM THE SURVEY

Figure 1: Changes in the OWASP Top Ten, 2017 to 2021.

RANK	CATEGORY	CWES MAPPED	MAX INCIDENCE RATE	AVG INCIDENCE RATE	MAX COVERAGE	AVG COVERAGE	AVG WEIGHTED EXPLOIT	AVG WEIGHTED IMPACT
A01:2021	Broken Access Control	34	55.97%	3.81%	94.55%	47.72%	6.93	5.93
A02:2021	Cryptographic Failures	29	46.44%	4.49%	79.33%	34.85%	7.29	6.81
A03:2021	Injection	33	19.09%	3.37%	94.04%	47.90%	7.25	7.15
A04:2021	Insecure Design	40	24.19%	3.00%	77.25%	42.51%	6.46	6.78
A05:2021	Security Misconfiguration	20	19.84%	4.51%	89.58%	44.84%	8.12	6.56
A06:2021	Vulnerable and Outdated Components	3	27.96%	8.77%	51.78%	22.47%	5.00	5.00
A07:2021	Identification And Authentication Failures	22	14.84%	2.55%	79.51%	45.72%	7.40	6.50
A08:2021	Software And Data Integrity Failures	10	16.67%	2.05%	75.04%	45.35%	6.94	7.94
A09:2021	Security Logging And Monitoring Failures	4	19.23%	6.51%	53.67%	39.97%	6.87	4.99
A10:2021	Server-Side Request Forgery	1	2.72%	2.72%	67.72%	67.72%	8.28	6.72

Figure 2: Research results for the 2021 OWASP Top Ten.

02

The 2021 Owasp Top Ten: Categories Continued, Combined, and Added

The 2021 OWASP Top Ten are as follows. Readers may refer to Figure 2 to see the metrics on each line item from the telemetry data. It should be noted that Contrast Labs conducts similar research that is the basis for the annual Application Security Observability Report and the bimonthly Application Security Intelligence reports.[3] There are two significant differences between the Contrast Labs research and that of OWASP. First, Contrast's data comes from direct measurements of running applications using instrumentation-based security, which is dramatically more accurate than the scanning tools used by many vendors in the OWASP study. Second, Contrast includes the operational view of attacks on production applications. Here Contrast's RiskScore Index gives a numerical indication of the relative risk of different vulnerabilities at a given time.

A01: Broken access control

This category moved up from fifth position in 2017—a trend that Contrast also observed from its own data as reported in the 2021 Application Security Observability Report.[4] Since access control features control who can perform functions, see and manipulate data, and do administrative tasks, failures of these controls can have devastating consequences.

A02: Cryptographic failures

Formerly known as Sensitive Data Exposure, this category of vulnerabilities focuses on the correct use of encryption, hashing, and other cryptographic mechanisms. Mistakes can result in significant compliance penalties for organizations under the jurisdiction of the E.U.'s General Data Protection Regulation (GDPR), the California Consumer Protection Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), and other laws governing the disclosure of personally identifiable information (PII), personal health information (PHI), and financial data for publicly traded companies.

> “
>
> OWASP's approach necessarily sorts for applications that organizations are willing to pay to protect. As a result, this is a study of the most important applications out there.
>
> Jeff Williams, "The Forthcoming 2021 OWASP Top Ten Shows That Threat Modeling Is No Longer Optional," Contrast Security AppSec Observer Blog, September 8, 2021.

[3] "2021 Application Security Observability Report," Contrast Security, August 2021; "Application Security Intelligence Bimonthly Report, May-June 2021," Contrast Security, May-June 2021.

[4] "2021 Application Security Observability Report," Contrast Security, August 2021.

A03: Injection

Several types of injection were combined into a single category in 2017, including SQL, NoSQL, LDAP, Command, and Expression Language (EL) Injection. For 2021, another common vulnerability type was added to this category—Cross-Site Scripting (XSS). These vulnerabilities enable attackers to relay malicious code through an application to another system and often result in a complete takeover of the target host.

A04: Insecure design

New for 2021, Insecure Design relates to the increased risk posed by applications with an underlying architecture that is not secure. Threat modeling is now required by OWASP, NIST, and the PCI Councils, so organizations should accelerate adoption of secure design patterns and reference architectures. Avoiding this element of the OWASP Top Ten must begin before the first line of code is written, making security an integral part of the initial design rather than an afterthought.

A05: Security misconfiguration

This category now includes XML External Entities (XEE) along with the vulnerability types it represented in 2017. Configuration errors are common in applications in production, and misconfiguration vulnerabilities can make these human errors even more likely by failing to harden security across the software stack. Including unnecessary features, ports, or privileges is an example, as is enabling default passwords.

A06: Vulnerable and outdated components

This category relates to the hygiene of keeping open-source libraries and frameworks up to date and ensuring that newly discovered CVEs are remediated. It is important to understand which libraries and library classes are used by the software, as these pose the most imminent risk.

A07: Identification and authentication failures

Formerly known as Broken Authentication, issues with identification were added to this category in 2021. This category of vulnerabilities can enable tactics such as credential stuffing, brute-force attacks, and exploitation of weak credential recovery processes.

A08: Software And Data Integrity Failures

This new category, identified through the industry survey, is confusing because it bundles two unrelated items together: software supply chain issues and data integrity mistakes such as digital signatures, hashes, and checksums. To make things more complicated, unsafe deserialization was added to the category, which at its root is more of an injection problem.

Nevertheless, the category highlights the need for integrity of application code and the data accessed through applications. The devastating SolarWinds attack in late 2020 is a prime example of a software integrity failure, as cyber criminals were able to insert malware into a routine software update for SolarWinds Orion infrastructure software, impacting thousands of networks. An insecure continuous integration/continuous deployment (CI/CD) infrastructure can result in such an attack.

A09: Security logging and monitoring failures

This category relates to ongoing incident response processes employed by security operations teams. At the end of the day, applications should be able to detect and block attacks. If security tools are in place that log attacks, then organizations should do something to respond, rather than simply letting them sit in a forgotten log. When applications have inadequate logging and monitoring features, breaches cannot be detected. When penetration tests, application security scans, and security logs do not trigger alerts of an active attack, organizations cannot mount a defense.

A010: Server-side request forgery (SSRF)

New for 2021, SSRF was selected because of its prevalence in both the 2021 industry survey and the collected data as an emerging threat. SSRF vulnerabilities enable an attacker to trick the targeted application or application programming interface (API) into sending a crafted request to an unexpected destination—turning a vulnerable application into a sort of attack relay that gives an attacker access to internal systems. OWASP's intent in adding this category to the Top Ten is to raise awareness and potentially roll it into another category in the next edition.

> “
>
> We spent several months grouping and categorizing cwes and could have continued for additional months. We had to stop at some point.
>
> OWASP Top Ten 2021, Draft for Peer Review

03

Contrast's Platform Approach: Doubly Important for the New Top Ten

Traditional application security tools and processes were designed at a time when software development was more manual, more methodical, and significantly slower. These approaches became less effective as methodologies like Agile and DevOps improved the speed and efficiency of software development.

Traditional practices involve lengthy security scans, the results of which security team members must analyze and return to developers days or weeks after the fact. Many scan results turn out to be false positives, wasting hours of staff time. And by the time developers learn of vulnerabilities, multiple layers of additional code have been added, making remediation more complicated. The result of these myriad delays is slower release cycles—and ultimately, less secure software. Ironically, these delays often do not result in a more secure application.

A consistent approach across the SDLC

A platform approach yields much better results. The Contrast Application Security Platform provides comprehensive application security across the SDLC, from the beginning of development through production. This enables full observability from a single console and robust reporting for compliance and other security measurements.

Contrast's platform is powered by instrumentation, leveraging sensors embedded in the application code to monitor it continuously throughout the SDLC. These sensors detect vulnerabilities as they are created—or added to an application via an open-source library or framework. Developers then receive immediate feedback on how to remediate the vulnerability that was just created—without help from a member of the security team.

Unlike most application security tools, the Contrast platform delivers highly accurate results throughout development and into production. This is because Contrast focuses on vulnerabilities that are actually exploited, rather than generating alerts for every potential threat. This significantly reduces the vulnerability space that analysts need to address, virtually eliminating false positives and the staff time wasted dealing with them. And as the number of CWEs included in the Top Ten continues to grow, accuracy is an increasingly important feature of application security tools.

Prioritization of vulnerability management with route intelligence

The Route Intelligence feature in Contrast Assess automatically analyzes all the possible “routes” a user can take through an application at runtime, getting a more accurate and nuanced view of the actual attack surface. Contrast research has found that only 26% of the code in the typical application is actually invoked by the software. The remaining 74% of code comes from inactive open-source libraries and inactive classes within active libraries, and vulnerabilities within this code pose no risk.

Route Intelligence in Contrast Assess enables organizations to identify which vulnerabilities are in active code and prioritize those for remediation. This can help them to more quickly resolve issues included in all of the Top Ten and more effectively manage the Vulnerable and Outdated Components category.

Support for threat modeling and secure architecture

The new Insecure Design category, and to a lesser extent the Software and Data Integrity Failures category, point to the need for a more security-focused approach to software design. Indeed, the 2021 OWASP Top Ten clearly indicates that threat modeling is a nonnegotiable part of application security going forward.

The Flow Map feature of Contrast Assess shows an accurate and explorable representation of a running application and associated layers of technology, including back-end connected systems. It shows what is connected to a running application and how an application stack interacts with other assets on the network. The user-friendly graphical format provides an excellent start for conversations about the underlying structure of a piece of software.

Whole application analysis to detect more vulnerabilities

The Contrast Application Security Platform goes beyond mere analysis of the source code. Whole application analysis covers the entire codebase, fully assembled with custom code, third-party libraries and frameworks, the application server, and platform runtime. This is important because many libraries are provided by the operational environment, not determined by what is in a source-code repository. This allows Contrast to detect vulnerabilities—including risky ones that are a part of the OWASP Top Ten—that other tools simply cannot see.

Runtime protection to avoid fire drills in production

Contrast Protect safeguards applications against vulnerabilities being exploited at runtime—a critical piece of managing the OWASP Top Ten. For applications in production, the process of remediating newly discovered vulnerabilities can take months—going back into development, testing, security testing, building, and deployment. This is a disruptive, expensive fire drill—and the running applications are very vulnerable to attack in the meantime. Contrast Protect allows applications to remain protected, enabling teams to remediate OWASP Top Ten issues as a part of the normal software development process—rather than as a fire drill.

The contrast application security platform enables comprehensive application security observability across the software development life cycle (sdlc), from the beginning of development through production.

Contrast Appsec Observability Platform

DEV

EMPOWER DEVELOPERS TO WRITE SECURE SOFTWARE QUICKLY.

+

TEST

ENSURE HIGH ASSURANCE SOFTWARE DELIVERY.

+

PROD

KNOW YOUR ATTACKERS. STOP EXPLOITS COLD.

Contrast Scan

World's fastest and most accurate code scanner. Works early in development to help developers write secure code.

Contrast SCA

Ensure supply-chain and open-source security. Understands how libraries are used by applications and APIs and reports known vulnerabilities instantly.

Contrast Assess

Continuously test application security from within, with full context of running applications/API. Fastest, most accurate, and most scalable AST solution.

Contrast Protect

Create visibility around application/API attacks and ensure that code and library vulnerabilities are not exploited. High performance and accuracy.

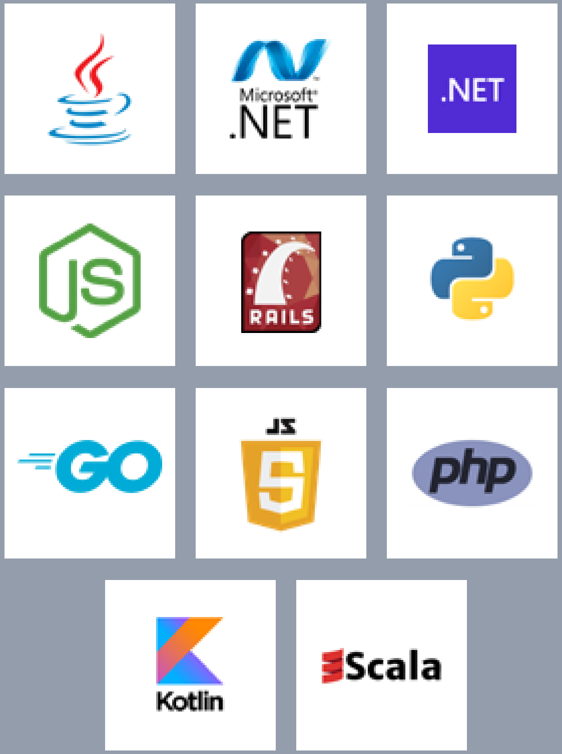


Figure 3: Contrast Application Security Observability Platform.

04 Contrast Security Policies: Identifying Vulnerabilities

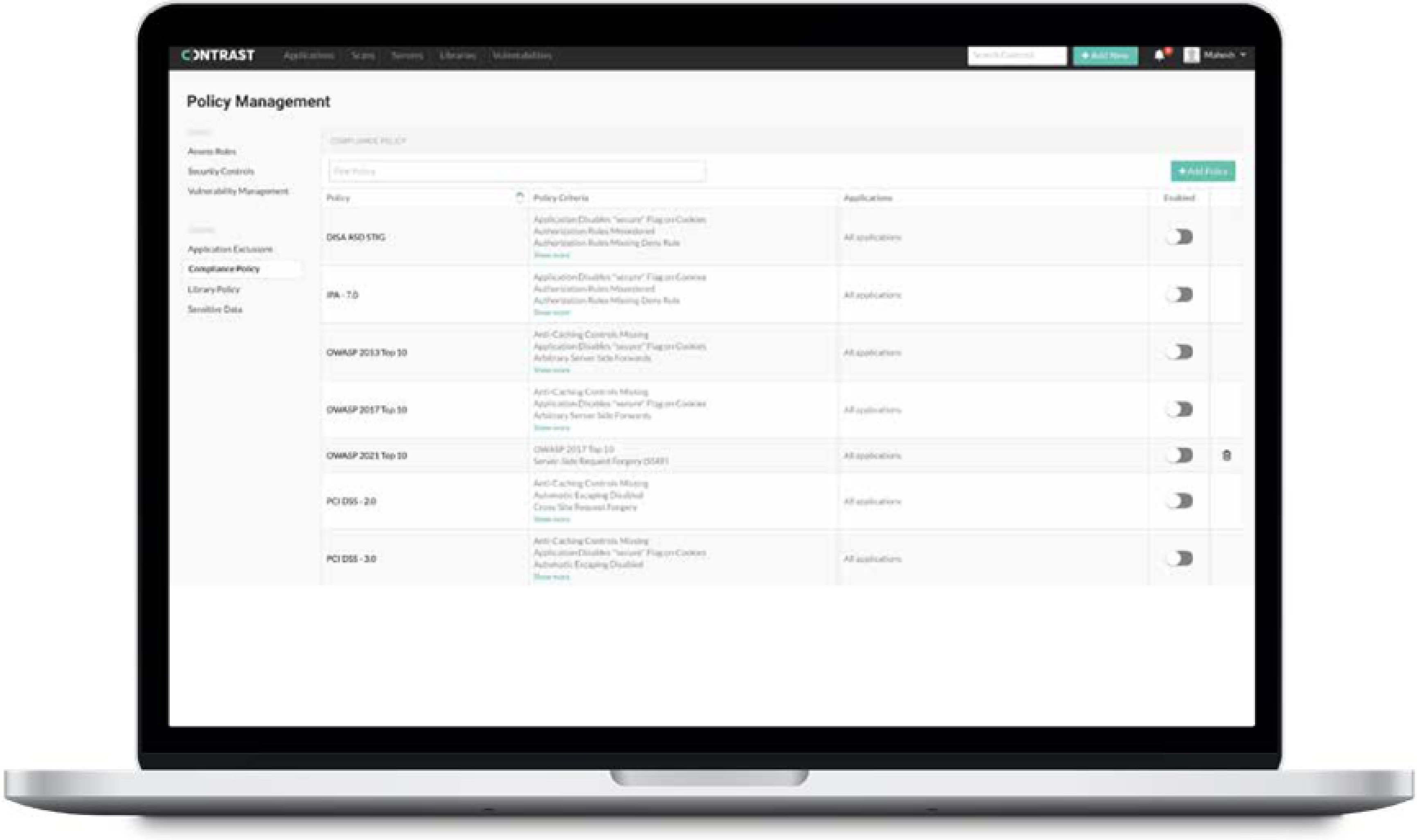
Contrast's continuous security testing is powered by policies, or rules, that define different kinds of vulnerabilities. These rules are leveraged across the SDLC, from early static scans using **Contrast Scan**, to continuous scanning throughout development with **Contrast Assess**, to tracking of open-source vulnerabilities with **Contrast SCA**, to runtime protection in production with **Contrast Protect**. Only Contrast can both identify OWASP Top Ten vulnerabilities—in custom and open-source code—and protect against attacks targeting them.

The Contrast platform includes rules to identify hundreds of CWEs, including all in the OWASP Top Ten. Beyond the definition of the rules, access to runtime data enables Contrast to safely parse the URL to determine if the vulnerability influences an important part of the URL (e.g., the protocol, host,

or path)—and therefore presents risk. This feature greatly enhances accuracy and virtually eliminates false positives, something that many other application security tools cannot achieve.

As open-source libraries and frameworks occupy a growing part of the typical application's codebase, the Contrast platform not only identifies the CVEs present in open-source code, but it also scans it for unknown vulnerabilities using the same rule set, just as it does with custom code.

> In the context of application security testing, 'accuracy' means you get a better score For every one you get right, but you also get points taken away every time you're wrong. By this measure, the accuracy of almost all current testing tools is abysmal.
>
> Arshan Dabirsiaghi, "IAST Is the Only Way To Accurately Detect SSRF," Contrast Security AppSec Observer Blog, September 20, 2021.



Policy Management

Policy	Policy Criteria	Applications	Enabled
DISA ASD STIG	Application Disables "secure" Flag on Cookies Authorization Rules Misordered Authorization Rules Missing Deny Rule Show more	All applications	●
IPA - 7.0	Application Disables "secure" Flag on Cookies Authorization Rules Misordered Authorization Rules Missing Deny Rule Show more	All applications	●
OWASP 2013 Top 10	Anti-Caching Controls Missing Application Disables "secure" Flag on Cookies Arbitrary Server Side Forwards Show more	All applications	●
OWASP 2017 Top 10	Anti-Caching Controls Missing Application Disables "secure" Flag on Cookies Arbitrary Server Side Forwards Show more	All applications	●
OWASP 2021 Top 10	OWASP 2017 Top 10 Server Side Request Forgery (SSRF)	All applications	●
PCI DSS - 2.0	Anti-Caching Controls Missing Automatic Escaping Disabled Cross Site Request Forgery Show more	All applications	●
PCI DSS - 3.0	Anti-Caching Controls Missing Application Disables "secure" Flag on Cookies Automatic Escaping Disabled Show more	All applications	●

Figure 4: Policy management screen in Contrast Application Security Platform.

05

Contrast Reporting: Updating Stakeholders Using the OWASP Top Ten

The OWASP Top Ten identifies the biggest application security risks, and automating coverage for the Top Ten should be considered the minimum acceptable level of application security for an organization. Remediating the vulnerabilities in the Top Ten—and protecting applications from attacks on them in production—is the most important goal in terms of risk management.

But how does an organization and its leadership know that the vulnerability categories in the Top Ten are under control? And for organizations for which the OWASP Top Ten is a compliance requirement, how can they demonstrate full coverage to an auditor? The only easy way to answer these questions is with robust reporting capabilities.

The Contrast Application Security Platform provides out-of-the-box reports for several compliance regimes, including the OWASP Top Ten. At the click of a mouse, administrators can produce timestamped PDF reports that include a summary of the application's security status, details on each vulnerability and remediation guidance, how much risk each vulnerability poses, and a security scorecard. Users can also customize existing reports and build custom reports from scratch.

Out-of-the-box reports customized for the owasp top ten help keep internal Stakeholders and auditors up to date without wasted staff time.

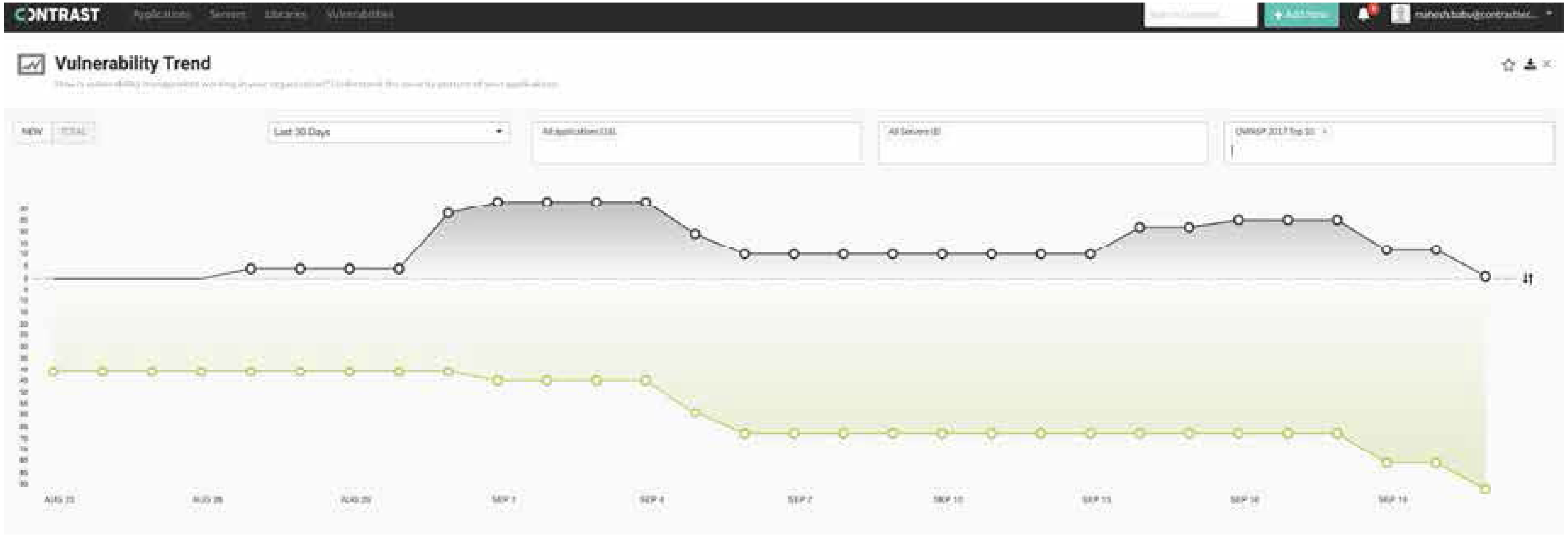


Figure 5. Contrast makes it possible to automatically generate reports demonstrating compliance with the OWASP Top Ten.

06

Conclusion: Threat Modeling is Critical

While every organization should have deployed threat modeling some time ago, the reality is that many have not done so. The 2021 OWASP Top Ten accentuates the need for change and the importance for threat modeling. As OWASP states in its documentation for the Insecure Design category, “Secure design requires a secure development lifecycle, some form of secure design pattern or paved road component library or tooling, and threat modeling.”[5]

In addition to OWASP, the National Institute of Standards and Technology (NIST) and the Payment Card Industry (PCI) have added threat modeling to their standards. This means a large percentage of companies that accept payment cards and/or provide services for the federal government now must have threat modeling in place. It is time for all other organizations to follow suit.

Threat modeling is the ultimate example of “shifting left” in application security coverage, as it advocates for emphasis on secure design before the first line of code is written. It is about prevention rather than remediation, and therefore helps with every element of the OWASP Top Ten. As OWASP puts it, “Secure design is a culture and methodology that constantly evaluates threats and ensures that code is robustly designed and tested to prevent known attack methods.”[6]

[5] OWASP Top Ten 2021, Draft for Peer Review.

[6] 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