Protect Against the OWASP Top 10

F5 Distributed Cloud WAAP

Contents

Introduction

The new world order

Despite two decades of security and risk management best practices, IT teams moving quickly to bring new apps to market frequently lack the visibility and consistent policy enforcement needed to manage risk across complex deployments that span clouds and architectures. Attackers target software and inherent business logic vulnerabilities with increasing sophistication and often use automation to scale—yet security operations still require considerable human intervention. With resources stretched, securing applications can feel like a constant firefight—but it's more important than ever for protecting the business in the new digital economy.

The new wave of risk

The OWASP Top 10 has long provided guidance for mitigating critical security risks. The 2021 update of the list, with its data-driven methodology, defines a new wave of risk in application security that considers both app design and implementation. After nearly 20 years with relative stability and minor changes among the rankings of risk categories, this seventh edition re-defines risk and addresses the need for security from end to end—from architecture to design.

OWASP Top 10 2021 Overview

The OWASP Top 10, first released in 2003, represents a broad consensus on the most critical security risks to web applications. For 20 years, the top risks remained largely unchanged—but the 2021 update makes significant changes to the risk calculus—including the recategorization of risk to align symptoms to root causes, new risk categories encompassing modern application architectures and development, and guidance for mitigating vulnerability exploits as well as business logic abuse.

The 2021 OWASP Top 10 defines a new wave of risk resulting from insecure design and implementation.

The 2021 OWASP Top 10

A01
Broken Access Control

A02
Cryptographic Failures

A03
Injection

A04
Insecure Design

A05
Security Misconfiguration

A06
Vulnerable and Outdated Components

A07
Identification and Authentication Failures

A08
Software and Data Integrity Failures

A09
Security Logging and Monitoring Failures

A10
Server-Side Request Forgery (SSRF)

Introducing F5 Distributed Cloud Web App and API Prottection (WAAP)

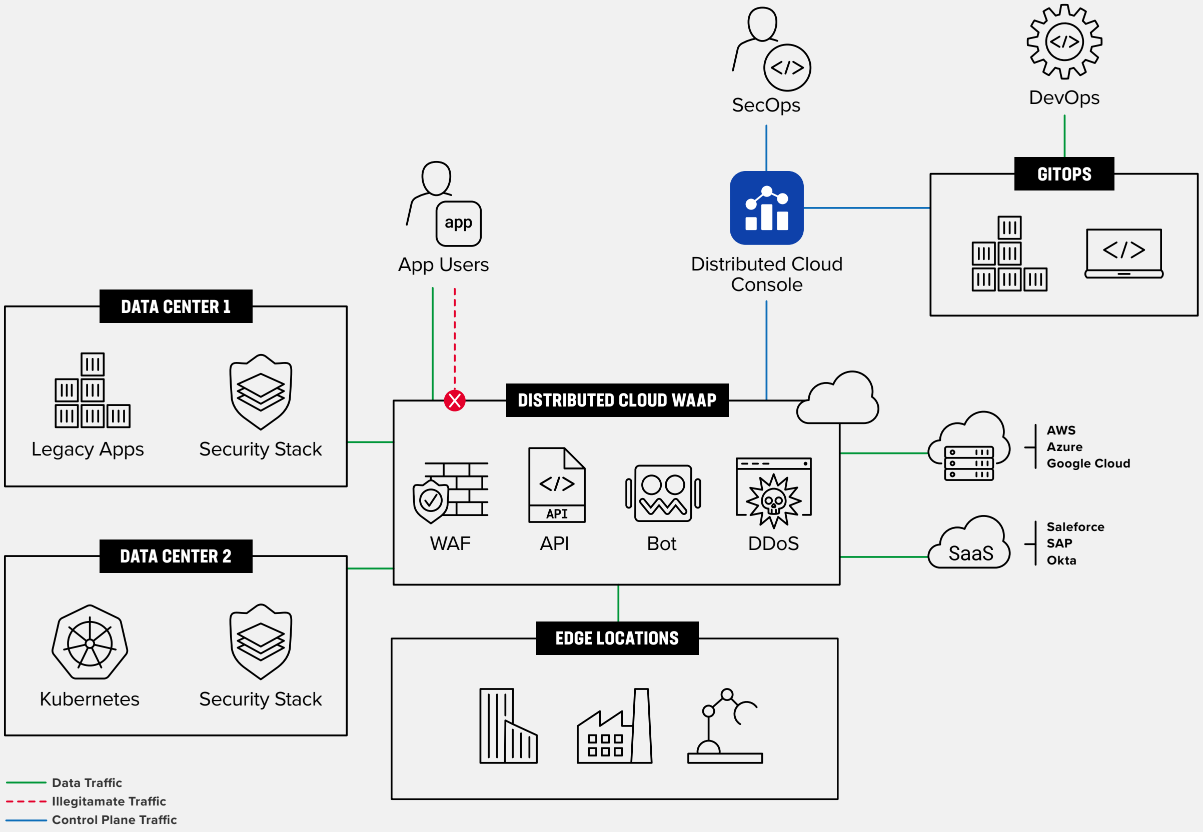
Attacks are growing in diversity and sophistication. Digital touchpoints are increasingly distributed across hybrid and multi-cloud environments. That means security must be intrinsically integrated into the entire application lifecycle.

Unforeseen risk from complex software supply chains, the proliferation of open-source software, and interdependencies common to API-based systems requires security to be both agile and resilient. This allows organizations to defend their entire digital footprint—wherever it is provisioned.

F5 Distributed Cloud WAAP enables organizations to consistently protect web apps and APIs across clouds and architectures—reducing complexity by integrating critical security controls such as web application firewall (WAF), bot defense, DDoS mitigation, with API discovery, and monitoring into a unified SaaS-based solution. This mitigates risk of vulnerability exploits, malicious automation, and attacks that bypass weak authentication and authorization controls.

By providing universal visibility, management, dynamic discovery and anomaly detection, and consistent policy enforcement through real-time threat intelligence and AI-based behavioral analysis, F5 Distributed Cloud WAAP maintains effectiveness no matter where apps and data are deployed. Let's dig into how F5 Distributed Cloud WAAP can protect organizations against OWASP Top 10 threats.

Figure 1: F5 Distributed Cloud WAAP enables organizations to mitigate web application attacks and vulnerabilities with comprehensive app security controls and uniform policy and observability, including simplified deployment and management of app security postures across environments and applications.



2021 OWASP Top 10 Breakdown

Today's most serious risk to web applications? Broken access control.

A01: 2021
Broken Access Control

Injection, historically at or near the top of successive OWASP lists, has been dethroned. Instead, the most serious risk today to web applications is broken access control, which moved up the list from fifth place.

Access control enforces policies that prevent users from accessing data, capabilities, or functions outside of the permissions intended for them. Access control vulnerabilities include flaws in the design of the web application that permit unauthorized access to sensitive objects such as a directory or record. For example, if access control fails, an anonymous user could view certain files on a website simply by knowing what URL to request, without validation that the user is authorized.

With 34 different CWEs mapped to broken access control, the OWASP data reflected more occurrences of this weakness than for any other category—318,487 occurrences in tested applications, which were associated with 19,013 common vulnerabilities and exposures (CVEs).

The real-world implications are significant, with potential regulatory and financial impacts. Broken access controls can lead to unauthorized information disclosure, modification or destruction of data, inappropriate escalation of user privileges, or the performance of actions—such as new account creation—that would otherwise not be permitted. The results can include account takeover (ATO), fraud, data breach, fines, and brand damage.

Mitigating broken access control

Access to all web application objects and pages should be denied by default, with an enforcement mechanism that grants explicit rights only to users associated with specific roles.

While organizations must fix their access control model to fully address broken access control, F5 Distributed Cloud WAAP can help you mitigate risk with robust and multi-layered defenses, including the security controls below.

Mitigation	Description
SERVICE POLICIES	Enables micro segmentation and support for advanced security at the application layer with development of allow/deny lists, Geo IP filtering and custom rule creation to act on incoming requests including match and request constraint criteria based on a variety of attributes/parameters TLS fingerprint, geo/country, IP prefix, HTTP method, path, headers, and more.
JWT VALIDATION	Stops JWT replay attacks and JWT tampering by cryptographically verifying incoming JWTs before they are passed to the target API.
CSRF PROTECTION	Allows users to easily configure/specify the appropriate, allowed source domains.
ALLOWED URLS AND FILETYPES	Allowlist for URLs and filetypes that bypass security checks.
FLOW ENFORCEMENT	Enforcing URL flows protects the web application from forceful browsing by ensuring access to web pages follows a predefined order.
ATTACK SIGNATURE	The F5 WAF signature engine has over 8,000 signatures for CVEs, plus other known vulnerabilities and techniques, including Bot Signatures identified by F5 Labs and threat researchers.

The most serious risk today to web applications is broken access control.

A02: 2021
Cryptographic Failures

The 2017 OWASP Top 10 included sensitive data exposure as the third most serious application risk. Now renamed to reflect the cause, rather than the symptom, the category of cryptographic failures rose to second place on the list.

Cryptographic failures—or in the worst-case scenario, a complete lack of encryption—can result in session hijacking or data leaks. Sensitive personal or financial data has obvious protection needs as defined by regulations such as the EU's General Data Protection Regulation (GDPR) or the PCI DSS. But data that needs protection can also include information about a web application's design that could be harvested by automated scanners. Examples of such information commonly leaked by web applications include:

- Error messages detailing how unexpected input is handled.
- Physical locations of files on the server.
- Specific versions of components and libraries.
- Stack traces from failed functions that could be decompiled and examined.
- "Forgot password" function error messages that reveal user ID validity, which can be used for brute force and credential stuffing attacks.

TLS 1.3 is the chosen encryption protocol for the majority of web servers running the top million websites, but F5 Labs has found that despite widespread TLS 1.3 adoption, old and vulnerable protocols are being left enabled, giving opportunities to attackers. Other failures relate to improper management of security components (such as keys or certificates) and enforcement tactics that allow them to become outdated. No organization is exempt; a 2021 National Cyber Awareness System (NCAS) Bulletin from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) recorded a vulnerability based on weak ciphers allowed by AWS CloudFront.

Mitigating cryptographic failures

Organizations cannot fully protect against cryptographic failures by using any one security solution. However, an integrated security platform like F5 Distributed Cloud WAAP dramatically reduces risk—specifically with these key controls.

Mitigation	Description
SSL/TLS FULL PROXY	Rich protocol, cipher, and authentication support.
HTTP STRICT TRANSPORT SECURITY (HSTS)	Dynamic insertion and enforcement of HTTP response header to prevent man-in-the-middle attacks such as HTTP downgrade attacks.
SENSITIVE DATA DETECTION	Scans app and API requests and responses for sensitive data, such as personally identifiable information (PII), credit card numbers, and social security numbers.
DATA GUARD	Prevents web server responses from exposing sensitive information, like credit card numbers and social security numbers, by masking the data.
CLIENT-SIDE DEFENSE	Extends protection to the web browser by providing multi-phase protection for web applications against Formjacking, Magecart, digital skimming and other malicious JavaScript attacks including detection, alerting, and mitigation.

Cryptographic failures rose to second place on the list.

A03: 2021
Injection

This risk category has grown broader by merging with cross-site scripting (XSS), but the adoption of strong development frameworks has helped to reduce related vulnerabilities, dropping it from first place on the list to third. Injection attacks can occur when an application improperly validates, filters, or sanitizes user input, whether that input occurs through ordinary forms or hidden web fields. When they're successful, attackers can add—or inject—their own instructions into a vulnerable application execution process to alter the normal operation of the process.

For example, an attacker might inject malicious commands such as SQL, LDAP, or XPath, which are processed by the application's interpreter. The commands then can be passed to either the local system or a dependent one. This gives the attacker unauthorized access to escalate privileges, cause a denial of service, plant malware, or achieve other nefarious objectives. Injection attacks have been used successfully to delete entire databases, modify records, and exfiltrate sensitive data.

The significance and persistence of this type of threat are reflected in the inclusion of injection and XSS in every Top 10 list since OWASP began. For the 2021 list, OWASP data reflected 274,228 occurrences of this weakness in tested applications, and it was associated with 32,078 CVEs. F5 Labs analysis also validates the risk of these attacks: overall, injection attacks and XSS rank the highest.

Moreover, the CVEs associated with injection weaknesses were among the most severe. In 2021, 17 CVEs scored the maximum of 10.0 for CWE-89, SQL injection, and 4 CVEs scored over 9.0 for CWE-79, XSS. Any score of 9.0 or above is considered critical.

Mitigating injection attacks

F5 Distributed Cloud WAAP mitigates the risk of web app and API injection flaws with the following capabilities.

Mitigation	Description
OWASP TOP 10 SIGNATURES	The F5 WAF signature engine has over 8,000 signatures for CVEs, OWASP top 10 categories, and other known vulnerabilities and techniques, including Bot Signatures identified by F5 Labs and threat researchers.
THREAT CAMPAIGNS	Delivers protection against sophisticated, multi-vector, coordinated attack campaigns via fully vetted attack campaign signatures developed by F5 threat researchers.
SERVICE POLICIES	Enables micro segmentation and support for advanced security at the application layer with development of allow/deny lists, Geo IP filtering and custom rule creation to act on incoming requests including match and request constraint criteria based on a variety of attributes/parameters, TLS fingerprint, geo/country, IP prefix, HTTP method, path, headers and more.
DYNAMIC IP REPUTATION	Analyzes IP threats and publishes a dynamic data set of millions of high-risk IP addresses maintained by F5 to protect app endpoints from inbound traffic from malicious IPs. IP threat categories include Spam Sources, Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Services, Phishing and more.

Additionally, organizations should always patch apps and APIs to address any discovered vulnerabilities based on their respective development lifecycles.

Overall, injection attacks and XSS rank the highest.

A04: 2021
Insecure Design

This new category represents weaknesses resulting from ineffective security controls or flaws within the application architecture or design. It introduces a new OWASP paradigm with complementary implications: A secure design may still suffer implementation defects that lead to vulnerabilities that may be exploited, but an insecure design cannot be fixed even by perfect implementation. By definition, the security controls needed to defend against specific attacks have not been created; therefore, mitigation must encompass architecture, design, and implementation.

Unlike the other Top 10 categories, insecure design can apply to every application, and this category includes 40 mapped CWEs with average weighted exploit scores and impacts above 6.0. The real-world effects of this type of weakness include a campaign of data breaches against schools in California made possible by an exploitable vulnerability in a vendor's e-learning software.

Mitigating insecure design

Organizations should integrate security from the very first design stages. However, development teams may struggle to achieve this. F5 Distributed Cloud WAAP helps organizations shift left faster to prevent design insecurities from compromising their apps and APIs.

Mitigation	Description
API-DRIVEN DEPLOYMENT AND MAINTENANCE	Integration into development frameworks and CI/CD pipelines including native Terraform registry.
ANTI-AUTOMATION CONTROLS	Bot signatures and behavioral analysis to uncover header anomalies.
BOT DEFENSE	Specialized controls that protect critical business logic from fraud and abuse from automated attacks by leveraging JavaScript and API calls to collect telemetry and mitigate sophisticated attacks with constant machine learning (ML) based analysis of signal data. This allows rapid responses to bot retooling and dynamic updates of real-time detection models designed to deter attacks including credential stuffing, account takeover, and fake accounts as detailed in the OWASP Automated Threats project.

An insecure design cannot be fixed even by perfect implementation.

A05: 2021
Security Misconfiguration

Security policy can be misconfigured for a variety of reasons ranging from simple human error to overlooked defaults. In a multi-cloud world, default configurations vary by cloud provider, and architectural sprawl across clouds increases the risk of security misconfiguration and inconsistencies in security policy.

In addition, most web applications depend on other software (such as Apache, IIS, or NGINX) and may leverage other applications, libraries, and databases (such as PHP, ASP, or SQL)I It's difficult to quantify the unintended risk of leveraging these common components. Finally, the rapid development cycles of modern applications, the pervasive reuse of software to save development time, and a trend toward creating highly configurable software specifically so it can be reused make misconfiguration more likely than ever.

Confusion about boundaries and responsibilities in cloud deployments significantly elevates the risk. The severity of weaknesses in this category, which now incorporates XML external entities (XXE), is high, with the 20 CWEs mapped to it averaging a weighted exploit score greater than 8.0.

Mitigating security misconfiguration

By definition, Security Misconfiguration covers multiple aspects of application security. It also requires organizations to properly configure security controls. F5 Distributed Cloud WAAP provides universal visibility and consistent security enforcement across distributed environments to mitigate misconfiguration of apps, APIs, and underlying cloud infrastructure.

Mitigation	Description
UNIFIED POLICY MANAGEMENT	Construct, deploy, and enforce security policies and controls (WAF, DDoS mitigation, bot defense and API discovery and security) across hybrid and multi-cloud environments, including on-premises.
HTTP HEADER PROCESSING	Dynamic WAF response headers and body rules for specific tasks such as capturing the real client IP and proxy chaining authentication headers.
BOT DEFENSE	Specialized controls that consistently deter automated threats detailed in the OWASP Automated Threats project across hybrid and multi-cloud environments with connectors into application proxies, platforms, and CDNs.
DYNAMIC API DISCOVERY	Delivers advanced machine learning, enabling markup and analysis of API endpoints for applications for API endpoint discovery and behavioral analysis, including request and response schemas, sensitive data detection and authentication status. This enables security teams to inventory known and shadow API sets with OpenAPI spec (OAS) generation.

A06: 2021

Vulnerable and Outdated Components

Open source and third-party components undoubtedly speed application development and time to market, but vulnerabilities within them account for many significant and costly data breaches. F5 Labs has found that a critical vulnerability with the potential for remote code execution is released every 9 hours. The complexity of known vulnerabilities is on the rise, too, in part because dependencies continue to expand, particularly in cloud deployments with varying interdependencies and permissions. As a result, attacks on popular software can have massive impacts, for example, the log4j2 vulnerability in 2021, and the MOVEit vulnerability in 2023.

Application testing and risk assessment for this category is challenging. Nonetheless, vulnerability data was sufficient for this category to move up the list from ninth place in 2017. It ranked even higher, at number two, in the OWASP community survey. And as the recent Log4j2 vulnerability shows, OWASP's diligent approach to risk management has once again proven effective.

Mitigating vulnerable and outdated components

The rate at which vulnerabilities are discovered is far too frequent to patch them all, so prioritization is key. But even when vulnerabilities come to light after implementation, administrators may resist change for fear of breaking functionality, reluctant to lose a valuable legacy feature—or they simply may be unable to free resources to do it.

While such concerns are valid, successful exploits against a known vulnerability can result in significant losses. Creating an inventory of open-source components and their associated vulnerabilities and then proactively updating to eliminate critical vulnerabilities is ideal.

As noted in the F5 Labs report The Evolving CVE Landscape—a 20-year retrospective on the Common Vulnerabilities and Exposures (CVE) database—there are a growing number of vendors reporting CVEs and a growing diversity of underlying flaws.

New vulnerability territory is being uncovered every day

F5 Distributed Cloud WAAP integrates natively into development frameworks and CI/CD pipelines through its API-driven approach and provides several controls to mitigate vulnerable software.

Mitigation	Description
ATTACK SIGNATURES	The F5 WAF signature engine has over 8,000 signatures for CVEs, plus other known vulnerabilities and techniques, including bot signatures identified by F5 Labs and threat researchers.
THREATS CAMPAIGNS	Delivers protection against sophisticated, multi-vector, coordinated attack campaigns via fully vetted attack campaign signatures developed by F5 threat researchers.
SERVICE POLICIES	Dynamic intercept and redirect of requests to known vulnerable software based on attributes/parameters TLS fingerprint, geo/country, IP prefix, HTTP method, path, headers, and more.
IP REPUTATION	Analyzes IP threats and publishes a dynamic data set of millions of high-risk IP addresses maintained by F5 to protect app endpoints from inbound traffic from malicious IPs. IP threat categories include spam sources, Windows exploits, web attacks, botnets, scanners, denial of services, phishing, and more.
CLIENT-SIDE DEFENSE	Extends protection to the web browser, provides multi-phase protection for web applications against formjacking, Magecart, digital skimming, and other malicious JavaScript attacks. This multi-phase protection includes detection, alerting, and mitigation.

F5 Distributed Cloud customers automatically received signatures and threat campaigns for the Log4j and MOVEit vulnerabilities. The next critical vulnerability may be as pervasive and it is imperative for security teams to secure apps and APIs consistently across all environments.

A07: 2021

Identification and Authentication Failures

Every application that authenticates users or has a login process is vulnerable to bypass, and the availability of compromised credentials, botnets, and sophisticated automation tools make this an attractive attack with a high return for attackers. F5 Labs research found the average time for credential spills to be discovered is 327 days. That's a lot of time for attackers to work and many are remarkably successful.

Mitigating identification and authentication failures

F5 Distributed Cloud WAAP deters automated threats that can otherwise lead to account takeover (ATO) and fraud by leveraging both real-time threat intelligence and AI-based retrospective analysis—deterring bots and human fraudsters while optimizing the experience for real customers.

The average time for credential spills to be discovered is 327 days.

Mitigation	Description
BOT DEFENSE	Protects apps from automated attacks by leveraging JavaScript and API calls to collect telemetry and mitigate sophisticated attacks with constant machine learning (ML)-based analysis of signal data. This allows rapid responses to bot retooling and dynamic updates of real-time detection models designed to deter automated threats detailed in the OWASP Automated Threats project.
RATE LIMITING	Control the rate of requests coming into or going out of an application origin at the user or API level. Rate limiting can be controlled for apps and APIs using key identifiers such as IP address, cookie name, and HTTP header name.
MALICIOUS USER DETECTION	AI/ML-powered user behavior analysis and auto-mitigation that assigns a suspicion score and threat level based on the activity of each user. Client interactions are analyzed on how they compare to others—the number of WAF rules hit, forbidden access attempts, login failures, error rates, and more.
THREAT CAMPAIGNS	Delivers protection against sophisticated, multi-vector, coordinated attack campaigns via fully vetted attack campaign signatures developed by F5 threat researchers.
DYNAMIC API DISCOVERY	Discovery of authentication status, and potential anomalies, plus JSON Web Token (JWT) validation.
ATTACK SIGNATURES	The F5 WAF signature engine has over 8,000 signatures for CVEs, plus other known vulnerabilities and techniques including bot signatures identified by F5 Labs and threat researchers.

A08: 2021
Software and Data Integrity Failures

One word: SolarWinds. In one of the more damaging attacks in recent memory, automated updates spread malware as the result of a failure in this new category, which also includes insecure deserialization.

Data integrity can be violated in or through the application or through the update mechanism. Essentially all modern applications with a user interface are vulnerable, and weaknesses may also be introduced through CI/CD pipelines without integrity verification. In fact, as noted by F5 Labs researchers, “if DevSecOps is enforced properly, it would be very difficult to cheat the system and deploy things that bypass the pipeline.”

With 1,152 mapped CVEs, this category scored one of the highest weighted CVE/CVSS impacts.

Organizations should always patch web applications to address any discovered vulnerabilities based on their development lifecycle.

Mitigating software and data integrity failure

Organizations can help mitigate software and data integrity failures using these F5 Distributed Cloud WAAP capabilities.

Mitigation	Description
OWASP TOP 10 SIGNATURES	The F5 WAF signature engine has over 8,000 signatures for CVEs, OWASP top 10 categories, plus other known vulnerabilities and techniques including bot signatures identified by F5 Labs and threat researchers.
DYNAMIC API DISCOVERY	Delivers advanced machine learning, enabling markup and analysis of API endpoints for applications to discover API endpoints and perform behavioral analysis. This includes request and response schemas, sensitive data detection, and authentication status. Provides inventory and shadow API sets with OpenAPI spec (OAS) generation.
SCHEMA VALIDATION	API specification enforcement functionality enables a positive security model for APIs, allowing organizations to easily enforce desired API behavior based on characteristics for valid, API requests based on a learned or imported schema. These characteristics are used to validate input and output data for things like data type, min or max length, permitted characters, or valid value ranges.
EVASION HANDLING	Detect encoding methods that normal attack signatures do not detect.
CLIENT-SIDE DEFENSE	Extends protection to the web browser, provides multi-phase protection for web applications against formjacking, Magecart, digital skimming, and other malicious JavaScript attacks.

Organizations should always patch web applications to address any discovered vulnerabilities based on their development lifecycle.

A09: 2021
Security Logging and Monitoring Failures

Logging and monitoring can be difficult to test, but their reliability and sufficiency are critical for quick detection of attacks and appropriate mitigation responses. As security experts note, breaches often do not lead immediately to attack; attackers often need time to construct their exploits. But the longer an attacker has access, the more likely it is that the system will be exploited.

Failures in this category—now expanded beyond merely insufficient logging and monitoring—directly impact the visibility, incident alerting, and forensics efforts that can prevent unauthorized access from causing real harm. They can also hinder fast service recovery.

No wonder logging and monitoring was a top-three concern in the OWASP community survey. Testing mapped the category to 53,615 occurrences in applications, including weaknesses such as the inclusion of sensitive information in log files.

> The longer an attacker has access, the more likely it is that the system will be exploited.

Mitigating security logging and monitoring failures

F5 Distributed Cloud WAAP provides multiple capabilities to provide organizations with greater visibility into attacks, including:

Mitigation	Description
VISIBILITY	Correlated insights across data centers, clouds, application platforms, and CDNs.
MONITORING	Comprehensive monitoring and security dashboards with violation details and drill down capability.
GLOBAL LOG RECEIVER	Pipe logs and event data to SIEMs and other forensic tools. Enables log distribution to external log collection systems such as Amazon S3, Datadog, Splunk, SumoLogic and other tools and includes request (access) logs, security events, and audit logs.
DATA GUARD	Sensitive log masking data in request logs can easily be masked by specifying http header name, cookie name, or query parameter name. Only values are masked. By default, values of query parameters card, pass, pwd, and password are masked.
F5 OPERATIONS AND SUPPORT	24/7/365 operations and support team focused on monitoring and risk mitigation.

A10: 2021
Server-Side Request Forgery (SSRF)

This new category of risk ranked as the number one concern in the OWASP community survey. SSRF happens when web applications fetch a remote resource without validating the user-supplied URL—despite the protection of a firewall, VPN, or other network access control. Although application testing for this type of weakness found it at a relatively low rate, it received an above-average exploit score of 8.28 as well as an above-average impact score.

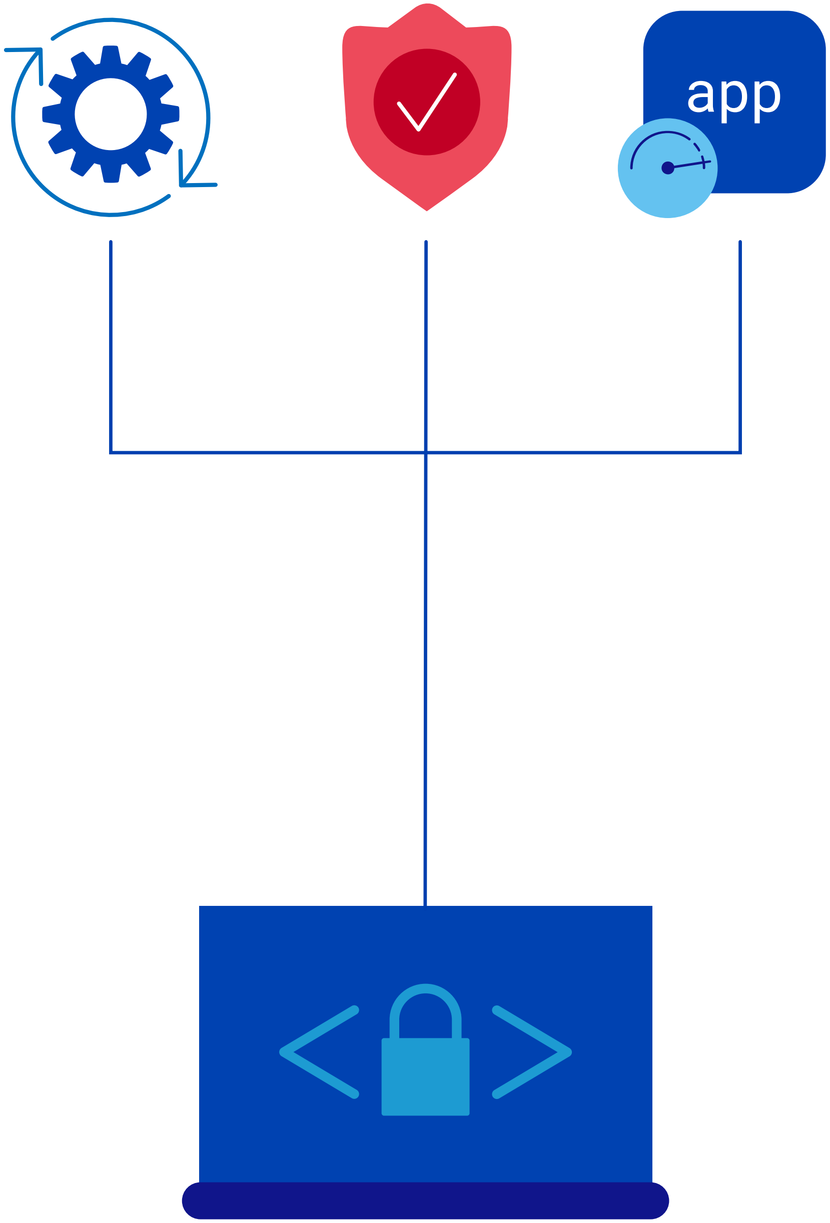
Fetching a URL has become common as modern web applications offer convenient features to users, architecture becomes increasingly decentralized, and interconnectivity via APIs and integration rises. As a result, SSRF is on the rise and also impacts APIs, as noted in the OWASP API Security Top 10.

SSRF is on the rise and also impacts APIs, as noted in the OWASP API Security Top 10.

Mitigating SSRF

F5 Distributed Cloud Services WAAP can prevent server-side request forgery with a variety of controls.

Mitigation	Description
WAF SIGNATURES	The F5 WAF signature engine has over 8,000 signatures for CVEs, plus other known vulnerabilities and techniques including SSRF risks identified by F5 Labs and threat researchers.
SERVICE POLICIES	Enables micro-segmentation and support for advanced security at the application layer for customer SSRF protection with development of allow/deny lists, Geo IP filtering, and custom rule creation to act on incoming requests, including match and request constraint criteria based on a variety of attributes/parameters—TLS fingerprint, geo/country, IP prefix, HTTP method, path, headers and more.



The OWASP Top 10: Merely the Tip of the Iceberg

The OWASP Top 10 requires security to be fundamental to applications in their architecture and design and in their implementation. Just as organizations release and update applications to gain competitive advantage, cybercriminals orchestrate and adapt attacks to monetize their efforts in a continuously changing risk landscape.

It's important to remember that when it comes to securing web applications, the OWASP Top 10 is merely the tip of the iceberg. Fortunately, a comprehensive security strategy with robust tools, processes, and training can protect applications and facilitate more secure development, helping to defeat the Top 10—and the other threats lurking beneath.

> A comprehensive security strategy with robust tools, processes, and training can protect applications and facilitate more secure development.

Learn more

Get more information on how to mitigate application vulnerabilities, secure APIs, and deter fraud and abuse to protect modern and legacy applications from emerging threats.

ABOUT F5

BRINGING A BETTER DIGITAL WORLD TO LIFE

F5 is a multi-cloud application services and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure and optimize apps and APIs anywhere—on premises, in the cloud, or at the edge. F5 enables organizations to provide exceptional, secure digital experiences for their customers and continuously stay ahead of threats. For more information, go to f5.com. (NASDAQ: FFIV).

Learn more at f5.com/solutions/web-app-and-api-protection