WHITE PAPER

Mitigating Application Security Threats

OWASP Top 10

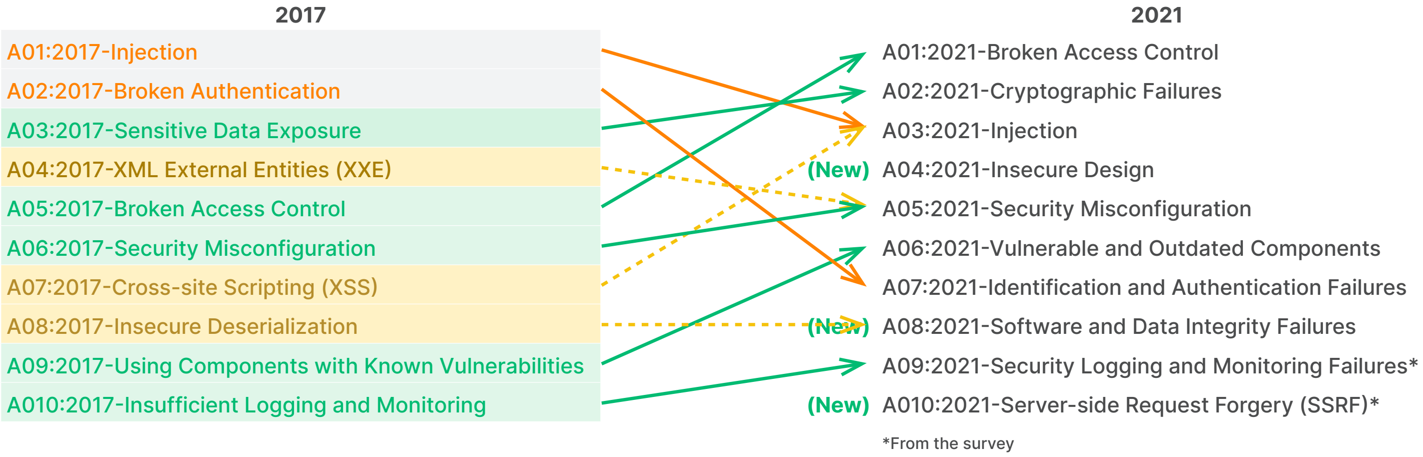
Introduction

The Open Web Application Security Project (OWASP) Top 10 identifies a set of common web application security flaws and provides a powerful tool for raising awareness about web application security issues. Produced by a community of security experts from around the world, the OWASP Top 10 represents a broad consensus about the most critical web application security flaws that should be addressed as part of an overall web application security program.

The OWASP Top 10 influences and informs a wide array of industry standards and requirements, including the Payment Card Industry (PCI) DSS standard and many government regulations. There are multiple approaches to mitigating against the OWASP Top 10, including secure coding practices and code reviews, but deployment of a web application firewall (WAF) remains the primary tool for addressing requirements that reference the OWASP Top 10.

Updating the Top 10 List

The OWASP team updates the Top 10 list periodically as the threat landscape changes, new technologies are leased, and the tactics of threat actors evolve. In 2021, changes included introducing new categories, renaming some, and consolidating several others. The table below from OWASP summarizes those changes:


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
A010:2017-Insufficient Logging and Monitoring
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A010:2021-Server-side Request Forgery (SSRF)*
*From the survey

Web Application Security Challenges

Web applications continue to be attractive targets to threat actors. Public-facing web apps must be exposed to the internet to deliver the line-of-business tools that modern organizations require. Those web apps connect to backend databases that can touch some of our most sensitive data—customer information, credit card data, employee information, and more—making these applications a prime target for threat actors.

According to the 2021 Verizon Data Breach Report (VDBR), Basic Web Application Attacks (defined as "simple web application attacks with a small number of steps/additional actions after the initial web application compromise") were involved in more than 20% of breaches.[1] Attackers continue to probe for web application vulnerabilities, as documented by FortiGuard Labs in Global Threat Landscape Reports Q1 2022. (See figure on the next page, *Prevalence of top IPS detections by technology during 2H 2021.*)

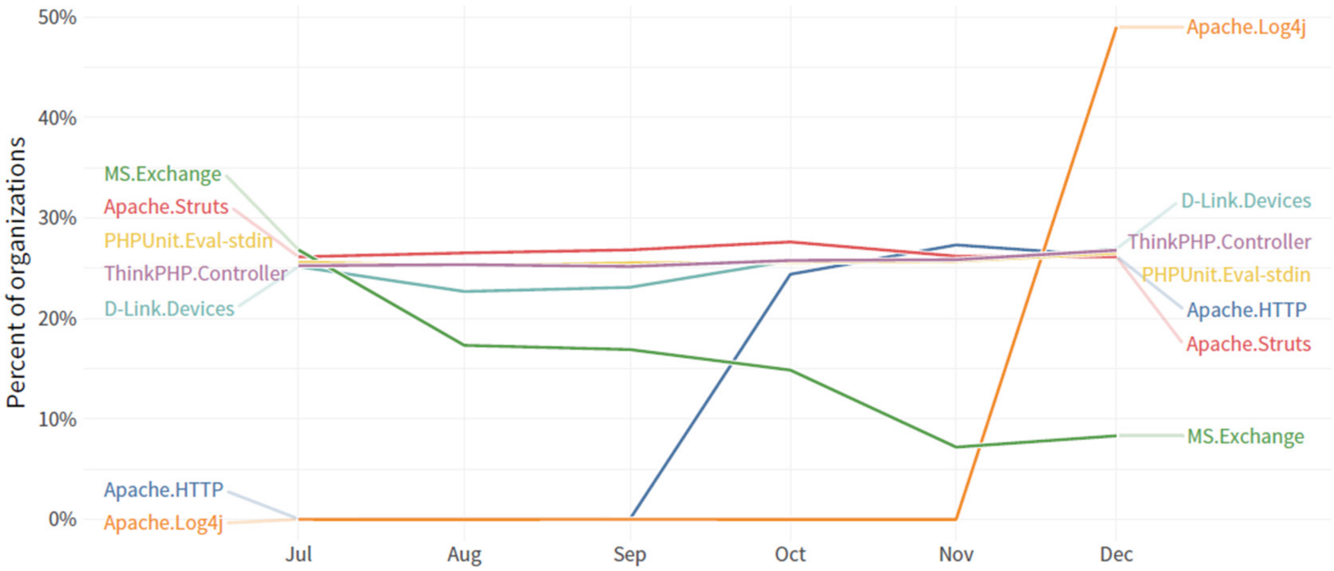


Figure 1: Prevalence of top IPS detections by technology during 2H 2021

Public-facing web applications require a different approach to security. Unlike applications and services that can be securely walled off from direct internet access, web applications must allow access to function effectively. How do you define security policies to allow/block traffic to/from multiple applications, each consisting of hundreds and sometimes thousands of different elements (URLs, parameters, and cookies)? Manually creating different policies for each element is unrealistic and does not scale as the number of web applications and their complexity grows. Web applications also change frequently—on average, companies publish 25 software updates into production per application every month (see *Cybersecurity Insider's 2021 Application Security Report*).[2]

FortiWeb Web Application and API Security: A Multilayered Approach

FortiWeb's positive security model, multilayer approach provides two key benefits: 1) superior threat detection and 2) improved operational efficiency. FortiWeb's ability to detect anomalous behavior, using sophisticated two-layer machine learning relative to the specific application being protected, enables the solution to block unknown, never-before-seen exploits. This provides the best protection against zero-day attacks targeting your application.

By creating a comprehensive security model of the application, FortiWeb can defend against a full range of known or unknown vulnerabilities, including SQL Injection, cross-site scripting, and other application layer attacks. Operationally, FortiWeb machine learning relieves you of time-consuming tasks, such as remediating false positives or manually tuning WAF rules. FortiWeb continually updates the model of your application as it evolves, enabling you to get your code into production faster by eliminating the need for time-consuming manual WAF rules tuning and troubleshooting the false positives that plague less advanced WAF solutions.

The FortiWeb product line protects against known and zero-day attacks using both positive and negative security models. FortiWeb enables enterprises to protect against application-level attacks, combining analytics derived from FortiGuard Labs threat intelligence with advanced machine-learning capabilities. The analytics use advanced techniques to protect against SQL injection, cross-site scripting, and a range of other attacks, while FortiWeb's machine learning models your application's actual usage and looks for malicious anomalies.

FortiWeb protects sensitive data while ensuring application availability, providing flexible and reliable security to address the OWASP Top 10 by utilizing a range of in-depth security modules and technologies. Sophisticated attacks are blocked using a multilayered security approach. Incorporating a positive and a negative security module based on bidirectional traffic analysis and an embedded, machine-learning, behavioral-based anomaly detection engine, FortiWeb protects against a broad range of threats without the need for network re-architecture and application changes.

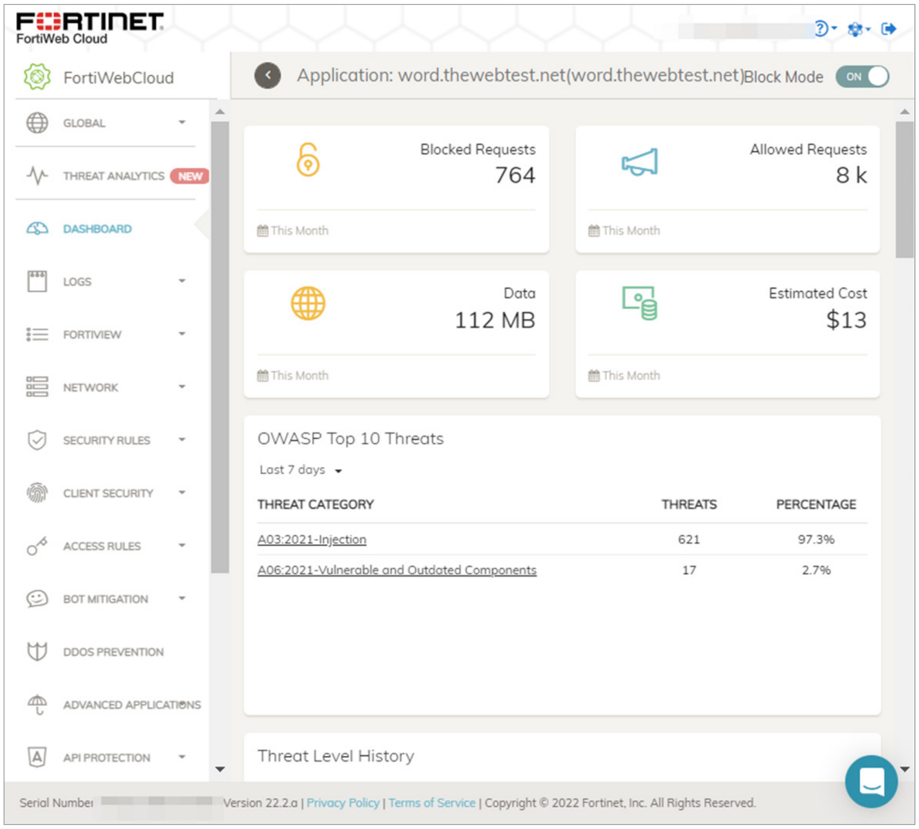
Backed by FortiGuard Labs

FortiWeb includes a full application signature dictionary to protect against known application layer attacks and application logic attacks. A sophisticated engine scans both inbound and outbound traffic, matching elements with pre-defined known exploits. Also, the solution provides an enhanced flexible engine that allows customers to write their own signatures using a regular expression engine which provides the ability to create new and customized signatures for every application and vulnerability.

FortiWeb's signature dictionary is updated regularly and automatically via FortiGuard Labs, a security subscription service that delivers continuous, automated updates and offers dynamic protection based on the work of Fortinet's Global Security Research Team, which researches and develops protection against known and potential security threats.

Reporting

FortiWeb includes visual reporting tools that provide a detailed analyses of attack sources, types, and other elements, mapping specific incidents to the OWASP Top 10 categories (see figure 2) and providing a summary dashboard of OWASP TOP 10 dashboard reports (see figure 3).



[redacted]

Application: word.thewebtest.net(word.thewebtest.net)Block Mode ON

Blocked Requests 764 — This Month

Allowed Requests 8 k — This Month

Data 112 MB — This Month

Estimated Cost $13 — This Month

OWASP Top 10 Threats

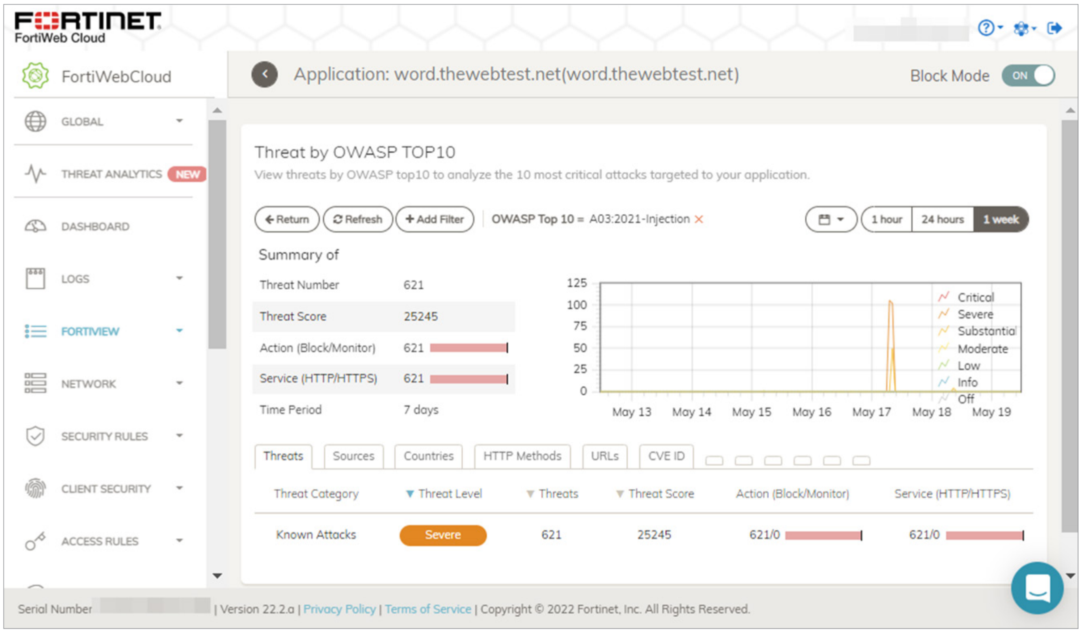
Last 7 days

THREAT CATEGORY	THREATS	PERCENTAGE
A03:2021-Injection	621	97.3%
A06:2021-Vulnerable and Outdated Components	17	2.7%

Threat Level History

Serial Number [redacted] Version 22.2.a | Privacy Policy | Terms of Service | Copyright © 2022 Fortinet, Inc. All Rights Reserved.

Figure 2: OWASP Top 10 Threats dashboard element



Application: word.thewebtest.net(word.thewebtest.net)

Threat by OWASP TOP10

View threats by OWASP top10 to analyze the 10 most critical attacks targeted to your application.

OWASP Top 10 = A03:2021-Injection ×

Summary of

Threat Number	621
Threat Score	25245
Action (Block/Monitor)	621
Service (HTTP/HTTPS)	621
Time Period	7 days

Threat Category	Threat Level	Threats	Threat Score	Action (Block/Monitor)	Service (HTTP/HTTPS)
Known Attacks	Severe	621	25245	621/0	621/0

Serial Number [redacted] | Version 22.2.a | Privacy Policy | Terms of Service | Copyright © 2022 Fortinet, Inc. All Rights Reserved.

Figure 3: FortiWeb Cloud example alert for A03:2021 injection

Data Leak Prevention and Information Disclosure

With predefined and custom policies for masking sensitive data, customers can be assured that sensitive data logged by FortiWeb is protected from unauthorized access. An important part of the OWASP Top 10, sensitive data masking is a critical task.

Even when access to the system is authorized, the data itself is masked and valuable sensitive information cannot be read. Customers can use the predefined policy and have the option to create their own custom policies to automatically mask additional fields in logs.

OWASP Top 10 and FortiWeb Mitigations

The table below lists the OWASP Top 10 for 2021 and the corresponding FortiWeb mitigation techniques.

OWASP Top 10	Description	FortiWeb Mitigation
1. Broken Access Control	Broken access control occurs when users can access resources they were not originally intended to. Access to resources should only be provided based on least privileges and denied to users without permissions.	■ Build strong access control mechanisms by implementing FortiWeb authentication and using correct user groups. ■ Use FortiWeb API Gateway to verify API keys, manage users, hide URLs, and rate limit access to APIs. ■ Enable FortiWeb attack signatures to protect against path traversal, forceful browsing, and access to sensitive files that can invoke permission elevation. ■ Use the FortiGuard Labs credential stuffing defense service.
2. Cryptographic Failures	As applications handle sensitive data, especially data covered by privacy and financial regulations (for example, GDPR or PCI-DSS), appropriate protection for data-in-transit and data-at-rest must be provided.	■ Use FortiWeb to force access over TLS encryption even to those applications that can be accessed via HTTP. Use HSTS and the secure attribute when possible. ■ Protect client and server-side communication by only using stronger ciphers on FortiWeb. ■ Enable FortiWeb Attack signatures to protect against direct access to sensitive files such as etc/passwd. ■ Use FortiWeb signatures to block sensitive data leakage in headers and other locations. ■ Enable cookie encryption. ■ Mask all sensitive fields in FortiWeb logs to make sure sensitive data cannot be read by anyone, not even administrators.

OWASP Top 10	Description	FortiWeb Mitigation
3. Injection	One of the oldest and still widely popular attacks, an attacker injects malicious code into a request hoping the application will not sanitize it. If unsanitized, the code will do something it wasn't supposed to do, such as retrieve data that does not belong to the user. SQL injection is a very common form of injection attacks but there are many other injection types such as LDAP, OS commands, email header injections, and others. Cross-site scripting is a very dangerous and popular attack that now is included in the Injection category of OWASP Top 10 2021.	■ Enable FortiWeb Attack signatures to protect against injection and cross-site scripting attacks. ■ Enable machine learning for anomaly detection to protect against zero-day injection attacks. Since injection attacks try to exploit a vulnerability within the logic of the application and not necessarily a vulnerability in the code itself (meaning, no validation/sanitization of input) anomaly detection protection is critical here. ■ Enable machine learning for API protection to automatically defend APIs from zero-day attacks. Alternatively, enforce XML and JSON schema validation based on uploaded schema.
4. Insecure Design	This new category in the OWASP Top 10 for 2021 focuses on risks related to design and architectural flaws. These are primarily around SLDC, not something that can be rectified by an implementation. An insecure design cannot be fixed by a perfect implementation as, by definition, needed security controls were never created to defend against specific attacks.	Out of Scope: To help prevent insecure design, follow programming best practices and establish a secure software development lifecycle (SSDLC).
5. Security	Security misconfiguration is the failure in implementing all necessary security controls for an application. These misconfigurations can be default user accounts and passwords that weren't disabled upon deployment, enabled software components that aren't needed, cloud permissions not set correctly and so on. In the OWASP Top 10 for 2021, Security Misconfiguration also includes XML External Entities (XXE), previously a separate OWASP category. In this attack XML input containing a reference to an external entity is being manipulated and exploited when the XML parser isn't configured correctly.	■ Enable FortiWeb Attack signatures to detect attempts to retrieve sensitive information and block access to known default system URLs. ■ Enable FortiWeb's Forbidden XML Entities protection with External Entity, Entity Expansion and XInclude to protect against XML external entity attacks. ■ Introduce FortiWeb authentication layer and force all users to authenticate. ■ Enforce file security to block access to certain file types.
6. Vulnerable and Outdated Components	Vulnerable and outdated components refer to known vulnerabilities (also referred to as CVEs) in components, modules, libraries, or software packages. Many of these are third-party or open-source packages that are not controlled by customers, but are widely deployed and incorporated in most customer applications as they provide standard software capability. Take OpenSSL as an example. Vulnerabilities in these components can result in a threat to the application like any other vulnerability and can be exploited using the standard Injection attacks, XSS, buffer overflow, and other exploits. The Log4J vulnerability is a good example of this category.	■ Enable FortiWeb attack signatures to detect attempts to exploit known CVEs. ■ Regularly scan applications for known vulnerabilities using standard vulnerability assessment tools. Integrate the tools with FortiWeb for automatic virtual patching.
7. Identification and Authentication Failures	Identification and authentication failures refer to confirmation of a user's identity, authentication, and session management, which is critical to protect against authentication-related attacks. This category moved from second to down seventh position this year. This category can include credential stuffing attacks, brute force attacks, session hijacking, session fixation, and others exploits.	■ Enable client management so FortiWeb can track every user session. ■ Enable credential stuffing protection to verify users aren't logging in with previously identified breached credentials. ■ Enable session fixation protection and enforce session timeout. ■ Enable cookie security "signed" or "encrypted" to prevent session hijacking. ■ Enable FortiWeb attack signatures.

OWASP Top 10	Description	FortiWeb Mitigation
8. Software and Data Integrity Failures	Software and data integrity failures refer to code and infrastructure that is vulnerable to integrity violations. An example is an application that relies on plugins, libraries, or modules from untrusted sources and repositories that are not correctly verified and could be tampered or corrupted with. This can lead to allowing attackers to exploit the application once the malicious code has been installed. This was the main cause of the SolarWinds 2020 supply chain attack that impacted thousands of organizations globally. Software and data integrity failures cannot by itself be protected by a WAF as it relates to the software integrity itself. However, a WAF can help with the exploitation of the vulnerability it creates.	■ Introduce FortiWeb authentication to application specific admin interfaces and/or other sensitive URLs. ■ Enable FortiWeb attack signatures to protect against buffer overflows, command injection, and other attack types.
9. Security Logging and Monitoring Failures	Security logging and monitoring failures were previously named “Insufficient Logging and Monitoring.” These failures involve weaknesses in an application’s ability to detect security risks and respond to them. Logging suspicious activity is an integral role of every security system. Without logging and monitoring, breaches cannot be detected.	The FortiWeb solution includes advanced monitoring and logging capability to quickly understand events, correlate attacks over time, and help administrators zoom in on the most severe threats immediately. ■ Attack logs include a coherent, easy to read presentation that highlight the violation. ■ FortiView helps administrators dice and slice logs according to various criteria such as source IP, geo IP, headers, URLs and many others. ■ Use threat analytics. It simplifies threat detection and response and speeds up WAF alerts security investigation. Using machine learning, attacks are analyzed across all your web applications to identify common characteristics and patterns and group them into meaningful security incidents. ■ Enable traffic log forward to a remote server for safe keeping and future security investigation.
10. Server-side Request Forgery	Newly introduced in 2021, the server-side request forgery (SSRF) vulnerability occurs when a web application pulls data from a remote resource based on a user-specified URL, without validating the URL. The attacker can force the application to send requests to access unintended resources, often bypassing security controls. Successful SSRF attacks can result in data exfiltration, sensitive data leakage, and data theft.	■ Enable attack signatures to protect against SSRF attacks in known applications. ■ Enable machine learning anomaly detection to protect against zero-day SSRF attacks.

Summary

The OWASP Top 10 provides a great starting point for customers to assess their current application security posture and prioritize their risk mitigation priorities. Widely adopted by many standards organizations as a baseline security metric, the OWASP Top 10 helps organizations refine their focus on application security.

FortiWeb delivers the OWASP Top 10 security you need, along with API discovery and protection, bot mitigation, and advanced threat detection.

[1] 2021 DBIR Summary of Findings, Verizon.

[2] Application Security Report, Cybersecurity Insiders, 2021.

FORTINET

www.fortinet.com

June 24, 2022 3:11 PM

1617247-0-0-EN