cymulate

SOLUTION BRIEF

Web Application Firewall Validation

Web Application Vulnerabilities Are a Constant Threat for Cyber Attacks

Threat actors have increased their intensity for exploiting web application vulnerabilities to disrupt business operations with denial-of-service attacks and manipulate applications to gain unauthorized access to data and systems.

In recent years, there has been a 137% increase in denial-of-service attacks targeting web applications and their APIs. And if that weren't enough, malicious bot activity is up 61%, creating a constant threat to web applications.[1]

Web App Firewalls Require Continuous Validation to Block the Latest Cyber Threats

Cybersecurity leaders need to constantly test and optimize the effectiveness of their web application firewalls and policies to protect their applications and APIs from attacks that target backend data and disrupt operations.

Cymulate enables your security team to conduct comprehensive assessments of your web application firewalls, to test and validate using common methods used by threat actors to inject malicious code and manipulate applications and their APIs. The best-practice assessment simulates different types of web application attack types, including:

- **SQL/NoSQL injection**
- **Command injection**
- **XML injection**
- **File inclusion**
- **Cross-site scripting (XSS)**
- **Server-side request forgery (SSRF)**
- **Path (directory) traversal**
- **WAF bypass**

The results of these assessments highlight the gaps and weaknesses in your web app firewall that could be used to manipulate your applications and APIs, leading to a cyber attack.

> **We used Cymulate to assess the protection of one of our web applications and received a very high score, which was strange because we configured our WAF to protect the site. After some internal checks, we discovered that our WAF was not actually protecting the site. We would have been left completely vulnerable had Cymulate not shown us this gap.**
> – Security Leader, Telecom Industry

[1] Radware Global Threat Analysis Report

Solution Benefits

Continuous validation

Automated continuous testing of web application firewalls and policies against the latest web-based threats.

Identify gaps

Find gaps and weaknesses in your web application firewall that could expose your application to cyber threats.

Optimize controls

Configure and tune your web application firewall with mitigation guidance to block malicious activity.

Reduce exposure

Continuously measure and improve your web application firewalls to reduce the risk of a cyber attack.

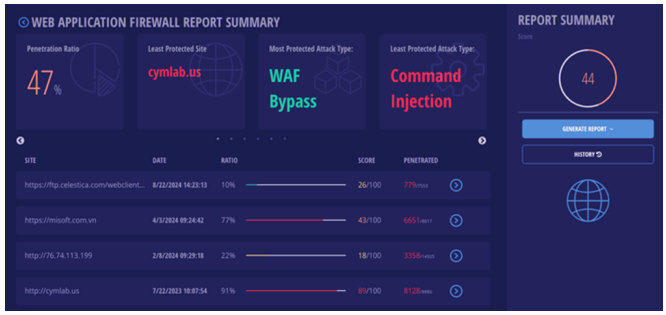
Automated Security Validation for Your Web Application Firewalls

The Cymulate platform includes breach and attack simulation to deliver production-safe security testing of your web application firewalls, using a wide range of malicious payload variants to simulate common web application attack methods. The solution lets you identify the gaps and weaknesses in your firewalls that could enable malicious code to exploit your applications or a malicious payload to reach your systems and initiate a cyber attack on your environment. The assessment enables you to optimize the investment you have made in your web application firewalls by configuring and tuning your web defenses with mitigation guidance from Cymulate.

Detailed Report and Findings

Gain deep insight into the effectiveness of your web application firewalls and policies with detailed reports and findings that include:

- **Risk score** to measure the overall performance of your web application firewalls.
- **Exposure level** to measure your security posture.
- **Penetration ratio** highlighting the number of attack methods and payloads not blocked by the firewall.
- **Ratio by site** to focus efforts on least-protected websites and applications.
- **High-risk forms and inputs** to highlight web application forms and inputs that can be manipulated by different attack methods.
- **Least-protected attack types** to highlight which attack types are most successful.
- **Mitigation guidance** to help optimize firewalls and enhance policies.



Why choose Cymulate?

Depth of attack simulations

The assessment contains a comprehensive suite of over 7,000 malicious payloads to fully validate the effectiveness of your web application firewalls.

Production safe

The full suite of test cases is completely production-safe with no malicious payload or code execution that could impact your production environment.

Automated validation

The assessment is fully automated, enabling continuous validation and performance optimization of your web application firewall effectiveness every week.

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation. For more information, visit www.cymulate.com.

Get a Demo