cymulate

SOLUTION BRIEF

Web Application Firewall Validation

Web Applications Remain Prime Targets for Attackers

Threat actors continue to exploit web application vulnerabilities to disrupt business operations, exfiltrate data and gain unauthorized access to systems. In recent years, there has been a 137% increase in denial-of-service attacks targeting web applications and their APIs. In parallel, malicious bot activity has increased by 61%, posing a constant threat to web-exposed assets.1

Cybersecurity teams must continually test and optimize their web application firewalls (WAFs) to protect applications and APIs from attacks that target backend data and disrupt operations.

Validate WAF Across Public and Authenticated Applications

Cymulate enables security teams to perform comprehensive WAF assessments, validating the effectiveness of their protection against the same attack methods threat actors use to inject malicious code or manipulate applications and APIs.

These assessments simulate multiple 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**

Cymulate supports configuring and validating web applications that use OAuth 2.0 authentication, enabling assessment of sites protected by modern single sign-on (SSO) methods from identity providers such as Okta, Azure AD, Ping Identity, Google Workspace and Auth0. This allows realistic validation of WAF protections within authenticated areas of enterprise web applications.

Assessment results highlight gaps and weaknesses in WAF policies that could be exploited to manipulate applications and APIs or gain unauthorized access to data. Mitigation guidance is provided in the form of WAF rules, expressed in regular expression and, for select WAF platforms, translated into vendor-specific WAF rules to help teams address the identified gaps.

> **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

Solution Benefits

Continuous validation

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

Identify gaps

Find gaps and weaknesses in your WAFs that could expose your applications to malicious activity.

Optimize controls

Configure and tune your WAF with actionable mitigation guidance and WAF rules for application-layer threats, tailored to your environment.

Reduce exposure

Continuously measure and improve your WAFs to reduce the risk of a cyber attack.

[1] Radware Global Threat Analysis Report

Comprehensive and Authenticated Security Validation for Modern Web Applications

The Cymulate Platform delivers production-safe, automated validation of web application firewalls using breach and attack simulation. It safely launches a wide range of malicious payload variants to simulate common web application attack methods and observe how defenses respond.

Support for modern authentication protocols such as OAuth 2.0 ensures complete coverage across both public and authenticated routes. This provides a realistic assessment of WAF behavior under production-like conditions, offering actionable guidance for tuning security configurations.

How it works

Cymulate conducts WAF attack simulations that align with OWASP and common application exploits. Because the assessment focuses solely on web-facing components, no internal test point is required.

Security teams provide Cymulate with the URLs or endpoints of the web applications to be tested; typically, the organization's publicly accessible assets. The WAF assessment then launches simulated exploit payloads directly against those endpoints, replicating techniques such as SQL injection (SQLi), cross-site scripting (XSS), remote file inclusion (RFI) and command injection.

These controlled simulations test whether the WAF and application-layer defenses, such as input validation, code sanitization and authentication logic, successfully detect, prevent or block malicious activity.

Each assessment generates detailed results identifying:

- Exploit attempts prevented or not prevented
- Application and WAF responses to harmful requests
- The overall effectiveness of threat mitigation controls

For identified security gaps, Cymulate provides detailed mitigation guidance to help security teams fine-tune WAF policies, strengthen application-layer protections and build threat-informed security. This guidance includes WAF rules expressed in regular expression, as well as structured WAF rules that support translation into vendor-specific formats based on the attack behavior validated during the assessment.

Why Choose Cymulate?

Comprehensive attack simulations

Validate WAF effectiveness with over 7,000 attack payloads that test protection across public and authenticated web apps.

Modern authentication coverage

Assess applications secured by OAuth 2.0 and SSO supported by Okta, Azure AD, Ping Identity, Google Workspace, etc.

Actionable mitigation guidance

Build threat-informed defenses with mitigation guidance and custom WAF rules for stronger protection of web apps and APIs.

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