

Web Application Firewall (WAF) Assessment

Solution Brief



Testing Your WAF Security

Cymulate Web Application Firewall (WAF) vector enables you to test and optimize the security posture of your web security controls. This vector challenges your WAF against a comprehensive set of attacks and together with the results, provides actionable remediation guidelines.

Attack Vector Overview

Web application attacks are frequently used by threat actors to steal information or penetrate an organization through its externally facing web applications. Attacks such as SQL injection (SQLi) and other forms of command injections are used to exploit web application and web infrastructure vulnerabilities that can lead to a breach.

Where web application security measures often fall short is through misconfiguration and lack of optimization. The best web application firewall implementation will no longer be effective, within a few months, or even weeks, to evolving hacker tools and techniques.

Continuous Testing

The Cymulate WAF vector simulates the behavior of an adversary attacking the web application and web infrastructure of an organization.

It tests the effectiveness of the web security controls against these attacks and is constantly updated with new tactics and techniques. After each assessment a test reports will identify the security gaps and provides actionable steps to remediate them. Continuous testing enables you to maintain optimal effectiveness of your web security controls.

How It Works

The Cymulate WAF assessment operates in several phases to provide a well-covered and controlled assessment.

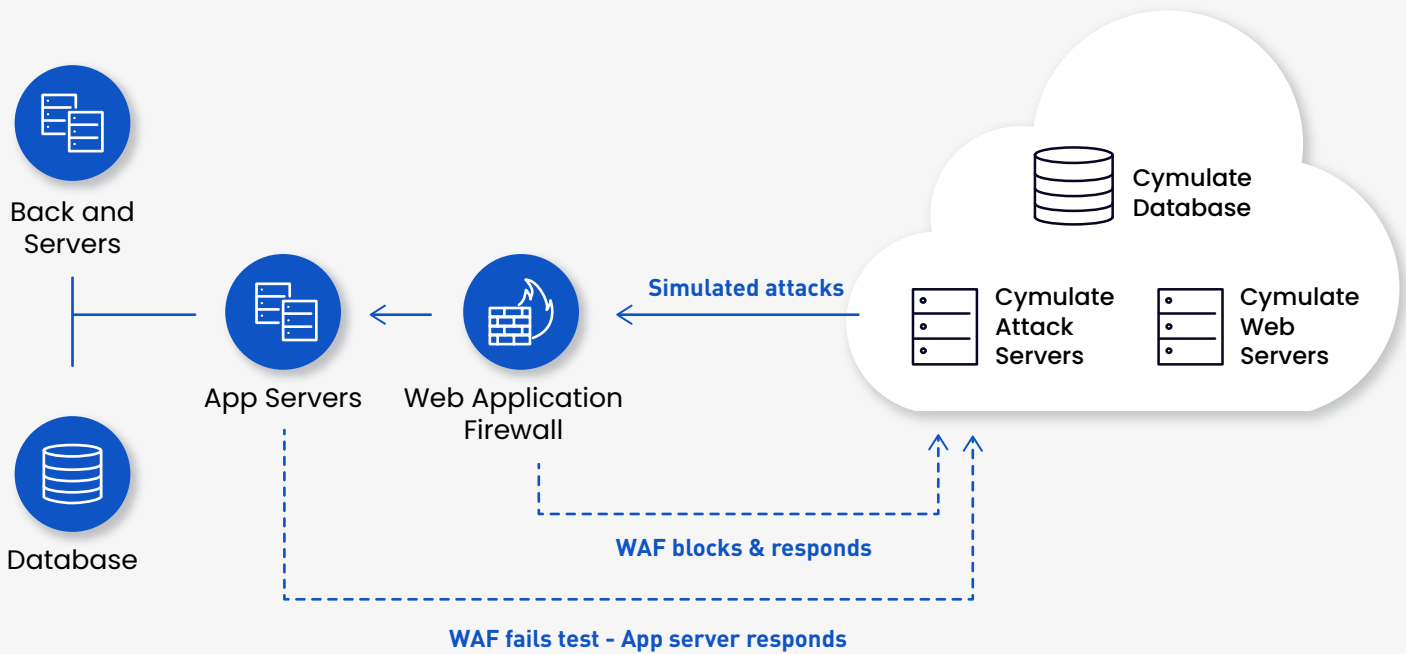
Test Setup – WAF security assessments are based on a library of web attacks in the platform, out-of-the-box. Each of the categories contains a library of web attacks. The libraries include:

- SQL injection
- Cross-site scripting (XSS)
- File inclusion for remote code execution
- Command injection
- Vulnerability scanning

Test Execution – Assessments can be executed on-demand or scheduled. The testing is performed on target URLs that the end user defines. Once initiated, the Cymulate attack servers crawl the target URL to map forms and other means of data import.

The attack servers send malicious payloads for every form and data import and compare the response of the WAF to each attack. Expected responses from the WAF are pre-configured on the Cymulate platform in the setup.

Test Results and Remediation – After each test, a technical and an executive security assessment report is generated, and a risk score is calculated. The reports provide test results and guidance to remediate the gaps found by the test in order to reduce your cyber-exposure.



Key Features

- Leverage Cymulate's extensive library of web attack types to test your WAF security efficacy against thousands of payloads mapped to OWASP TOP 10.
- All stages of the test are automatic, including the initial crawling of the target websites and the response comparison.
- The testing does not affect the websites since no exploitation is performed.
- Test continuously from anywhere, anytime.

Actionable Insights

The simulation results are presented in an easy-to-understand comprehensive report. Mitigation recommendations are offered for each security gap discovered depending on the type of simulated attack, enabling IT and security teams to take the appropriate countermeasures.

About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company—and every company—will be.

Contact us for a live demo, or get started with a free trial

[Start Your Free Trial](#)