Signal Sciences

Detection and Blocking

SUMMARY

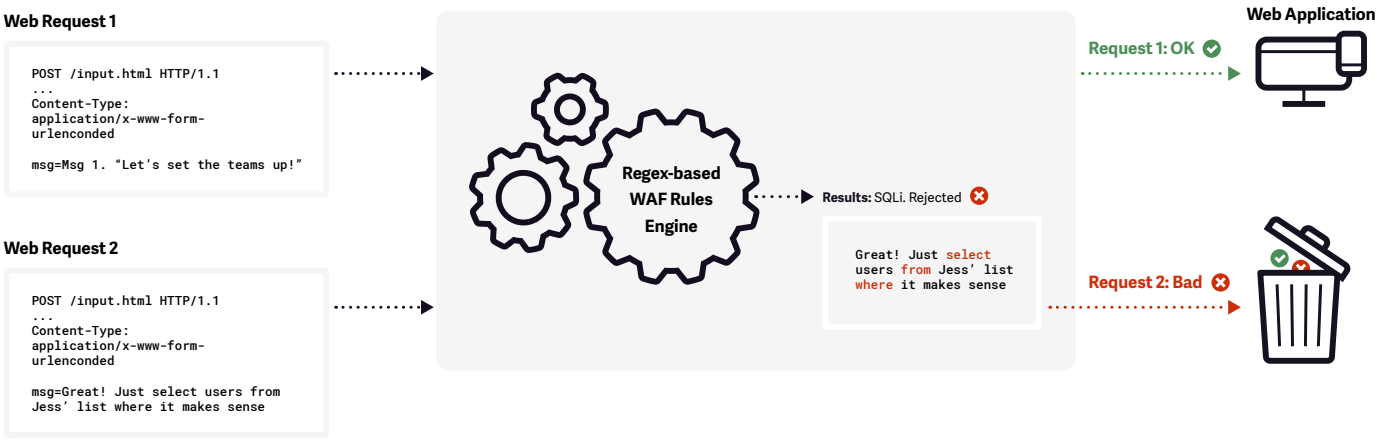
- Signal Sciences next-gen WAF was designed by security practitioners.
- Legacy WAF solutions use a set of regex rules that often result in false positives, blocking legitimate traffic.
- Signal Sciences next-gen WAF provides faster and more reliable detection of attacks with fewer false positives and no tuning required

The Limitations of Legacy Detection and Blocking Techniques

Anyone with experience deploying a web application firewall (WAF) knows that an extensive tuning period is required to ensure that default rule sets do not generate false positives and block legitimate traffic for their applications.

The legacy approach of using default rules leaves organizations with subpar options: they can enable only a small number of rules they've validated as "safe," leaving the application exposed; or they can enable more rules that risk blocking legitimate traffic in order to catch more potential attacks.

Legacy Regex-Based WAF Approach



Legacy WAF solutions use a set of regex rules to distinguish between normal requests and malicious requests. This often results in false positives, preventing legitimate traffic from reaching the application.

A Superior Approach to Detection

Signal Sciences next-gen WAF was designed by security practitioners that have lived the pain of this constant tuning process and have seen where pattern matching and signature-based rule sets fall short.

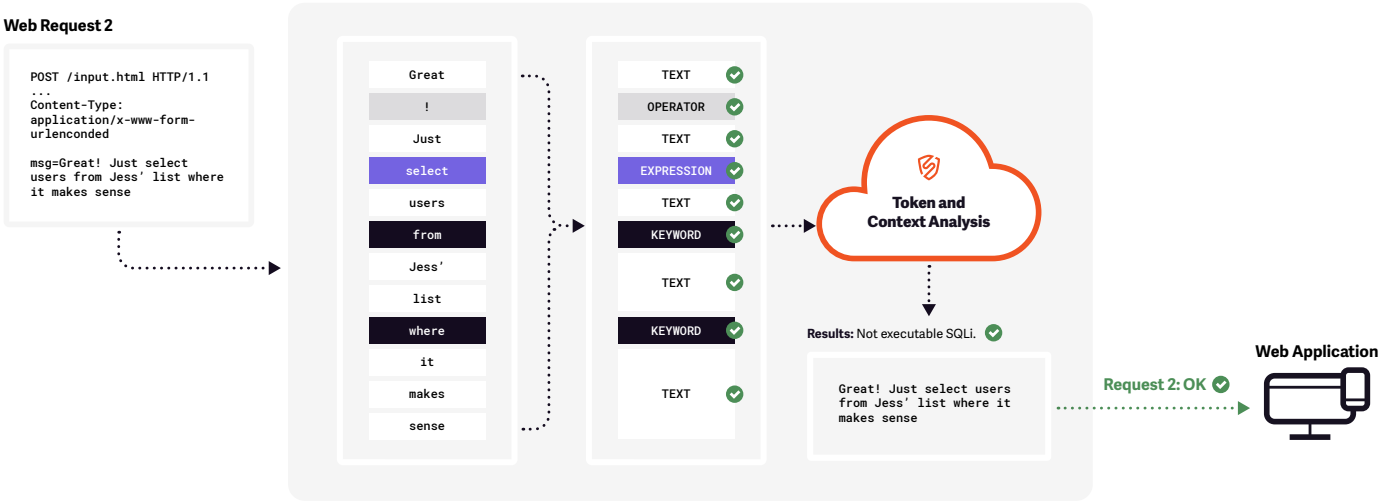
Compared to legacy WAFs that rely on regex matching and are rarely used in blocking mode, 95% of Signal Sciences customers enable full blocking mode across all default attack types without any tuning. The key to our reliable, accurate decisions is our patented architecture and proprietary detection technology called SmartParse, which makes instantaneous decisions in line to determine if malicious or anomalous payloads are present.

By evaluating the context of the request and how it would actually execute, SmartParse makes highly accurate detections. Through a combination of SmartParse and Power Rules that enable more advanced, customized detections and blocking, Signal Sciences delivers automated defense against OWASP Top 10 threats—and beyond.

Injection Attacks

With injection attacks via SQLi or XSS, untrusted data is sent to an interpreter as part of a command or query. SmartParse analyzes request parameters to determine whether the code is actually executable and tokenizes the results. The tokenized representation of the request is analyzed, at runtime, to detect attacks such as SQLi, XSS, and other OWASP Top 10 injection attacks. This approach has a much lower false positive rate and is much faster than signature-based detection approaches.

Signal Sciences SmartParse Detection Method



Signal Sciences SmartParse tokenizes web requests to provide more accurate detections.

With this approach, Signal Sciences delivers significant benefits to DevOps and security teams:

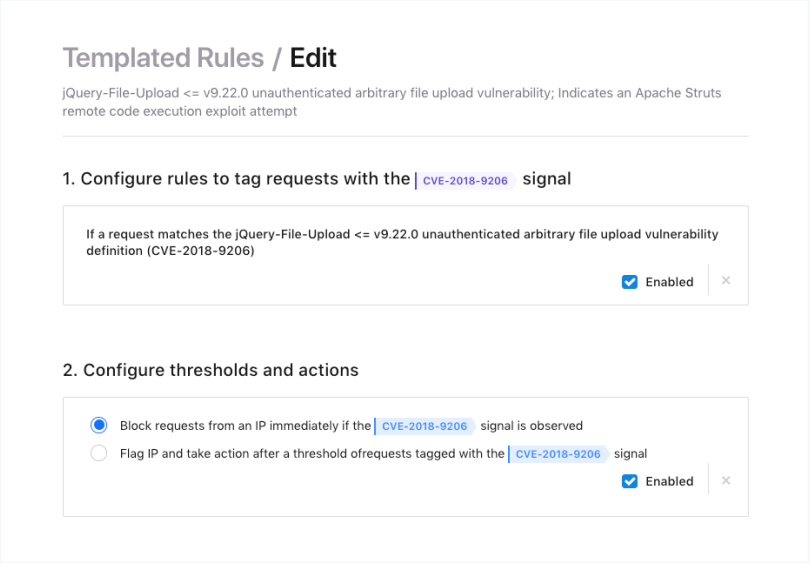
- Faster, more reliable detection of attacks
- No manual rules tuning
- Less time wasted on false positives
- Securing applications without breaking them

Coverage Beyond Injection Attacks

Beyond detection and blocking of SQLi and XSS attacks, Signal Sciences enables customers to automatically detect all other OWASP Top 10 attacks with Power Rules. With Power Rules, users can set up thresholds, automatic blocking, and alert triggers specific to their web application and business logic within the Signal Sciences Console. Power Rules can also apply vulnerability patches to address outdated or otherwise compromised components, such as libraries, frameworks, and other software modules, that run with the same privileges as an application.

Vulnerability Virtual Patching with Power Rules

A virtual patch prevents the exploitation of a known vulnerability in either a module or framework. A virtual patch analyzes transactions and intercepts attacks in transit, so malicious traffic never reaches the web application. The resulting outcome from applying a virtual patch is that, while the actual source code of the application itself has not been modified, the exploitation attempt does not succeed. This buys time in the development process to fix the underlying vulnerability while the patch is protecting the application at runtime.



In this example templated Power Rule, Signal Sciences will block requests that attempt to exploit the Apache Struts vulnerability that leads to remote code execution.

With Power Rules, Signal Sciences enables customers to apply virtual patches that address various Common Vulnerability and Exposures (CVEs) and immediately block requests containing the CVE exploit. Within the Console, customers can use templated Power Rules that cover various CVEs in a default list.

A Superior Approach to Blocking

Signal Sciences vastly improves detection accuracy by separating blocking decisions from initial detections using a threshold-based approach. Instead of the legacy approach of blocking any incoming request that matches a regular expression (regex) immediately, Signal Sciences uses SmartParse detections coupled with time-based thresholds and anomaly data around the request and response to make informed blocking decisions.

When incoming requests contain attacks, a snippet of that request is sent to Signal Sciences Cloud Engine (see the Privacy FAQ to learn how this is done in a safe and private manner). The Cloud Engine aggregates attacks from across all deployed agents—including other customers' agents through our proprietary Network Learning Exchange (NLX). When enough malicious activity is seen from a potential attacker based on pre-defined yet customizable thresholds built using big data analytics, the engine flags that user for blocking. This method results in highly accurate detections and provides broader context around various attacks.

Using a combination of default detections plus Power Rules functionality, users of Signal Sciences are able to gain more accurate and far greater blocking coverage across the OWASP Top 10 than ever before.

Additional resources

Learn more about our patented solution to securing web applications:

- Signal Sciences Architecture
- Signal Sciences Next-Gen WAF

Request a demo

Request a demo and we'll get you set up with one of our experts.

Any App

Cloud, Containers, PaaS, and Serverless

Web Servers and Languages

Gateways and Proxies

Any Attack

OWASP Top 10

Application DoS

Brute force attacks

+ MORE

Any DevOps Toolchain

Slack

Datadog

Webhooks

Splunk

SIEM/SOC tools via APIs

+ MORE