Detection and Blocking

The Challenges In Legacy Detection & Blocking Techniques

Anyone with experience deploying a Web Application Firewall (WAF) is all too familiar with the extensive tuning period required to ensure that the canned rule-sets do not generate false positives and block legitimate traffic for their applications.

The Signal Sciences Web Protection Platform 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.

The legacy approach of using canned rules leaves organizations with few options other than only enabling a small number of rules they have been able to validate as "safe", or risk blocking legitimate traffic in order to be able to catch more potential attacks.

Key Takeaways

✓ **Key Takeaway 1**
The Signal Sciences Web Protection Platform 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.

✓ **Key Takeaway 2**
WAF solutions use a set of regex rules to distinguish between normal requests and malicious requests, but this often results in false positives, preventing legitimate traffic from reaching the application.

✓ **Key Takeaway 2**
Signal Sciences' Web Protection Platform benefits include: Faster and more reliable detection of attacks, No manual tuning needed of rules, and Less time wasted on false positives, giving you security without breaking your applications.

The World's Top Companies Trust Signal Sciences

yelp EAT24 · Adobe · DUO · vimeo · tenable · SHINOLA DETROIT · UNDER ARMOUR · Etsy

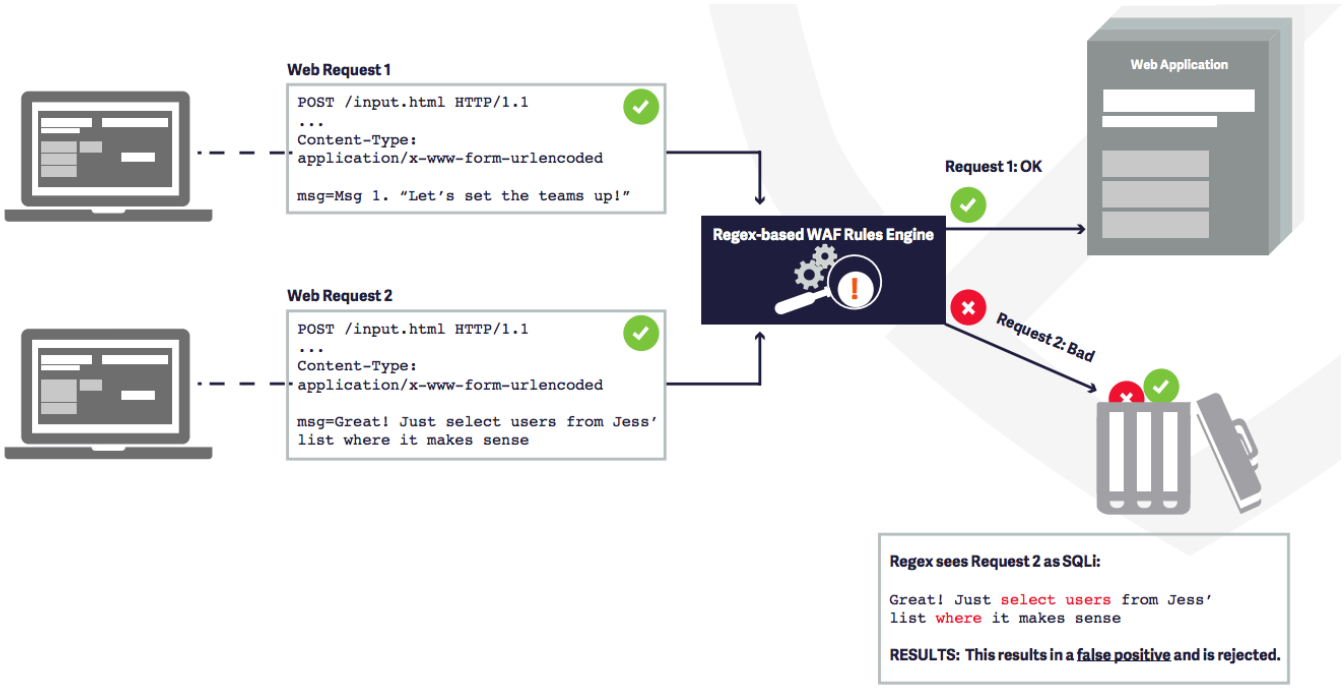


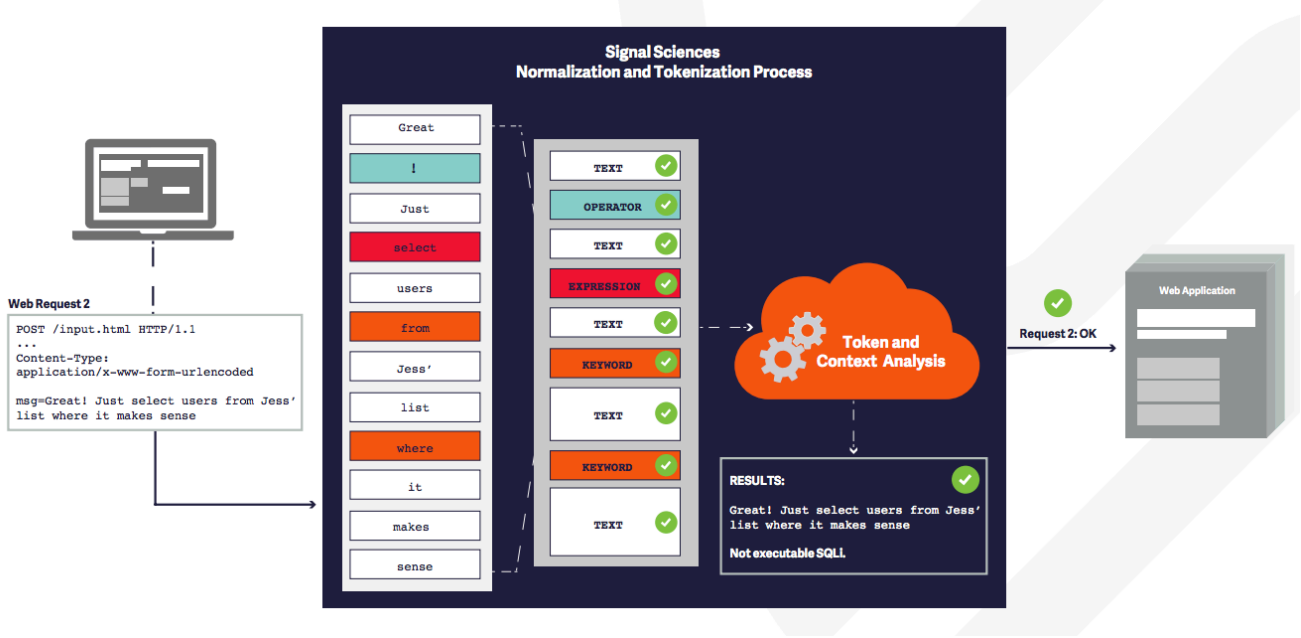
FIGURE 1: Traditional Regex-Based WAF Approach

A Different Approach to Detection & Blocking

The key to Signal Sciences advanced detection is a proprietary technique that analyzes request parameters 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.

In the case of SQLi, the tokenized results are parsed by a lightweight SQL parser to determine whether the code is actually executable. This approach has a much lower false positive rate and is much faster than signature-based detection approaches.

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



Signal Sciences Attack Chain Without False Positives

Signal Sciences vastly improves detection accuracy by separating blocking decisions from initial detections. Instead of the legacy approach of blocking any incoming request that matches a regular expression or anomaly threshold at the time of the first request, Signal Sciences uses highly accurate detections and anomaly data to build an attack chain.

When incoming requests contain attacks, a snippet of that request is sent to the Signal Sciences cloud analysis 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, and when enough malicious activity is seen from a potential attacker the engine flags that user for blocking. This method results in highly accurate detection and gives a fuller context of the attack.

With this approach, Signal Sciences' Web Protection Platform benefits include:

- Faster and more reliable detection of attacks
- No manual tuning needed of rules
- Less time wasted on false positives, giving you security without breaking your applications