Trustwave®

DATA SHEET

Trustwave Modsecurity Rules & Support

HIGHLY ACCURATE RULE PACKAGE FOR WEB APPLICATION VULNERABILITIES

Benefits

- Quick time-to-value with pre-configured rules ready to work with ModSecurity
- Save time and resources chasing fewer false positive vulnerabilities
- Protect applications with virtual patches without needing developer time
- Leverage expertise of and intelligence gathered by the SpiderLabs research team

ModSecurity, the popular open source web application firewall (WAF), has a long history of protecting web applications. Today, Trustwave and the Trustwave SpiderLabs team is the primary custodian of ModSecurity. Trustwave also participates in the OWASP ModSecurity Core Rule Set (CRS) project, as well as develops and supports our own commercial ruleset for the ModSecurity WAF.

Why Use A Ruleset With Modsecurity?

Using a ruleset is an important part of protecting web applications with ModSecurity. ModSecurity provides very little protection on its own. To be useful, it must be configured with rules. An open source option is available – the OWASP ModSecurity CRS. It offers a set of generic attack detection rules that provide a base level of protection for any web application. While the OWASP CRS is a good start for protecting web applications, the Trustwave ModSecurity Rules & Support offer specific benefits above-and-beyond what is provided with the OWASP CRS, including:

- **Saving you time.** You'll save time and resources by chasing fewer false positives.
- **Offering regular updates.** You'll get regular rules updates to protect you against the latest vulnerabilities and threats.
- **Providing support.** Use the TrustKeeper customer support portal to help related to alert analysis, rules configuration questions and exception assistance.

The Trustwave ModSecurity Rules can complement the OWASP CRS or be used on their own.

Highly Accurate Rules from Trustwave Spiderlabs Experts

The Trustwave ModSecurity Rules are developed and maintained by the SpiderLabs research team. The SpiderLabs Research Team monitors public vulnerability lists such as ExploitDB, FullDisclosure and Bugtraq to identify when new vulnerabilities are released for public web software (both open source and commercial) as well as get intelligence information on new vulnerabilities and "0-days" from other sources, including our own Threat Intelligence team. They then create new rules to help prevent exploitation of the vulnerability and add it to the commercial rules feed where customers can download the latest archive daily.

Customers using the Trustwave ModSecurity rules can choose which ones to apply to the ModSecurity WAF which enables them to build an exact profile to protect their web site and applications without overloading the WAF with unneeded vulnerability signatures.

Key Features of Trustwave Modsecurity Rules

The Trustwave ModSecurity Rules includes many features to protect web applications, including:

- Virtual Patches: Thousands of rules that block exploit activity against known vulnerabilities in public software such as WordPress, Joomla, Drupal, and Microsoft SharePoint.
- IP Reputation monitoring: Detection or blocking of traffic originating from IP addresses of malicious clients, as well as Anonymous Proxies, and TOR Exit Nodes.
- Webshell/Backdoor Detection: Facilitated the thousands of captured webshells and backdoors from web honeypot attacks and forensic investigations collected by the SpiderLabs team.
- Botnet Attack Detection: Identify and cut off web attacks generated by botnet clients with Trustwave SpiderLabs custom botnet fingerprints.
- HTTP Denial of Service (DoS) Attack Detection: Detect and shut down traffic originating from application-level denial of service tools such as HOIC/LOIC, Pandora, Drive, and more with custom fingerprints developed by Trustwave SpiderLabs

Support & Services

A Trustwave ModSecurity Rules subscription includes the rules themselves, regular updates from the SpiderLabs team, and technical assistance. Experts in the Trustwave Technical Assistance Center (TAC) is available to provide ModSecurity customers with help related to alert analysis, rules configuration questions and exception assistance related to either the commercial rules or the OWASP ModSecurity Core Rule Set.

For organizations that want more assistance, professional services, and additional training is also available. Services available include:

- **ModSecurity Professional Services:** Receive hands-on assistance directly from SpiderLabs ModSecurity experts for installation help, advanced/custom configurations, and virtual patching.
- **ModSecurity Training:** Through online or on-site seminars from one-to-three-days long, students learn from SpiderLabs ModSecurity experts how to defend web applications through hands-on lab activities.

About Spiderlabs

In addition to developing and supporting the Trustwave ModSecurity Rules, the Trustwave SpiderLabs team offers a variety of services to help organizations with security and compliance.

The SpiderLabs team at Trustwave includes security and penetration testers, incident responders, forensic investigators, malware reversers, security researchers, published authors and sought-after speakers.

Trustwave SpiderLabs is known for:

- Delivering expert security and penetration testing services
- Incident readiness and data breach forensic investigations
- Threat intelligence that fuels industry-leading managed security services and technologies
- Innovative security research and major threat discoveries
- Contributions to the community including the annual Global Security Report, the SpiderLabs blog as well as the open-source ModSecurity web application firewall.

To learn more about the SpiderLabs team and services, visit https://www.trustwave.com/Company/SpiderLabs/

For more information: www.trustwave.com