SERVICE DESCRIPTION

MODSecurity Rules

Service Description

The ModSecurity Web application firewall (WAF) engine assists in providing powerful protection against threats to data via applications. However, in order to become effective, ModSecurity must be configured with rules that help it recognize threats and defend against them. Trustwave SpiderLabs provides a commercial certified rule set for ModSecurity 2.x that helps protect against known attacks that target vulnerabilities in public software.

ModSecurity Rules from Trustwave SpiderLabs complement the open source OWASP ModSecurity Core Rules Set (CRS) by enhancing the basic payload protection offered by CRS. But CRS does not correlate specific attack vector locations (such as URL and parameters) from publicly disclosed vulnerabilities. This is where ModSecurity Rules from Trustwave SpiderLabs can help; these rules create custom virtual patches for various public vulnerabilities.

Trustwave SpiderLabs correlates data from numerous sources to generate commercial rules, automatically updating daily and as needed.

- Public vulnerability data such as the Open Source Vulnerability Database (OSVDB)
- Honeypot systems such as the WASC Distributed Web Honeypot Project (http://projects.webappsec.org/Distributed-Web-Honeypots)
- Trustwave WAF Customer Data Analysis

Copyright © 2019 Trustwave Holdings, Inc. All rights reserved.