OWASP ModSecurity CRS

Overview

The OWASP (Open Web Application Security Project) ModSecurity™ CRS (Core Rule Set) is a set of rules that Apache's ModSecurity™ module can use to help protect your server. While these rules do not make your server impervious to attacks, they greatly increase the amount of protection for your web applications.

About OWASP

Why should I use the OWASP ModSecurity rule set?

- **Protection from insecure web application design** — ModSecurity rule sets can provide a layer of protection for web applications such as WordPress, phpBB, or other types of web applications. It can potentially protect against vulnerabilities in out-of-date web applications that protect against vulnerabilities in unpatched, out-of-date applications. If the developer of an application makes a security mistake, ModSecurity may block a security attack before it can access the vulnerable application.
- **Protection against operating system level attack** — ModSecurity rule sets can protect against attacks that exploit the operating system of your server. For example, in 2014, there was a security flaw in the Bash shell program that Linux servers use. Security experts created ModSecurity rules to disallow the use of the exploit thought Apache. Server administrators used these ModSecurity rules and added additional security to their system until the release of a security patch for Bash shell.
- **Protect against generalized malicious traffic** — Some of the security threats that server administrators face may not directly attack a program or application on your server. DoS (Denial of Service) attacks, for example, are common attacks. You can reduce the impact of such malicious traffic through the use of ModSecurity rules.

What are the risks?

As with any mechanism that blocks web traffic, OWASP rules could block legitimate traffic (false positives). While both OWASP and cPanel, Inc. aim to curate the OWASP rule set to reduce the potential for false positives, the rule set may block legitimate traffic. Review the *ModSecurity Tools* interface (*WHM >> Home >> Security Center >> ModSecurity™ Tools*) routinely to evaluate the traffic that the rule set blocks and whether these blocks affect legitimate users.

How do I use the OWASP ModSecurity rule set?

Select the ModSecurity (`mod_security`) Apache module when you use *EasyApache 4* interface (*WHM >> Home >> Software >> EasyApache 4*). After you install the ModSecurity Apache module, use the *ModSecurity Vendors* interface (*WHM >> Home >> Security Center >> ModSecurity™ Vendors*) to install the OWASP rule set. When you enable the configuration files, the rules become active. To review the logged notifications and blocked traffic from these rules, use the *ModSecurity Tools* interface (*WHM >> Home >> Security Center >> ModSecurity™ Tools*).

How do I report a possible issue with an OWASP ModSecurity rule?

You can report a OWASP rule with which you find a problem, perform the following steps:

1. Navigate to WHM's *ModSecurity Tools* interface (*WHM >> Home >> Security Center >> ModSecurity™ Tools*).
2. Locate the hit that the rule generated in the *Hits List* and click *More*.
3. Click *Report this hit.*

> **Note:**
> This option does **not** appear if the vendor does not accept reports.

4. Enter your email address, the reason for the report, and any additional comments for the vendor.
5. Click *Review Report*.
6. Verify the information in your report and click *Submit.*

Configuration files

The OWASP ModSecurity CRS uses configuration files that contain the rules that help protect your server. These configuration files group similar rules together to make them easier to manage.

> **Note:**
> OWASP renumbered the configuration files in 2016. We **strongly** recommend that you update your rulesets.

cPanel & WHM version 64 and newer cPanel & WHM version 62 and earlier

REQUEST-901-INITIALIZATION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-901-INITIALIZATION.conf
```

This ruleset contains configuration information for subsequent rules in the ModSecurity CRS ruleset.

> **Warning:**
> If you disable this ruleset, other rulesets may **not** perform correctly.

REQUEST-905-COMMON-EXCEPTIONS

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-905-COMMON-EXCEPTIONS.conf
```

Other rules may incorrectly flag some traffic as bad (false positive). The rules in this configuration file detects those false positives and allows the traffic to pass through.

> **Warning:**
> If you disable this configuration file, it could cause excessive false positive rule hits.

REQUEST-910-IP-REPUTATION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-910-IP-REPUTATION.conf
```

The rule in this configuration file denies traffic from IP addresses that are involved in malicious activity or are in a region known for high rates of malicious activity.

> **Note:**
> - This type of check is an IP Reputation check.
> - These checks are useful for some sites but may deny legitimate traffic from users in the affected regions.

REQUEST-912-DOS-PROTECTION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-912-DOS-PROTECTION.conf
```

The rules in this configuration file attempt to reduce the impact of DoS (Denial of Service) attacks on your server.

> **Note:**
> A DoS attack can take various forms, but often involves large bursts of traffic that deplete the server resources and cause legitimate requests to fail.

REQUEST-913-SCANNER-DETECTION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-913-SCANNER-DETECTION.conf
```

The rules in this configuration file use the request headers to block requests from known security scanner software.

> **Note:**
> The value of this protection is limited because these headers are easy to change. However, the rules may reduce wasteful HTTP requests from automated scanners.

REQUEST-920-PROTOCOL-ENFORCEMENT

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf
```

The rules in this configuration file enable enforcement of certain HTTP restrictions on invalid or unusable data sent from clients. Block these request to help prevent the exploitation of a web application that did not expect the request.

REQUEST-921-PROTOCOL-ATTACK

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-921-PROTOCOL-ATTACK.conf
```

The rules in this configuration file enable specific checks for requests to mitigate HTTP Request Smuggling and Response Splitting attacks. These attacks can cause HTTP servers and proxies to mistakenly accept or return data that hide from other checks or rules due to a false Content-Length.

REQUEST-930-APPLICATION-ATTACK-LFI

The configuration file path:

`modsec_vendor_configs/OWASP/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf`

The rules in this configuration file enable protection against Local File Inclusion (LFI) attacks. During a LFI attack, a malicious client causes an application to serve or otherwise process a file from the local server's file system. These local server files would not normally be publicly accessible.

REQUEST-931-APPLICATION-ATTACK-RFI

The configuration file path:

`modsec_vendor_configs/OWASP/rules/REQUEST-931-APPLICATION-ATTACK-RFI.conf`

The rules in this configuration file enable protection against RFI (Remote File Inclusion) attacks. During a RFI attack, a malicious client exploits the server's software to embed a client-specified file into the content of the page.

Note:
This kind of attack executes malicious code either on the server or client side, based on the nature of the vulnerability.

REQUEST-933-APPLICATION-ATTACK-PHP

The configuration file path:

`modsec_vendor_configs/OWASP/rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf`

The rules in this configuration file enable protection against attacks against PHP. These attacks include PHP object injection, variable function calls, PHP I/O streams, PHP script uploads, and others.

REQUEST-941-APPLICATION-ATTACK-XSS

The configuration file path:

`modsec_vendor_configs/OWASP/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf`

The rules in this configuration file enable protection against XSS (cross-site scripting) attacks. During an XSS attack, the attacker injects scripts into web pages that other users view. These may do damage to either the server or to the viewer of the web page, or they allow a user to acquire and exploit other users' accounts or web sessions.

REQUEST-942-APPLICATION-ATTACK-SQLI

The configuration file path:

`modsec_vendor_configs/OWASP/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf`

The rules in this configuration file enable protection against SQL injection attacks. During a SQL injection attack, a client is able to pass a

specially crafted HTTP request to the server. This HTTP request causes the server to mistakenly execute a malicious query.

REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/RREQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION.conf
```

The rules in this configuration file enable protection against Session Fixation attacks. During a Session Fixation attack, attackers to force a user's session ID to be predictable. With the session ID, the attacker can take over a session that belongs to another user.

REQUEST-949-BLOCKING-EVALUATION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-949-BLOCKING-EVALUATION.conf
```

The rules in this configuration file blocks traffic that various other configuration files request.

Warning:
Other rules in the rule set depend on this configuration file to block incoming attacks. If you disable this configuration file, other rules will detect, but not block, incoming attacks.

RESPONSE-950-DATA-LEAKAGES

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/RESPONSE-950-DATA-LEAKAGES.conf
```

The rules in this configuration file enable protection against certain types of data leakages from the server to the client.

Note:
For example, these rules prevent directory listings.

RESPONSE-951-DATA-LEAKAGES-SQL

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/RESPONSE-951-DATA-LEAKAGES-SQL.conf
```

The rules in this configuration file enable protection against the leakage of inappropriate types of internal database information from the server to clients.

Note:
For example, if a SQL syntax error occurs, these rules will hide it. This protection reduces the chance that users will see the internal SQL errors of the application.

RESPONSE-952-DATA-LEAKAGES-JAVA

The configuration file path:

`modsec_vendor_configs/OWASP/rules/RESPONSE-952-DATA-LEAKAGES-JAVA.conf`

The rule in this configuration file attempts to prevent that exposure of details about server-side Java applications to the client.

Note:
For example, if a Java application returns an exception or raw code to a web page, these rules help prevent the display of the errors or raw code.

RESPONSE-953-DATA-LEAKAGES-PHP

The configuration file path:

`modsec_vendor_configs/OWASP/rules/RESPONSE-953-DATA-LEAKAGES-PHP.conf`

The rules in this configuration file enable protection against PHP-related data and source code leakage from the server to the client.

Note:
For example, a PHP application could produce an error that reveals internal implementation details about the application. This protection reduces the chance that users will see these details.

RESPONSE-954-DATA-LEAKAGES-IIS

The configuration file path:

`modsec_vendor_configs/OWASP/rules/RESPONSE-954-DATA-LEAKAGES-IIS.conf`

The rules in this configuration file enable protection against data leakages that relate to the Microsoft IIS® web server.

Note:
This rule set is only needed if your Apache server processes proxy requests to an IIS server or IIS-hosted application.

RESPONSE-959-BLOCKING-EVALUATION

The configuration file path:

`modsec_vendor_configs/OWASP/rules/RESPONSE-959-BLOCKING-EVALUATION.conf`

The rules in this configuration file enable a rule that blocks flagged anomalous traffic. This classification can occur as a result of hits that other configuration files produce.

Warning:

Other rules in the rule set depend on this configuration file to block incoming attacks. If you disable this configuration file, other rules will detect, but not block, incoming attacks.

RESPONSE-980-CORRELATION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/RESPONSE-980-CORRELATION.conf
```

The rules in this configuration file facilitate the gathering of data about successful and unsuccessful attacks on the server.

REQUEST-01-COMMON-EXCEPTIONS

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-01-COMMON-EXCEPTIONS.conf
```

Other rules may incorrectly flag some traffic as bad (false positive). The rules in this configuration file detects those false positives and allows the traffic to pass through.

Warning:
If you disable this configuration file, it could cause excessive false positive rule hits.

REQUEST-10-IP-REPUTATION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-10-IP-REPUTATION.conf
```

The rule in this configuration file denies traffic from IP addresses that are involved in malicious activity or are in a region known for high rates of malicious activity.

Note:

- This type of check is an IP Reputation check.
- These checks are useful for some sites but may deny legitimate traffic from users in the affected regions.

REQUEST-12-DOS-PROTECTION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-12-DOS-PROTECTION.conf
```

The rules in this configuration file attempt to reduce the impact of DoS (Denial of Service) attacks on your server.

Note:
A DoS attack can take various forms, but often involves large bursts of traffic that deplete the server resources and cause legitimate requests to fail.

REQUEST-13-SCANNER-DETECTION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-13-SCANNER-DETECTION.conf
```

The rules in this configuration file use the request headers to block requests from known security scanner software.

> **Note:**
> The value of this protection is limited because these headers are easy to change. However, the rules may reduce wasteful HTTP requests from automated scanners.

REQUEST-20-PROTOCOL-ENFORCEMENT

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-20-PROTOCOL-ENFORCEMENT.conf
```

The rules in this configuration file enable enforcement of certain HTTP restrictions on invalid or unusable data sent from clients. Block these request to help prevent the exploitation of a web application that did not expect the request.

REQUEST-21-PROTOCOL-ATTACK

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-21-PROTOCOL-ATTACK.conf
```

The rules in this configuration file enable specific checks for requests to mitigate HTTP Request Smuggling and Response Splitting attacks. These attacks can cause HTTP servers and proxies to mistakenly accept or return data that hide from other checks or rules due to a false Content-Length.

REQUEST-30-APPLICATION-ATTACK-LFI

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-30-APPLICATION-ATTACK-LFI.conf
```

The rules in this configuration file enable protection against Local File Inclusion (LFI) attacks. During a LFI attack, a malicious client causes an application to serve or otherwise process a file from the local server's file system. These local server files would not normally be publicly accessible.

REQUEST-31-APPLICATION-ATTACK-RFI

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-31-APPLICATION-ATTACK-RFI.conf
```

The rules in this configuration file enable protection against RFI (Remote File Inclusion) attacks. During a RFI attack, a malicious client exploits the server's software to embed a client-specified file into the content of the page.

Important:
You **must** disable the rules in this configuration file if you wish to add redirects in cPanel's *Redirects* interface (*cPanel* >> *Home* >> *Domains* >> *Redirects*).

Note:
This kind of attack executes malicious code either on the server or client side, based on the nature of the vulnerability.

REQUEST-41-APPLICATION-ATTACK-XSS

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf
```

The rules in this configuration file enable protection against XSS (cross-site scripting) attacks. During an XSS attack, the attacker injects scripts into web pages that other users view. These may do damage to either the server or to the viewer of the web page, or they allow a user to acquire and exploit other users' accounts or web sessions.

REQUEST-42-APPLICATION-ATTACK-SQLI

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-42-APPLICATION-ATTACK-SQLI.conf
```

The rules in this configuration file enable protection against SQL injection attacks. During a SQL injection attack, a client is able to pass a specially crafted HTTP request to the server. This HTTP request causes the server to mistakenly execute a malicious query.

REQUEST-43-APPLICATION-ATTACK-SESSION-FIXATION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-43-APPLICATION-ATTACK-SESSION-FIXATION.conf
```

The rules in this configuration file enable protection against Session Fixation attacks. During a Session Fixation attack, attackers force a user's session ID to be predictable. With the session ID, the attacker can take over a session that belongs to another user.

REQUEST-49-BLOCKING-EVALUATION

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/REQUEST-49-BLOCKING-EVALUATION.conf
```

The rules in this configuration file blocks traffic that various other configuration files request.

Warning:
Other rules in the rule set depend on this configuration file to block incoming attacks. If you disable this configuration file, other rules will detect, but not block, incoming attacks.

RESPONSE-50-DATA-LEAKAGES-IIS

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/RESPONSE-50-DATA-LEAKAGES-IIS.conf
```

The rules in this configuration file enable protection against data leakages that relate to the Microsoft IIS web server.

Note:
This rule set is only needed if your Apache server processes proxy requests to an IIS server or IIS-hosted application.

RESPONSE-50-DATA-LEAKAGES-JAVA

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/RESPONSE-50-DATA-LEAKAGES-JAVA.conf
```

The rule in this configuration file attempts to prevent that exposure of details about server-side Java applications to the client.

Note:
For example, if a Java application returns an exception or raw code to a web page, these rules help prevent the display of the errors or raw code.

RESPONSE-50-DATA-LEAKAGES-PHP

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/RESPONSE-50-DATA-LEAKAGES-PHP.conf
```

The rules in this configuration file enable protection against PHP-related data and source code leakage from the server to the client.

Note:
For example, a PHP application could produce an error that reveals internal implementation details about the application. This protection reduces the chance that users will see these details.

RESPONSE-50-DATA-LEAKAGES

The configuration file path:

```
modsec_vendor_configs/OWASP/rules/RESPONSE-50-DATA-LEAKAGES.conf
```

The rules in this configuration file enable protection against certain types of data leakages from the server to the client.

Note:
For example, these rules prevent directory listings.

RESPONSE-51-DATA-LEAKAGES-SQL

The configuration file path:

`modsec_vendor_configs/OWASP/rules/RESPONSE-51-DATA-LEAKAGES-SQL.conf`

The rules in this configuration file enable protection against the leakage of inappropriate types of internal database information from the server to clients.

Note:
For example, if a SQL syntax error occurs, these rules will hide it. This protection reduces the chance that users will see the internal SQL errors of the application.

RESPONSE-59-BLOCKING-EVALUATION

The configuration file path:

`modsec_vendor_configs/OWASP/rules/RESPONSE-59-BLOCKING-EVALUATION.conf`

The rules in this configuration file enable a rule that blocks flagged anomalous traffic. This classification can occur as a result of hits that other configuration files produce.

Warning:
Other rules in the rule set depend on this configuration file to block incoming attacks. If you disable this configuration file, other rules will detect, but not block, incoming attacks.

RESPONSE-80-CORRELATION

The configuration file path:

`modsec_vendor_configs/OWASP/rules/RESPONSE-80-CORRELATION.conf`

The rules in this configuration file facilitate the gathering of data about successful and unsuccessful attacks on the server.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- The ModSecurity Guardian Log
- OWASP ModSecurity CRS
- How to Create a Report Receiver API for the ModSecurity Rule Reports
- How to Create a ModSecurity Vendor

Content by label

There is no content with the specified labels

- The ModSecurity Guardian Log
- OWASP ModSecurity CRS
- How to Create a Report Receiver API for the ModSecurity Rule Reports
- How to Create a ModSecurity Vendor

- WHM API 1 Sections - ModSecurity
- UAPI Modules - ModSecurity
- WHM API 1 Functions - modsec_discard_rule_changes
- WHM API 1 Functions - modsec_discard_all_rule_changes
- WHM API 1 Functions - modsec_disable_vendor_updates