## List of enabled standard WAF rules

OWASP (Ver. 3.2):

General:

Description:

Rules:

RuleId Description

------ -----------

200004 Possible Multipart Unmatched Boundary.

REQUEST-911-METHOD-ENFORCEMENT:

Description:

Rules:

RuleId Description

------ -----------

911100 Method is not allowed by policy

REQUEST-913-SCANNER-DETECTION:

Description:

Rules:

RuleId Description

------ -----------

913100 Found User-Agent associated with security scanner

913101 Found User-Agent associated with scripting/generic HTTP client

913102 Found User-Agent associated with web crawler/bot

913110 Found request header associated with security scanner

913120 Found request filename/argument associated with security scanner

REQUEST-920-PROTOCOL-ENFORCEMENT:

Description:

Rules:

RuleId Description

------ -----------

920100 Invalid HTTP Request Line

920120 Attempted multipart/form-data bypass

920121 Attempted multipart/form-data bypass

920160 Content-Length HTTP header is not numeric.

920170 GET or HEAD Request with Body Content.

920171 GET or HEAD Request with Transfer-Encoding.

920180 POST request missing Content-Length Header.

920190 Range: Invalid Last Byte Value.

920200 Range: Too many fields (6 or more)

920201 Range: Too many fields for pdf request (35 or more)

920202 Range: Too many fields for pdf request (6 or more)

920210 Multiple/Conflicting Connection Header Data Found.

920220 URL Encoding Abuse Attack Attempt

920230 Multiple URL Encoding Detected

920240 URL Encoding Abuse Attack Attempt

920250 UTF8 Encoding Abuse Attack Attempt

920260 Unicode Full/Half Width Abuse Attack Attempt

920270 Invalid character in request (null character)

920271 Invalid character in request (non printable characters)

920272 Invalid character in request (outside of printable chars below ascii 127)

920273 Invalid character in request (outside of very strict set)

920274 Invalid character in request headers (outside of very strict set)

920280 Request Missing a Host Header

920290 Empty Host Header

920300 Request Missing an Accept Header

920310 Request Has an Empty Accept Header

920311 Request Has an Empty Accept Header

920320 Missing User Agent Header

920330 Empty User Agent Header

920340 Request Containing Content, but Missing Content-Type header

920341 Request containing content requires Content-Type header

920350 Host header is a numeric IP address

920420 Request content type is not allowed by policy

920430 HTTP protocol version is not allowed by policy

920440 URL file extension is restricted by policy

920450 HTTP header is restricted by policy (%{MATCHED\_VAR})

920460 Abnormal Escape Characters

920470 Illegal Content-Type header

920480 Restrict charset parameter within the content-type header

REQUEST-921-PROTOCOL-ATTACK:

Description:

Rules:

RuleId Description

------ -----------

921110 HTTP Request Smuggling Attack

921120 HTTP Response Splitting Attack

921130 HTTP Response Splitting Attack

921140 HTTP Header Injection Attack via headers

921150 HTTP Header Injection Attack via payload (CR/LF detected)

921151 HTTP Header Injection Attack via payload (CR/LF detected)

921160 HTTP Header Injection Attack via payload (CR/LF and header-name detected)

921170 HTTP Parameter Pollution

921180 HTTP Parameter Pollution (%{TX.1})

REQUEST-930-APPLICATION-ATTACK-LFI:

Description:

Rules:

RuleId Description

------ -----------

930100 Path Traversal Attack (/../)

930110 Path Traversal Attack (/../)

930120 OS File Access Attempt

930130 Restricted File Access Attempt

REQUEST-931-APPLICATION-ATTACK-RFI:

Description:

Rules:

RuleId Description

------ -----------

931100 Possible Remote File Inclusion (RFI) Attack: URL Parameter using IP Address

931110 Possible Remote File Inclusion (RFI) Attack: Common RFI Vulnerable Parameter Name used w/URL

Payload

931120 Possible Remote File Inclusion (RFI) Attack: URL Payload Used w/Trailing Question Mark

Character (?)

931130 Possible Remote File Inclusion (RFI) Attack: Off-Domain Reference/Link

REQUEST-932-APPLICATION-ATTACK-RCE:

Description:

Rules:

RuleId Description

------ -----------

932100 Remote Command Execution: Unix Command Injection

932105 Remote Command Execution: Unix Command Injection

932106 Remote Command Execution: Unix Command Injection

932110 Remote Command Execution: Windows Command Injection

932115 Remote Command Execution: Windows Command Injection

932120 Remote Command Execution: Windows PowerShell Command Found

932130 Remote Command Execution: Unix Shell Expression Found

932140 Remote Command Execution: Windows FOR/IF Command Found

932150 Remote Command Execution: Direct Unix Command Execution

932160 Remote Command Execution: Unix Shell Code Found

932170 Remote Command Execution: Shellshock (CVE-2014-6271)

932171 Remote Command Execution: Shellshock (CVE-2014-6271)

932180 Restricted File Upload Attempt

932190 Remote Command Execution: Wildcard bypass technique attempt

REQUEST-933-APPLICATION-ATTACK-PHP:

Description:

Rules:

RuleId Description

------ -----------

933100 PHP Injection Attack: Opening/Closing Tag Found

933110 PHP Injection Attack: PHP Script File Upload Found

933111 PHP Injection Attack: PHP Script File Upload Found

933120 PHP Injection Attack: Configuration Directive Found

933130 PHP Injection Attack: Variables Found

933131 PHP Injection Attack: Variables Found

933140 PHP Injection Attack: I/O Stream Found

933150 PHP Injection Attack: High-Risk PHP Function Name Found

933151 PHP Injection Attack: Medium-Risk PHP Function Name Found

933160 PHP Injection Attack: High-Risk PHP Function Call Found

933161 PHP Injection Attack: Low-Value PHP Function Call Found

933170 PHP Injection Attack: Serialized Object Injection

933180 PHP Injection Attack: Variable Function Call Found

933190 PHP Injection Attack: PHP Closing Tag Found

933200 PHP Injection Attack: Wrapper scheme detected

933210 PHP Injection Attack: Variable Function Call Found

REQUEST-941-APPLICATION-ATTACK-XSS:

Description:

Rules:

RuleId Description

------ -----------

941100 XSS Attack Detected via libinjection

941101 XSS Attack Detected via libinjection.

941110 XSS Filter - Category 1: Script Tag Vector

941120 XSS Filter - Category 2: Event Handler Vector

941130 XSS Filter - Category 3: Attribute Vector

941140 XSS Filter - Category 4: Javascript URI Vector

941150 XSS Filter - Category 5: Disallowed HTML Attributes

941160 NoScript XSS InjectionChecker: HTML Injection

941170 NoScript XSS InjectionChecker: Attribute Injection

941180 Node-Validator Blacklist Keywords

941190 XSS Using style sheets

941200 XSS using VML frames

941210 XSS using obfuscated JavaScript

941220 XSS using obfuscated VB Script

941230 XSS using 'embed' tag

941240 XSS using 'import' or 'implementation' attribute

941250 IE XSS Filters - Attack Detected.

941260 XSS using 'meta' tag

941270 XSS using 'link' href

941280 XSS using 'base' tag

941290 XSS using 'applet' tag

941300 XSS using 'object' tag

941310 US-ASCII Malformed Encoding XSS Filter - Attack Detected.

941320 Possible XSS Attack Detected - HTML Tag Handler

941330 IE XSS Filters - Attack Detected.

941340 IE XSS Filters - Attack Detected.

941350 UTF-7 Encoding IE XSS - Attack Detected.

941360 JavaScript obfuscation detected.

REQUEST-942-APPLICATION-ATTACK-SQLI:

Description:

Rules:

RuleId Description

------ -----------

942100 SQL Injection Attack Detected via libinjection

942110 SQL Injection Attack: Common Injection Testing Detected

942120 SQL Injection Attack: SQL Operator Detected

942130 SQL Injection Attack: SQL Tautology Detected.

942140 SQL Injection Attack: Common DB Names Detected

942150 SQL Injection Attack

942160 Detects blind sqli tests using sleep() or benchmark().

942170 Detects SQL benchmark and sleep injection attempts including conditional queries

942180 Detects basic SQL authentication bypass attempts 1/3

942190 Detects MSSQL code execution and information gathering attempts

942200 Detects MySQL comment-/space-obfuscated injections and backtick termination

942210 Detects chained SQL injection attempts 1/2

942220 Looking for intiger overflow attacks, these are taken from skipfish, except

3.0.00738585072007e-308 is the \"magic number\" crash

942230 Detects conditional SQL injection attempts

942240 Detects MySQL charset switch and MSSQL DoS attempts

942250 Detects MATCH AGAINST, MERGE and EXECUTE IMMEDIATE injections

942251 Detects HAVING injections

942260 Detects basic SQL authentication bypass attempts 2/3

942270 Looking for basic sql injection. Common attack string for mysql, oracle and others.

942280 Detects Postgres pg\_sleep injection, waitfor delay attacks and database shutdown attempts

942290 Finds basic MongoDB SQL injection attempts

942300 Detects MySQL comments, conditions and ch(a)r injections

942310 Detects chained SQL injection attempts 2/2

942320 Detects MySQL and PostgreSQL stored procedure/function injections

942330 Detects classic SQL injection probings 1/2

942340 Detects basic SQL authentication bypass attempts 3/3

942350 Detects MySQL UDF injection and other data/structure manipulation attempts

942360 Detects concatenated basic SQL injection and SQLLFI attempts

942361 Detects basic SQL injection based on keyword alter or union

942370 Detects classic SQL injection probings 2/2

942380 SQL Injection Attack

942390 SQL Injection Attack

942400 SQL Injection Attack

942410 SQL Injection Attack

942420 Restricted SQL Character Anomaly Detection (cookies): # of special characters exceeded (8)

942421 Restricted SQL Character Anomaly Detection (cookies): # of special characters exceeded (3)

942430 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12)

942431 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (6)

942432 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (2)

942440 SQL Comment Sequence Detected.

942450 SQL Hex Encoding Identified

942460 Meta-Character Anomaly Detection Alert - Repetitive Non-Word Characters

942470 SQL Injection Attack

942480 SQL Injection Attack

942490 Detects classic SQL injection probings 3/3

942500 MySQL in-line comment detected.

REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION:

Description:

Rules:

RuleId Description

------ -----------

943100 Possible Session Fixation Attack: Setting Cookie Values in HTML

943110 Possible Session Fixation Attack: SessionID Parameter Name with Off-Domain Referer

943120 Possible Session Fixation Attack: SessionID Parameter Name with No Referer

REQUEST-944-APPLICATION-ATTACK-JAVA:

Description:

Rules:

RuleId Description

------ -----------

944100 Remote Command Execution: Apache Struts, Oracle WebLogic

944110 Detects potential payload execution

944120 Possible payload execution and remote command execution

944130 Suspicious Java classes

944200 Exploitation of Java deserialization Apache Commons

944210 Possible use of Java serialization

944240 Remote Command Execution: Java serialization

944250 Remote Command Execution: Suspicious Java method detected

OWASP (Ver. 3.1):

General:

Description:

Rules:

RuleId Description

------ -----------

200004 Possible Multipart Unmatched Boundary.

REQUEST-911-METHOD-ENFORCEMENT:

Description:

Rules:

RuleId Description

------ -----------

911100 Method is not allowed by policy

REQUEST-913-SCANNER-DETECTION:

Description:

Rules:

RuleId Description

------ -----------

913100 Found User-Agent associated with security scanner

913101 Found User-Agent associated with scripting/generic HTTP client

913102 Found User-Agent associated with web crawler/bot

913110 Found request header associated with security scanner

913120 Found request filename/argument associated with security scanner

REQUEST-920-PROTOCOL-ENFORCEMENT:

Description:

Rules:

RuleId Description

------ -----------

920100 Invalid HTTP Request Line

920120 Attempted multipart/form-data bypass

920121 Attempted multipart/form-data bypass

920130 Failed to parse request body.

920140 Multipart request body failed strict validation: PE %{REQBODY\_PROCESSOR\_ERROR}, BQ

%{MULTIPART\_BOUNDARY\_QUOTED}, BW %{MULTIPART\_BOUNDARY\_WHITESPACE}, DB %{MULTIPART\_DATA\_BEFORE}, DA

%{MULTIPART\_DATA\_AFTER}, HF %{MULTIPART\_HEADER\_FOLDING}, LF %{MULTIPART\_LF\_LINE}, SM

%{MULTIPART\_SEMICOLON\_MISSING}, IQ %{MULTIPART\_INVALID\_QUOTING}, IH %{MULTIPART\_INVALID\_HEADER\_FOLDING},

FLE %{MULTIPART\_FILE\_LIMIT\_EXCEEDED}

920160 Content-Length HTTP header is not numeric.

920170 GET or HEAD Request with Body Content.

920171 GET or HEAD Request with Transfer-Encoding.

920180 POST request missing Content-Length Header.

920190 Range: Invalid Last Byte Value.

920200 Range: Too many fields (6 or more)

920201 Range: Too many fields for pdf request (35 or more)

920202 Range: Too many fields for pdf request (6 or more)

920210 Multiple/Conflicting Connection Header Data Found.

920220 URL Encoding Abuse Attack Attempt

920230 Multiple URL Encoding Detected

920240 URL Encoding Abuse Attack Attempt

920250 UTF8 Encoding Abuse Attack Attempt

920260 Unicode Full/Half Width Abuse Attack Attempt

920270 Invalid character in request (null character)

920271 Invalid character in request (non printable characters)

920272 Invalid character in request (outside of printable chars below ascii 127)

920273 Invalid character in request (outside of very strict set)

920274 Invalid character in request headers (outside of very strict set)

920280 Request Missing a Host Header

920290 Empty Host Header

920300 Request Missing an Accept Header

920310 Request Has an Empty Accept Header

920311 Request Has an Empty Accept Header

920320 Missing User Agent Header

920330 Empty User Agent Header

920340 Request Containing Content, but Missing Content-Type header

920341 Request containing content requires Content-Type header

920350 Host header is a numeric IP address

920420 Request content type is not allowed by policy

920430 HTTP protocol version is not allowed by policy

920440 URL file extension is restricted by policy

920450 HTTP header is restricted by policy (%{MATCHED\_VAR})

920460 Abnormal Escape Characters

920470 Illegal Content-Type header

920480 Restrict charset parameter within the content-type header

REQUEST-921-PROTOCOL-ATTACK:

Description:

Rules:

RuleId Description

------ -----------

921110 HTTP Request Smuggling Attack

921120 HTTP Response Splitting Attack

921130 HTTP Response Splitting Attack

921140 HTTP Header Injection Attack via headers

921150 HTTP Header Injection Attack via payload (CR/LF detected)

921151 HTTP Header Injection Attack via payload (CR/LF detected)

921160 HTTP Header Injection Attack via payload (CR/LF and header-name detected)

921170 HTTP Parameter Pollution

921180 HTTP Parameter Pollution (%{TX.1})

REQUEST-930-APPLICATION-ATTACK-LFI:

Description:

Rules:

RuleId Description

------ -----------

930100 Path Traversal Attack (/../)

930110 Path Traversal Attack (/../)

930120 OS File Access Attempt

930130 Restricted File Access Attempt

REQUEST-931-APPLICATION-ATTACK-RFI:

Description:

Rules:

RuleId Description

------ -----------

931100 Possible Remote File Inclusion (RFI) Attack: URL Parameter using IP Address

931110 Possible Remote File Inclusion (RFI) Attack: Common RFI Vulnerable Parameter Name used w/URL

Payload

931120 Possible Remote File Inclusion (RFI) Attack: URL Payload Used w/Trailing Question Mark

Character (?)

931130 Possible Remote File Inclusion (RFI) Attack: Off-Domain Reference/Link

REQUEST-932-APPLICATION-ATTACK-RCE:

Description:

Rules:

RuleId Description

------ -----------

932100 Remote Command Execution: Unix Command Injection

932105 Remote Command Execution: Unix Command Injection

932106 Remote Command Execution: Unix Command Injection

932110 Remote Command Execution: Windows Command Injection

932115 Remote Command Execution: Windows Command Injection

932120 Remote Command Execution: Windows PowerShell Command Found

932130 Remote Command Execution: Unix Shell Expression Found

932140 Remote Command Execution: Windows FOR/IF Command Found

932150 Remote Command Execution: Direct Unix Command Execution

932160 Remote Command Execution: Unix Shell Code Found

932170 Remote Command Execution: Shellshock (CVE-2014-6271)

932171 Remote Command Execution: Shellshock (CVE-2014-6271)

932180 Restricted File Upload Attempt

932190 Remote Command Execution: Wildcard bypass technique attempt

REQUEST-933-APPLICATION-ATTACK-PHP:

Description:

Rules:

RuleId Description

------ -----------

933100 PHP Injection Attack: Opening/Closing Tag Found

933110 PHP Injection Attack: PHP Script File Upload Found

933111 PHP Injection Attack: PHP Script File Upload Found

933120 PHP Injection Attack: Configuration Directive Found

933130 PHP Injection Attack: Variables Found

933131 PHP Injection Attack: Variables Found

933140 PHP Injection Attack: I/O Stream Found

933150 PHP Injection Attack: High-Risk PHP Function Name Found

933151 PHP Injection Attack: Medium-Risk PHP Function Name Found

933160 PHP Injection Attack: High-Risk PHP Function Call Found

933161 PHP Injection Attack: Low-Value PHP Function Call Found

933170 PHP Injection Attack: Serialized Object Injection

933180 PHP Injection Attack: Variable Function Call Found

933190 PHP Injection Attack: PHP Closing Tag Found

REQUEST-941-APPLICATION-ATTACK-XSS:

Description:

Rules:

RuleId Description

------ -----------

941100 XSS Attack Detected via libinjection

941101 XSS Attack Detected via libinjection.

941110 XSS Filter - Category 1: Script Tag Vector

941120 XSS Filter - Category 2: Event Handler Vector

941130 XSS Filter - Category 3: Attribute Vector

941140 XSS Filter - Category 4: Javascript URI Vector

941150 XSS Filter - Category 5: Disallowed HTML Attributes

941160 NoScript XSS InjectionChecker: HTML Injection

941170 NoScript XSS InjectionChecker: Attribute Injection

941180 Node-Validator Blacklist Keywords

941190 XSS Using style sheets

941200 XSS using VML frames

941210 XSS using obfuscated JavaScript

941220 XSS using obfuscated VB Script

941230 XSS using 'embed' tag

941240 XSS using 'import' or 'implementation' attribute

941250 IE XSS Filters - Attack Detected.

941260 XSS using 'meta' tag

941270 XSS using 'link' href

941280 XSS using 'base' tag

941290 XSS using 'applet' tag

941300 XSS using 'object' tag

941310 US-ASCII Malformed Encoding XSS Filter - Attack Detected.

941320 Possible XSS Attack Detected - HTML Tag Handler

941330 IE XSS Filters - Attack Detected.

941340 IE XSS Filters - Attack Detected.

941350 UTF-7 Encoding IE XSS - Attack Detected.

REQUEST-942-APPLICATION-ATTACK-SQLI:

Description:

Rules:

RuleId Description

------ -----------

942100 SQL Injection Attack Detected via libinjection

942110 SQL Injection Attack: Common Injection Testing Detected

942120 SQL Injection Attack: SQL Operator Detected

942130 SQL Injection Attack: SQL Tautology Detected.

942140 SQL Injection Attack: Common DB Names Detected

942150 SQL Injection Attack

942160 Detects blind sqli tests using sleep() or benchmark().

942170 Detects SQL benchmark and sleep injection attempts including conditional queries

942180 Detects basic SQL authentication bypass attempts 1/3

942190 Detects MSSQL code execution and information gathering attempts

942200 Detects MySQL comment-/space-obfuscated injections and backtick termination

942210 Detects chained SQL injection attempts 1/2

942220 Looking for intiger overflow attacks, these are taken from skipfish, except

3.0.00738585072007e-308 is the \"magic number\" crash

942230 Detects conditional SQL injection attempts

942240 Detects MySQL charset switch and MSSQL DoS attempts

942250 Detects MATCH AGAINST, MERGE and EXECUTE IMMEDIATE injections

942251 Detects HAVING injections

942260 Detects basic SQL authentication bypass attempts 2/3

942270 Looking for basic sql injection. Common attack string for mysql, oracle and others.

942280 Detects Postgres pg\_sleep injection, waitfor delay attacks and database shutdown attempts

942290 Finds basic MongoDB SQL injection attempts

942300 Detects MySQL comments, conditions and ch(a)r injections

942310 Detects chained SQL injection attempts 2/2

942320 Detects MySQL and PostgreSQL stored procedure/function injections

942330 Detects classic SQL injection probings 1/2

942340 Detects basic SQL authentication bypass attempts 3/3

942350 Detects MySQL UDF injection and other data/structure manipulation attempts

942360 Detects concatenated basic SQL injection and SQLLFI attempts

942361 Detects basic SQL injection based on keyword alter or union

942370 Detects classic SQL injection probings 2/2

942380 SQL Injection Attack

942390 SQL Injection Attack

942400 SQL Injection Attack

942410 SQL Injection Attack

942420 Restricted SQL Character Anomaly Detection (cookies): # of special characters exceeded (8)

942421 Restricted SQL Character Anomaly Detection (cookies): # of special characters exceeded (3)

942430 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12)

942431 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (6)

942432 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (2)

942440 SQL Comment Sequence Detected.

942450 SQL Hex Encoding Identified

942460 Meta-Character Anomaly Detection Alert - Repetitive Non-Word Characters

942470 SQL Injection Attack

942480 SQL Injection Attack

942490 Detects classic SQL injection probings 3/3

REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION:

Description:

Rules:

RuleId Description

------ -----------

943100 Possible Session Fixation Attack: Setting Cookie Values in HTML

943110 Possible Session Fixation Attack: SessionID Parameter Name with Off-Domain Referer

943120 Possible Session Fixation Attack: SessionID Parameter Name with No Referer

REQUEST-944-APPLICATION-ATTACK-JAVA:

Description:

Rules:

RuleId Description

------ -----------

944100 Remote Command Execution: Apache Struts, Oracle WebLogic

944110 Detects potential payload execution

944120 Possible payload execution and remote command execution

944130 Suspicious Java classes

944200 Exploitation of Java deserialization Apache Commons

944210 Possible use of Java serialization

944240 Remote Command Execution: Java serialization

944250 Remote Command Execution: Suspicious Java method detected

OWASP (Ver. 3.0):

General:

Description:

Rules:

RuleId Description

------ -----------

200004 Possible Multipart Unmatched Boundary.

REQUEST-911-METHOD-ENFORCEMENT:

Description:

Rules:

RuleId Description

------ -----------

911100 Method is not allowed by policy

REQUEST-913-SCANNER-DETECTION:

Description:

Rules:

RuleId Description

------ -----------

913100 Found User-Agent associated with security scanner

913101 Found User-Agent associated with scripting/generic HTTP client

913102 Found User-Agent associated with web crawler/bot

913110 Found request header associated with security scanner

913120 Found request filename/argument associated with security scanner

REQUEST-920-PROTOCOL-ENFORCEMENT:

Description:

Rules:

RuleId Description

------ -----------

920100 Invalid HTTP Request Line

920120 Attempted multipart/form-data bypass

920130 Failed to parse request body.

920140 Multipart request body failed strict validation: PE %{REQBODY\_PROCESSOR\_ERROR}, BQ

%{MULTIPART\_BOUNDARY\_QUOTED}, BW %{MULTIPART\_BOUNDARY\_WHITESPACE}, DB %{MULTIPART\_DATA\_BEFORE}, DA

%{MULTIPART\_DATA\_AFTER}, HF %{MULTIPART\_HEADER\_FOLDING}, LF %{MULTIPART\_LF\_LINE}, SM

%{MULTIPART\_SEMICOLON\_MISSING}, IQ %{MULTIPART\_INVALID\_QUOTING}, IH %{MULTIPART\_INVALID\_HEADER\_FOLDING},

FLE %{MULTIPART\_FILE\_LIMIT\_EXCEEDED}

920160 Content-Length HTTP header is not numeric.

920170 GET or HEAD Request with Body Content.

920180 POST request missing Content-Length Header.

920190 Range: Invalid Last Byte Value.

920200 Range: Too many fields (6 or more)

920201 Range: Too many fields for pdf request (35 or more)

920202 Range: Too many fields for pdf request (6 or more)

920210 Multiple/Conflicting Connection Header Data Found.

920220 URL Encoding Abuse Attack Attempt

920230 Multiple URL Encoding Detected

920240 URL Encoding Abuse Attack Attempt

920250 UTF8 Encoding Abuse Attack Attempt

920260 Unicode Full/Half Width Abuse Attack Attempt

920270 Invalid character in request (null character)

920271 Invalid character in request (non printable characters)

920272 Invalid character in request (outside of printable chars below ascii 127)

920273 Invalid character in request (outside of very strict set)

920274 Invalid character in request headers (outside of very strict set)

920280 Request Missing a Host Header

920290 Empty Host Header

920300 Request Missing an Accept Header

920310 Request Has an Empty Accept Header

920311 Request Has an Empty Accept Header

920320 Missing User Agent Header

920330 Empty User Agent Header

920340 Request Containing Content, but Missing Content-Type header

920350 Host header is a numeric IP address

920420 Request content type is not allowed by policy

920430 HTTP protocol version is not allowed by policy

920440 URL file extension is restricted by policy

920450 HTTP header is restricted by policy (%{MATCHED\_VAR})

920460 Abnormal Escape Characters

REQUEST-921-PROTOCOL-ATTACK:

Description:

Rules:

RuleId Description

------ -----------

921100 HTTP Request Smuggling Attack.

921110 HTTP Request Smuggling Attack

921120 HTTP Response Splitting Attack

921130 HTTP Response Splitting Attack

921140 HTTP Header Injection Attack via headers

921150 HTTP Header Injection Attack via payload (CR/LF detected)

921151 HTTP Header Injection Attack via payload (CR/LF detected)

921160 HTTP Header Injection Attack via payload (CR/LF and header-name detected)

921170 HTTP Parameter Pollution

921180 HTTP Parameter Pollution (%{TX.1})

REQUEST-930-APPLICATION-ATTACK-LFI:

Description:

Rules:

RuleId Description

------ -----------

930100 Path Traversal Attack (/../)

930110 Path Traversal Attack (/../)

930120 OS File Access Attempt

930130 Restricted File Access Attempt

REQUEST-931-APPLICATION-ATTACK-RFI:

Description:

Rules:

RuleId Description

------ -----------

931100 Possible Remote File Inclusion (RFI) Attack: URL Parameter using IP Address

931110 Possible Remote File Inclusion (RFI) Attack: Common RFI Vulnerable Parameter Name used w/URL

Payload

931120 Possible Remote File Inclusion (RFI) Attack: URL Payload Used w/Trailing Question Mark

Character (?)

931130 Possible Remote File Inclusion (RFI) Attack: Off-Domain Reference/Link

REQUEST-932-APPLICATION-ATTACK-RCE:

Description:

Rules:

RuleId Description

------ -----------

932100 Remote Command Execution: Unix Command Injection

932105 Remote Command Execution: Unix Command Injection

932110 Remote Command Execution: Windows Command Injection

932115 Remote Command Execution: Windows Command Injection

932120 Remote Command Execution: Windows PowerShell Command Found

932130 Remote Command Execution: Unix Shell Expression Found

932140 Remote Command Execution: Windows FOR/IF Command Found

932150 Remote Command Execution: Direct Unix Command Execution

932160 Remote Command Execution: Unix Shell Code Found

932170 Remote Command Execution: Shellshock (CVE-2014-6271)

932171 Remote Command Execution: Shellshock (CVE-2014-6271)

REQUEST-933-APPLICATION-ATTACK-PHP:

Description:

Rules:

RuleId Description

------ -----------

933100 PHP Injection Attack: Opening/Closing Tag Found

933110 PHP Injection Attack: PHP Script File Upload Found

933111 PHP Injection Attack: PHP Script File Upload Found

933120 PHP Injection Attack: Configuration Directive Found

933130 PHP Injection Attack: Variables Found

933131 PHP Injection Attack: Variables Found

933140 PHP Injection Attack: I/O Stream Found

933150 PHP Injection Attack: High-Risk PHP Function Name Found

933151 PHP Injection Attack: Medium-Risk PHP Function Name Found

933160 PHP Injection Attack: High-Risk PHP Function Call Found

933161 PHP Injection Attack: Low-Value PHP Function Call Found

933170 PHP Injection Attack: Serialized Object Injection

933180 PHP Injection Attack: Variable Function Call Found

REQUEST-941-APPLICATION-ATTACK-XSS:

Description:

Rules:

RuleId Description

------ -----------

941100 XSS Attack Detected via libinjection

941110 XSS Filter - Category 1: Script Tag Vector

941120 XSS Filter - Category 2: Event Handler Vector

941130 XSS Filter - Category 3: Attribute Vector

941140 XSS Filter - Category 4: Javascript URI Vector

941150 XSS Filter - Category 5: Disallowed HTML Attributes

941160 NoScript XSS InjectionChecker: HTML Injection

941170 NoScript XSS InjectionChecker: Attribute Injection

941180 Node-Validator Blacklist Keywords

941190 XSS Using style sheets

941200 XSS using VML frames

941210 XSS using obfuscated JavaScript

941220 XSS using obfuscated VB Script

941230 XSS using 'embed' tag

941240 XSS using 'import' or 'implementation' attribute

941250 IE XSS Filters - Attack Detected.

941260 XSS using 'meta' tag

941270 XSS using 'link' href

941280 XSS using 'base' tag

941290 XSS using 'applet' tag

941300 XSS using 'object' tag

941310 US-ASCII Malformed Encoding XSS Filter - Attack Detected.

941320 Possible XSS Attack Detected - HTML Tag Handler

941330 IE XSS Filters - Attack Detected.

941340 IE XSS Filters - Attack Detected.

941350 UTF-7 Encoding IE XSS - Attack Detected.

REQUEST-942-APPLICATION-ATTACK-SQLI:

Description:

Rules:

RuleId Description

------ -----------

942100 SQL Injection Attack Detected via libinjection

942110 SQL Injection Attack: Common Injection Testing Detected

942120 SQL Injection Attack: SQL Operator Detected

942130 SQL Injection Attack: SQL Tautology Detected.

942140 SQL Injection Attack: Common DB Names Detected

942150 SQL Injection Attack

942160 Detects blind sqli tests using sleep() or benchmark().

942170 Detects SQL benchmark and sleep injection attempts including conditional queries

942180 Detects basic SQL authentication bypass attempts 1/3

942190 Detects MSSQL code execution and information gathering attempts

942200 Detects MySQL comment-/space-obfuscated injections and backtick termination

942210 Detects chained SQL injection attempts 1/2

942220 Looking for intiger overflow attacks, these are taken from skipfish, except

3.0.00738585072007e-308 is the \"magic number\" crash

942230 Detects conditional SQL injection attempts

942240 Detects MySQL charset switch and MSSQL DoS attempts

942250 Detects MATCH AGAINST, MERGE and EXECUTE IMMEDIATE injections

942251 Detects HAVING injections

942260 Detects basic SQL authentication bypass attempts 2/3

942270 Looking for basic sql injection. Common attack string for mysql, oracle and others.

942280 Detects Postgres pg\_sleep injection, waitfor delay attacks and database shutdown attempts

942290 Finds basic MongoDB SQL injection attempts

942300 Detects MySQL comments, conditions and ch(a)r injections

942310 Detects chained SQL injection attempts 2/2

942320 Detects MySQL and PostgreSQL stored procedure/function injections

942330 Detects classic SQL injection probings 1/2

942340 Detects basic SQL authentication bypass attempts 3/3

942350 Detects MySQL UDF injection and other data/structure manipulation attempts

942360 Detects concatenated basic SQL injection and SQLLFI attempts

942370 Detects classic SQL injection probings 2/2

942380 SQL Injection Attack

942390 SQL Injection Attack

942400 SQL Injection Attack

942410 SQL Injection Attack

942420 Restricted SQL Character Anomaly Detection (cookies): # of special characters exceeded (8)

942421 Restricted SQL Character Anomaly Detection (cookies): # of special characters exceeded (3)

942430 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12)

942431 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (6)

942432 Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (2)

942440 SQL Comment Sequence Detected.

942450 SQL Hex Encoding Identified

942460 Meta-Character Anomaly Detection Alert - Repetitive Non-Word Characters

REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION:

Description:

Rules:

RuleId Description

------ -----------

943100 Possible Session Fixation Attack: Setting Cookie Values in HTML

943110 Possible Session Fixation Attack: SessionID Parameter Name with Off-Domain Referer

943120 Possible Session Fixation Attack: SessionID Parameter Name with No Referer

OWASP (Ver. 2.2.9):

General:

Description:

Rules:

RuleId Description

------ -----------

200004 Possible Multipart Unmatched Boundary.

crs\_20\_protocol\_violations:

Description:

Rules:

RuleId Description

------ -----------

950107 URL Encoding Abuse Attack Attempt

950108 URL Encoding Abuse Attack Attempt

950109 Multiple URL Encoding Detected

950116 Unicode Full/Half Width Abuse Attack Attempt

950801 UTF8 Encoding Abuse Attack Attempt

958230 Range: Invalid Last Byte Value.

958231 Range: Too many fields

958291 Range: field exists and begins with 0.

958295 Multiple/Conflicting Connection Header Data Found.

960000 Attempted multipart/form-data bypass

960011 GET or HEAD Request with Body Content.

960012 POST request missing Content-Length Header.

960016 Content-Length HTTP header is not numeric.

960018 Invalid character in request

960020 Pragma Header requires Cache-Control Header for HTTP/1.1 requests.

960022 Expect Header Not Allowed for HTTP 1.0.

960901 Invalid character in request

960902 Invalid Use of Identity Encoding.

960911 Invalid HTTP Request Line

960912 Failed to parse request body.

960914 Multipart request body failed strict validation: PE %{REQBODY\_PROCESSOR\_ERROR}, BQ

%{MULTIPART\_BOUNDARY\_QUOTED}, BW %{MULTIPART\_BOUNDARY\_WHITESPACE}, DB %{MULTIPART\_DATA\_BEFORE}, DA

%{MULTIPART\_DATA\_AFTER}, HF %{MULTIPART\_HEADER\_FOLDING}, LF %{MULTIPART\_LF\_LINE}, SM

%{MULTIPART\_SEMICOLON\_MISSING}, IQ %{MULTIPART\_INVALID\_QUOTING}, IH %{MULTIPART\_INVALID\_HEADER\_FOLDING},

FLE %{MULTIPART\_FILE\_LIMIT\_EXCEEDED}

960915 Multipart parser detected a possible unmatched boundary.

981227 Apache Error: Invalid URI in Request.

crs\_21\_protocol\_anomalies:

Description:

Rules:

RuleId Description

------ -----------

960006 Empty User Agent Header

960007 Empty Host Header

960008 Request Missing a Host Header

960009 Request Missing a User Agent Header

960015 Request Missing an Accept Header

960017 Host header is a numeric IP address

960021 Request Has an Empty Accept Header

960904 Request Containing Content, but Missing Content-Type header

crs\_23\_request\_limits:

Description:

Rules:

RuleId Description

------ -----------

960208 Argument value too long

960209 Argument name too long

960335 Too many arguments in request

960341 Total arguments size exceeded

960342 Uploaded file size too large

960343 Total uploaded files size too large

crs\_30\_http\_policy:

Description:

Rules:

RuleId Description

------ -----------

960010 Request content type is not allowed by policy

960032 Method is not allowed by policy

960034 HTTP protocol version is not allowed by policy

960035 URL file extension is restricted by policy

960038 HTTP header is restricted by policy

crs\_35\_bad\_robots:

Description:

Rules:

RuleId Description

------ -----------

990002 Request Indicates a Security Scanner Scanned the Site

990012 Rogue web site crawler

990901 Request Indicates a Security Scanner Scanned the Site

990902 Request Indicates a Security Scanner Scanned the Site

crs\_40\_generic\_attacks:

Description:

Rules:

RuleId Description

------ -----------

950000 Session Fixation

950002 System Command Access

950003 Session Fixation

950005 Remote File Access Attempt

950006 System Command Injection

950008 Injection of Undocumented ColdFusion Tags

950009 Session Fixation Attack

950010 LDAP Injection Attack

950011 SSI injection Attack

950012 HTTP Request Smuggling Attack.

950018 Universal PDF XSS URL Detected.

950019 Email Injection Attack

950117 Remote File Inclusion Attack

950118 Remote File Inclusion Attack

950119 Remote File Inclusion Attack

950120 Possible Remote File Inclusion (RFI) Attack: Off-Domain Reference/Link

950907 System Command Injection

950910 HTTP Response Splitting Attack

950911 HTTP Response Splitting Attack

958976 PHP Injection Attack

958977 PHP Injection Attack

959151 PHP Injection Attack

960024 Meta-Character Anomaly Detection Alert - Repetative Non-Word Characters

981133 Rule 981133

981134 Rule 981134

crs\_41\_sql\_injection\_attacks:

Description:

Rules:

RuleId Description

------ -----------

950001 SQL Injection Attack

950007 Blind SQL Injection Attack

950901 SQL Injection Attack: SQL Tautology Detected.

950908 SQL Injection Attack.

959070 SQL Injection Attack

959071 SQL Injection Attack

959072 SQL Injection Attack

959073 SQL Injection Attack

981172 Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded

981173 Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded

981231 SQL Comment Sequence Detected.

981240 Detects MySQL comments, conditions and ch(a)r injections

981241 Detects conditional SQL injection attempts

981242 Detects classic SQL injection probings 1/2

981243 Detects classic SQL injection probings 2/2

981244 Detects basic SQL authentication bypass attempts 1/3

981245 Detects basic SQL authentication bypass attempts 2/3

981246 Detects basic SQL authentication bypass attempts 3/3

981247 Detects concatenated basic SQL injection and SQLLFI attempts

981248 Detects chained SQL injection attempts 1/2

981249 Detects chained SQL injection attempts 2/2

981250 Detects SQL benchmark and sleep injection attempts including conditional queries

981251 Detects MySQL UDF injection and other data/structure manipulation attempts

981252 Detects MySQL charset switch and MSSQL DoS attempts

981253 Detects MySQL and PostgreSQL stored procedure/function injections

981254 Detects Postgres pg\_sleep injection, waitfor delay attacks and database shutdown attempts

981255 Detects MSSQL code execution and information gathering attempts

981256 Detects MATCH AGAINST, MERGE, EXECUTE IMMEDIATE and HAVING injections

981257 Detects MySQL comment-/space-obfuscated injections and backtick termination

981260 SQL Hex Encoding Identified

981270 Finds basic MongoDB SQL injection attempts

981272 Detects blind sqli tests using sleep() or benchmark().

981276 Looking for basic sql injection. Common attack string for mysql, oracle and others.

981277 Looking for integer overflow attacks, these are taken from skipfish, except

2.2.90738585072007e-308 is the \"magic number\" crash

981300 Rule 981300

981301 Rule 981301

981302 Rule 981302

981303 Rule 981303

981304 Rule 981304

981305 Rule 981305

981306 Rule 981306

981307 Rule 981307

981308 Rule 981308

981309 Rule 981309

981310 Rule 981310

981311 Rule 981311

981312 Rule 981312

981313 Rule 981313

981314 Rule 981314

981315 Rule 981315

981316 Rule 981316

981317 SQL SELECT Statement Anomaly Detection Alert

981318 SQL Injection Attack: Common Injection Testing Detected

981319 SQL Injection Attack: SQL Operator Detected

981320 SQL Injection Attack: Common DB Names Detected

crs\_41\_xss\_attacks:

Description:

Rules:

RuleId Description

------ -----------

958000 Cross-site Scripting (XSS) Attack

958001 Cross-site Scripting (XSS) Attack

958002 Cross-site Scripting (XSS) Attack

958003 Cross-site Scripting (XSS) Attack

958004 Cross-site Scripting (XSS) Attack

958005 Cross-site Scripting (XSS) Attack

958006 Cross-site Scripting (XSS) Attack

958007 Cross-site Scripting (XSS) Attack

958008 Cross-site Scripting (XSS) Attack

958009 Cross-site Scripting (XSS) Attack

958010 Cross-site Scripting (XSS) Attack

958011 Cross-site Scripting (XSS) Attack

958012 Cross-site Scripting (XSS) Attack

958013 Cross-site Scripting (XSS) Attack

958016 Cross-site Scripting (XSS) Attack

958017 Cross-site Scripting (XSS) Attack

958018 Cross-site Scripting (XSS) Attack

958019 Cross-site Scripting (XSS) Attack

958020 Cross-site Scripting (XSS) Attack

958022 Cross-site Scripting (XSS) Attack

958023 Cross-site Scripting (XSS) Attack

958024 Cross-site Scripting (XSS) Attack

958025 Cross-site Scripting (XSS) Attack

958026 Cross-site Scripting (XSS) Attack

958027 Cross-site Scripting (XSS) Attack

958028 Cross-site Scripting (XSS) Attack

958030 Cross-site Scripting (XSS) Attack

958031 Cross-site Scripting (XSS) Attack

958032 Cross-site Scripting (XSS) Attack

958033 Cross-site Scripting (XSS) Attack

958034 Cross-site Scripting (XSS) Attack

958036 Cross-site Scripting (XSS) Attack

958037 Cross-site Scripting (XSS) Attack

958038 Cross-site Scripting (XSS) Attack

958039 Cross-site Scripting (XSS) Attack

958040 Cross-site Scripting (XSS) Attack

958041 Cross-site Scripting (XSS) Attack

958045 Cross-site Scripting (XSS) Attack

958046 Cross-site Scripting (XSS) Attack

958047 Cross-site Scripting (XSS) Attack

958049 Cross-site Scripting (XSS) Attack

958051 Cross-site Scripting (XSS) Attack

958052 Cross-site Scripting (XSS) Attack

958054 Cross-site Scripting (XSS) Attack

958056 Cross-site Scripting (XSS) Attack

958057 Cross-site Scripting (XSS) Attack

958059 Cross-site Scripting (XSS) Attack

958404 Cross-site Scripting (XSS) Attack

958405 Cross-site Scripting (XSS) Attack

958406 Cross-site Scripting (XSS) Attack

958407 Cross-site Scripting (XSS) Attack

958408 Cross-site Scripting (XSS) Attack

958409 Cross-site Scripting (XSS) Attack

958410 Cross-site Scripting (XSS) Attack

958411 Cross-site Scripting (XSS) Attack

958412 Cross-site Scripting (XSS) Attack

958413 Cross-site Scripting (XSS) Attack

958414 Cross-site Scripting (XSS) Attack

958415 Cross-site Scripting (XSS) Attack

958416 Cross-site Scripting (XSS) Attack

958417 Cross-site Scripting (XSS) Attack

958418 Cross-site Scripting (XSS) Attack

958419 Cross-site Scripting (XSS) Attack

958420 Cross-site Scripting (XSS) Attack

958421 Cross-site Scripting (XSS) Attack

958422 Cross-site Scripting (XSS) Attack

958423 Cross-site Scripting (XSS) Attack

973300 Possible XSS Attack Detected - HTML Tag Handler

973301 XSS Attack Detected

973302 XSS Attack Detected

973303 XSS Attack Detected

973304 XSS Attack Detected

973305 XSS Attack Detected

973306 XSS Attack Detected

973307 XSS Attack Detected

973308 XSS Attack Detected

973309 XSS Attack Detected

973310 XSS Attack Detected

973311 XSS Attack Detected

973312 XSS Attack Detected

973313 XSS Attack Detected

973314 XSS Attack Detected

973315 IE XSS Filters - Attack Detected.

973316 IE XSS Filters - Attack Detected.

973317 IE XSS Filters - Attack Detected.

973318 IE XSS Filters - Attack Detected.

973319 IE XSS Filters - Attack Detected.

973320 IE XSS Filters - Attack Detected.

973321 IE XSS Filters - Attack Detected.

973322 IE XSS Filters - Attack Detected.

973323 IE XSS Filters - Attack Detected.

973324 IE XSS Filters - Attack Detected.

973325 IE XSS Filters - Attack Detected.

973326 IE XSS Filters - Attack Detected.

973327 IE XSS Filters - Attack Detected.

973328 IE XSS Filters - Attack Detected.

973329 IE XSS Filters - Attack Detected.

973330 IE XSS Filters - Attack Detected.

973331 IE XSS Filters - Attack Detected.

973332 IE XSS Filters - Attack Detected.

973333 IE XSS Filters - Attack Detected.

973334 IE XSS Filters - Attack Detected.

973335 IE XSS Filters - Attack Detected.

973336 XSS Filter - Category 1: Script Tag Vector

973337 XSS Filter - Category 2: Event Handler Vector

973338 XSS Filter - Category 3: Javascript URI Vector

973344 IE XSS Filters - Attack Detected.

973345 IE XSS Filters - Attack Detected.

973346 IE XSS Filters - Attack Detected.

973347 IE XSS Filters - Attack Detected.

973348 IE XSS Filters - Attack Detected.

981018 Rule 981018

981136 Rule 981136

crs\_42\_tight\_security:

Description:

Rules:

RuleId Description

------ -----------

950103 Path Traversal Attack

crs\_45\_trojans:

Description:

Rules:

RuleId Description

------ -----------

950110 Backdoor access

950921 Backdoor access

crs\_49\_inbound\_blocking:

Description:

Rules:

RuleId Description

------ -----------

981175 Inbound Attack Targeting OSVDB Flagged Resource.

981176 Inbound Anomaly Score Exceeded (Total Score: %{TX.ANOMALY\_SCORE},

SQLi=%{TX.SQL\_INJECTION\_SCORE}, XSS=%{TX.XSS\_SCORE}): Last Matched Message: %{tx.msg}

Microsoft\_BotManagerRuleSet (Ver. 0.1):

KnownBadBots:

Description:

Rules:

RuleId Description

------ -----------

1 Malicious Bots