Attacks Description - Action Policy

https://campus.barracuda.com/doc/29819001/

The following table describes the attack actions under each attack group:

Protocol Violations

Protocol Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**
16	Directory Traversal Beyond Root	DIRECTORY_TRAVERSAL_BEYOND_ROOT	Attempted access to files and commands beyond the document root directory/CGI root directory.	Alert	Forceful Browsing
125	Get Request with Content Length	GET_REQUEST_WITH_CONTENT_LENGTH	HTTP GET request with Content-Length request header was detected.	Alert	Protocol Violations
126	Missing Host Header	MISSING_HOST_HEADER	An HTTP/ 1.1 version request lacked the mandatory Host request header.	Alert	Protocol Violations
121	Invalid Header	INVALID_HEADER	An invalid HTTP request header name-value pair was detected.	Alert	Protocol Violations
118	Invalid Method	INVALID_METHOD	An invalid HTTP method detected in request.	Alert	Protocol Violations
77	Invalid or Malformed HTTP Request	INVALID_OR_MALFORMED_REQUEST	Normalizing a request URI or header components determined it was invalid or malformed.	Alert	Protocol Violations

129	Parameter Too Large	PARAM_TOO_LARGE	An HTTP POST method request had a URL-encoded parameter value exceeding 1024 KB.	Alert	Limits Violation
123	Malformed Content Length	MALFORMED_CONTENT_LEN	Content-Length request header contained non-numeric characters (e.g., Meta characters or alphabetic characters).	Alert	Protocol Violations
124	Malformed Cookie	MALFORMED_COOKIE	A cookie not conforming to the HTTP cookie specifications was detected.	Alert	Protocol Violations
120	Malformed Request Line	MALFORMED_REQUEST_LINE	An HTTP request end of line lacked the mandatory /r/n characters.	Alert	Protocol Violations
122	Malformed Header	MALFORMED_HEADER_LINE	A header name did not conform to the HTTP protocol specifications.	Alert	Protocol Violations
128	Malformed Parameter	MALFORMED_PARAM	Normalizing and parsing the name or value of a parameter in a query or POST body revealed the request contained a malformed parameter.	Alert	Protocol Violations
119	Malformed Version	MALFORMED_VERSION	An HTTP request sent with a protocol version number other than 0.9, 1.0 or 1.1 was detected.	Alert	Protocol Violations

127	Multiple Content Length	MULTIPLE_CONTENT_LENGTH	An HTTP request contained more than one Content-Length HTTP request header.	Alert	Protocol Violations
25	Post Without Content Length	POST_WITHOUT_CONTENT_LENGTH	A POST request lacked the mandatory Content-Length HTTP request header.	Alert	Protocol Violation
60	Pre-1.0 Request	PRE_1_0_REQUEST	An HTTP request lacked a protocol version number, indicating it was an HTTP/0.9 request.	Alert	Protocol Violations

Request Policy Violations

Request Policy Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**
141	Cookie Count Exceeded	COOKIE_COUNT_EXCEEDED	A request exceeded the maximum number of cookies specified in **Max Number of Cookies** on the **SECURITY POLICIES > Request Limits** page.	Alert	Limits Violation

32	Cookie Expired	COOKIE_EXPIRED	A session cookie **Cookie Max Age** on the **SECURITY POLICIES > Cookie Security** page has been exceeded on the client browser.	Warning	Session Tamper Attacks
41	Cookie Length Exceeded	COOKIE_LENGTH_EXCEEDED	A cookie exceeded the maximum allowable length specified in **Max Cookie Value Length** on the **SECURITY POLICIES > Request Limits** page.	Alert	Limits Violation
142	Cookie Name Length Exceeded	COOKIE_NAME_LENGTH_EXCEEDED	A cookie name length exceeded the maximum allowable length specified in **Max Cookie Name Length** on the **SECURITY POLICIES > Request Limits** page.	Alert	Limits Violation

31	Cookie Tampered	COOKIE_TAMPERED	A request cookie secured with cookie signing or encryption had been tampered. The cookie **Tamper Proof Mode** on the **SECURITY POLICIES > Cookie Security** page was **Encrypted** or **Signed**.	Warning	Session Tamper Attacks
44	Header Count Exceeded	HEADER_COUNT_EXCEEDED	The number of request headers exceeded the maximum allowed, specified in **Max Number of Headers** on the **SECURITY POLICIES > Request Limits** page.	Alert	Limits Violation
143	Header Name Length Exceeded	HEADER_NAME_LENGTH_EXCEEDED	The length of the request header name exceeded the maximum allowed, specified in **Max Header Name Length** on the **SECURITY POLICIES > Request Limits** page.	Alert	Limits Violation

6	Header Value Length Exceeded	HEADER_VALUE_LENGTH_EXCEEDED	The request header value length exceeded the maximum allowed, specified in **Max Header Value Length** on the **SECURITY POLICIES > Request Limits** page.	Alert	Limits Violation
11	Invalid URL Encoding	INVALID_URL_ENCODING	The characters encoded in the URL do not conform to the URL encoding scheme specified in **Default Character Set** on the **SECURITY POLICIES > URL Normalization** page.	Alert	Injection Attacks

116	Mismatched Header Cookie Replay Attack	COOKIE_REPLAY_MISMATCHED_HEADER	The embedded and signed cookie header value sent to the client does not match the incoming value in a subsequent client request. **Cookie Replay Protection Type** is set to "*Custom Headers*" or "*IP and Custom Headers*" on the **SECURITY POLICIES > Cookie Security** page to detect this attack.	Warning	Session Tamper Attacks
117	Mismatched IP Cookie Replay Attack	COOKIE_REPLAY_MISMATCHED_IP	The cookie IP address information does not match the source IP address of the incoming client request. **Cookie Replay Protection Type** is set to "*IP*" or "*IP and Custom Headers*" on the **SECURITY POLICIES > Cookie Security** page to detect this attack.	Warning	Session Tamper Attacks

14	Slash-dot in URL Path	SLASH_DOT_IN_URL	Requested URL contained a slash (/) followed by a dot (.). This is a potential hidden file disclosure attack.	Alert	Forceful Browsing
15	Tilde in URL Path	TILDE_IN_URL	Requested URL contained a tilde (~). This is a potential hidden file disclosure attack.	Alert	Forceful Browsing
144	Too Many Sessions for IP	TOO_MANY_SESSIONS_FOR_IP	Client attempted to exceed **New Session Count** maximum set under **Session Tracking** on the **WEBSITES > Advanced Security** page.	Alert	DDOS Attacks
0	Request Length Exceeded	REQUEST_LENGTH_EXCEEDED	The request exceeded the total maximum allowable length (including the Request Line, and all HTTP request headers such as User Agent, Cookies, Referer, etc.) specified in **Max Request Length** on the **SECURITY POLICIES > Request Limits** page.	Alert	Limits Violation

140	Total Request Line Length Exceeded	REQUEST_LINE_LENGTH_EXCEEDED	The request line exceeded the maximum allowable length specified in **Max Request Line Length** on the **SECURITY POLICIES > Request Limits** page.	Alert	Limits Violation
30	Unrecognized Cookie	UNRECOGNIZED_COOKIE	The incoming request cookie was unrecognized. **Allow Unrecognized Cookies** is set to **Never** or **Custom** on the **SECURITY POLICIES > Cookie Security** page. Unrecognized cookies are cookies not encrypted by the Barracuda Web Application Firewall.	Warning	Session Tamper Attacks
42	URL Length Exceeded	URL_LENGTH_EXCEEDED	The URL in the request exceeded the maximum allowable URL length specified in **Max URL Length** on the **SECURITY POLICIES > Request Limits** page.	Alert	Limits Violation

43	Query Length Exceeded	QUERY_LENGTH_EXCEEDED	The length of the query string portion of the URL exceeded the maximum allowable length specified in **Max Query Length** on the **SECURITY POLICIES > Request Limits** page.	Alert	Limits Violation

Response Violations

Response Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**
300	CAPTCHA Validation Required	DDOS_CAPTCHA_SEND_CAPTCHA	The **Response Page** from the **SECURITY POLICIES > Action Policy** page was sent to the client because the back-end server was not reached.	Information	Outbound Attacks
62	Custom Error Response Page	CUSTOM_ERR_RESPONSE_PAGE	The custom error **Response Page** from the **SECURITY POLICIES > Action Policy** page was sent to the client because the back-end server was not reached.	Alert	Other Attacks

17	Error Response Suppressed	ERROR_RESPONSE_SUPPRESSED	The response from the back-end server contained a 4xx or 5xx response code and was blocked. The **Suppress Return Code** is set to **Yes** on the **SECURITY POLICIES > Cloaking** page.	Notice	Outbound Attacks
63	Identity Theft Pattern Matched	IDENTITY_THEFT_PATTERN_MATCHED	The response body (contents) from the back-end server matched an identity theft pattern on the **ADVANCED > Libraries** page.	Error	Outbound Attacks
61	Response Header Suppressed	RESPONSE_HEADER_SUPPRESSED	Response header suppressed as it matched **Headers to Filter** on the **SECURITY POLICIES > Cloaking** page.	Information	Outbound Attacks

Header Violations

Header Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**

331	Apache Struts Attack in Header	APACHE_STRUTS_ATTACKS_MEDIUM_IN_HEADER	Header value matched an Apache Struts attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks
37	Cross-Site Scripting in Header	CROSS_SITE_SCRIPTING_IN_HEADER	Header value matched a Cross-Site Scripting pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	XSS Injections
35	Custom Attack Pattern in Header	CUSTOM_ATTACK_PATTERN_IN_HEADER	Header value matched a custom attack pattern defined under **Attack Types** on the **ADVANCED > Libraries** page.	Alert	Other Attacks
39	Directory Traversal in Header	DIRECTORY_TRAVERSAL_IN_HEADER	Header value matched a Directory Traversal pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks
330	HTTP Specific Attack in Header	HTTP_SPECIFIC_ATTACKS_MEDIUM_IN_HEADER	Header value matched an HTTP specific attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns page.**	Alert	Injection Attacks

328	LDAP Injection in Header	LDAP_INJECTION_MEDIUM_IN_HEADER	Header value matched an LDAP Injection attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks
7	Metacharacter Matched in Header	HEADER_META_VIOLATION	Metacharacter in header matched the Denied Metacharacters defined under **Header: Allow/Deny Rules** on the **WEBSITES > Allow/Deny** page.	Alert	Other Attacks
38	OS Command Injection in Header	OS_CMD_INJECTION_IN_HEADER	Header value matched an OS Command injection pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks
329	Python PHP Attack in Header	PYTHON_PHP_ATTACKS_MEDIUM_IN_HEADER	Header value matched a Python PHP attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks
332	Remote File Inclusion in Header	REMOTE-FILE-INCLUSION-PATTERN-IN-HEADER	The header contained a Remote file inclusion pattern that matched an attack pattern defined under the header ACL.	Alert	Injection Attacks

36	SQL Injection in Header	SQL_INJECTION_IN_HEADER	Header value matched an SQL injection pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	SQL Attacks

Application Profile Violations

Application Profile Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**
130	No Domain Match in Profile	NO_DOMAIN_MATCH_IN_PROFILE	The domain attribute of session cookie does not match the attribute specified on the **WEBSITES > Website Profiles** page. This is enforced when **Strict Profile Check** and **URL Profile** is set to **Yes**.	Alert	Forceful Browsing
131	No URL Profile Match	NO_URL_PROFILE_MATCH	The request does not match any of the configured URL Profiles on the **WEBSITES > Website Profiles** page. This is enforced when **Strict Profile Check** and **URL Profile** is set to **Yes**.	Alert	Forceful Browsing

URL Profile Violations

URL Profile Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**

327	Apache Struts Attack in URL	APACHE_STRUTS_ATTACKS_MEDIUM_IN_URL	The value in a URL matched an Apache Struts attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks
40	Content Length Exceeded	CONTENT_LENGTH_EXCEEDED	The request body content exceeded the maximum allowable length defined in the URL Profile for the URL space. Max Content Length specified on: • **SECURITY POLICIES > URL Protection**, OR • **WEBSITES > Website Profiles > URL Profiles** Enforced when **Use Profile** is set to *Yes* and URL Profile created.	Alert	Limits Violation

167	Cross-Site Scripting in URL	CROSS_SITE_SCRIPTING_IN_URL	The value in a URL matched a Cross-Site Scripting pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	XSS Injections
171	Custom Attack Pattern in URL	CUSTOM_ATTACK_PATTERN_IN_URL	The value in a URL matched a custom attack pattern defined under **Attack Types** on the **ADVANCED > Libraries** page.	Alert	Other Attacks
326	HTTP Specific Attack in URL	HTTP_SPECIFIC_ATTACKS_MEDIUM_IN_URL	The value in a URL matched an HTTP specific attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks

324	LDAP Injection in URL	LDAP_INJECTION_MEDIUM_IN_URL	The value in a URL matched an LDAP Injection attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks
5	Method Not Allowed	METHOD_NOT_ALLOWED	The HTTP method in the request is denied as it is not configured in the **Allowed Method** list under **URL Profile** on the **WEBSITES > Website Profiles** page.	Alert	Forceful Browsing
163	No Param Profile Match	NO_PARAM_PROFILE_MATCH	The request failed to match the configured parameter profiles on the **WEBSITES > Website Profiles** page for this URL space.	Alert	Forceful Browsing

168	OS Command Injection in URL	OS_CMD_INJECTION_IN_URL	The URL matched an OS command injection pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks
147	Parameter Name Length Exceeded	PARAM_NAME_LENGTH_EXCEEDED	The length of the parameter in the request exceeds the maximum allowable length defined either on **SECURITY POLICIES > URL Protection** or **WEBSITES > Website Profiles > URL Profiles** (Only when **Use Profile** is set to **Yes** and **URL Profile** created).	Alert	Other Attacks

325	Python PHP Attack in URL	PYTHON_PHP_ATTACKS_MEDIUM_IN_URL	The value in a URL matched a Python PHP attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks
132	Query String not Allowed	QUERY_STR_NOT_ALLOWED	Request blocked because a query string was detected in the URL. Enforced when query strings disallowed on **WEBSITES > Website Profile > URL Profiles**.	Alert	Forceful Browsing
170	Remote File Inclusion in URL	REMOTE_FILE_INCLUSION_IN_URL	The URL matched a Remote File Inclusion pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	Injection Attacks

161	Session not Found	SESSION_NOT_FOUND	The Barracuda Web Application Firewall maintains a session for every form and URL fetched by the client when CSRF is enabled. If the request does not have the valid session token embedded in it, the Barracuda Web Application Firewall logs it as session not found.	Alert	Forceful Browsing
166	SQL Injection in URL	SQL_INJECTION_IN_URL	The URL matched an SQL injection pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	SQL Attacks

149	Too Many Parameters	TOO_MANY_PARAMS	The parameters in a GET query string and/or in the request body in a POST request exceeded **MAX Parameters** on the **SECURITY POLICIES > URL Protection** page.	Alert	DDOS Attacks
148	Too Many Uploaded Files	TOO_MANY_UPLOADED_FILES	The request exceeds the maximum number of form parameters that can be of file-upload type. Max Upload Files specified on: • **SECURITY POLICIES > URL Protection** exceeded, OR • **WEBSITES > Website Profiles > URL Profiles** exceeded. This is only when **Use Profile** is set to *Yes* and URL Profile created.	Alert	DDOS Attacks

26	Unknown Content Type	UNKNOWN_CONTENT_TYPE	The content type in the POST body of the URL does not match any **Allowed Content Types** under **URL Profile** on the **WEBSITES > Website Profiles** page.	Alert	Injection Attacks

Parameter Profile Violations

Parameter Profile Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**
323	Apache Struts Attack in Parameter	APACHE_STRUTS_ATTACKS_MEDIUM_IN_PARAM	The parameter matched an Apache Struts attack pattern in the associated **Parameter Class** of the parameter profile on the **WEBSITES > Website Profiles** page, or in the **SECURITY POLICIES > Parameter Protection** page (if no parameter profile).	Alert	Injection Attacks
165	Cross-Site Request Forgery	CROSS_SITE_REQUEST_FORGERY	The state parameter 'ncforminfo' was not found or was found tampered in the form that matched the URL profile.	Alert	Forceful Browsing

158	Cross-Site Scripting in Parameter	CROSS_SITE_SCRIPTING_IN_PARAM	The parameter matched a cross-site scripting attack pattern in the associated **Parameter Class** of the parameter profile on the **WEBSITES > Website Profiles** page, or in the **SECURITY POLICIES > Parameter Protection** page (if no parameter profile).	Alert	XSS Injections
155	Custom Attack Pattern in Parameter	CUSTOM_ATTACK_PATTERN_IN_PARAM	The parameter matched a custom attack pattern in the associated **Parameter Class** of the parameter profile on the **WEBSITES > Website Profiles** page or in the **SECURITY POLICIES > Parameter Protection** page (if no parameter profile).	Alert	Other Attacks
160	Directory Traversal in Parameter	DIRECTORY_TRAVERSAL_IN_PARAM	The parameter matched a directory traversal pattern in the associated **Parameter Class** of the parameter profile on the **WEBSITES > Website Profiles** page or in the **SECURITY POLICIES > Parameter Protection** page (if no parameter profile).	Alert	Injection Attacks

151	File Upload Size Exceeded	FILE_UPLOAD_SIZE_EXCEEDED	The uploaded file in the request exceeds the **Maximum Upload File Size** on the **SECURITY POLICIES > Parameter Protection** page.	Alert	DDOS Attacks
150	Forbidden File Extension	FILE_EXTENSION_NOT_ALLOWED	The extension of the uploaded file does not match any configured extension in **File Upload Extensions** on the: • **SECURITY POLICIES > Parameter Protection** page, or • **WEBSITES > Website Profiles > Parameter Profile** section.	Alert	Injection Attacks
296	Forbidden File Mime Type	FILE_MIME_TYPE_NOT_ALLOWED	The extension of the uploaded file does not match any configured extension in **File Upload Mime Types** on the: • **SECURITY POLICIES > Parameter Protection** page, or • **WEBSITES > Website Profiles > Parameter Profile** section.	Alert	File Attacks

322	HTTP Specific Attack in Parameter	HTTP_SPECIFIC_ATTACKS_MEDIUM_IN_PARAM	The parameter matched an HTTP specific attack pattern in the associated **Parameter Class** of the parameter profile on the **WEBSITES > Website Profiles** page, or on the **SECURITY POLICIES > Parameter Protection** page (if no parameter profile).	Alert	Injection Attacks
320	LDAP Injection in Parameter	LDAP_INJECTION_MEDIUM_IN_PARAM	The parameter matched an LDAP Injection attack pattern in the associated **Parameter Class** of the parameter profile on the **WEBSITES > Website Profiles** page, or on the **SECURITY POLICIES > Parameter Protection** page (if no parameter profile).	Alert	Injection Attacks
138	Mandatory Parameter Missing	MISSING_MANDATORY_PARAM	The URL request lacks a required parameter. The Parameter profile associated with the URL profile has *Required* set to Yes under **Parameter Profiles** on the **WEBSITES > Website Profiles** page.	Alert	Injection Attacks

137	Maximum Instances of Parameter Exceeded	TOO_MANY_PARAM_INSTANCES	The instances of a parameter exceeds **Maximum Instances** on the: • **SECURITY POLICIES > Parameter Protection** page, or • **WEBSITES > Website Profiles > Parameter Profile** section.	Alert	DDOS Attacks
152	Metacharacter in Parameter	METACHARACTER_IN_PARAMETER	The parameter contained a metacharacter that matched an attack pattern in the **Parameter Class** associated with the Parameter profile on the **WEBSITES > Website Profiles** page, or on the **SECURITY POLICIES > Parameter Protection** page (if no parameter profile).	Alert	Other Attacks

159	OS Command Injection in Parameter	OS_CMD_INJECTION_IN_PARAM	The parameter contained an OS command injection pattern that matched an attack pattern in the **Parameter Class** associated with the Parameter profile on the **WEBSITES > Website Profiles** page, or on the **SECURITY POLICIES > Parameter Protection** page (if no parameter profile).	Alert	Injection Attacks
156	Parameter Input Validation Failed	PARAM_INPUT_VALIDATION_FAILED	The parameter failed to match input type validation configured under **Parameter Profiles** on the **WEBSITES > Website Profiles** page.	Alert	Injection Attacks
154	Parameter Length Exceeded	PARAM_LENGTH_EXCEEDED	The parameter value in the request exceeded the **Maximum Parameter Value Length** on the: • **SECURITY POLICIES > Parameter Protection** page, or • **WEBSITES > Website Profiles > Parameter Profile** section.	Alert	Limits Violation

139	Parameter Value not Allowed	PARAM_VAL_NOT_ALLOWED	The **Global Choice** parameter did not match values configured under **Parameter Profiles** on the **WEBSITES > Website Profiles** page.	Alert	Injection Attacks
321	Python PHP Attack in Parameter	PYTHON_PHP_ATTACKS_MEDIUM_IN_PARAM	The parameter matched a Python PHP attack pattern in the associated **Parameter Class** of the parameter profile on the **WEBSITES > Website Profiles** page, or on the **SECURITY POLICIES > Parameter Protection** page (if no parameter profile).	Alert	Injection Attacks
134	Read-Only or Hidden Parameter Tampered	READ_ONLY_PARAM_TAMPERED	The read-only parameter did not match the value learned by the Barracuda Web Application Firewall based on the form sent to the browser.	Alert	Injection Attacks

164	Remote File Inclusion	REMOTE_FILE_INCLUSION	The parameter contained a remote file inclusion pattern that matched an attack pattern in the **Parameter Class** associated with the Parameter profile on the **WEBSITES > Website Profiles** page, or on the **SECURITY POLICIES > Parameter Protection** page (if no parameter profile).	Alert	Injection Attacks
136	Session Choice Parameter Tampered	SESSION_CHOICE_PARAM_TAMPERED	The session choice parameter did not match the value learned by the Barracuda Web Application Firewall based on the form sent to the browser for this session.	Alert	Session Tamper Attacks
162	Session Context not Found	SESSION_CONTEXT_NOT_FOUND	The session parameter (parameter type=read-only, session-choice or session-invariant) value does not match the learned value in the parameter profile, indicating possible tampering with the session parameter value.	Alert	Forceful Browsing

135	Session Invariant Parameter Tampered	SESSION_INVARIANT_PARAM_TAMPERED	The session-invariant parameter did not match the value learned by Barracuda Web Application Firewall based on the form sent to the browser for this session.	Alert	Session Tamper Attacks
157	SQL Injection in Parameter	SQL_INJECTION_IN_PARAM	The parameter matched an SQL injection pattern in the **Parameter Class** associated with the Parameter profile on the **WEBSITES > Website Profiles** page.	Alert	SQL Attacks

Advanced Policy Violations

Advanced Policy Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**
341	Barracuda Blocklist Policy Matched	grip-validation-failed	Incoming request is from IP addresses that have been identified as potential originators of spam, malware and bots by Barracuda's threat intelligence engine.	Alert	Forceful Browsing
146	Brute force from All Sources	BRUTE_FORCE_FROM_ALL_SOURCES	Requests from all sources are blocked when **Max Allowed Accesses From All Sources**is exceeded in the **Count Window** under **Edit Bruteforce Prevention** on the **WEBSITES > Advanced Security** page.	Alert	DDOS Attacks
145	Brute force from IP	BRUTE_FORCE_FROM_IP	Requests from a particular IP address are blocked when**Max Allowed Accesses Per IP** is exceeded in the **Count Window** under **Edit Bruteforce Prevention** on the **WEBSITES > Advanced Security** page.	Alert	DDOS Attacks

299	Unanswered CAPTCHA Limit Exceeded	DDOS_CAPTCHA_MAX_UNANSWERED_EXCEEDED	The number of client attempts to fetch the CAPTCHA image exceeded **Max Unanswered CAPTCHA** on the **WEBSITES > DDoS Prevention** page.	Alert	DDOS Attacks
297	CAPTCHA Attempt Limit Exceeded	DDOS_CAPTCHA_TRIES_EXCEEDED	The number of client attempts to solve a CAPTCHA challenge exceeded **Max CAPTCHA Attempts** on the **WEBSITES > DDoS Prevention** page.	Alert	DDOS Attacks
298	CAPTCHA Session Limit Exceeded	DDOS_CAPTCHA_MAX_NODES_EXCEEDED	The client request IP address has exceeded the CAPTCHA session limit. For a CAPTCHA enabled service, the client must answer a CAPTCHA challenge before accessing the service. Each CAPTCHA challenge sent to the client, is maintained in a session table for that client (based on the IP address). The CAPTCHA Session Limit for an IP address is 512 (hard coded limit). If the client attempts to append more than 512 sessions (concurrent CAPTCHA answered sessions), the request is denied with an error "CAPTCHA-Max-Sessions-Exceeded". If multiple clients access the CAPTCHA protected service from the same network, or if there is a device doing Source NAT in front of the Barracuda Web Application Firewall and more than 512 clients accessing the service, the 513th client may see the “CAPTCHA Session Limit Exceeded” error. Client access could be granted when an existing session expires (by an idle time).	Alert	DDOS Attacks
342	GeoIP Policy Matched	GEO_IP_BLOCKED	Incoming request has an IP Address from a country that does not have permissions to access the resource.	Alert	Forceful Browsing
12	Invalid URL Character Set	INVALID_URL_CHARSET	Request contained invalid character for configured character set. The relevant character set is determined using several configuration elements like Default Character Set, Detect Response Charset and Response Charset.	Warning	Injection Attacks
75	Rate Control Intrusion	RATE_CONTROL_INTRUSION	The rate of requests exceeds **Maximum Active Requests** and **Maximum Per Client Backlog** of the rate control pool associated with the Service.	Alert	DDOS Attacks
293	Secure Browsing	SECURE_BROWSING	Unable to validate session key in a request matching the URL specified in Secure Browsing policies.	Alert	Forceful Browsing

295	Slowloris Attack	SLOWLORIS_ATTACK	Slowloris attack detected. Request exceeded **Max Request Timeout** and **Incremental Request Timeout** for the Service under **Slow Client Prevention** on the **WEBSITES > DDoS Prevention** page.	Alert	DDOS Attacks
302	Slow Read Attack	SLOW_READ_ATTACK	Slow Read Attack detected. Response exceeded **Max Response Timeout** and **Incremental Response Timeout** for the Service under **Slow Client Prevention** on the **WEBSITES > DDoS Prevention** page.	Alert	DDOS Attacks
343	Tor Node Policy Matched	TOR-IP-BLOCKED	IP address for the incoming request matched the IP address of a ToR exit node.	Alert	Forceful Browsing
301	URL Encryption	URL_ENCRYPTION	Request violated the URL encryption policy configured in the **WEBSITES > URL Encryption** page.	Alert	Forceful Browsing
204	Virus Found	VIRUS_IN_POST_REQUEST	Virus detected in uploaded file. All files uploaded through multipart/form-data messages are scanned for viruses. Requests containing virus signatures are denied when **Enable Virus Scan** is set to **Yes** under **Advanced Security** on the **WEBSITES > Advanced Security** page.	Alert	File Attacks
338	Web Scraping Bots	WS_BOTS	Request violated the web scraping policy configured in the **WEBSITES > Web Scraping** page.	Alert	Forceful Browsing
339	Web Scraping Fake Bots	WS_FAKE_BOTS	Request violated the web scraping policy configured in the **WEBSITES > Web Scraping** page.	Alert	Forceful Browsing

XML Firewall DoS Violations

XML Firewall DoS Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**

185	DTD Found	XDOS_DTD	An XML service rejected a SOAP message containing Document Type Definition (DTD), which is NOT allowed by the SOAP standard.**Block DTDs** is set to *Yes* on the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations
187	External URI Reference Found	XDOS_EXT_ENTITY	Request contains external entities including external URI references or external DTDs. **Block External Entities** is set to *Yes* on the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations

188	Malformed XML	XDOS_MALFORMED	An XML parser detected a malformed XML document. A malformed XML document contains illegal characters, mismatched element tags (a starting tag with no matching ending tag) or trailing content after the document element.	Alert	XML Violations
178	Max Attribute Name Length Exceeded	XDOS_MAX_ATTRIBUTE_NAME_LENGTH	The XML document exceeds the maximum attribute name length limit specified in the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations
179	Max Attribute Value Length Exceeded	XDOS_MAX_ATTRIBUTE_VALUE_LENGTH	The XML document exceeds the maximum attribute value length limit specified in the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations

182	Max Document Size Exceeded	XDOS_MAX_FILE_SIZE	The XML document exceeds the maximum document size limit specified in the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations
177	Max Element Attributes Exceeded	XDOS_MAX_ATTRIBUTES	The XML document exceeds the maximum allowable attributes of an element specified in the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations
184	Max Element Children Exceeded	XDOS_MAX_ELEMENT_CHILDREN	The XML document exceeds the maximum allowable children per node in a tree specified in the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations

175	Max Element Name Length Exceeded	XDOS_MAX_ELEMENT_NAME_LENGTH	The XML document exceeds the maximum allowable length for the name of an element specified in the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations
176	Max Elements in Tree Exceeded	XDOS_MAX_ELEMENTS	The XML document exceeds the maximum allowable number of nodes/elements in a tree specified in the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations
181	Max Text Size Exceeded	XDOS_CDATA_LENGTH	The XML document exceeds the maximum allowable size of the XML document.	Alert	XML Violations

174	Max Tree Depth Exceeded	XDOS_MAX_ELEMENT_DEPTH	The XML document exceeds the maximum allowable nesting depths of nodes specified in the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations
183	Min Document Size Limit	XDOS_MIN_FILE_SIZE	The XML document exceeds the minimum allowable size of the XML document specified in the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations
186	Processing Instructions Found	XDOS_PI	Request contains Processing Instructions (PIs). A PI is a text data section ignored by the XML parser and passed on as instructions to applications. **Block Processing** Instructions is set to *Yes* on the **WEBSITES > XML Protection > XML Validation Settings** section.	Alert	XML Violations

XML Firewall WSI Assertions

XML Firewall WSI Assertions					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**
211	DOCTYPE Element	XML_WSI1007	The SOAP message contains a DOCTYPE element in the request. **WSI1007: Message Should Not Include SOAP:Header or SOAP:Body elements as Defined in the included DTD** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
228	Message Contains a WS-I Conformance Claim with a “SOAP:MustUnderstand” Attribute	XML_WSI1111	The SOAP message contains a WS-I conformance claim with a “soap:mustUnderstand” attribute. **WSI1111: WS-I Conformance Claims Should Not Contain the SOAP:MustUnderstand Attribute** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
227	WS-I Conformance Claim Does Not Adhere to the WS-I Conformance Claim Schema	XML_WSI1110	The SOAP message contains a WS-I conformance claim which fails to adhere to the WS-I conformance claim schema. **WSI1110: WS-I Conformance Claims Should Adhere to the WS-I Conformance Claim Schema** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
226	Message Contains a WS-I Conformance Claim Which is Not a Child of the “SOAP:Header” Element	XML_WSI1109	The SOAP message contains a WS-I conformance claim which is not a child of the "SOAP:Header" element.**WSI1109: WS-I Conformance Claim Should be a Child of the SOAP:Header Element** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
219	Attributes in SOAP Envelope Header Body	XML_WSI1032	Message contains attributes in the envelope, header and body portion of the data. **WSI1032: SOAP:Envelope, SOAP:Header and SOAP:Body Elements Should Not Have Attributes in Namespace** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
240	EncodingStyle in Envelope Namespace Elements	XML_WSI1307	Message contains "soap:encodingStyle" attributes on any elements whose namespace is http://schemas.xmlsoap.org/soap/envelope/. **WSI1307: SOAP:Envelope Namespace Elements Should Not Have the SOAP:EncodingStyle Attribute** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
244	EncodingStyle Attribute Found in Grandchild of SOAP Body	XML_WSI1318	The message in an rpc-literal binding contains "soap:encodingStyle" attribute on an element that is a grandchild of “soap:body”. **WSI1318: Grandchildren of SOAP:Body Should Not Have the SOAP:EncodingStyle Attribute** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations

220	Envelope Namespace is 1998	XML_WSI1033	The message with an envelope contains the namespace declaration xmlns:xml=http://www.w3.org/XML/1998/namespace. **WSI1033: SOAP:Envelope Namespace Should Not be 1998** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
245	SOAP:Envelope or SOAP:Body Does Not Conform to XML 1.0	XML_WSI1601	The message with "soap:envelope" or "soap:body" does not conform to XML 1.0. **WSI1601: SOAP:Envelope and SOAP:Body Should Conform to XML 1.0** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
246	Envelope Does Not Conform to SOAP Schema	XML_WSI1701	The message whose "soap:envelope" does not conform to the SOAP schema. **WSI1701: SOAP:Envelope Should Conform to the SOAP Schema** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
242	SOAP:Envelope Has a Direct Child After the "SOAP:Body" Element	XML_WSI1309	The message contains element children of "soap:Envelope" following the "soap:Body" element. **WSI1309: SOAP:Envelope Should Not Have Direct Children After the SOAP:Body Element** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
225	Message Contains Undefined “SOAPBind:Fault” Element(s)	XML_WSI1107	A fault detected in the message which is not defined in wsdl:binding. A wsdl:binding should contain a "soapbind:fault" describing each known fault. **WSI1107: Fault Response Should be Defined in WSDL:Binding** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
218	SOAP 1.1 Dot Notation is Used By the “SOAP:Fault” Element	XML_WSI1031	The message contains a faultcode element with dot (.) notation. **WSI1031: SOAP:Fault Element Should Not Use SOAP 1.1 Dot Notation** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
221	Good Response is Not Using HTTP 200 OK	XML_WSI1100	The SOAP message does not contain soap:Fault and does not use 200 OK HTTP Status code for responses. **WSI1100: Good Response Uses HTTP 200 OK Status** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
206	Message is Not Sent Using HTTP1.0 or HTTP1.1	XML_WSI1002	Message not sent using HTTP version 1.0 or 1.1. **WSI1002: Message Should be Sent using HTTP 1.1 or HTTP 1.0** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
205	Message is Not Sent Using HTTP1.1	XML_WSI1001	Message not sent using HTTP version 1.1. **WSI1001: Message Should be Sent Using HTTP 1.1** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
207	Message is Not UTF8 or UTF16	XML_WSI1003	The XML schema in the request is not using UTF-8 or UTF16 encoding. **WSI1003: Message is UTF-8 or UTF-16** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations

230	SOAP:Envelope Does Not Have v1.1 Namespace	XML_WSI1201	Message contains a soap:Envelope with a document element “Envelope”, but the namespace name is not http://schemas.xmlsoap.org/soap/envelope/. **WSI1201: SOAP:Envelope Should Have v1.1 Namespace** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
213	Message Does Not Include All Headers	XML_WSI1009	Message does not contain all the "soapbind:headers" specified in the WSDL file. **WSI1009: Message Should Include All Specified Headers** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
212	Message Part Accessors Have No Namespace	XML_WSI1008	Name space not defined in the incoming soap message. **WSI1008: Message Part Accessor Elements in Parameters and Return Value Should Have Proper Namespace** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
236	Attribute “MustUnderstand” is neither 1 nor 0	XML_WSI1301	Message with a "soap:mustUnderstand" value of neither 1 nor 0. **WSI1301: Attribute "MustUnderstand" Value Should be Either "1" or "0"** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
216	SOAP:Fault Not Generated for Bad Envelope Namespace	XML_WSI1012	A soap:Fault not generated for a document element named "Envelope" where the namespace name is not "http://schemas.xmlsoap.org/soap/envelope/". **WSI1012: SOAP:Fault Should be Generated for Bad Envelope Namespace** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
223	Non POST Request Does Not Contain 405 HTTP Status Code	XML_WSI1103	A SOAP message sent as part of a non-POST method request received an HTTP response with status code other than 405. **WSI1103: Response to a Non POST Request Should Contain 405 HTTP Status Code** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
224	Non XML Request Does Not Contain 415 HTTP Status Code	XML_WSI1104	A SOAP message sent as part of non-XML request received an HTTP response with status code other than 415. **WSI1104: Response to Non XML Request Should Contain 415 HTTP Status Code** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
214	One-Way Response Contains a SOAP:Envelope	XML_WSI1010	An HTTP one-way response contains a SOAP envelope (that is, HTTP entity-body is not empty). **WSI1010: One-Way Response Should Not Contain a SOAP:Envelope** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
235	Part Accessors Have “xsi: nil” Attribute	XML_WSI1211	Message with rpc-literal binding contains xsi:nil attribute with value of “1” or ‘true’ on the part accessors. **WSI1211: Part Accessors Should Not Have "xsi: nil" Attribute with Value "1" or "True"** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations

222	Processed Response Status is Neither 200 nor 202	XML_WSI1101	Response message without embedded SOAP message. **WSI1101: Processed Response Should Use Either 200 or 202 HTTP Status Code** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
215	Request Does Not Match the WSDL:Definition	XML_WSI1011	Content of request message does not conform to the WSDL file definition. **WSI1011: Request Content Should Match WSDL:Definition** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
208	Request Message is Not an HTTP POST Message	XML_WSI1004	Message not sent using the HTTP POST method. **WSI1004: Request Message Should be an HTTP POST Message** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
209	Response Wrapper Does Not Match the Name Attribute on WSDL:Operation	XML_WSI1005	Wrapper element in the response message does not match the name attribute on the wsdl:operation element concatenated by the string "Response". A response with a wrapper not named after the wsdl:operation name. **WSI1005: Response Wrapper Should Match the Name Attribute on WSDL:Operation** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
217	Response Does Not Match the WSDL:Definition	XML_WSI1013	The content of the response message does not conform to the WSDL file definition. **WSI1013: Response Content Should Match WSDL:Definition** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
231	Children Elements in SOAP:Body are Not Namespace Qualified	XML_WSI1202	Message with a child element of the soap:Body element is not namespace qualified. **WSI1202: Children Elements in SOAP:Body Should be Namespace Qualified** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
241	Children Elements in SOAP:Body Have “SOAP:EncodingStyle” Attribute	XML_WSI1308	Message with a child element of the soap:Body element has a soap:encodingStyle attribute. **WSI1308: Children Elements of SOAP:Body Should Not Have the SOAP:EncodingStyle Attribute** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
243	SOAP:Fault Children are Qualified	XML_WSI1316	Message contains a "soap:Fault" element with a qualified child element. **WSI1316: SOAP:Fault Children Should be Unqualified** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
239	SOAP:Fault Children Elements are Not Namespace Qualified	XML_WSI1306	SOAP message has one or more "soap:Fault" non standard children elements, i.e., the child element(s) is neither soap:faultcode, soap:faultstring, soap:faultactor nor soap:detail. **WSI1306: SOAP:Fault Children Elements Should be Namespace Qualified** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations

232	SOAP:Fault Has Non-Foreign Namespace	XML_WSI1203	The soap:Fault message contains detail element with qualified attributes, but with a non-foreign namespace. Non-foreign namespace means the namespace should be anything other than “http://schemas.xmlsoap.org/soap/envelope/". **WSI1203: Namespace on the Detail Element in the SOAP:Fault Should be a Foreign Namespace** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
238	SOAP:Fault Message Not Found in the HTTP 500 Response	XML_WSI1305	The SOAP fault response message does not have "500 Internal Server Error" HTTP status code. **WSI1305: SOAP:Fault Message Should Contain HTTP 500 Error Code** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
237	SOAP:Faultcode is Not Standard or Namespace Qualified	XML_WSI1302	Message contains a faultcode element which is neither a fault code defined in SOAP 1.1 nor a namespace qualified fault code. **WSI1302: SOAP:Faultcode Should be Standard or Namespace Qualified** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
229	SOAPAction Header Does Not Contain the Correct String Value	XML_WSI1116	SOAP message whose SOAPAction HTTP header field does not match the WSDL soapAction attribute in soapbind:operation (either the same value or a blank quoted string if not present). **WSI1116: SOAPAction Header Should Match the SOAPBind:Operation/@SOAPAction Attribute** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
210	SOAPAction Header Does Not Contain Quoted String	XML_WSI1006	The value of the "SOAPAction" HTTP header field in an HTTP request is not a quoted string. **WSI1006: SOAPAction Header Should Contain Quoted String** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
233	SOAP: Body Contains the “SOAPEnc:ArrayType” Attribute	XML_WSI1204	Message contains a faultcode element which is neither a fault code defined in SOAP 1.1 nor a namespace qualified fault code. **WSI1302: SOAP:Faultcode Should be Standard or Namespace Qualified** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations
234	SOAP Message Contains XML Processing Instructions	XML_WSI1208	SOAP message contains XML Processing instructions. **WSI1208: SOAP Message Should Not Include XML Processing Instructions** is set to *Yes* on the **WEBSITES > XML Protection > WS-I Basic Profile Assertions** section.	Alert	XML Violations

XML Firewall SOAP Violations

XML Firewall SOAP Violations

Attack ID	Attack Name	Attack Name in Export Logs	Description	Severity	Attack Category
193	Additional SOAP Headers rcvd	XML_VALIDATION_WSDL_SOAP_UNKNOWN_HEADERS	SOAP message contains additional headers not specified in the WSDL file. **Allow Additional SOAP Headers** is set to *Yes* on the **WEBSITES > XML Protection > SOAP Validations** section.	Alert	XML Violations
192	Invalid SOAP Body	XML_VALIDATION_WSDL_SOAP_HEADERS	SOAP message body does not conform to the schema defined in the WSDL file. **Validate SOAP body from WSDL schema** is set to *Yes* on the **WEBSITES > XML Protection > SOAP Validations** section.	Alert	XML Violations

190	Invalid SOAP Envelope	XML_VALIDATION_WSDL_SOAP_ENVELOPE	SOAP message with soap:envelope does not conform to the SOAP standard. **Validate SOAP Envelope** is set to *Yes* on the **WEBSITES > XML Protection > SOAP Validations** section.	Alert	XML Violations
191	Invalid SOAP Header	XML_VALIDATION_WSDL_SOAP_BODY	SOAP message contains a header that does not conform to the policies defined in the WSDL file. **Validate SOAP headers defined in WSDL** is set to *Yes* on the **WEBSITES > XML Protection > SOAP Validations** section.	Alert	XML Violations

JSON Policy Violations

JSON Policy Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**

309	Max Array Values Exceeded	JSON_MAX_ARRAY_VALUES	A JSON request exceeded the maximum allowable number of elements in a array specified in **Max Array Elements** on the **WEBSITES > JSON Security** page.	Alert	JSON Violations
305	Max Key Length Exceeded	JSON_MAX_KEY_LENGTH	A JSON request exceeded the maximum allowable length for JSON **keys** specified in **Max Key Length** on the **WEBSITES > JSON Security** page.	Alert	JSON Violations
310	Max Number Value Exceeded	JSON_MAX_NUMBER_VALUE	A JSON request exceeded the maximum allowable value for JSON **Number datatype** specified in **Max Number Value** on the **WEBSITES > JSON Security** page.	Alert	JSON Violations
307	Max Object Child Exceeded	JSON_MAX_OBJECT_CHILD	A JSON request exceeded the maximum allowable number of elements in a single JSON object specified in **Max Child** on the **WEBSITES > JSON Security** page.	Alert	JSON Violations
306	Max Object Keys Exceeded	JSON_MAX_OBJECT_KEYS	A JSON request exceeded the maximum allowable keys specified in **Max Keys** on the **WEBSITES > JSON Security** page.	Alert	JSON Violations
308	Max Value Length Exceeded	JSON_MAX_VALUE_LENGTH	A JSON request exceeded the maximum allowable length for JSON string value specified in **Max Value Length** on the **WEBSITES > JSON Security** page.	Alert	JSON Violations

304	Object Depth Exceeded	JSON_MAX_OBJECT_DEPTH	A JSON request exceeded the maximum allowable depth for nested JSON structure specified in **Max Tree Depth** on the **WEBSITES > JSON Security** page.	Alert	JSON Violations

JSON Profile Violations

JSON Profile Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**
313	Malformed JSON	JSON_MALFORMED	A request not conforming to the JSON RFC specifications was detected.	Alert	JSON Violations
336	Apache Struts Attack in JSON Data	APACHE_STRUTS_ATTACKS_IN_JSON_PARAM	The key/value in JSON data matched an Apache Struts attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	JSON Violations

315	Cross-Site Scripting in JSON Data	XSS_INJECTION_IN_JSON_PARAM	The key/value in JSON data matched a Cross-Site Scripting pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	JSON Violations
319	Custom Attack Pattern in JSON Data	CUSTOM_ATTACK_PATTERN_IN_JSON_PARAM	The key/value in JSON data matched a custom attack pattern defined under **Attack Types** on the **ADVANCED > Libraries** page.	Alert	JSON Violations
317	Directory Traversal Attack in JSON Data	DIRECTORY_TRAVERSAL_IN_JSON_PARAM	The key/value in JSON data matched a Directory Traversal pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	JSON Violations

335	HTTP Specific Attack in JSON Data	HTTP_SPECIFIC_ATTACKS_IN_JSON_PARAM	The key/value in JSON data matched an HTTP specific attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	JSON Violations
333	LDAP Injection in JSON Data	LDAP_INJECTION_IN_JSON_PARAM	The key/value in JSON data matched an LDAP Injection attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	JSON Violations
316	OS Command Injection in JSON Data	OS_CMD_INJECTION_IN_JSON_PARAM	The key/value in JSON data matched an OS Command Injection pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	JSON Violations

334	Python PHP Attack in JSON Data	PYTHON_PHP_ATTACKS_IN_JSON_PARAM	The key/value in JSON data matched a Python PHP attack pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	JSON Violations
318	Remote File Inclusion in JSON Data	RFI_VIOLATION_IN_JSON_PARAM	The key/value in JSON data matched a Remote File Inclusion pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	JSON Violations
314	SQL Injection in JSON Data	SQL_INJECTION_IN_JSON_PARAM	The key/value in JSON data matched an SQL Injection pattern defined under **Attack Types** on the **ADVANCED > View Internal Patterns** page.	Alert	JSON Violations

340	JSON Key Validation Failed	json-key-validation-failed	The Request does not match with the JSON Key Profile configured on the **WEBSITES > JSON Security** page. OR The request failed to match the configured JSON Key profile on the **WEBSITES > JSON Security** page.	Alert	JSON Violations

Client Violations

Client Violations					
Attack ID	**Attack Name**	**Attack Name in Export Logs**	**Description**	**Severity**	**Attack Category**
346	Brute force from Fingerprint	BRUTE_FORCE_FROM_FINGERPRINT	Identify Brute Force attacks based on the Client Fingerprint. The Client Fingerprint identifies a specific client down to the browser level, and is useful to identify an individual client from behind an IP. This ensures that an entire NAT'ed IP is not blocked, and only a specific attacking client is blocked.	Alert	advanced-policy-violations

401	Referer Spam	REFERER_SPAM	Identifies bots based on the Referrer header using the SPAM URL list in the Referrer Spam settings. This ensures that your analytics are not skewed by such bots visiting your sites.	Alert	Bot-mitigation-violations
402	Comment Spam	Comment_SPAM	Block spam comments on your web application based on the list of terms in the Spam URL list.	Alert	Bot-mitigation-violations
403	Blacklisted Category	BLACKLISTED_CATEGORY	Provides the list of blacklisted clients that should be blocked by Barracuda WAF.	Alert	Bot-mitigation-violations
404	Credential Stuffing Detected	CREDENTIAL_STUFFING_DETECTED	When configured, this validates incoming username/password pairs against the cloud-based Credential Stuffing detection database. If the credentials are already in the database, this attack id is generated.	Alert	Bot-mitigation-violations
421	Fingerprint Challenges Exceeded	FINGERPRINT_CHALLENGES_EXCEEDED	The client that did not allow itself to be fingerprinted even after multiple attempts from the WAF	Alert	Bot-mitigation-violations
422	Missing Referer Header	MISSING_REFERER_HEADER	The attack generated when “Referer” header is not present in the request.	Alert	Protocol Violations
423	Missing Referer Domain	MISSING_REFERER_DOMAIN	The attack generated when “Referer” header is present but there is no domain specified in the “Referer” field.	Alert	Protocol Violations
424	Referer Domain Not Matching Host	REFERER_DOMAIN_NOT_MATCHING_HOST	The attack generated when "Referer” domain doesn’t match with the “Host” header present in the request.	Alert	Protocol Violations

425	Missing UserAgent Header	MISSING_USERAGENT_HEADER	The attack generated when “User-Agent” header is not present in the request.	Alert	Protocol Violations
426	Fingerprint Risk Level Bad Client	FINGERPRINT_RISK_LEVEL_BAD_CLIENT	Client is marked bad as client is having higher risk score than configured for Risk Score Level for Bad Clients on the **SECURITY POLICIES > Client Profile** page.	Alert	Client-violations
427	Fingerprint Risk Level Suspected Client	FINGERPRINT_RISK_LEVEL_SUSPECTED_CLIENT	Client is marked suspected as client is having higher risk score than configured for Risk Score Level for Suspected Clients on the **SECURITY POLICIES > Client Profile** page.	Alert	Client-violations

Below is the list of attacks that are logged in the **BASIC > Web Firewall Logs** page, but are not part of the action policy list:

Attack ID	Attack Name	Attack Name in Export Logs	Description	Severity	Attack Category
1	Deny ACL matched	DENY_ACL_MATCHED	The URL in the request matched the Deny ACL rule configured in the **WEBSITES > Allow/Deny > URL: Allow/Deny Rules** section, or in the **SECURITY POLICIES > Global ACLs** page.	Alert	Forceful Browsing
303	Session timed out	SESSION_TIMEOUT_EXCEEDED	The request exceeded the idle time specified for a session in **Session Timeout** on the **BASIC > Services** page	Alert	DDOS Attacks

56	Redirect ACL matched	REDIRECT_ACL_MATCHED	The URL in the request matched the redirect ACL rule configured in the **WEBSITES > Allow/Deny > URL: Allow/Deny Rules** section, or in the **SECURITY POLICIES > Global ACLs** page.	Information	Other Attacks
78	Access Control cookie expired	ACCESS_CONTROL_COOKIE_EXPIRED	The session cookie for the authenticated user exceeded the idle time specified in **Idle Timeout** under **Authentication** on the **ACCESS CONTROL > Authentication Policies** page.	Warning	Auth Attacks
79	Access Control cookie invalid	ACCESS_CONTROL_COOKIE_INVALID	The session cookie sent by the client is invalid.	Warning	Auth Attacks
80	Access Control access denied	ACCESS_CONTROL_ACCESS_DENIED	The authenticated user is denied access to the requested resource as the user is not configured in **Allowed Users** or **Allowed Groups** under **Authorization** on the **ACCESS CONTROL > Authorization Policies** page.	Warning	Auth Attacks
81	Access Control no cookie found	ACCESS_CONTROL_NO_COOKIE	Session cookie not found in the request to access the restricted resource. The user is not authenticated to access the requested resource.	Warning	Auth Attacks

113	Blocked by FTP command-blocking policy	FTP_COMMAND_BLOCKED	The FTP command in the request does not match the commands configured in **FTP Allowed Verbs** on the **WEBSITES > FTP Security** page.	Alert	Other Attacks
292	Virus Scan	VIRUS_SCAN	The scan of the uploaded file detected no virus. All files uploaded through multipart/form-data messages are scanned for viruses. Requests containing virus signatures are denied when **Enable Virus Scan** is set to **Yes** under **Advanced Security** on the **WEBSITES > Advanced Security** page.	Notice	FILE Attacks