



FortiWeb Log Message Reference

VERSION 6.2.2

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<https://cookbook.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



December 19, 2019

FortiWeb 6.2.2 Log Message Reference

1st Edition

TABLE OF CONTENTS

Introduction	5
Scope	5
How to interpret FortiWeb logs	6
Header & body fields	6
Log ID numbers	16
Types	16
Subtypes	16
Priority level	17
Message IDs	18
Event	19
Attack	33
20000001	38
20000002	39
20000003	40
20000004	41
20000005	42
20000006	43
20000007	44
20000008	45
20000009	46
20000010	47
20000011	48
20000012	49
20000013	50
20000014	51
20000015	52
20000016	53
20000017	54
20000018	55
20000021	56
20000022	57
20000023	58
20000024	59
20000025	60
20000026	61
20000027	63
20000028	64
20000029	65
20000030	66
20000031	67
20000033	68

20000035	69
20000036	70
20000037	71
20000038	72
20000039	73
20000040	74
20000041	75
20000042	76
20000043	77
Traffic	79

Introduction

This document is a detailed reference of all of your FortiWeb appliance's possible log messages. It is organized primarily by the log type:

- [Event](#)
- [Attack](#)
- [Traffic](#)

To look up the meaning of a specific log message, go to the section that matches its **Type** (`type`) field, then look for the table that matches its **ID** (`log_id`).

This document also explains the general structure of FortiWeb log messages, and the meanings of common fields (see [How to interpret FortiWeb logs on page 6](#)).

Scope

This document provides administrators information about log messages that can be recorded by a FortiWeb appliance.

This document does **not** cover how to configure logging. It assumes you have already configured it, and need to know how to interpret the log messages. For instructions on how to configure logging, see the [FortiWeb Administration Guide](#) or [FortiWeb CLI Reference](#).

How to interpret FortiWeb logs

This section explains the composition of FortiWeb log messages.

In some cases, to avoid flooding attack logs with entries, FortiWeb collects multiple attack log messages into a single message. See [Attack on page 33](#).

Header & body fields	6
Log ID numbers	16
Types	16
Subtypes	16
Priority level	17
Message IDs	18

Header & body fields

Each log message is comprised of several field-value pairs. The names may vary slightly between **Raw** versus **Formatted** views in the web UI.

ID (log_id) header field and its value

#	ID	Sub Type
(6)		DDOS based on source IP
1	00070038	DDOS based on source IP
2	00070038	DDOS based on source IP
3	00070038	DDOS based on source IP
4	00070038	DDOS based on source IP
5	00070038	DDOS based on source IP
6	00070038	DDOS based on source IP
(24)		waf_signature_detection
7	00070010	waf_signature_detection

All log messages' fields belong to one of two parts:

- **Header** — Contains the time and date the log originated, a log identifier, a message identifier, the administrative domain (ADOM), the type of log, the severity level (priority) and where the log message originated. **These fields exist in all logs.**
- **Body** — Describes the reason why the log was created, plus any actions that the FortiWeb appliance took to respond to it. **These fields vary by log type.**

Log message header and body

For example, this is a raw-format event log message. Body fields are in **bold**.

```
date=2013-10-07 time=11:30:53 log_id=10000017 msg_id=000000001117 device_id=FVVM040000010871 vd="root"
timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy=""
user=admin ui=GUI action=login status=success msg="User admin login successfully from GUI
(172.20.120.47)"
```

This attack log message contains the same header fields, but its body fields are different.

```
date=2016-02-19 time=11:23:45 log_id=20000010 msg_id=000139289631 device_id=FV-1KD3A15800072 vd="root"
timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=attack subtype="waf_signature_detection"
pri=alert trigger_policy="" severity_level=Medium proto=tcp service=http action=Alert policy="123"
src=172.22.6.234 src_port=60554 dst=10.0.9.13 dst_port=80 http_method=get http_
url="/preview.php?file=../" http_host="10.0.9.123" http_agent="Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:43.0) Gecko/20100101 Firefox/43.0" http_session_id=3B9864AEKNQSLLODNTILCG37M2FZ6A88 msg="
[Signatures name: 123] [main class name: Generic Attacks(Extended)] [sub class name: Directory
Traversal]: 060150002" signature_subclass="Directory Traversal" signature_id="060150002"
srccountry="Reserved" content_switch_name="none" server_pool_name="123" false_positive_
mitigation="none" log_type=LOG_TYPE_SCORE_SUM event_score=3 score_message="[score_type: total_
score] [score_scope: TCP Session] [score_threshold: 5] [score_sum: 7]" entry_sequence="000139289630"
```

Similarly, traffic log body fields are different.

```
date=2014-06-26 time=00:43:37 log_id=30000000 msg_id=000001351251 device_id=FV-1KD3A14800059 vd="root"
timezone="(GMT-8:00)Pacific Time(US&Canada)" type=traffic subtype="http" pri=notice proto=tcp service=http
status=success reason=none policy=Auto-policy src=10.0.8.103 src_port=8142 dst=10.20.8.22 dst_port=80
http_request_time=0 http_response_time=0 http_request_bytes=444 http_response_bytes=401 http_
method=get http_url="/" http_host="10.0.8.22" http_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT
5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; " http_retcode=200
msg="HTTP GET request from 10.0.8.103:8142 to 10.20.8.22:80" srccountry="Reserved" content_switch_
name="testa" server_pool_name="Auto-ServerFarm"
```

The following table describes each possible header or body field, according to its name as it appears in the **Formatted** or **Raw** view.

Log message fields

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traf-fic	
Header					
Date (date)	The year, month, and day when the log message was	+	+	+	date=2013-10-08

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traf-fic	
	recorded.				
Time (time)	The hour (according to a 24-hour clock, where 15:00 is 3:00 PM), minute, and second that the log message was recorded.	+	+	+	time=15:38:01
ID (log_id)	See Log ID numbers on page 16 .	+	+	+	log_id=00041101
MSG ID (msg_id)	See Message IDs on page 18 .	+	+	+	msg_id=000000000153
Device ID (device_id)	The identifier, typically the serial number, of the appliance which originally recorded the log.	+	+	+	device_id=FV-1KD2B34567890
ADOM (vd)	The administrative domain (ADOM) in which the log message was recorded	+	+	+	vd="root"
Time Zone (timezone)	The name, geographical region, and Greenwich Mean Time (GMT) adjustment of the time zone in which the appliance is located.	+	+	+	timezone="(GMT-5:00)Eastern Time(US & Canada)"
Type (type)	See Types on page 16 .	+	+	+	type=event
Sub Type (subtype)	See Subtypes on page 16 .	+	+	+	subtype=admin
Level (pri)	See Priority level on page 17 .	+	+	+	pri=alert
Body					
Protocol (proto)	tcp	-	+	+	proto=tcp

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traf-fic	
	The protocol used by web traffic. By definition, for FortiWeb, this is always TCP.				
Service (service)	http or https The name of the application-layer protocol used by the traffic. By definition, for FortiWeb, this is always HTTP or HTTPS.	-	+	+	service=http
Source (src)	The IP address of the traffic's origin. The source varies by the direction: <ul style="list-style-type: none"> In HTTP requests, this is the web browser or other client. In HTTP responses, this is the physical server. 	-	+	+	scr=10.0.0.0
Source Port (src_port)	The port number of the traffic's origin.	-	+	+	src_port=3471
Destination (dst)	The IP address of the traffic's destination. The source varies by the direction: <ul style="list-style-type: none"> In HTTP requests, this is the physical server. In HTTP responses, this is the web browser or other client. 	-	+	+	dst=10.0.0.1
Destination Port (dst_port)	The port number of the traffic's destination.	-	+	+	dst_port=8080
Policy (policy)	The name of the server policy governing the traffic which	-	+	+	policy="policy1"

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traf-fic	
	caused the log message.				
User (user)	The daemon or name of the administrator account that performed the action that caused the log message.	+	-	-	user=admin
User Interface (ui)	<p>The type of management interface used by the administrative session which caused the log message.</p> <p>Either:</p> <ul style="list-style-type: none"> • GUI • sshd • telnet • console • none <p>Unless the user is a daemon (which don't have a user interface), logins from <code>none</code> indicate that an administrator used the JavaScript CLI Console widget on System > Status > Status in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.</p> <p>Logins from <code>console</code> indicate use of CLI via the local serial console port.</p>	+	-	-	ui=GUI
Action (action)	<p>The action associated with the log message or policy violation, such as:</p> <p>login</p> <p>or</p> <p>Alert</p>	+	+	-	action=Alert
Status (status)	The result of the action.	+	-	+	status=failure

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traf-fic	
Reason (reason)	The reason for the status, if any.	+	-	+	reason=name_invalid
Return Code (http_retcode)	The HTTP return code. If FortiWeb is configured to redirect, this is the rewritten code, not the original one from the server.	-	-	+	http_retcode=200
Request Time (http_request_time)	The amount of time it took FortiWeb to process the client request, in milliseconds (ms).	-	-	+	http_request_time=10
Response Time (http_response_time)	The amount of processing time for the response in milliseconds (ms). This can be a useful measure of performance issues, especially if processing involves regular expressing matching.	-	-	+	http_response_time=10
Request Bytes (http_request_bytes)	The size of the request in bytes.	-	-	+	http_request_bytes=2
Response Bytes (http_response_bytes)	The size of the individual response in bytes (B). For chunked responses, this is for each reply; it does not aggregate all related chunks.	-	-	+	http_response_bytes=136
Method (http_method)	The method, such as GET or POST, used by the HTTP request.	-	+	+	http_method=get

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
URL (http_url)	<p>The URL in the HTTP header of the original HTTP request, such as:</p> <pre>/images/buttons/hintOver.png</pre> <p>This does not include the service (http://) nor host name (example.nl). If FortiWeb is configured to rewrite the URL, this is the original URL from the client, not the rewritten one.</p>	-	+	+	http_url="/image/up.png"
Host (http_host)	<p>The <code>Host:</code> field in the HTTP header of the HTTP request, such as:</p> <pre>www.example.com</pre> <p>or</p> <pre>10.0.0.1:8080</pre> <p>This is typically a fully qualified domain name (FQDN) or IP address and port number that resolves or routes to the virtual server on the FortiWeb appliance.</p> <p>This may be different from your internal DNS name (if any) for the web server, or, if you are using HTTP <code>Host:</code> rewrites, different from the virtual host on the web server. For example, this might be <code>www.example.co.jp</code> instead of <code>www1.local</code> or the virtual host that serves responses for all DNS names, <code>www.example.com</code>.</p>	-	+	+	http_host="example.com"
User Agent	<p>The name and version of the HTTP client, usually a web browser. This is reported by</p>	-	+	+	http_agent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36"

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traf-fic	
(http_agent)	User-Agent: HTTP header. In attacks, it is often fake.				(KHTML, like Gecko) Chrome/27.0.1453.110 Safari/537.36"
FortiWeb Session ID (http_session_id)	The session identifier for a client's related HTTP requests (if any). The ID may be unknown if the Session Management option is not enabled in the applied protection profile, and therefore FortiWeb has not injected a session cookie nor inferred a session ID from the protected web application.	-	+	-	http_session_id=K8BXT3TNYUM710UEGWC8IQBTPX9PRWHB
Severity Level (severity_level)	The severity that the administrator configured in the rule or policy governing the traffic which caused the log message.	-	+	-	severity_level=High
Trigger Policy (trigger_policy)	The name of the notification servers used to record and/or deliver this log message (if any). The trigger policy value may be an empty string if no trigger policy was selected.	+	+	-	trigger_policy=notification-server-group1
Signature Subclass (signature_subclass)	The name of the signature subclass. If the current signature has no subclass, the main class is displayed.	-	+	-	"Cross Site Scripting"
Signature ID	The ID of the specific signature within the subclass that triggered the log message.	-	+	-	"010000001"

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traf-fic	
(signatu re_id)					
Source Country (srccoun try)	The country that is the source of the traffic.	-	+	+	"United States"
Message (msg)	<p>Details describing the reason why the log message was created.</p> <p>The message varies by the nature of the cause.</p> <p>The <code>msg</code> log field has the lowest priority in the disk log. When the total size of all the log fields exceeds the disk log size limit, FortiWeb truncates the <code>msg</code> field, which helps preserve other log information.</p>	+	+	+	msg="User admin changed dns from GUI (172.20.120.47) "
HTTP Content Routing (conten t_ switch_ name)	The name of the associated HTTP content routing policy.	-	+	+	content_switch_name="httproutes1"
Server Pool (server_ pool_ name)	The name of the server pool in the associated server policy.	-	+	+	server_pool_name="Auto-ServerFarm"
False Positive Mitigation	For violations of SQL injection signatures, specifies whether FortiWeb identified the attack	-	+	-	false_positive_mitigation="yes"

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Eve-nt	Atta-ck	Traf-fic	
false_positive_mitigation	using the signature and additional SQL syntax validation (yes) or the just the signature (no).				
Threat Scoring log_type event_score score_message entry_sequence	Information about the threat score, which FortiWeb generates based on multiple signature violations by a client, instead of a single signature violation. For details, see Attack log fields .	-	+	-	log_type=LOG_TYPE_SCORE_SUM event_score=3 score_message="[score_type: total_score] [score_scope: TCP Session] [score_threshold: 5] [score_sum: 7]" entry_sequence="000139289630"
Detailed Information (N/A)	This column contains the entire log message in raw format. If your Column Settings show this column, the entire raw log message will be included in the row under this column, next to the formatted column view of the same log message. This way, if you want to view the entire raw log message, you can simply scroll the page, instead of switching the entire page back and forth from Raw to Formatted log views. This column appears only when using the Formatted log view. It does not actually exist as a field in the raw logs.	+	+	+	date=2013-10-10 time=00:38:58 log_id=20000051 msg_id=0000000000008...

Log ID numbers

The **ID** (`log_id`) is an 8-digit field located in the header, immediately following the time and date fields.

The `log_id` field is a number assigned to all permutations of the same message. It classifies a log message by the nature of the cause of the log message, such as administrator authentication failures or traffic. Other log messages that share the same cause will share the same `log_id`.

For example, creating an administrator account always has the log ID `00003401`.

Types

Each log message contains a **Type** (`type`) field that indicates its category, and in which log file it is stored.

FortiWeb appliances can record the following categories of log messages:

Log types

Log type	Description
Event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.
Traffic	Records traffic flow information, such as an HTTP/HTTPS request and its response, if any.
Attack	Records attack and intrusion attempts.



Avoid recording highly frequent log types such as traffic logs to the local hard disk for an extended period of time. **Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.**

Subtypes

Each log message contains a **Sub Type** (`subtype`) field that further subdivides its category according to the feature involved with the cause of the log message.

For example:

- In event logs, some may have a `subtype` of `admin`, `system`, or other subtypes.
- In attack logs, they have main type and subtypes to reflect the classification of the attacks.
- In traffic logs, the `subtype` is always `http` even if the service is HTTPS.

Priority level

Each log message contains a **Level** (`pri`) field that indicates the estimated severity of the event that caused the log message, such as `pri=warning`, and therefore how high a priority it is likely to be.



Level (`pri`) associations with the descriptions below are not always uniform. They also may not correspond with **your own** definitions of how severe each event is. If you require notification when a specific event occurs, either configure SNMP traps or alert email by administrator-defined Severity Level (`severity_level`) or ID (`log_id`), **not** by Level (`pri`).

Approximate log priority levels

Level (0 is highest)	Name	Description
0	Emergency	The system has become unusable.
1	Alert	Immediate action is required. Used in attack logs.
2	Critical	Functionality is affected.
3	Error	An error condition exists and functionality could be affected.
4	Warning	Functionality could be affected.
5	Notification	Information about normal events. Used in traffic logs, and in event logs for administrator logins, time changes, and normal daemon actions.
6	Information	General information about system operations. Used in event logs for configuration changes.

For each location where the FortiWeb appliance can store log files (disk, memory, Syslog or FortiAnalyzer), you can define a severity threshold. The FortiWeb appliance will store all log messages equal to or exceeding the log severity level you select.

For example, if you select **Error**, the FortiWeb appliance will store log messages whose log severity level is **Error**, **Critical**, **Alert**, and **Emergency**.



Avoid recording log messages using low log severity thresholds such as information or notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

Message IDs

The **MSG ID** (`msg_id`) field is a 12-digit number located in the header, incremented with each individual log message generated by the FortiWeb appliance. It is used only for numbering each entry in the database, and does not necessarily reflect its cause.

Each `msg_id` number is a unique identifier for that specific log entry. No other log messages, regardless of cause, share the same `msg_id`.

Event

Event log messages record subsystem events such as NTP-based time changes, reboots and RAID level changes. They also record configuration changes.

Unless noted as otherwise in each event log's description:

- **Level** (`pri`) field is `information`
- **User** (`user`) field is the name of the administrator account that caused the event
- **User Interface** (`ui`) field is according to [User Interface on page 10](#)

To go to a sample, additional information, and solution (if applicable) for an event log message, click the **ID** (`log_id`) field in the table.

Event logs by subtype & ID

ID (<code>log_id</code>)	Sub Type (<code>subtype</code>)
00001002	admin
00001012	admin
00001052	admin
00001062	admin
00002202	admin
00002801	admin
00002802	admin
00002811	admin
00003401	admin
00003402	admin
00003411	admin
00003801	admin
00003802	admin
00003811	admin
00004401	admin
00004402	admin
00004411	admin
00004902	admin
00006001	admin

ID (log_id)	Sub Type (subtype)
00006002	admin
00006011	admin
00006102	admin
00006202	admin
00006302	admin
00006501	admin
00006502	admin
00006511	admin
00006541	admin
00006542	admin
00006551	admin
00007302	admin
00007402	admin
00008101	admin
00008102	admin
00008111	admin
00008602	admin
00008701	admin
00008702	admin
00008711	admin
00008801	admin
00008811	admin
00008901	admin
00008911	admin
00009001	admin
00009011	admin
00009101	admin
00009111	admin
00009201	admin
00009211	admin

ID (log_id)	Sub Type (subtype)
00009301	admin
00009311	admin
00009401	admin
00009402	admin
00009411	admin
00009501	admin
00009502	admin
00009511	admin
00009702	admin
00010001	admin
00010002	admin
00010011	admin
00010201	admin
00010202	admin
00010211	admin
00010401	admin
00010402	admin
00010411	admin
00010501	admin
00010502	admin
00010511	admin
00010601	admin
00010602	admin
00010611	admin
00010701	admin
00010711	admin
00011521	admin
00011522	admin
00011531	admin
00011671	admin

ID (log_id)	Sub Type (subtype)
00011672	admin
00011681	admin
00019001	admin
00019011	admin
00019102	admin
00019202	admin
00020088	admin
00020201	admin
00020202	admin
00020211	admin
00020301	admin
00020302	admin
00020311	admin
00020701	admin
00020702	admin
00020711	admin
00020801	admin
00020802	admin
00020811	admin
00020901	admin
00020902	admin
00020911	admin
00021002	admin
00021102	admin
00021140	admin
00021202	admin
00021302	admin
00021402	admin
00022997	admin
00030001	admin

ID (log_id)	Sub Type (subtype)
00030002	admin
00030011	admin
00032006	admin
00039001	admin
00039002	admin
00039011	admin
00039321	admin
00039322	admin
00039331	admin
00040001	admin
00040002	admin
00040011	admin
00040301	admin
00040302	admin
00040311	admin
00040501	admin
00040502	admin
00040511	admin
00040601	admin
00040602	admin
00040611	admin
00040623	admin
00040631	admin
00040632	admin
00040641	admin
00040751	admin
00040752	admin
00040761	admin
00040801	admin
00040802	admin

ID (log_id)	Sub Type (subtype)
00040811	admin
00040901	admin
00040902	admin
00040911	admin
00041001	admin
00041002	admin
00041011	admin
00041101	admin
00041102	admin
00041111	admin
00041201	admin
00041202	admin
00041211	admin
00041302	admin
00041401	admin
00041402	admin
00041411	admin
00041601	admin
00041602	admin
00041611	admin
00041801	admin
00041802	admin
00041811	admin
00042401	admin
00042402	admin
00042411	admin
00043001	admin
00043002	admin
00043011	admin
00044001	admin

ID (log_id)	Sub Type (subtype)
00044002	admin
00044011	admin
00044401	admin
00044411	admin
00044501	admin
00044502	admin
00044511	admin
00046001	admin
00046002	admin
00046011	admin
00050001	admin
00050002	admin
00050011	admin
00050201	admin
00050202	admin
00050211	admin
00050401	admin
00050402	admin
00050411	admin
00051001	admin
00051002	admin
00051011	admin
00051201	admin
00051202	admin
00051211	admin
00051401	admin
00051402	admin
00051411	admin
00051601	admin
00051602	admin

ID (log_id)	Sub Type (subtype)
00051611	admin
00051801	admin
00051802	admin
00051811	admin
00052201	admin
00052202	admin
00052211	admin
00052401	admin
00052402	admin
00052411	admin
00052601	admin
00052602	admin
00052611	admin
00053201	admin
00053202	admin
00053211	admin
00053701	admin
00053711	admin
00053901	admin
00053902	admin
00053911	admin
00054401	admin
00054402	admin
00054411	admin
00054601	admin
00054602	admin
00054611	admin
00054801	admin
00054802	admin
00054811	admin

ID (log_id)	Sub Type (subtype)
00055301	admin
00055302	admin
00055311	admin
00055501	admin
00055502	admin
00055511	admin
00055701	admin
00055702	admin
00055711	admin
00055901	admin
00055902	admin
00055911	admin
00055971	admin
00056401	admin
00056402	admin
00056411	admin
00056421	admin
00056601	admin
00056602	admin
00056611	admin
00058601	admin
00058602	admin
00058611	admin
00058621	admin
00058622	admin
00058631	admin
00059801	admin
00059802	admin
00059811	admin
00060001	admin

ID (log_id)	Sub Type (subtype)
00060002	admin
00060011	admin
00060201	admin
00060202	admin
00060211	admin
00061201	admin
00061202	admin
00061211	admin
00061401	admin
00061402	admin
00061411	admin
00061801	admin
00061802	admin
00061811	admin
00062001	admin
00062002	admin
00062011	admin
00062201	admin
00062202	admin
00062211	admin
00062401	admin
00062402	admin
00062411	admin
00063401	admin
00063402	admin
00063411	admin
00064401	admin
00064402	admin
00064411	admin
00065002	admin

ID (log_id)	Sub Type (subtype)
00065501	admin
00065502	admin
00065511	admin
00066002	admin
00066011	admin
00066101	admin
00066102	admin
00066111	admin
00066151	admin
00066201	admin
00066202	admin
00066211	admin
00066301	admin
00066302	admin
00066311	admin
00066401	admin
00066402	admin
00066411	admin
00066451	admin
00066452	admin
00066461	admin
00066501	admin
00066502	admin
00066511	admin
00066551	admin
00066552	admin
00066561	admin
00066601	admin
00066711	admin
00066801	admin

ID (log_id)	Sub Type (subtype)
00066802	admin
00066811	admin
00066901	admin
00066911	admin
00066921	admin
00066931	admin
00068001	admin
00068002	admin
00068011	admin
00068301	admin
00068302	admin
00068311	admin
00068401	admin
00068402	admin
00068411	admin
00068701	admin
00068711	admin
00068801	admin
00068802	admin
00068811	admin
00090001	admin
00090002	admin
00090011	admin
00090101	admin
00090102	admin
00090111	admin
00091101	admin
00091102	admin
00091111	admin
00093001	admin

ID (log_id)	Sub Type (subtype)
00093002	admin
00093011	admin
00093501	admin
00093502	admin
00093511	admin
10000009	system
10000010	system
10000011	system
10000012	system
10000013	system
10000014	system
10000015	system
10000016	system
10000017	system
10000018	system
10000019	system
10000020	system
10000021	system
10000022	system
10000023	system
10000027	system
10000028	system
10000031	system
10000048	system
11001008	system
11002003	system
11002004	system
11003601	system
11004002	system
11004601	system

ID (log_id)	Sub Type (subtype)
11004602	system
11004603	system
11004605	system
11004606	system
11004608	system
11005901	system
11006004	system
11006005	system
11006006	system
11006701	system
19999496	system
19999497	system
19999498	system

Attack

Attack log messages record traffic that violated its matching policy. Log ID numbers of this type are listed in the table [Attack logs by main type, subtype & ID](#).

The operating mode, network topology, and the rule's configured **Action** can all affect how a policy responds to an attack, data leak, or server information disclosure. Depending on your configuration, violating traffic is either:

- blocked
- sanitized, then passed through
- allowed to continue unmodified (that is, logged only)

Attacks that generate log messages periodically

FortiWeb does not record the following types of attack logs individually. Instead, it records them periodically while the attack is ongoing, even if the attack has multiple sources:

- DoS attacks
- Padding oracle attacks
- HTTP/HTTPS protocol constraints

This aggregation prevents FortiWeb from flooding attack logs with identical or very similar messages. To differentiate logs caused by individual attacks from those caused by multiple attacks in the same category, FortiWeb records whether it generated the attack log message after matching multiple signatures.

In the attack log, the message field of aggregated log messages displays the message `rule_name : Custom Access Violation`.

In aggregated attacks log, the type field displays the message `Multiple Custom access rule Violations`.

Logging for threat scoring

By default, FortiWeb does not display all signature violations that contributed to a threat scoring attack log message as individual entries in the attack log. Instead, a single attack log message is displayed for the signature violations that contributed to a combined threat score that exceeded the maximum. However, all the signature violations that contributed to the score are displayed in the message details. (Double-click the message to display its details.)

Also by default, FortiWeb does not display messages for signature violations that generated a threat score but did not exceed the threat scoring threshold.

Use the following CLI command to display the signature violations that contributed to a threat scoring attack log message as individual entries and to display any signature violations that generated a threat score but did not exceed the threat scoring threshold:

```
config log attack-log
set show-all-log {enable | disable}
```

For more information on CLI commands, see *FortiWeb CLI Reference*:

<http://docs.fortinet.com/fortiweb/reference>

Threat scoring attack log messages are also displayed in the aggregated attacks log.

Attack log descriptions

To locate a description for an attack log message, match the **ID** (`log_id`) field in the attack log message with that shown in the table [Attack logs by main type, subtype & ID on page 34](#). All attack log messages have the same body fields, described in "Attack log fields" on page 1.

For attack log messages generated by a HTTP protocol constraint, the associated policy name is displayed in the raw view (`[policy_name:<protocol_constraint_name>]`) but not in the formatted view.

Attack logs by main type, subtype & ID

ID	main type	sub-type
20000001	Allow Method	N/A
20000002	Protected Hostnames	N/A
20000003	Page Access	N/A
20000004	Start Pages	N/A
20000005	Parameter Validation	N/A
20000006	Black IP List	N/A
20000007	URL Access	N/A
20000008	Signature Detection	<ul style="list-style-type: none"> • Cross Site Scripting • Cross Site Scripting (Extended) • Generic Attacks • Generic Attacks (Extended) • Bad Robot • Information Disclosure • Known Exploits • SQL Injection • SQL Injection (Extended) • SQL Injection (Syntax Based Detection) • Personally Identifiable Information • Trojans
20000009	Custom Signature Detection	N/A
20000011	Hidden Fields	N/A
20000012	Site Publish	Account Lockout
20000014	DoS Protection	<ul style="list-style-type: none"> • HTTP Flood Prevention • Malicious IPs • HTTP Access Limit • TCP Flood Prevention

ID	main type	sub-type
20000015	SYN Flood Protection	N/A
20000016	HTTPS Connection Failure	N/A
20000017	File Upload Restriction	<ul style="list-style-type: none"> • Antivirus Detection • Trojan Detection • FortiSandbox Detection • Illegal File Type • Illegal File Size
20000018	GEO IP	N/A
20000021	Custom Access	<ul style="list-style-type: none"> • Predefined-Crawler • Predefined-Vulnerability Scanning • Predefined-Slow-Attack • Predefined-Content-Scraping
20000022	IP Reputation	<ul style="list-style-type: none"> • Botnet • Anonymous Proxy • Phishing • Spam • Tor • Others
20000023	Padding Oracle	N/A
20000024	CSRF Protection	N/A
20000025	Quarantined IPs	N/A
20000026	HTTP Protocol Constraints	<ul style="list-style-type: none"> • Header Length Violation • Header Line Violation • Body Length Violation • Content Length Violation • Parameter Length Violation • HTTP Request Length Violation • URL Parameter Length Violation • Illegal HTTP Version • Cookie Number Overflow • Request Header Line number Overflow • URL Parameter Number Overflow • Illegal Hostname • Range Header Violation • Illegal HTTP Method • Illegal Content Length • Illegal Content Type • Illegal Response Code

ID	main type	sub-type
		<ul style="list-style-type: none"> • Missing POST Content Type • Body Parameter Length Violation • Header Name Length Violation • Header Value Length Violation • NULL Character in Parameter Name • NULL Character in Paramter Value • Illegal Header Name • Illegal Header Value • HTTP Request Filename Violation • Web Socket Protocol • Illegal Frame Type • Illegal Frame Flag • Illegal Connection Preface • HTTP/2 Header Table Size Overflow • HTTP/2 Concurrent Stream Number Overflow • HTTP/2 Initial Window Size Overflow • HTTP/2 Frame Size Overflow • HTTP/2 Header List Overflow • Illegal URL Parameter Name • Illegal URL Parameter Value • URL Parameter Name Overflow • URL Parameter Value Overflow • NULL Character in URL • Illegal Character in URL • Redundant HTTP Header • Malformed URL • Illegal Chunk Size • HTTP Parsing Error • HTTP Duplicated Parameter Name • Odd and Even Space Attack
20000027	Credential Stuffing Defense	<ul style="list-style-type: none"> • User Tracking • Site Publish
20000028	User Tracking	N/A
20000029	XML Validation Violation	<ul style="list-style-type: none"> • XML Schema Validation Violation • XML Element Attribute Number Overflow • XML Element Attribute Name Length Violations • XML Element Attribute Value Length Violations • XML Element Cdata Length Violations • XML Element Depth Violations • XML Element Name Length Violations • XML External Entity Violation • XML Entity Expansion Violations • XML XInclude Violation

ID	main type	sub-type
		<ul style="list-style-type: none"> XML SchemaLocation Violation XML SOAP Protocol Violation XML SOAPAction Violation XML SOAP Header Violation XML SOAP Body Violation SOAP Signature Error SOAP Signature Verification Error SOAP Encryption Error SOAP Decryption Error
20000030	Cookie Security	<ul style="list-style-type: none"> Cookie Decryption Error Cookie Signed Verification Failed IP replay protection violation
20000031	FTP Command Restriction	N/A
20000033	Timeout Session	N/A
20000035	FTP File Security	<ul style="list-style-type: none"> FTP Antivirus Detection FTP FortiSandbox Detection
20000036	FTPS Connection Failure	N/A
20000037	Machine Learning	<ul style="list-style-type: none"> Anomaly in http argument HTTP Method violation Charset detect failed
20000038	Openapi Validation Violation	<ul style="list-style-type: none"> Openapi Query Parameter Violation Openapi Path Parameter Violation Openapi Cookie Parameter Violation Openapi Header Parameter Violation Openapi Request Body Violation
20000039	WebSocket Security	<ul style="list-style-type: none"> Disallow WebSocket Disallow Extensions Illegal Format Illegal Frame Size Illegal Message Size Disallow Origin Parse error
20000040	MiTB AJAX Security	N/A
20000041	Bot Detection	N/A
20000042	CORS Check Security	<ul style="list-style-type: none"> Invalid Origin Disallow CORS Disallow Origin

ID	main type	sub-type
		<ul style="list-style-type: none"> Disallow method Disallow header
20000043	JSON Validation Security	<ul style="list-style-type: none"> JSON Schema Validation Violation JSON Format Invalid Violation JSON Data Size Violation JSON Key Size Violation JSON Key Number Violation JSON Value Size Violation JSON Value Number Violation JSON Value Number in Array Violation JSON Object Depth Violation

20000001

Meaning

HTTP Method Violation

Field name	Description
log_id	20000001 See Log ID numbers on page 16 .
main_type	Allow Method
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=10:16:34 log_id=20000001 msg_id=000000225550 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Allow Method" sub_type="N/A" trigger_policy="" severity_level=Low proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=61330 dst=10.101.0.1 dst_port=80 http_method=trace http_url="/74lyJ2d0QY" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="HTTP Method Violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A6:2017-Security Misconfiguration"
```

20000002

Meaning

Protected Hostnames violation

Field name	Description
log_id	20000002 See Log ID numbers on page 16 .
main_type	Protected Hostnames
subtype	N/A

Examples

```
v009xxxxdate=2019-09-21 time=06:57:02 log_id=20000002 msg_id=000034349837 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="Protected Hostnames" sub_type="N/A"
trigger_policy="" severity_level=Low proto=tcp service=http backend_service=unknown action=Alert_
Deny policy="FWB_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=56756 dst=10.114.0.1 dst_
port=80 http_method=get http_url="/autotest/dwg/common.html" http_host="10.0.0.22:8080" http_
agent="python-for-fortiweb" http_session_id=None msg="HTTP Host Violation" signature_subclass="N/A"
signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_
pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_
status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_
threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_
probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000
ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_
accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_
top10="A6:2017-Security Misconfiguration" bot_info="none"
```

20000003

Meaning

Page Access Rule Violation.

Field name	Description
log_id	20000003 See Log ID numbers on page 16 .
main_type	Page Access
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=13:17:43 log_id=20000003 msg_id=000000268842 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Page Access" sub_type="N/A" trigger_policy="" severity_level=High proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=52970 dst=10.101.0.1 dst_port=80 http_method=get http_url="/AUTOTEST/page_access/7.html" http_host="fortinet.fortiwab.com" http_agent="python-for-fortiwab" http_session_id=32D5D781HT1HRR9IV948UYOHNVMY9030 msg="Page Access Rule Violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A6:2017-Security Misconfiguration"
```

20000004

Meaning

Start Page Violation.

Field name	Description
log_id	20000004 See Log ID numbers on page 16 .
main_type	Start Pages
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=13:18:30 log_id=20000004 msg_id=000000269047 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Start Pages" sub_type="N/A" trigger_policy="" severity_level=Low proto=tcp service=http action=Alert policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=53128 dst=10.101.0.1 dst_port=80 http_method=get http_url="/autotest/test2.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Start Page Violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A6:2017-Security Misconfiguration"
```

20000005

Meaning

Parameter name - (URI) triggered paramater validation.

Field name	Description
log_id	20000005 See Log ID numbers on page 16 .
main_type	Parameter Validation
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=13:26:14 log_id=20000005 msg_id=000000270760 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Parameter Validation" sub_type="N/A" trigger_policy="" severity_level=Low proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=54777 dst=10.101.0.1 dst_port=80 http_method=get http_url="/autotest/dwg/common.html?input=88888" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Parameter name - (input) triggered paramater validation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=30 history_threat_weight=0 threat_level=High ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A6:2017-Security Misconfiguration"
```

20000006

Meaning

IP in black list was blocked.

Field name	Description
log_id	20000006 See Log ID numbers on page 16 .
main_type	Black IP List
subtype	N/A

Examples

```
v007xxxxdate=2019-08-02 time=22:42:11 log_id=20000006 msg_id=000000083367 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Black IP List" sub_type="N/A" trigger_policy="" severity_level=High proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=50744 dst=10.101.0.1 dst_port=80 http_method=get http_url="/autotest/test1.html" http_host="10.0.0.22:8080" http_agent="python-for-fortiweb" http_session_id=none msg="IP in black list was blocked" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" s_rccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=30 history_threat_weight=0 threat_level=High ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A"
```

20000007

Meaning

URL Access rule violation

Field name	Description
log_id	20000007 See Log ID numbers on page 16 .
main_type	URL Access
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=10:16:18 log_id=20000007 msg_id=000000225382 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="URL Access" sub_type="N/A" trigger_policy="" severity_level=Low proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=61304 dst=10.101.0.1 dst_port=80 http_method=get http_url="/php/test.php" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="URL Access rule (FWB_protection_profile-6) violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A5:2017-Broken Access Control"
```

20000008

Meaning

Parameter, URL, or other elements in the packets triggered signatures included in the signature policy.

Field name	Description
log_id	20000008 See Log ID numbers on page 16 .
main_type	Signature Detection
subtype	<ul style="list-style-type: none"> • Cross Site Scripting • Cross Site Scripting (Extended) • Generic Attacks • Generic Attacks (Extended) • Bad Robot • Information Disclosure • Known Exploits • SQL Injection • SQL Injection (Extended) • SQL Injection (Syntax Based Detection) • Personally Identifiable Information • Trojans

Examples

```
v007xxxxdate=2019-08-03 time=10:17:12 log_id=20000008 msg_id=000000225902 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Signature Detection" sub_type="Cross Site Scripting" trigger_policy="" severity_level=High proto=tcp service=http action=Alert policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=61385 dst=10.101.0.1 dst_port=80 http_method=get http_url="/examples/jsp/snp/snoop.jsp??picfilename=image_w3default.gif onmousedown="alert('xss success')"&passwd=&ok" http_host="fortinet.fortiwab.com" http_agent="python-for-fortiwab" http_session_id=none msg="Parameter(?picfilename) triggered signature ID 010000063 of Signatures policy Scanner Integration" signature_subclass="Cross Site Scripting" signature_id="010000063" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=30 history_threat_weight=0 threat_level=High ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A7:2017-Cross-Site Scripting (XSS)"
```

20000009

Meaning

custom signature rule violation.

Field name	Description
log_id	20000009 See Log ID numbers on page 16 .
main_type	Custom Signature Detection
subtype	N/A

Examples

```
v007xxxxdate=2019-08-02 time=20:38:36 log_id=20000009 msg_id=000000042790 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Custom Signature Detection" sub_type="N/A" trigger_policy="" severity_level=High proto=tcp service=http action=Alert policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=59778 dst=10.101.0.1 dst_port=80 http_method=get http_url="/autotest/test.html?para1=auto1test" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Parameter triggered custom signature rule FWB_custom_protection_rule" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=30 history_threat_weight=0 threat_level=High ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A"
```

20000010

Meaning

Brute Force Login Violation

Field name	Description
log_id	20000010 See Log ID numbers on page 16 .
main_type	Brute Force Login
subtype	<ul style="list-style-type: none"> Based on TCP Session Based on Source IP

Examples

```
v007xxxxdate=2019-08-02 time=23:24:16 log_id=20000010 msg_id=000000098389 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Brute Force Login" sub_type="Based on TCP Session" trigger_policy="" severity_level=High proto=tcp service=http action=Period_Block policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=57948 dst=10.0.1.5 dst_port=80 http_method=post http_url="/autotest/site_publishing_helper/login_check/0" http_host="fbqa-win2k3.fbqa.com" http_agent="python-for-fortiweb" http_session_id=None msg="Brute Force Login Violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool_10.0.1.5" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=50 history_threat_weight=0 threat_level=Critical ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A2:2017-Broken Authentication"
```

20000011

Meaning

Hidden Field Manipulation

Field name	Description
log_id	20000011 See Log ID numbers on page 16 .
main_type	Hidden Fields
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=00:54:36 log_id=20000011 msg_id=000000124602 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Hidden Fields" sub_type="N/A" trigger_policy="" severity_level=High proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=52513 dst=10.101.0.1 dst_port=80 http_method=post http_url="/autotest/price.jsp" http_host="fortinet.fortiwab.com" http_agent="python-for-fortiwab" http_session_id=FFFFFFFFFNJLRBBMQB9CDNEZOWKXLBB5C msg="Hidden Field Manipulation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=30 history_threat_weight=0 threat_level=High ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A6:2017-Security Misconfiguration"
```

20000012

Meaning

User defined in site publish has been locked out.

Field name	Description
log_id	20000012 See Log ID numbers on page 16 .
main_type	Site Publish
subtype	Account Lockout See Subtypes on page 16 .

Examples

```
v007xxxxdate=2019-08-03 time=13:38:38 log_id=20000012 msg_id=000000274786 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Site Publish" sub_type="Account Lockout" trigger_policy="" severity_level=Low proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=56642 dst=10.0.1.5 dst_port=80 http_method=post http_url="/autotest/site_publishing_helper/login_check/0" http_host="fwbqa-win2k3.fwbqa.com" http_agent="python-for-fortiweb" http_session_id=None msg="User qa002 [Site Publish] has been locked out" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool_10.0.1.5" false_positive_mitigation="none" user_name="qa002" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A2:2017-Broken Authentication"
```

20000013

Meaning

HTTP Parsing Error.

Field name	Description
log_id	20000013 See Log ID numbers on page 16 .
main_type	HTTP Parsing Error
subtype	HTTP Parsing Error

Examples

```
v009xxxxdate=2019-09-23 time=11:20:29 log_id=20000013 msg_id=000034681747 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="HTTP Parsing Error" sub_type="HTTP
Parsing Error" trigger_policy="" severity_level=Low proto=tcp service=http backend_service=unknown
action=Alert policy="FWB_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=56020
dst=10.114.0.1 dst_port=80 http_method=get http_url="none" http_host="none" http_agent="none" http_
session_id=none msg="Too Many Parameters" signature_subclass="N/A" signature_id="N/A" signature_
cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="none" false_
positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_
version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_
mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_
prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_
types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0
ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none"
```

20000014

Meaning

DoS protection violation.

Field name	Description
log_id	20000014 See Log ID numbers on page 16 .
main_type	DoS Protection
subtype	<ul style="list-style-type: none"> • HTTP Flood Prevention • Malicious IPs • HTTP Access Limit • TCP Flood Prevention

Examples

```
v009xxxxdate=2019-09-23 time=11:20:42 log_id=20000014 msg_id=000034681947 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="DoS Protection" sub_type="TCP Flood
Prevention" trigger_policy="" severity_level=High proto=tcp service=http backend_service=tcp
action=Period_Block policy="FWB_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=56039
dst=10.114.0.1 dst_port=443 http_method=none http_url="none" http_host="none" http_agent="none"
http_session_id=none msg="TCP Flood Prevention Violation" signature_subclass="N/A" signature_
id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_
name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_
status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" es=0 threat_weight=0
history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_
hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_
mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_
svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none"
owasp_top10="N/A" bot_info="none"
```

20000015

Meaning

Field name	Description
log_id	20000015 See Log ID numbers on page 16 .
main_type	SYN Flood Protection
subtype	N/A

Examples

```
v009xxxxdate=2019-09-27 time=16:20:06 log_id=21000015 msg_id=000306703852 device_id=FV-3KE3217000031 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="SYN Flood Protection" sub_type="N/A" trigger_policy="" severity_level=Low proto=tcp service=tcp backend_service=tcp action=Alert policy="" src=0.0.0.0 src_port=0 dst=10.200.10.115 dst_port=0 http_method=none http_url="none" http_host="none" http_agent="none" http_session_id=none msg="DoS Attack: SYN Flood" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Unknown" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none"
```

20000016

Meaning

HTTPS Connection Failure.

Field name	Description
log_id	20000016 See Log ID numbers on page 16 .
main_type	HTTPS Connection Failure
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=14:00:27 log_id=20000016 msg_id=000000288836 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="HTTPS Connection Failure" sub_type="N/A" trigger_policy="" severity_level=Low proto=tcp service=https/tls1.2 action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=64643 dst=10.200.10.111 dst_port=443 http_method=none http_url="none" http_host="none" http_agent="none" http_session_id=none msg="SSL Error(267) - wrong version number" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A"
```

20000017

Meaning

File upload restrictions violation

Field name	Description
log_id	20000017 See Log ID numbers on page 16 .
main_type	File Upload Restriction
subtype	<ul style="list-style-type: none"> • Antivirus Detection • Trojan Detection • FortiSandbox Detection • Illegal File Type • Illegal File Size

Examples

```
v007xxxxdate=2019-08-02 time=22:38:50 log_id=20000017 msg_id=000000079768 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="File Upload Restriction" sub_type="Illegal File Type" trigger_policy="" severity_level=Medium proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=63865 dst=10.101.0.1 dst_port=80 http_method=post http_url="/upload/servlet/UploadServlet" http_host="10.0.0.147:8090" http_agent="Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)" http_session_id=none msg="filename [filup.pdf]: Illegal file type" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="http://10.12.0.39:1001/upload/~upload" http_version="1.x" dev_id="none" threat_weight=30 history_threat_weight=0 threat_level=High ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A6:2017-Security Misconfiguration"
```

20000018

Meaning

Unauthorized Geo IP.

Field name	Description
log_id	20000018 See Log ID numbers on page 16 .
main_type	GEO IP
subtype	N/A

Examples

```
v009xxxxdate=2019-09-21 time=05:34:41 log_id=20000018 msg_id=000034329692 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="GEO IP" sub_type="N/A" trigger_policy=""
severity_level=Low proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_
Policy_Default_AutoTest_ttp" src=60.28.176.170 src_port=65379 dst=10.114.0.1 dst_port=80 http_
method=get http_url="/" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_
session_id=none msg="Unauthorized Geo IP from United States was not allowed" signature_
subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="United States" content_switch_
name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_
name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0
threat_weight=30 history_threat_weight=0 threat_level=High ftp_mode="N/A" ftp_cmd="N/A" cipher_
suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_
sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_
types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_
method="none" owasp_top10="N/A" bot_info="none"
```

20000021

Meaning

Custom Access rule violation

Field name	Description
log_id	20000021 See Log ID numbers on page 16 .
main_type	Custom Access
subtype	<ul style="list-style-type: none"> • Predefined-Crawler • Predefined-Vulnerability Scanning • Predefined-Slow-Attack • Predefined-Content-Scraping

Examples

```
v007xxxxdate=2019-08-03 time=01:20:56 log_id=20000021 msg_id=000000131425 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Custom Access" sub_type="N/A" trigger_policy="" severity_level=Medium proto=tcp service=http action=Alert policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=55799 dst=10.101.0.1 dst_port=80 http_method=get http_url="/autotest/test.html" http_host="fortinet.fortiwab.com" http_agent="python-for-fortiwab" http_session_id=none msg="Custom Access rule (custom_access_rule) violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=30 history_threat_weight=0 threat_level=High ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A"
```

20000022

Meaning

IP reputation violation.

Field name	Description
log_id	20000022 See Log ID numbers on page 16 .
main_type	IP Reputation
subtype	<ul style="list-style-type: none"> • Botnet • Anonymous Proxy • Phishing • Spam • Tor • Others

Examples

```
v009xxxxdate=2019-09-21 time=12:51:52 log_id=20000022 msg_id=000034397278 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="IP Reputation" sub_type="Anonymous
Proxy" trigger_policy="" severity_level=Low proto=tcp service=http backend_service=unknown
action=Alert_Deny policy="FWB_Policy_Default_AutoTest_ttp" src=154.73.109.83 src_port=50708
dst=154.73.109.165 dst_port=80 http_method=post http_url="/autotest/test.html?a=@import" http_
host="fortinet.fortiwab.com" http_agent="python-for-fortiwab" http_session_id=none msg="Bad IP
triggered ip reputation category Anonymous Proxy" signature_subclass="N/A" signature_id="N/A"
signature_cve_id="N/A" srccountry="Libya" content_switch_name="none" server_pool_name="FWB_
server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_
refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=50 history_threat_weight=0 threat_
level=Critical ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000
ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_
svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_
index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none"
```

20000023

Meaning

Padding Oracle Attack.

Field name	Description
log_id	20000023 See Log ID numbers on page 16 .
main_type	Padding Oracle
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=07:37:43 log_id=20000023 msg_id=000000201150 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Padding Oracle" sub_type="N/A" trigger_policy="" severity_level=Medium proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=53807 dst=10.101.0.1 dst_port=80 http_method=get http_url="/autotest/bruteforce/raw.html?uid=000000000000xSd8Qu5Jotox2Oyn7E0GRpGckz-uozJfKxzyZh3FlnBA6rw8JO2FISDG5NpWAXBSAzlcKK2SfLGcYJnEuYg7n8i1LjPpC8Q=" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Padding Oracle Attack" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=50 history_threat_weight=0 threat_level=Critical ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A9:2017-Using Components with Known Vulnerabilities"
```

Related

- [00040001](#)
- [00040002](#)
- [00040011](#)

20000024

Meaning

CSRF Detection.

Field name	Description
log_id	20000024 See Log ID numbers on page 16 .
main_type	CSRF Protection
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=08:14:27 log_id=20000024 msg_id=000000203862 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="CSRF Protection" sub_type="N/A" trigger_policy="" severity_level=Low proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=55269 dst=10.101.0.1 dst_port=80 http_method=get http_url="/autotest/CSRF/request_information.php?a=100&tkfv=xx3D9671241PBUEX6HI9YPTULP5AEGB80Dxx" http_host="10.0.0.22:8080" http_agent="python-for-fortiweb" http_session_id=3D9671241PBUEX6HI9YPTULP5AEGB80D msg="CSRF Detection" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=30 history_threat_weight=0 threat_level=High ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A5:2017-Broken Access Control"
```

20000025

Meaning

Quarantined IPs.

Field name	Description
log_id	20000025 See Log ID numbers on page 16 .
main_type	Quarantined IPs
subtype	N/A

Examples

```
date=2019-09-27 time=16:20:26 log_id=20000025 msg_id=000000271216 device_id=FV-1KE4417900091 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Quarantined IPs" sub_type="N/A" trigger_policy="" severity_level=High proto=tcp service=http backend_service=tcp action=Alert policy="FWB_Policy_Default_AutoTest" src=10.51.1.13 src_port=60500 dst=10.51.1.241 dst_port=8090 http_method=none http_url="none" http_host="none" http_agent="none" http_session_id=none msg="FortiGate Quarantined IP- A new connection from a FortiGate Quarantined IP address 10.51.1.13:60500" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none"
```

20000026

Meaning

HTTP Protocol Constraints violation.

Field name	Description
log_id	20000026 See Log ID numbers on page 16 .
main_type	HTTP Protocol Constraints
subtype	<ul style="list-style-type: none"> • Header Length Violation • Header Line Violation • Body Length Violation • Content Length Violation • Parameter Length Violation • HTTP Request Length Violation • URL Parameter Length Violation • Illegal HTTP Version • Cookie Number Overflow • Request Header Line number Overflow • URL Parameter Number Overflow • Illegal Hostname • Range Header Violation

Field name	Description
	<ul style="list-style-type: none">• Illegal HTTP Method• Illegal Content Length• Illegal Content Type• Illegal Response Code• Missing POST Content Type• Body Parameter Length Violation• Header Name Length Violation• Header Value Length Violation• NULL Character in Parameter Name• NULL Character in Parameter Value• Illegal Header Name• Illegal Header Value• HTTP Request Filename Violation• Web Socket Protocol• Illegal Frame Type• Illegal Frame Flag• Illegal Connection Preface• HTTP/2 Header Table Size Overflow• HTTP/2 Concurrent Stream Number Overflow• HTTP/2 Initial Window Size Overflow• HTTP/2 Frame Size Overflow• HTTP/2 Header List Overflow• Illegal URL Parameter Name• Illegal URL Parameter Value• URL Parameter Name Overflow• URL Parameter Value Overflow• NULL Character in URL• Illegal Character in URL• Redundant HTTP Header• Malformed URL• Illegal Chunk Size• HTTP Parsing Error• HTTP Duplicated Parameter Name• Odd and Even Space Attack

Examples

```
v007xxxxdate=2019-08-03 time=10:16:50 log_id=20000026 msg_id=000000225718 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="HTTP Protocol Constraints" sub_type="Header Name Length Violation" trigger_policy="" severity_level=High proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=61358 dst=10.101.0.1 dst_port=80 http_method=get http_url="/" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="[policy_name=FWB_protection_profile] : Header Name Length Exceeded: (The HTTP header name length (51) exceeded the maximum allowed - 50)" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A6:2017-Security Misconfiguration"
```

20000027

Meaning

Credential stuffing defense violation.

Field name	Description
log_id	20000027 See Log ID numbers on page 16 .
main_type	Credential Stuffing Defense
subtype	<ul style="list-style-type: none"> User Tracking Site Publish

Examples

```
v009xxxxdate=2019-09-21 time=12:55:57 log_id=20000027 msg_id=000034399096 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="Credential Stuffing Defense" sub_
type="User Tracking" trigger_policy="" severity_level=Informative proto=tcp service=http backend_
service=unknown action=Alert policy="FWB_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_
port=51271 dst=10.114.0.1 dst_port=80 http_method=post http_url="/autotest/user_tracking/login.php"
http_host="login.fwbqa.com" http_agent="python-for-fortiweb" http_session_id=none msg="Triggered by
user bjrehdorf@hotmail.com : Credential Stuffing Defense Violation" signature_subclass="N/A"
signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_
pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_
status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=10 history_
threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_
hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_
mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_
svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none"
owasp_top10="A3:2017-Sensitive Data Exposure" bot_info="none"
```

20000028

Meaning

User tracking rules violation.

Field name	Description
log_id	20000028 See Log ID numbers on page 16 .
main_type	User Tracking
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=13:42:24 log_id=20000028 msg_id=000000275262 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="User Tracking" sub_type="N/A" trigger_policy="" severity_level=Low proto=tcp service=http action=Alert policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=57030 dst=10.101.0.1 dst_port=80 http_method=get http_url="/autotest/serverfarm/belonghost.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Triggered by user user4 : Session Timeout Enforcement" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="user4" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A5:2017-Broken Access Control"
```

20000029

Meaning

XML Validation Violation.

Field name	Description
log_id	20000029 See Log ID numbers on page 16 .
main_type	XML Validation Violation
subtype	<ul style="list-style-type: none"> XML Schema Validation Violation XML Element Attribute Number Overflow XML Element Attribute Name Length Violations XML Element Attribute Value Length Violations XML Element Cdata Length Violations XML Element Depth Violations XML Element Name Length Violations XML External Entity Violation XML Entity Expansion Violations XML XInclude Violation XML SchemaLocation Violation XML SOAP Protocol Violation XML SOAPAction Violation

Field name	Description
	<ul style="list-style-type: none"> • XML SOAP Header Violation • XML SOAP Body Violation • SOAP Signature Error • SOAP Signature Verification Error • SOAP Encryption Error • SOAP Decryption Error

Examples

```
v007xxxxdate=2019-08-03 time=12:18:31 log_id=20000029 msg_id=000000251750 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="XML Validation Violation" sub_type="XML Schema Validation Violation" trigger_policy="" severity_level=Medium proto=tcp service=http action=Alert policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=50895 dst=10.101.0.1 dst_port=80 http_method=post http_url="/testPath" http_host="172.22.6.4:8080" http_agent="none" http_session_id=none msg="XML Schema Validation Violation : Failed to validate schema schemaSingle.xsd" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A"
```

20000030

Meaning

Cookie Security violation.

Field name	Description
log_id	20000030 See Log ID numbers on page 16 .
main_type	Cookie Security
subtype	<ul style="list-style-type: none"> • Cookie Decryption Error • Cookie Signed Verification Failed • IP replay protection violation

Examples

```
v007xxxxdate=2019-08-03 time=13:09:31 log_id=20000030 msg_id=000000260055 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Cookie Security" sub_type="Cookie Signed Verification Failed" trigger_policy="" severity_level=High proto=tcp service=http action=Alert policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=60533 dst=10.101.0.1 dst_port=80 http_method=post http_url="/autotest/multicookie.php" http_host="fortinet.fortiwab.com" http_agent="python-for-fortiwab" http_session_id=32D5D77FTV9D5OXVBFQ7GFNBH2I03C1F msg="Cookie name (vimay), signed verification failed; [123 -> 123456]; Domain: fortinet.fortiwab.com; Path: /autotest/" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=30 history_threat_weight=0 threat_level=High ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A5:2017-Broken Access Control"
```

20000031

Meaning

FTP Command Restriction.

Field name	Description
log_id	20000031 See Log ID numbers on page 16 .
main_type	FTP Command Restriction
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=12:59:58 log_id=20000031 msg_id=000000259165 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="FTP Command Restriction" sub_type="N/A" trigger_policy="" severity_level=High proto=tcp service=ftp action=Alert policy="FWB_FTP_Policy" src=10.200.10.100 src_port=59713 dst=10.200.10.114 dst_port=21 http_method=RETR http_url="none" http_host="none" http_agent="none" http_session_id=none msg="FTP command RETR is Illegal command type" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FTP_ServerPool" false_positive_mitigation="none" user_name="vimay2" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="Passive" ftp_cmd="RETR /123.txt" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A"
```

20000033

Meaning

Session was timed out.

Field name	Description
log_id	20000033 See Log ID numbers on page 16 .
main_type	Timeout Session
subtype	N/A

Examples

```
v009xxxxdate=2019-09-21 time=02:49:44 log_id=20000033 msg_id=000034295233 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="Timeout Session" sub_type="N/A" trigger_
policy="" severity_level=Low proto=tcp service=http backend_service=tcp action=Alert_Deny
policy="FWB_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=51347 dst=10.114.0.1 dst_
port=80 http_method=none http_url="none" http_host="none" http_agent="none" http_session_id=none
msg="Received 0 byte since this connection established" signature_subclass="N/A" signature_id="N/A"
signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="none"
false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none"
http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_
mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_
prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_
types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0
ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none"
```

20000035

Meaning

FTP File Security violation.

Field name	Description
log_id	20000035 See Log ID numbers on page 16 .
main_type	FTP File Security
subtype	<ul style="list-style-type: none"> FTP Antivirus Detection FTP FortiSandbox Detection

Examples

```
v009xxxxdate=2019-09-27 time=16:17:03 log_id=20000035 msg_id=000007146026 device_id=FV-1KE4417900002 vd="adomain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="FTP File Security" sub_type="FTP Antivirus Detection" trigger_policy="" severity_level=Medium proto=tcp service=ftp backend_service=ftp action=Alert policy="FWB_FTP_Policy" src=10.200.10.200 src_port=56714 dst=10.200.10.114 dst_port=49655 http_method=STOR http_url="none" http_host="none" http_agent="none" http_session_id=none msg="filename [level3.zip] virus name [Jerusalem.2080]: FTP file security virus violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FTP_ServerPool" false_positive_mitigation="none" user_name="vimay2" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" es=0 threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="Passive" ftp_cmd="STOR /level3.zip" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none"
```

20000036

Meaning

FTPS connection failure.

Field name	Description
log_id	20000036 See Log ID numbers on page 16 .
main_type	FTPS Connection Failure
subtype	N/A

Examples

```
v007xxxxdate=2019-08-03 time=16:40:01 log_id=20000036 msg_id=000000345704 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="FTPS Connection Failure" sub_type="N/A" trigger_policy="" severity_level=Low proto=tcp service=ftps action=Alert_Deny policy="FWB_FTP_Policy" src=10.200.10.100 src_port=58278 dst=10.200.10.114 dst_port=21 http_method=AUTH http_url="none" http_host="none" http_agent="none" http_session_id=none msg="SSL Error(1070) - tlsv1 alert protocol version" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FTP_ServerPool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="Positive" ftp_cmd="AUTH /" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A"
```

20000037

Meaning

Machine Learning anomaly detection violation.

Field name	Description
log_id	20000037 See Log ID numbers on page 16 .
main_type	Machine Learning
subtype	<ul style="list-style-type: none"> Anomaly in http argument HTTP Method violation Charset detect failed

Examples

```
v007xxxxdate=2019-08-03 time=13:15:52 log_id=20000037 msg_id=000000265622 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Machine Learning" sub_type="HTTP Method violation" trigger_policy="" severity_level=High proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=49825 dst=10.101.0.1 dst_port=80 http_method=post http_url="/autotest/mlhan/test.html?mypara=12345" http_host="mydefault.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=None msg="Machine Learning - Allow Method violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=0 history_threat_weight=0 threat_level=Critical ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=17217361460600949737 ml_url_dbid=4 ml_arg_dbid=0 ml_allow_method="GET:2;" owasp_top10="A6:2017-Security Misconfiguration"
```

20000038

Meaning

OpenAPI validation violation.

Field name	Description
log_id	20000038 See Log ID numbers on page 16 .
main_type	Openapi Validation Violation
subtype	<ul style="list-style-type: none"> • Openapi Query Parameter Violation • Openapi Path Parameter Violation • Openapi Cookie Parameter Violation • Openapi Header Parameter Violation • Openapi Request Body Violation

Examples

```
v009xxxxdate=2019-09-21 time=07:53:22 log_id=20000038 msg_id=000034364271 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="Openapi Validation Violation" sub_
type="Openapi Header Parameter Violation" trigger_policy="" severity_level=Low proto=tcp service=http
backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest_ttp"
src=10.114.0.102 src_port=63445 dst=10.114.0.1 dst_port=80 http_method=get http_
url="/inheader/requiredfalse/false?pid=30" http_host="www.openapi.io" http_agent="python-for-fortiweb"
http_session_id=none msg="API Validation violation - Header parameter "X-FWB-HEADER" validation
failure, Failed to validate schema in-header-required-false-type-boolean.yaml" signature_subclass="N/A"
signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_
pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_
status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=10 history_
threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_
hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_
mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_
svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none"
owasp_top10="N/A" bot_info="none"
```

20000039

Meaning

WebSocket security violation.

Field name	Description
log_id	20000039 See Log ID numbers on page 16 .
main_type	WebSocket Security
subtype	<ul style="list-style-type: none"> • Disallow WebSocket • Disallow Extensions • Illegal Format • Illegal Frame Size • Illegal Message Size • Disallow Origin • Parse error

Examples

```
v007xxxxdate=2019-08-03 time=13:29:28 log_id=20000039 msg_id=000000271734 device_id=FV-1KE4417900002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="WebSocket Security" sub_type="Disallow WebSocket" trigger_policy="" severity_level=Low proto=tcp service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=10.200.10.100 src_port=55417 dst=10.200.10.114 dst_port=8081 http_method=get http_url="/autotest/input_rule/1.html" http_host="10.200.10.111:8090" http_agent="none" http_session_id=none msg="[policy_name=websocketsecurityPolicy] : WebSocket request not allowed" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A"
```

20000040

Meaning

MITB AJAX security violation.

Field name	Description
log_id	20000040 See Log ID numbers on page 16 .
main_type	MITB AJAX Security
subtype	N/A

Examples

```
v009xxxxdate=2019-09-21 time=08:17:55 log_id=20000040 msg_id=000034369491 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="MiTB AJAX Security" sub_type="N/A"
trigger_policy="" severity_level=Low proto=tcp service=http backend_service=http action=Alert
policy="FWB_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=51426 dst=10.114.0.1 dst_
port=80 http_method=get http_url="http://10.200.10.210:91/autotest/cors.html" http_host="10.114.0.1"
http_agent="Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0" http_
session_id=none msg="MITB AJAX Detection" signature_subclass="N/A" signature_id="N/A" signature_
cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_
pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_
refer="http://10.114.0.1/autotest/mitb/ajax/ajax_cors.html" http_version="1.x" dev_id="none" es=0
threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_
suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_
sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_
types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_
method="none" owasp_top10="N/A" bot_info="none"
```

20000041

Meaning

Machine learning bot detection violation.

Field name	Description
log_id	20000041 See Log ID numbers on page 16 .
main_type	Bot Detection
subtype	N/A

Examples

```
v009xxxxdate=2019-09-21 time=08:54:03 log_id=20000041 msg_id=000034371543 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="Bot Detection" sub_type="N/A" trigger_
policy="" severity_level=High proto=tcp service=http backend_service=tcp action=Alert policy="FWB_
Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=53734 dst=10.114.0.1 dst_port=80 http_
method=none http_url="none" http_host="none" http_agent="none" http_session_id=none msg="Bot
Verification failed (Real Browser Enforcement)" signature_subclass="N/A" signature_id="N/A" signature_
cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="none" false_
positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_
version="Unknown" dev_id="none" es=0 threat_weight=10 history_threat_weight=0 threat_level=Medium
ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_
sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_
main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_
dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="{\"dimen_count\": 13,
\"boxplot_info\": [{\"id\": 1, \"value\": [1.00, 1.00, 1.00]}, {\"id\": 2, \"value\": [1.00, 2.00, 2.00]}, {\"id\": 3, \"value\":
[0.00, 0.00, 0.00]}, {\"id\": 4, \"value\": [0.00, 0.00, 0.00]}, {\"id\": 5, \"value\": [1.00, 1.00, 1.00]}, {\"id\": 6,
\"value\": [0.00, 0.00, 0.00]}, {\"id\": 7, \"value\": [0.00, 0.00, 0.00]}, {\"id\": 8, \"value\": [1.00, 1.00, 1.00]}, {\"id\":
9, \"value\": [0.00, 0.00, 0.00]}, {\"id\": 10, \"value\": [0.00, 0.00, 0.00]}, {\"id\": 11, \"value\": [0.00, 0.00, 0.00]},
{\"id\": 12, \"value\": [1.00, 1.00, 2.00]}, {\"id\": 13, \"value\": [1.00, 1.00, 1.00]}], \"vector\":
[100.00,100.00,0.00,0.00,100.00,0.00,0.00,100.00,0.00,0.00,0.00,2.00,2.00]}\"
```

20000042

Meaning

CORS check security violation.

Field name	Description
log_id	20000042 See Log ID numbers on page 16 .
main_type	CORS Check Security
subtype	<ul style="list-style-type: none"> Invalid Origin Disallow CORS Disallow Origin Disallow method Disallow header

Examples

```
v009xxxxdate=2019-09-21 time=10:28:23 log_id=20000042 msg_id=000034383205 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="CORS Check Security" sub_type="Disallow
Origin" trigger_policy="" severity_level=Low proto=tcp service=http backend_service=unknown
action=Return_403_error policy="FWB_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=58078
dst=10.114.0.1 dst_port=91 http_method=get http_url="/autotest/test.html" http_
host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="[policy_
name=Fwb_Cors_Policy] : Origin http://123.com is not allowed" signature_subclass="N/A" signature_
id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_
name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_
status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=10 history_
threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_
hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_
mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_
svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none"
owasp_top10="N/A" bot_info="none"
```

20000043

Meaning

JSON validation security violation.

Field name	Description
log_id	20000043 See Log ID numbers on page 16 .
main_type	JSON Validation Security
subtype	<ul style="list-style-type: none"> JSON Schema Validation Violation JSON Format Invalid Violation JSON Data Size Violation JSON Key Size Violation JSON Key Number Violation JSON Value Size Violation JSON Value Number Violation JSON Value Number in Array Violation JSON Object Depth Violation

Examples

```
v009xxxxdate=2019-09-21 time=12:54:05 log_id=20000043 msg_id=000034398160 device_
id=FV3K1E3216000005 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi"
timezone_dayst="GMTa-8" type=attack pri=alert main_type="JSON Validation Security" sub_type="JSON
Data Size Violation" trigger_policy="" severity_level=Low proto=tcp service=http backend_
service=unknown action=Alert policy="FWB_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_
port=50997 dst=10.114.0.1 dst_port=80 http_method=post http_url="/autotest/server_protection/1.html"
http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="[rule_
name = FWB_json_protection_rule] : JSON Data Size Exceeded:(The json data size 1048 Bytes
exceeded the maximum allowed - 1024 Bytes)" signature_subclass="N/A" signature_id="N/A" signature_
cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_
pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_
refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=10 history_threat_weight=0 threat_
level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000
ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_
svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_
index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none"
```

Traffic

Traffic log messages record requests that a FortiWeb policy accepted or blocked. If the request was successful, it also includes the reply. Each log message represents its whole HTTP transaction.

Traffic logs do **not** record non-HTTP/HTTPS traffic such as FTP. This type of traffic is forwarded to your web servers if you have enabled IP-layer forwarding.

Traffic log messages are described below. For descriptions of header fields not mentioned here, see [Header & body fields on page 6](#).

Meaning

Traffic matching and complying with a policy passed through or by FortiWeb.

If there is an error in the message and the request/response used HTTPS, FortiWeb could not scan it.

Depending on the mode of operation, an attack could have bypassed FortiWeb.

Solution

Response times can often be improved by regular expression tuning, offloading SSL/TLS from your back-end server to your FortiWeb (especially if the model supports hardware acceleration), and/or offloading compression. For performance tips, see the [FortiWeb Administration Guide](#).

If HTTPS traffic is not flowing as you expect or not being inspected, and you have recently enabled HTTPS, typically this is due to a misconfiguration. The error message in the `msg` field will indicate the appropriate solution:

- `No Server Certificate for SSL Connection` — FortiWeb does not have the server certificate, so it cannot decode the SSL traffic. To fix this, upload the web server's certificate to FortiWeb.
- `SSL Certificate Key Mismatch` — An X.509 server certificate was uploaded to FortiWeb, but its private key did not match the one used by this HTTPS session. To fix this, upload the back-end web server's current certificate.
- `Ephemeral keys cannot be decrypted` — Ephemeral Diffie-Hellman key exchange can't be inspected due to the property of perfect forward secrecy, which makes real-time HTTPS inspection impossible. To fix this, disable ephemeral Diffie-Hellman on the back-end web server, and select a different key exchange method.
- `Unsupported Cipher for SSL Connection` — Either message digest (MAC) authentication failed or the MAC did not exist, or the transaction used an unsupported cipher suite. To fix this, on the back-end web server, disable cipher suites that are not supported by FortiWeb.
- `Unmonitored SSL Connection` — The HTTPS session was initiated before FortiWeb was deployed or before the server policy was enabled, so FortiWeb could not listen for the key exchange, and therefore cannot decrypt subsequent requests/responses in this HTTPS session. To fix this, on the back-end web server, clear HTTPS sessions and force clients to renegotiate.

If FortiWeb is operating in Reverse Proxy or True Transparent Proxy mode, the traffic was blocked and no attack could have passed through to your protected web servers. **No action is required except to make sure that you have uploaded to FortiWeb the correct certificate for all protected web servers.**

Otherwise, if your appliance was:

- operating in Offline Protection or Transparent Inspection mode **or**
- configured only to **monitor** traffic (e.g. **Monitor Mode** was enabled or the **Action** is **Alert**, not **Alert & Deny**)

Solution

examine the web server to determine whether or not an encrypted attack has passed through. You should also examine your web server's HTTPS configuration and disable cipher suites and key exchanges that are not supported by FortiWeb so that during negotiation with clients, your web server does not agree to use encryption that FortiWeb cannot scan for attacks.

By the nature of log-only actions, detected attack attempts are logged but **not** blocked. You may also want to determine if the attack is from a single source IP address or distributed: blacklisting an offending client may help you to efficiently prevent further attack attempts, improving performance, until you can take further action.

By the nature of the network topology for Offline Protection mode (which can potentially cause differences in speeds of the separate routing paths), and asynchronous inspection for Transparent Inspection mode, **blocking cannot be guaranteed and some key exchanges are not supported**. For details, see the [FortiWeb Administration Guide](#).

Field name	Description
ID (log_id)	30000000 All traffic log messages share the same ID (log_id=30000000). See Log ID numbers on page 16 .
Sub Type (subtype)	http All traffic log messages share the same subtype (subtype=http). See Subtypes on page 16 .
Level (pri)	notification See Priority level on page 17 .
Message (msg)	If the HTTP request triggered the FortiWeb web caching feature, the message begins with [Replied by Cache]. The HTTP/HTTPS request's: <ul style="list-style-type: none"> method IP layer source and destination address and port numbers (IPv6 addresses are surrounded by square brackets to better demarcate the port number, e.g. [2001:470:19:ad7:6::230]:443) such as: <ul style="list-style-type: none"> HTTP GET request from 10.0.2.5:8239 to 10.0.2.1:443 HTTP POST request from 10.0.2.5:8100 to 10.0.2.1:80 If the transaction used HTTPS, and there was an error when either decoding it or participating in the handshake, there may be an error message instead of the HTTP method, such as: HTTP request from 192.0.2.1:40170 to 10.0.2.1:443, Ephemeral keys cannot be decrypted
Source Country (srccountry)	The country that is the source of the traffic.
HTTP Content Routing (content_switch_name)	The name of the associated HTTP content routing policy.

Field name	Description
Server Pool Name (server_pool_name)	The name of the server pool in the associated server policy.

Examples

```
date=2014-06-26 time=00:43:37 log_id=30000000 msg_id=000001351251 device_id=FV-1KD3A14800059 vd="root"
timezone="(GMT-8:00)Pacific Time(US&Canada)" type=traffic subtype="http" pri=notice proto=tcp service=http
status=success reason=none policy=Auto-policy src=10.0.8.103 src_port=8142 dst=10.20.8.22 dst_port=80 http_
request_time=0 http_response_time=0 http_request_bytes=444 http_response_bytes=401 http_method=get http_
url="/" http_host="10.0.8.22" http_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;
.NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; " http_retcode=200 msg="HTTP GET request
from 10.0.8.103:8142 to 10.20.8.22:80" srccountry="Reserved" content_switch_name="testa" server_pool_
name="Auto-ServerFarm"
```

```
date=2014-04-11 time=09:26:22 log_id=30000000 msg_id=000000000156 device_id=FVVM00UNLICENSED
vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=traffic subtype="http" pri=notification proto=tcp
service=https status=success reason="none" policy="policy1" src=172.20.120.47 src_port=53817 dst=172.20.120.47
dst_port=80 http_request_time=18 http_response_time=1 http_request_bytes=464 http_response_bytes=3060 http_
method=get http_url="/index" http_host="172.20.120.48" http_agent="Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:24.0) Gecko/20100101 Firefox/24.0" http_retcode=200 msg="HTTPS GET request from 172.20.120.47:53817 to
172.20.120.47:80 " srccountry="United States" content_switch_name="testa" server_pool_name="Auto-ServerFarm"
```

```
date=2014-04-11 time=10:16:29 log_id=30000000 msg_id=000000000230 device_id=FVVM00UNLICENSED
vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=traffic subtype="http" pri=notification proto=tcp
service=http status=success reason="none" policy="policy1" src=172.20.120.46 src_port=49234 dst=172.20.120.48
dst_port=80 http_request_time=0 http_response_time=0 http_request_bytes=257 http_response_bytes=0 http_
method=get http_url="/admin" http_host="172.20.120.48" http_agent="Mozilla/5.0 (compatible; MSIE 10.0;
Windows NT 6.1; Trident/6.0)" http_retcode=500 msg="HTTP POST request from 172.20.120.46:49234 to
172.20.120.48:80 " srccountry="United States" content_switch_name="testa" server_pool_name="Auto-ServerFarm"
```