Action Policy

https://campus.barracuda.com/doc/45026391/

Action policy is a collection of settings that decide what action to be taken when a violation occurs. It consists of a set of attack groups and associated attack actions with it. The attack action specifies the action to be taken for a particular type of web attack.

To Retrieve Attack Groups

URL: /v1/security_policies/{policy_id}/attack_groups /v1/security_policies/{policy_id}/attack_groups/{attack_group_id}			
Method: GET			
Description: Lists all attack groups if “Attack_Group_ID” is not specified.			
Parameter Name	**Data Type**	**Mandatory**	**Description**
Input Parameters:			
parameters	Alphanumeric	Optional	Any specific parameter name that needs to be retrieved. See *Example 2*.

Example 1:

Request:

curl http://192.168.0.1:8000/restapi/v1/security_policies/new_policy/attack_groups/application-profile-violations -u 'eyJldCI6IjEzODAxNTYzNzQiLCJwYXNzd29yZCI6IjU1ZTkxMDA5NDAzMGVlOTY1N2QzMTI4NDQw\nNWZmMDkyIiwidXNlciI6ImFkbWluIn0=\n:' -X GET

Response:

{"object":"ActionPolicy","fields":null,"policy_id":"new_policy","data":[{"name":"domain-not-found-in-profile","response_page":"default","numeric_id":"130","attack_action_deny_response":"send_response","follow_up_action_time":"60","attack_group":"application-profile-violations","follow_up_action":null,"redirect_url":"","action":"protect_and_log","id":"domain-not-found-in-profile"},{"name":"no-url-profile-match","response_page":"default","numeric_id":"131","attack_action_deny_response":"send_response","follow_up_action_time":"60","attack_group":"application-profile-violations","follow_up_action":null,"redirect_url":"","action":"protect_and_log","id":"no-url-profile-match"}],"limit":null,"token":"eyJldCI6IjEzODAxNTczOTAiLCJwYXNzd29yZCI6Ijk5ZGNjMDRiZmQ5

YTUwMTkxYTVlMTZkMWFi\nMjI2MjZjIiwidXNlciI6ImFkbWluIn0=\n","offset":null}

Example 2:

Request:

curl http://192.168.0.1:8000/restapi/v1/security_policies/new_policy/attack_groups/application-profile-violations -u 'eyJldCI6IjE1MDE5MDUxMzkiLCJwYXNzd29yZCI6IjUwN2I1ZDRhMTc3Mzc4Zjc5NGY2ZmM3NTNh\nYTczM2IxIiwidXNlciI6ImFkbWluIn0=\n:' -X GET -G -d parameters=follow_up_action,deny_response

Response:

{"object":"ActionPolicy","fields":["follow_up_action","deny_response"],"policy_id":"new_policy","data":[{"attack_group":"application-profile-violations","follow_up_action":"none","deny_response":"send_response","id":"domain-not-found-in-profile"},{"attack_group":"application-profile-violations","follow_up_action":"block_client_ip","deny_response":"temporary_redirect","id":"no-url-profile-match"}],"limit":null,"token":"eyJldCI6IjE1MDQ0MDk4NTUiLCJwYXNzd29yZCI6IjNkZjhkYzE5MDhlYWQxOGIxN2UzYWY2OWMx\nNGEwOGIxIiwidXNlciI6ImFkbWluIn0=\n","offset":null}

To Retrieve Attack Actions

URL: /v1/security_policies/{policy_id}/attack_groups/{attack_group_id}/actions /v1/security_policies/{policy_id}/attack_groups/{attack_group_id}/actions/{action_id}			
Method: GET			
Description: Lists all attack actions for the given attack group if “action_id” is not specified.			
Parameter Name	**Data Type**	**Mandatory**	**Description**
Input Parameters:			
parameters	Alphanumeric	Optional	Any specific parameter name that needs to be retrieved. See *Example 2*.

Example 1:

Request:

curl http://192.168.0.1:8000/restapi/v1/security_policies/new_policy/attack_groups/application-profile-violations/actions/no-url-profile-match -u 'eyJldCI6IjEzODAxNTYzNzQiLCJwYXNzd29yZCI6IjU1ZTkxMDA5NDAzMGVlOTY1N2QzMTI4NDQw\nNWZmMDkyIiwidXNlciI6ImFkbWluIn0=\n:' -X GET

Response:

{"name":"no-url-profile-match","response_page":"default","numeric_id":"131","attack_action_deny_response":"send_response","follow_up_action_time":"60","attack_group":"application-profile-violations","follow_up_action":null,"redirect_url":"","action":"protect_and_log","id":"no-url-profile-match","token":"eyJldCI6IjEzODAxNTc0NjYiLCJwYXNzd29yZCI6Ijk5ODViNjk0ZjIxYjU4MGEyMmY2OWRmMzUz\nNjA2MzA0IiwidXNlciI6ImFkbWluIn0=\n"}

Example 2:

Request:

curl http://192.168.0.1:8000/restapi/v1/security_policies/new_policy/attack_groups/application-profile-violations/actions/no-url-profile-match -u 'eyJldCI6IjE1MDE5MDUxMzkiLCJwYXNzd29yZCI6IjUwN2I1ZDRhMTc3Mzc4Zjc5NGY2ZmM3NTNh\nYTczM2IxIiwidXNlciI6ImFkbWluIn0=\n:' -X GET -G -d parameters=follow_up_action,redirect_url,deny_response,action

Response:

{"attack_group":"application-profile-violations","action":"protect_and_log","redirect_url":"/abc.html","follow_up_action":"block_client_ip","deny_response":"temporary_redirect","id":"no-url-profile-match","token":"eyJldCI6IjE1MDQzMTYyOTQiLCJwYXNzd29yZCI6IjkwNDNjODQ1MjJjZDlhMzY0MDBhNjJhY2E0\nOWU2MDU2IiwidXNlciI6ImFkbWluIn0=\n"}

To Update an Action Policy

URL: /v1/security_policies/{policy_id}/attack_groups/{attack_group_id}/actions/{action_id}

Method: PUT			
Description: Updates the values of given parameters in the given action policy.			
Parameter Name	**Data Type**	**Mandatory**	**Description**
Input Parameters:			
action	Enumeration	Optional	The action to be taken for an invalid request. The enumerated values include: • none • protect_and_log • allow_and_log • protect_with_no_log
deny_response	Enumeration	Optional	The response to be sent to the client if the request is denied. The enumerated values include: • close_connection • send_response • temporary_redirect • permanent_redirect
redirect_url	Alphanumeric	Optional	The URL to be used to redirect the request. **Note**: Required ONLY when **deny_response** is set to *temporary_redirect* or *permanent_redirect.*
response_page	Enumeration	Optional	The response page to be sent to the client. The enumerated values include predefined response pages and custom response pages (if any): • default • default-virus • default-error-resp • default-captcha-tries-error-page • default-captcha-sessions-error-page • default-suspected-activity-error-page • default-captcha-response-page **Note**: Required ONLY when **deny_response** is set to *send_response*.
follow_up_action	Enumeration	Optional	The follow up action to be taken if the request is denied. The enumerated values include: • none • block_client_ip • challenge_with_captcha
follow_up_action_time	Numeric	Optional	The time in seconds to block the client IP. **Note**: Required ONLY when **follow_up_action** is set to *block_client_ip*.

Example:

Request:

curl http://192.168.0.1:8000/restapi/v1/security_policies/new_policy/attack_groups/application-profile-violations/actions/no-url-profile-match -u 'eyJldCI6IjEzODAxNTYzNzQiLCJwYXNzd29yZCI6IjU1ZTkxMDA5NDAzMGVlOTY1N2QzMTI4NDQw\nNWZmMDkyIiwidXNlciI6ImFkbWluIn0=\n:' -X PUT -H Content-Type:application/json -d '{"action":"allow_and_log"}'

Response:

{"msg":"Configuration Updated","id":"no-url-profile-match","token":"eyJldCI6IjEzODAxNTc1NTAiLCJwYXNzd29yZCI6IjZkM2IxNGU0ZjhhNGY2MWI1MGNlYjBmNmYz\nM2Q5OWQ1IiwidXNlciI6ImFkbWluIn0=\n"}

The table below lists the attack ID names to be used in the REST API commands:

Attack name displayed in the web interface	Attack ID to be used in REST API
protocol-violations	
Directory Traversal Beyond Root	directory-traversal-beyond-root
GET Request with Content Length	get-request-with-content-length-header
Invalid Header	invalid-header
Invalid Method	invalid-method
Invalid or Malformed HTTP Request	invalid-or-malformed-http-request
Malformed Content Length	malformed-content-length
Malformed Cookie	malformed-cookie
Malformed Header	malformed-header
Malformed Parameter	malformed-parameter
Malformed Request Line	malformed-end-of-request-line
Malformed Version	malformed-version
Missing Host Header	http-1.1-request-without-host
Multiple Content Length	multiple-content-length-headers
POST without Content Length	post-request-without-content-length
Parameter Too Large	large-parameter-in-post-data
Pre-1.0 Request	pre-1.0-request

request-policy-violations	
Cookie Count Exceeded	cookie-count-exceeded
Cookie Expired	cookie-expired
Cookie Length Exceeded	cookie-length-exceeded
Cookie Name Length Exceeded	cookie-name-length-exceeded
Cookie Tampered	cookie-tampered
Header Count Exceeded	header-count-exceeded
Header Name Length Exceeded	header-name-length-exceeded
Header Value Length Exceeded	header-value-length-exceeded
Invalid URL Encoding	invalid-url-encoding
Mismatched Header Cookie Replay Attack	mismatched-header-cookie-replay-attack
Mismatched IP Cookie Replay Attack	mismatched-ip-cookie-replay-attack
Query Length Exceeded	url-query-length-exceeded
Request Length Exceeded	total-request-length-exceeded
Session timed out	keepalive-timeout-exceeded
Slash-dot in URL Path	slash-dot-in-url-path
Tilde in URL Path	tilde-in-url-path
Too Many Sessions for IP	too-many-sessions-for-ip
Total Request Line Length Exceeded	total-request-line-length-exceeded
URL Length Exceeded	url-length-exceeded
Unrecognized Cookie	unrecognized-cookie
header-violations	
Apache Struts Attack in Header	apache-struts-attacks-medium-in-header
Cross-Site Scripting in Header	cross-site-scripting-in-header
Custom Attack Pattern in Header	custom-attack-pattern-in-header
Directory Traversal in Header	directory-traversal-in-header
HTTP Specific Attack in Header	http-specific-attacks-medium-in-header
LDAP Injection in Header	ldap-injection-medium-in-header
Metacharacter Matched in Header	metacharacter-matched-in-header
OS Command Injection in Header	os-command-injection-in-header
Python PHP Attack in Header	python-php-attacks-medium-in-header
Remote File Inclusion in Header	remote-file-inclusion-pattern-in-header
SQL Injection in Header	sql-injection-in-header
application-profile-violations	
No Domain Match in Profile	domain-not-found-in-profile
No URL Profile Match	no-url-profile-match

url-profile-violations	
Apache Struts Attack in URL	apache-struts-attacks-medium-in-url
Content Length Exceeded	content-length-exceeded
Cross-Site Scripting in URL	cross-site-scripting-pattern-in-url
Custom Attack Pattern in URL	custom-attack-pattern-in-url
HTTP Specific Attack in URL	http-specific-attacks-medium-in-url
LDAP Injection in URL	ldap-injection-medium-in-url
Method Not Allowed	forbidden-method
No Param Profile Match	no-param-profile-match
OS Command Injection in URL	os-command-injection-pattern-in-url
Parameter Name Length Exceeded	parameter-name-length-exceeded
Python PHP Attack in URL	python-php-attacks-medium-in-url
Query String not Allowed	query-string-not-allowed
Remote File Inclusion in URL	remote-file-inclusion-pattern-in-url
SQL Injection in URL	sql-injection-pattern-in-url
Session not Found	session-not-found
Too Many Parameters	too-many-parameters
Too Many Uploaded Files	too-many-uploaded-files
Unknown Content Type	unknown-content-type-in-post-body
param-profile-violations	
Apache Struts Attack in Parameter	apache-struts-attacks-medium-in-param
Cross-Site Request Forgery	cross-site-request-forgery-attack-detected
Cross-Site Scripting in Parameter	cross-site-scripting-pattern-in-parameter
Custom Attack Pattern in Parameter	custom-attack-pattern-in-parameter
Directory Traversal in Parameter	directory-traversal-pattern-in-parameter
File Upload Size Exceeded	file-upload-size-exceeded
Forbidden File Extension	forbidden-file-extension
Forbidden File Mime Type	forbidden-file-mime-type
HTTP Specific Attack in Parameter	http-specific-attacks-medium-in-param
LDAP Injection in Parameter	ldap-injection-medium-in-param
Mandatory Parameter Missing	mandatory-parameter-missing
Maximum Instances of Parameter Exceeded	max-instances-of-parameter-exceeded
Metacharacter in Parameter	metacharacter-in-parameter
OS Command Injection in Parameter	os-command-injection-pattern-in-parameter
Parameter Input Validation Failed	parameter-input-validation-failed
Parameter Length Exceeded	parameter-length-exceeded

Parameter Value not Allowed	parameter-value-not-allowed
Python PHP Attack in Parameter	python-php-attacks-medium-in-param
Read-Only or Hidden Parameter Tampered	read-only-or-hidden-parameter-tampered
Remote File Inclusion	remote-file-inclusion-pattern-in-parameter
SQL Injection in Parameter	sql-injection-pattern-in-parameter
Session Choice Parameter Tampered	session-choice-parameter-tampered
Session Context not Found	session-context-not-found
Session Invariant Parameter Tampered	session-invariant-parameter-tampered
response-violations	
CAPTCHA Validation Required	captcha-response-page
Custom Error Response Page	custom-error-response-page
Error Response Suppressed	error-response-suppressed
Identity Theft Pattern Matched	identity-theft-pattern-matched-in-response
Response Header Suppressed	response-header-suppressed
advanced-policy-violations	
Brute force from All Sources	brute-force-from-all-sources
Brute force from IP	brute-force-from-ip
CAPTCHA Attempt Limit Exceeded	captcha-tries-exceeded
CAPTCHA Session Limit Exceeded	captcha-max-sessions-exceeded
Invalid URL Character Set	invalid-url-character-set
Rate Control Intrusion	rate-control-intrusion
Secure Browsing	secure-browsing
Slow Read Attack	slow-read-attack
Slowloris Attack	slow-client-attack
URL Encryption	url-encryption
Unanswered CAPTCHA Limit Exceeded	captcha-max-unanswered-exceeded
Virus Found	virus-found-in-post-request
xmlfw-dos-violations	
DTD Found	dtd-found
External URI Reference Found	external-uri-ref-found
Malformed XML	malformed-xml
Max Attribute Name Length Exceeded	max-attribute-name-length-exceeded
Max Attribute Value Length Exceeded	max-attribute-value-length-exceeded
Max Document Size Exceeded	max-document-size-exceeded
Max Element Attributes Exceeded	max-element-attributes-exceeded
Max Element Children Exceeded	max-element-children-exceeded

Max Element Name Length Exceeded	max-element-name-length-exceeded
Max Elements in Tree Exceeded	max-elements-in-tree-exceeded
Max Text Size Exceeded	max-text-size-exceeded
Max Tree Depth Exceeded	max-tree-depth-exceeded
Min Document Size Limit	min-document-size-limit
Processing Instructions Found	processing-instructions-found
xmlfw-wsi-assertion-failures	
Attribute "MustUnderstand" is Neither 1 nor 0	mustunderstand-is-nither-1-nor-0
Attributes in SOAP Envelope Header Body	atts-in-soap-env-hdr-body
Children Elements in SOAP:Body Have "SOAP:EncodingStyle" Attribute	soap-encodingStyle-in-body-children
Children Elements in SOAP:Body are Not Namespace Qualified	soap-body-children-are-not-ns-qualified
DOCTYPE Element	DOCTYPE-element
EncodingStyle Attribute Found in Grandchild of SOAP Body	encodingStyle-in-rpc-literal-grand-children
EncodingStyle in Envelope Namespace Elements	encodingStyle-in-envelope-ns-elements
Envelope Does Not Conform to SOAP Schema	envelope-does-not-confirm-to-schema
Envelope Namespace is 1998	env-ns-is-1998
Good Response is Not Using HTTP 200 OK	good-resp-is-not-200ok
Message Contains Undefined "SOAPBind:Fault" Element(s)	fault-resp-is-not-defined-in-wsdl-binding
Message Contains a WS-I Conformance Claim Which is Not a Child of the SOAP:Header Element	WSI-confirmance-not-in-soap-hdr
Message Contains a WS-I Conformance Claim with a "SOAP:MustUnderstand" Attribute	WSI-confirmance-claims-are-not-mustunderstand
Message Does Not Include All Headers	msg-does-not-include-allhdrs
Message Part Accessors Have No Namespace	msg-part-accessors-have-no-ns
Message is Not Sent Using HTTP1.0 or HTTP1.1	message-is-not-HTTP1.0-or-HTTP1.1
Message is Not Sent Using HTTP1.1	message-is-not-HTTP1.1
Message is Not UTF8 or UTF16	message-is-not-UTF8-or-UTF16
Non POST Request Does Not Contain 405 HTTP Status Code	non-POST-req-does-not-get-405
Non XML Request Does Not Contain 415 HTTP Status Code	non-XML-req-does-not-get-415
One-Way Response Contains a SOAP:Envelope	oneway-resp-non-empty-body
Part Accessors Have "xsi: nil" Attribute	part-accessors-has-xsi-nil
Processed Response Status is Neither 200 nor 202	processed-resp-status-is-nither-200-nor-202

Request Does Not Match the WSDL:Definition	req-matches-wsdl
Request Message is Not an HTTP POST Message	request-is-not-HTTP-POST
Response Does Not Match the WSDL:Definition	resp-matches-wsdl
Response Wrapper Does Not Match the Name Attribute on WSDL:Operation	resp-has-no-wrapper-named-op
SOAP 1.1 Dot Notation is Used By the SOAP:Fault Element	faults-use-dot-notation
SOAP Message Contains XML Processing Instructions	xml-processing-instructions-in-body
SOAP:Body Contains the "SOAPEnc:ArrayType" Attribute	soapenc-arraytype-attr
SOAP:Envelope Does Not Have v1.1 Namespace	msg-body-is-not-soap-env-with-ns
SOAP:Envelope Has a Direct Child After the "SOAP:Body" Element	envelope-have-children-after-body
SOAP:Envelope or SOAP:Body Does Not Conform to XML 1.0	envelope-and-body-are-not-xml1.0
SOAP:Fault Children Elements are Not Namespace Qualified	soap-fault-does-not-have-allowed-children
SOAP:Fault Children are Qualified	soap-fault-children-are-qualified
SOAP:Fault Has Non-Foreign Namespace	soap-fault-has-envelope-ns
SOAP:Fault Message Not Found in the HTTP 500 Response	soap-fault-is-not-in-HTTP500-resp
SOAP:Fault Not Generated for Bad Envelope Namespace	no-fault-for-bad-env-ns
SOAP:Faultcode is Not Standard or Namespace Qualified	soap-faultcode-is-not-std
SOAPAction Header Does Not Contain Quoted String	soapaction-hdr-is-not-quoted
SOAPAction Header Does Not Contain the Correct String Value	soapaction-hdr-does-not-match-op-soapaction
WS-I Conformance Claim Does Not Adhere to the WS-I Conformance Claim Schema	WSI-confirmance-is-not-well-formed
xmlfw-soap-violations	
Additional SOAP Headers Received	additional-soap-headers-rcvd
Invalid SOAP Body	invalid-soap-body
Invalid SOAP Envelope	invalid-soap-envelope
Invalid SOAP Header	invalid-soap-header
json-limit-violations	
Malformed JSON	malformed-json
Max Array Values Exceeded	max-values-in-array-exceeded

Max Key Length Exceeded	max-key-length-exceeded
Max Number Value Exceeded	max-number-limit-exceeded
Max Object Child Exceeded	max-object-children-exceeded
Max Object Keys Exceeded	max-keys-in-object-exceeded
Max Value Length Exceeded	max-value-length-exceeded
Object Depth Exceeded	max-object-depth-exceeded
json-violations	
Apache Struts Attacks in JSON Data	apache-struts-attack-in-json
Cross-Site Scripting in JSON Data	cross-site-scripting-pattern-in-json
Custom Attack Pattern in JSON Data	custom-attack-pattern-in-json
Directory Traversal Attack in JSON Data	directory-traversal-pattern-in-json
HTTP Specific Attacks in JSON Data	http-specific-attack-in-json
LDAP Injection in JSON Data	ldap-injection-in-json
OS Command Injection in JSON Data	os-command-injection-pattern-in-json
Python PHP Attack in JSON Data	python-php-attack-in-json
Remote File Inclusion in JSON Data	remote-file-inclusion-pattern-in-json
SQL Injection in JSON Data	sql-injection-pattern-in-json