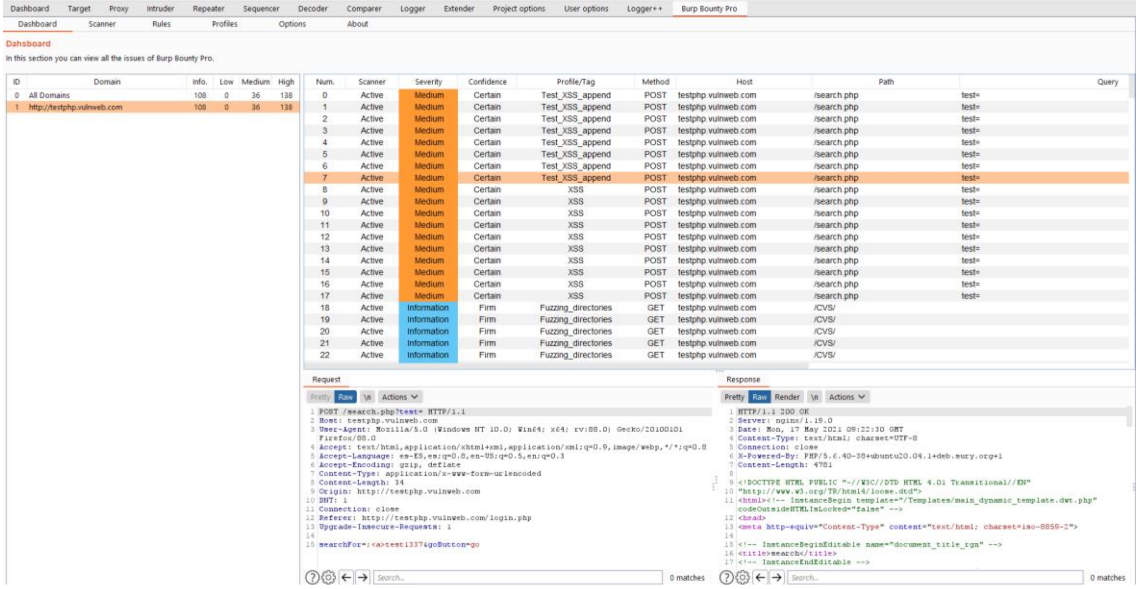
BURP BOUNTY PRO v2 DOCUMENTATION

1. Extension Sections

Dashboard

In the "Dashboard" tab you will see the vulnerabilities detected by Burp Bounty Pro scanners, both active and passive. You can change the domain and see only the issues belonging to that domain.



Dahsboard

In this section you can view all the issues of Burp Bounty Pro.

ID	Domain	Info.	Low	Medium	High
0	All Domains	108	0	36	138
1	http://testphp.vulnweb.com	108	0	36	138

Num.	Scanner	Severity	Confidence	Profile/Tag	Method	Host	Path	Query
0	Active	Medium	Certain	Test_XSS_append	POST	testphp.vulnweb.com	/search.php	test=
1	Active	Medium	Certain	Test_XSS_append	POST	testphp.vulnweb.com	/search.php	test=
2	Active	Medium	Certain	Test_XSS_append	POST	testphp.vulnweb.com	/search.php	test=
3	Active	Medium	Certain	Test_XSS_append	POST	testphp.vulnweb.com	/search.php	test=
4	Active	Medium	Certain	Test_XSS_append	POST	testphp.vulnweb.com	/search.php	test=
5	Active	Medium	Certain	Test_XSS_append	POST	testphp.vulnweb.com	/search.php	test=
6	Active	Medium	Certain	Test_XSS_append	POST	testphp.vulnweb.com	/search.php	test=
7	Active	Medium	Certain	Test_XSS_append	POST	testphp.vulnweb.com	/search.php	test=
8	Active	Medium	Certain	XSS	POST	testphp.vulnweb.com	/search.php	test=
9	Active	Medium	Certain	XSS	POST	testphp.vulnweb.com	/search.php	test=
10	Active	Medium	Certain	XSS	POST	testphp.vulnweb.com	/search.php	test=
11	Active	Medium	Certain	XSS	POST	testphp.vulnweb.com	/search.php	test=
12	Active	Medium	Certain	XSS	POST	testphp.vulnweb.com	/search.php	test=
13	Active	Medium	Certain	XSS	POST	testphp.vulnweb.com	/search.php	test=
14	Active	Medium	Certain	XSS	POST	testphp.vulnweb.com	/search.php	test=
15	Active	Medium	Certain	XSS	POST	testphp.vulnweb.com	/search.php	test=
16	Active	Medium	Certain	XSS	POST	testphp.vulnweb.com	/search.php	test=
17	Active	Medium	Certain	XSS	POST	testphp.vulnweb.com	/search.php	test=
18	Active	Information	Firm	Fuzzing_directories	GET	testphp.vulnweb.com	/CVS/	
19	Active	Information	Firm	Fuzzing_directories	GET	testphp.vulnweb.com	/CVS/	
20	Active	Information	Firm	Fuzzing_directories	GET	testphp.vulnweb.com	/CVS/	
21	Active	Information	Firm	Fuzzing_directories	GET	testphp.vulnweb.com	/CVS/	
22	Active	Information	Firm	Fuzzing_directories	GET	testphp.vulnweb.com	/CVS/	

Request

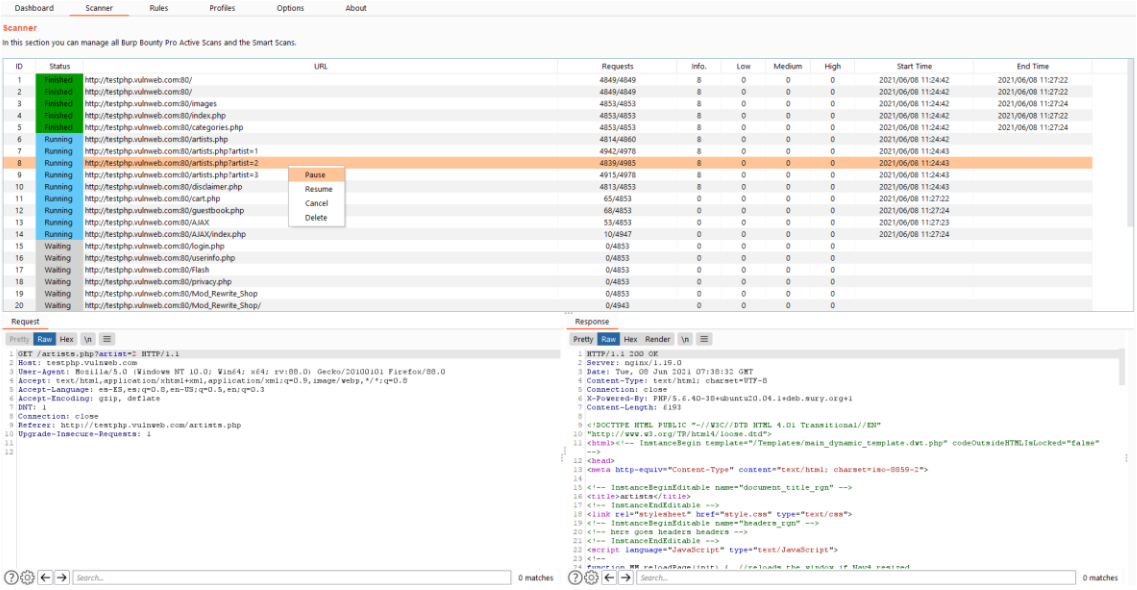
```
POST /search.php?test= HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://testphp.vulnweb.com
DNT: 1
Connection: close
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

searchFor=;<a>test1337&goButton=go
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 17 May 2021 09:22:30 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 4781

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>search</title>
<!-- InstanceEndEditable -->
```

Scanner

In the "Scanner" tab, you will be able to see the scans carried out or in progress. In this section you can see the “status” of each endpoint, you can select one or multiple scans and “pause”, “resume” or “cancel” them.



Scanner

In this section you can manage all Burp Bounty Pro Active Scans and the Smart Scans.

ID	Status	URL	Requests	Info.	Low	Medium	High	Start Time	End Time
1	Finished	http://testphp.vulnweb.com:80/	4849/4849	8	0	0	0	2021/06/08 11:24:42	2021/06/08 11:27:22
2	Finished	http://testphp.vulnweb.com:80/	4849/4849	8	0	0	0	2021/06/08 11:24:42	2021/06/08 11:27:22
3	Finished	http://testphp.vulnweb.com:80/images	4853/4853	8	0	0	0	2021/06/08 11:24:42	2021/06/08 11:27:24
4	Finished	http://testphp.vulnweb.com:80/index.php	4853/4853	8	0	0	0	2021/06/08 11:24:42	2021/06/08 11:27:22
5	Finished	http://testphp.vulnweb.com:80/categories.php	4853/4853	8	0	0	0	2021/06/08 11:24:42	2021/06/08 11:27:24
6	Running	http://testphp.vulnweb.com:80/artists.php	4814/4860	8	0	0	0	2021/06/08 11:24:42	
7	Running	http://testphp.vulnweb.com:80/artists.php?artist=1	4942/4978	8	0	0	0	2021/06/08 11:24:43	
8	Running	http://testphp.vulnweb.com:80/artists.php?artist=2	4839/4985	8	0	0	0	2021/06/08 11:24:43	
9	Running	http://testphp.vulnweb.com:80/artists.php?artist=3	4915/4978	8	0	0	0	2021/06/08 11:24:43	
10	Running	http://testphp.vulnweb.com:80/disclaimer.php	4813/4853	8	0	0	0	2021/06/08 11:24:43	
11	Running	http://testphp.vulnweb.com:80/cart.php	65/4853	0	0	0	0	2021/06/08 11:27:22	
12	Running	http://testphp.vulnweb.com:80/guestbook.php	68/4853	0	0	0	0	2021/06/08 11:27:24	
13	Running	http://testphp.vulnweb.com:80/AJAX	53/4853	0	0	0	0	2021/06/08 11:27:23	
14	Running	http://testphp.vulnweb.com:80/AJAX/index.php	10/4947	0	0	0	0	2021/06/08 11:27:24	
15	Waiting	http://testphp.vulnweb.com:80/login.php	0/4853	0	0	0	0		
16	Waiting	http://testphp.vulnweb.com:80/userinfo.php	0/4853	0	0	0	0		
17	Waiting	http://testphp.vulnweb.com:80/Flash	0/4853	0	0	0	0		
18	Waiting	http://testphp.vulnweb.com:80/privacy.php	0/4853	0	0	0	0		
19	Waiting	http://testphp.vulnweb.com:80/Mod_Rewrite_Shop	0/4853	0	0	0	0		
20	Waiting	http://testphp.vulnweb.com:80/Mod_Rewrite_Shop/	0/4943	0	0	0	0		

Request

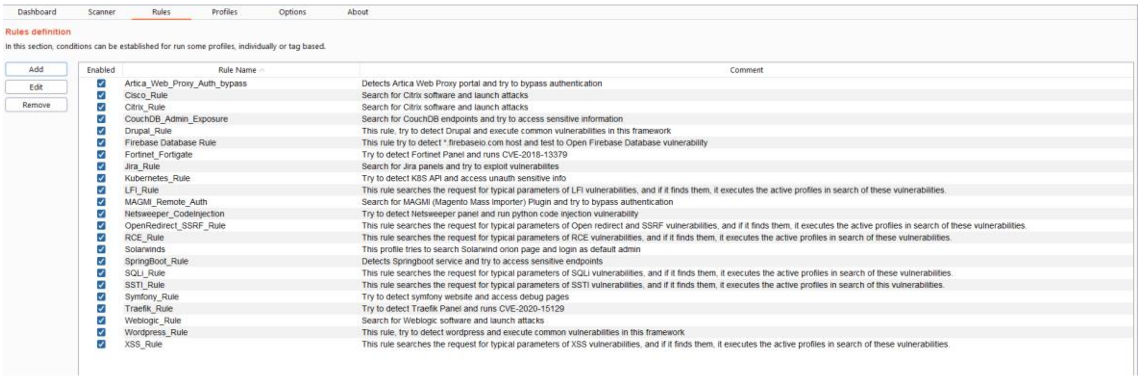
```
GET /artists.php?artist=2 HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://testphp.vulnweb.com/artists.php
Upgrade-Insecure-Requests: 1


```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Tue, 08 Jun 2021 07:38:32 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 6193

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false"
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>artists</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
```

Rules

In the tab "Rules" you can see the rules that will be used in the Smart Scan.



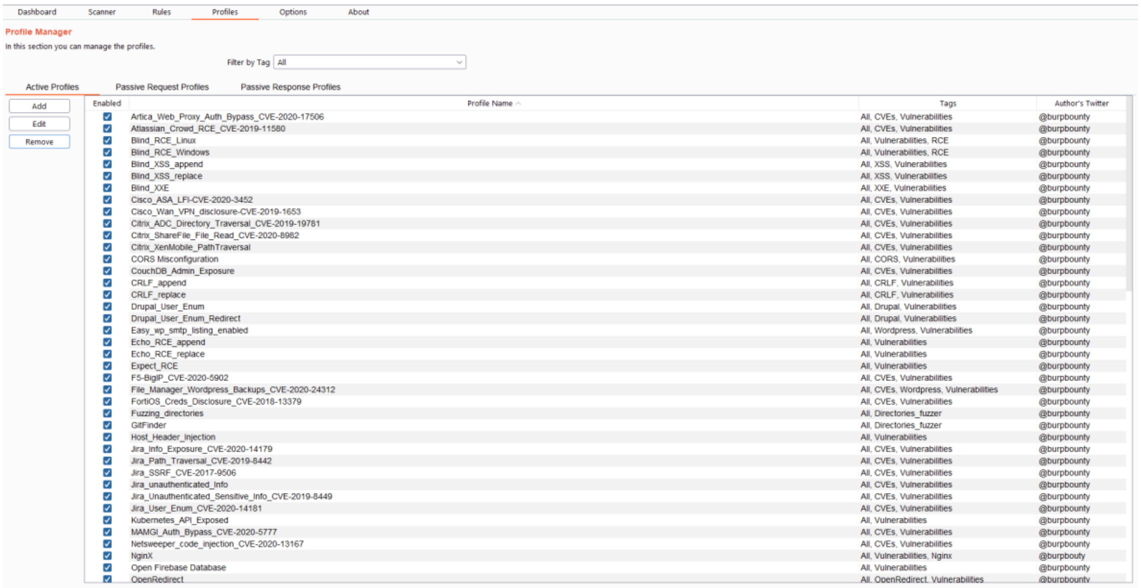
Rules definition

In this section, conditions can be established for run some profiles, individually or tag based.

Enabled	Rule Name	Comment
☑	Artica_Web_Proxy_Auth_bypass	Detects Artica Web Proxy portal and try to bypass authentication
☑	Cisco_Rule	Search for Citrix software and launch attacks
☑	Citrix_Rule	Search for Citrix software and launch attacks
☑	CouchDB_Admin_Exposure	Search for CouchDB endpoints and try to access sensitive information
☑	Drupal_Rule	This rule, try to detect Drupal and execute common vulnerabilities in this framework
☑	Firebase Database Rule	This rule try to detect * firebaseio com host and test to Open Firebase Database vulnerability
☑	Fortinet_Fortigate	Try to detect Fortinet Panel and runs CVE-2018-13379
☑	Jira_Rule	Search for Jira panels and try to exploit vulnerabilites
☑	Kubernetes_Rule	Try to detect K8S API and access unauth sensitive info
☑	LFI_Rule	This rule searches the request for typical parameters of LFI vulnerabilities, and if it finds them, it executes the active profiles in search of these vulnerabilities.
☑	MAGMI_Remote_Auth	Search for MAGMI (Magento Mass Importer) Plugin and try to bypass authentication
☑	Netsweeper_CodeInjection	Try to detect Netsweeper panel and run python code injection vulnerability
☑	OpenRedirect_SSRF_Rule	This rule searches the request for typical parameters of Open redirect and SSRF vulnerabilities, and if it finds them, it executes the active profiles in search of these vulnerabilities.
☑	RCE_Rule	This rule searches the request for typical parameters of RCE vulnerabilities, and if it finds them, it executes the active profiles in search of these vulnerabilities.
☑	Solarwinds	This profile tries to search Solarwind orion page and login as default admin
☑	SpringBoot_Rule	Detects Springboot service and try to access sensitive endpoints
☑	SQLi_Rule	This rule searches the request for typical parameters of SQLi vulnerabilities, and if it finds them, it executes the active profiles in search of these vulnerabilities.
☑	SSTI_Rule	This rule searches the request for typical parameters of SSTI vulnerabilities, and if it finds them, it executes the active profiles in search of this vulnerabilities.
☑	Symfony_Rule	Try to detect symfony website and access debug pages
☑	Traefik_Rule	Try to detect Traefik Panel and runs CVE-2020-15129
☑	Weblogic_Rule	Search for Weblogic software and launch attacks
☑	Wordpress_Rule	This rule, try to detect wordpress and execute common vulnerabilities in this framework
☑	XSS_Rule	This rule searches the request for typical parameters of XSS vulnerabilities, and if it finds them, it executes the active profiles in search of these vulnerabilities.

Profiles

In the tab "Profiles" you can see the active profiles, passive request and passive response. In this section you can add new profiles or edit existing ones.



Profile Manager

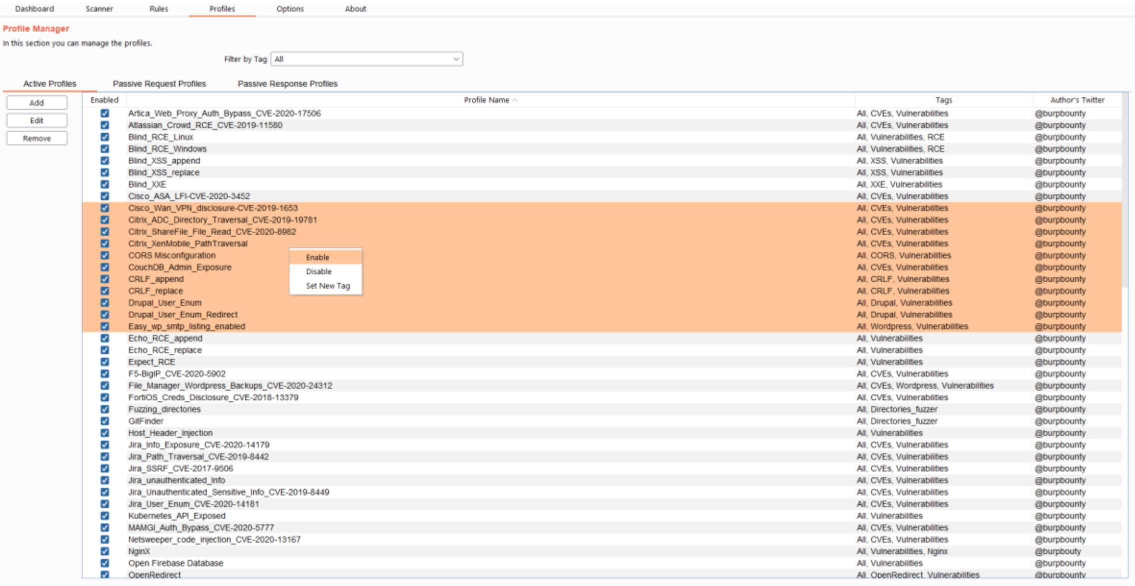
In this section you can manage the profiles.

Filter by Tag: All

Active Profiles | Passive Request Profiles | Passive Response Profiles

Enabled	Profile Name	Tags	Author's Twitter
☑	Artica_Web_Proxy_Auth_Bypass_CVE-2020-17506	All, CVEs, Vulnerabilities	@burpbounty
☑	Atlassian_Crowd_RCE_CVE-2019-11580	All, CVEs, Vulnerabilities	@burpbounty
☑	Blind_RCE_Linux	All, Vulnerabilities, RCE	@burpbounty
☑	Blind_RCE_Windows	All, Vulnerabilities, RCE	@burpbounty
☑	Blind_XSS_append	All, XSS, Vulnerabilities	@burpbounty
☑	Blind_XSS_replace	All, XSS, Vulnerabilities	@burpbounty
☑	Blind_XXE	All, XXE, Vulnerabilities	@burpbounty
☑	Cisco_ASA_LFI-CVE-2020-3452	All, CVEs, Vulnerabilities	@burpbounty
☑	Cisco_Wan_VPN_disclosure-CVE-2019-1653	All, CVEs, Vulnerabilities	@burpbounty
☑	Citrix_ADC_Directory_Traversal_CVE-2019-19781	All, CVEs, Vulnerabilities	@burpbounty
☑	Citrix_ShareFile_File_Read_CVE-2020-8982	All, CVEs, Vulnerabilities	@burpbounty
☑	Citrix_XenMobile_PathTraversal	All, CVEs, Vulnerabilities	@burpbounty
☑	CORS Misconfiguration	All, CORS, Vulnerabilities	@burpbounty
☑	CouchDB_Admin_Exposure	All, CVEs, Vulnerabilities	@burpbounty
☑	CRLF_append	All, CRLF, Vulnerabilities	@burpbounty
☑	CRLF_replace	All, CRLF, Vulnerabilities	@burpbounty
☑	Drupal_User_Enum	All, Drupal, Vulnerabilities	@burpbounty
☑	Drupal_User_Enum_Redirect	All, Drupal, Vulnerabilities	@burpbounty
☑	Easy_wp_smtp_listing_enabled	All, Wordpress, Vulnerabilities	@burpbounty
☑	Echo_RCE_append	All, Vulnerabilities	@burpbounty
☑	Echo_RCE_replace	All, Vulnerabilities	@burpbounty
☑	Expect_RCE	All, Vulnerabilities	@burpbounty
☑	F5-BigIP_CVE-2020-5902	All, CVEs, Vulnerabilities	@burpbounty
☑	File_Manager_Wordpress_Backups_CVE-2020-24312	All, CVEs, Wordpress, Vulnerabilities	@burpbounty
☑	FortiOS_Creds_Disclosure_CVE-2018-13379	All, CVEs, Vulnerabilities	@burpbounty
☑	Fuzzing_directories	All, Directories_fuzzer	@burpbounty
☑	GitFinder	All, Directories_fuzzer	@burpbounty
☑	Host_Header_Injection	All, Vulnerabilities	@burpbounty
☑	Jira_Info_Exposure_CVE-2020-14179	All, CVEs, Vulnerabilities	@burpbounty
☑	Jira_Path_Traversal_CVE-2019-8442	All, CVEs, Vulnerabilities	@burpbounty
☑	Jira_SSRF_CVE-2017-9506	All, CVEs, Vulnerabilities	@burpbounty
☑	Jira_unauthenticated_Info	All, CVEs, Vulnerabilities	@burpbounty
☑	Jira_Unauthenticated_Sensitive_Info_CVE-2019-8449	All, CVEs, Vulnerabilities	@burpbounty
☑	Jira_User_Enum_CVE-2020-14181	All, CVEs, Vulnerabilities	@burpbounty
☑	Kubernetes_API_Exposed	All, Vulnerabilities	@burpbounty
☑	MAMGI_Auth_Bypass_CVE-2020-5777	All, CVEs, Vulnerabilities	@burpbounty
☑	Netsweeper_code_injection_CVE-2020-13167	All, CVEs, Vulnerabilities	@burpbounty
☑	NginX	All, Vulnerabilities, Nginx	@burpbouty
☑	Open Firebase Database	All, Vulnerabilities	@burpbounty
☑	OpenRedirect	All, OpenRedirect, Vulnerabilities	@burpbounty

In this section you can also activate or deactivate one or more profiles by means of the right button.



Profile Manager

In this section you can manage the profiles.

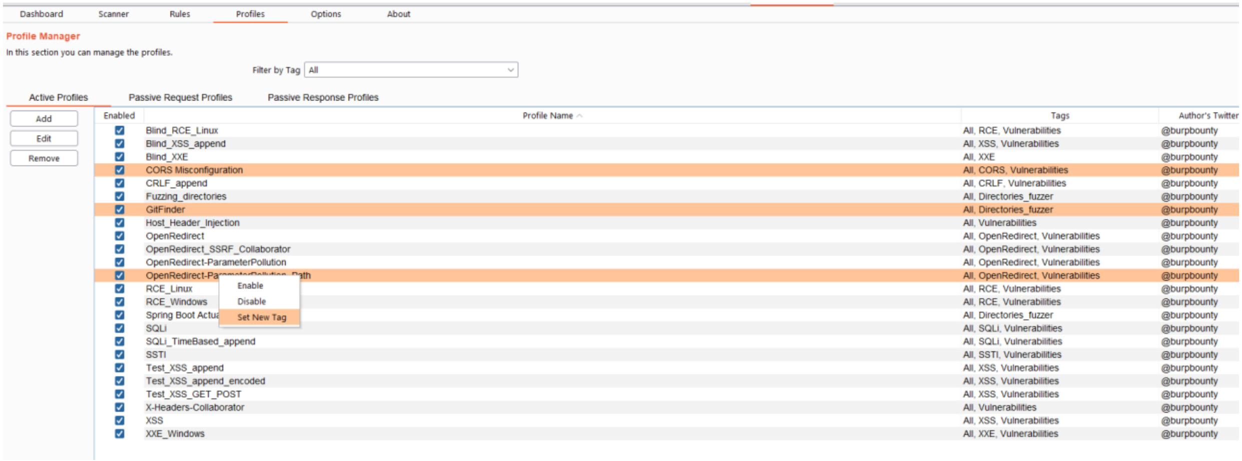
Filter by Tag: All

Active Profiles | Passive Request Profiles | Passive Response Profiles

Enabled	Profile Name	Tags	Author's Twitter
☑	Artica_Web_Proxy_Auth_Bypass_CVE-2020-17506	All, CVEs, Vulnerabilities	@burpbounty
☑	Atlassian_Crowd_RCE_CVE-2019-11580	All, CVEs, Vulnerabilities	@burpbounty
☑	Blind_RCE_Linux	All, Vulnerabilities, RCE	@burpbounty
☑	Blind_RCE_Windows	All, Vulnerabilities, RCE	@burpbounty
☑	Blind_XSS_append	All, XSS, Vulnerabilities	@burpbounty
☑	Blind_XSS_replace	All, XSS, Vulnerabilities	@burpbounty
☑	Blind_XXE	All, XXE, Vulnerabilities	@burpbounty
☑	Cisco_ASA_LFI-CVE-2020-3452	All, CVEs, Vulnerabilities	@burpbounty
☑	Cisco_Wan_VPN_disclosure-CVE-2019-1653	All, CVEs, Vulnerabilities	@burpbounty
☑	Citrix_ADC_Directory_Traversal_CVE-2019-19781	All, CVEs, Vulnerabilities	@burpbounty
☑	Citrix_ShareFile_File_Read_CVE-2020-8982	All, CVEs, Vulnerabilities	@burpbounty
☑	Citrix_XenMobile_PathTraversal	All, CVEs, Vulnerabilities	@burpbounty
☑	CORS Misconfiguration	All, CORS, Vulnerabilities	@burpbounty
☑	CouchDB_Admin_Exposure	All, CVEs, Vulnerabilities	@burpbounty
☑	CRLF_append	All, CRLF, Vulnerabilities	@burpbounty
☑	CRLF_replace	All, CRLF, Vulnerabilities	@burpbounty
☑	Drupal_User_Enum	All, Drupal, Vulnerabilities	@burpbounty
☑	Drupal_User_Enum_Redirect	All, Drupal, Vulnerabilities	@burpbounty
☑	Easy_wp_smtp_listing_enabled	All, Wordpress, Vulnerabilities	@burpbounty
☑	Echo_RCE_append	All, Vulnerabilities	@burpbounty
☑	Echo_RCE_replace	All, Vulnerabilities	@burpbounty
☑	Expect_RCE	All, Vulnerabilities	@burpbounty
☑	F5-BigIP_CVE-2020-5902	All, CVEs, Vulnerabilities	@burpbounty
☑	File_Manager_Wordpress_Backups_CVE-2020-24312	All, CVEs, Wordpress, Vulnerabilities	@burpbounty
☑	FortiOS_Creds_Disclosure_CVE-2018-13379	All, CVEs, Vulnerabilities	@burpbounty
☑	Fuzzing_directories	All, Directories_fuzzer	@burpbounty
☑	GitFinder	All, Directories_fuzzer	@burpbounty
☑	Host_Header_Injection	All, Vulnerabilities	@burpbounty
☑	Jira_Info_Exposure_CVE-2020-14179	All, CVEs, Vulnerabilities	@burpbounty
☑	Jira_Path_Traversal_CVE-2019-8442	All, CVEs, Vulnerabilities	@burpbounty
☑	Jira_SSRF_CVE-2017-9506	All, CVEs, Vulnerabilities	@burpbounty
☑	Jira_unauthenticated_Info	All, CVEs, Vulnerabilities	@burpbounty
☑	Jira_Unauthenticated_Sensitive_Info_CVE-2019-8449	All, CVEs, Vulnerabilities	@burpbounty
☑	Jira_User_Enum_CVE-2020-14181	All, CVEs, Vulnerabilities	@burpbounty
☑	Kubernetes_API_Exposed	All, Vulnerabilities	@burpbounty
☑	MAMGI_Auth_Bypass_CVE-2020-5777	All, CVEs, Vulnerabilities	@burpbounty
☑	Netsweeper_code_injection_CVE-2020-13167	All, CVEs, Vulnerabilities	@burpbounty
☑	NginX	All, Vulnerabilities, Nginx	@burpbouty
☑	Open Firebase Database	All, Vulnerabilities	@burpbounty
☑	OpenRedirect	All, OpenRedirect, Vulnerabilities	@burpbounty

You can add tags to multiples active profiles directly. You have to select the profiles that you want, and then right click->Set New Tag and add the Tag name.

1.



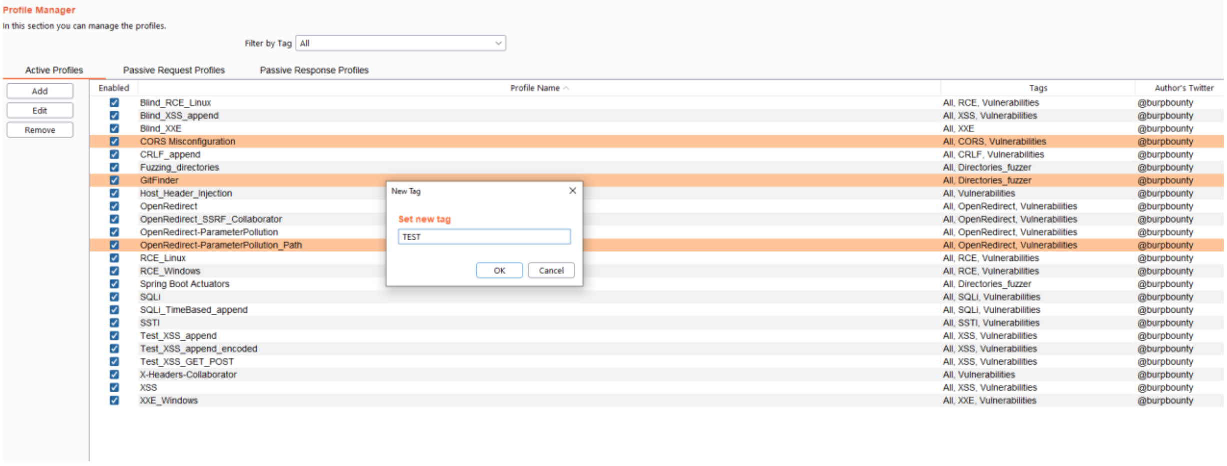
Profile Manager

In this section you can manage the profiles.

Filter by Tag: All

Enabled	Profile Name	Tags	Author's Twitter
☑	Blind_RCE_Linux	All, RCE, Vulnerabilities	@burpbounty
☑	Blind_XSS_append	All, XSS, Vulnerabilities	@burpbounty
☑	Blind_XXE	All, XXE	@burpbounty
☑	CORS Misconfiguration	All, CORS, Vulnerabilities	@burpbounty
☑	CRLF_append	All, CRLF, Vulnerabilities	@burpbounty
☑	Fuzzing_directories	All, Directories_fuzzer	@burpbounty
☑	GitFinder	All, Directories_fuzzer	@burpbounty
☑	Host_Header_Injection	All, Vulnerabilities	@burpbounty
☑	OpenRedirect	All, OpenRedirect, Vulnerabilities	@burpbounty
☑	OpenRedirect_SSRF_Collaborator	All, OpenRedirect, Vulnerabilities	@burpbounty
☑	OpenRedirect-ParameterPollution	All, OpenRedirect, Vulnerabilities	@burpbounty
☑	OpenRedirect-Pa Path	All, OpenRedirect, Vulnerabilities	@burpbounty
☑	RCE_Linux	All, RCE, Vulnerabilities	@burpbounty
☑	RCE_Windows	All, RCE, Vulnerabilities	@burpbounty
☑	Spring Boot Actua	All, Directories_fuzzer	@burpbounty
☑	SQLi	All, SQLi, Vulnerabilities	@burpbounty
☑	SQLi_TimeBased_append	All, SQLi, Vulnerabilities	@burpbounty
☑	SSTI	All, SSTI, Vulnerabilities	@burpbounty
☑	Test_XSS_append	All, XSS, Vulnerabilities	@burpbounty
☑	Test_XSS_append_encoded	All, XSS, Vulnerabilities	@burpbounty
☑	Test_XSS_GET_POST	All, XSS, Vulnerabilities	@burpbounty
☑	X-Headers-Collaborator	All, Vulnerabilities	@burpbounty
☑	XSS	All, XSS, Vulnerabilities	@burpbounty
☑	XXE_Windows	All, XXE, Vulnerabilities	@burpbounty

2.



Profile Manager

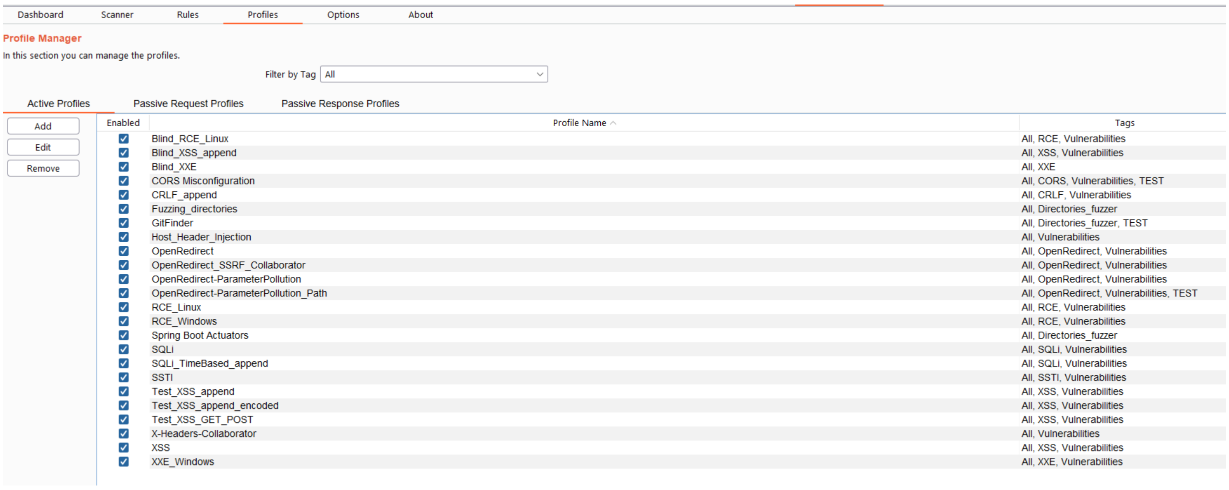
In this section you can manage the profiles.

Filter by Tag: All

Set new tag: TEST

Enabled	Profile Name	Tags	Author's Twitter
☑	Blind_RCE_Linux	All, RCE, Vulnerabilities	@burpbounty
☑	Blind_XSS_append	All, XSS, Vulnerabilities	@burpbounty
☑	Blind_XXE	All, XXE	@burpbounty
☑	CORS Misconfiguration	All, CORS, Vulnerabilities	@burpbounty
☑	CRLF_append	All, CRLF, Vulnerabilities	@burpbounty
☑	Fuzzing_directories	All, Directories_fuzzer	@burpbounty
☑	GitFinder	All, Directories_fuzzer	@burpbounty
☑	Host_Header_Injection	All, Vulnerabilities	@burpbounty
☑	OpenRedirect	All, OpenRedirect, Vulnerabilities	@burpbounty
☑	OpenRedirect_SSRF_Collaborator	All, OpenRedirect, Vulnerabilities	@burpbounty
☑	OpenRedirect-ParameterPollution	All, OpenRedirect, Vulnerabilities	@burpbounty
☑	OpenRedirect-ParameterPollution_Path	All, OpenRedirect, Vulnerabilities	@burpbounty
☑	RCE_Linux	All, RCE, Vulnerabilities	@burpbounty
☑	RCE_Windows	All, RCE, Vulnerabilities	@burpbounty
☑	Spring Boot Actuators	All, Directories_fuzzer	@burpbounty
☑	SQLi	All, SQLi, Vulnerabilities	@burpbounty
☑	SQLi_TimeBased_append	All, SQLi, Vulnerabilities	@burpbounty
☑	SSTI	All, SSTI, Vulnerabilities	@burpbounty
☑	Test_XSS_append	All, XSS, Vulnerabilities	@burpbounty
☑	Test_XSS_append_encoded	All, XSS, Vulnerabilities	@burpbounty
☑	Test_XSS_GET_POST	All, XSS, Vulnerabilities	@burpbounty
☑	X-Headers-Collaborator	All, Vulnerabilities	@burpbounty
☑	XSS	All, XSS, Vulnerabilities	@burpbounty
☑	XXE_Windows	All, XXE, Vulnerabilities	@burpbounty

3.



Profile Manager

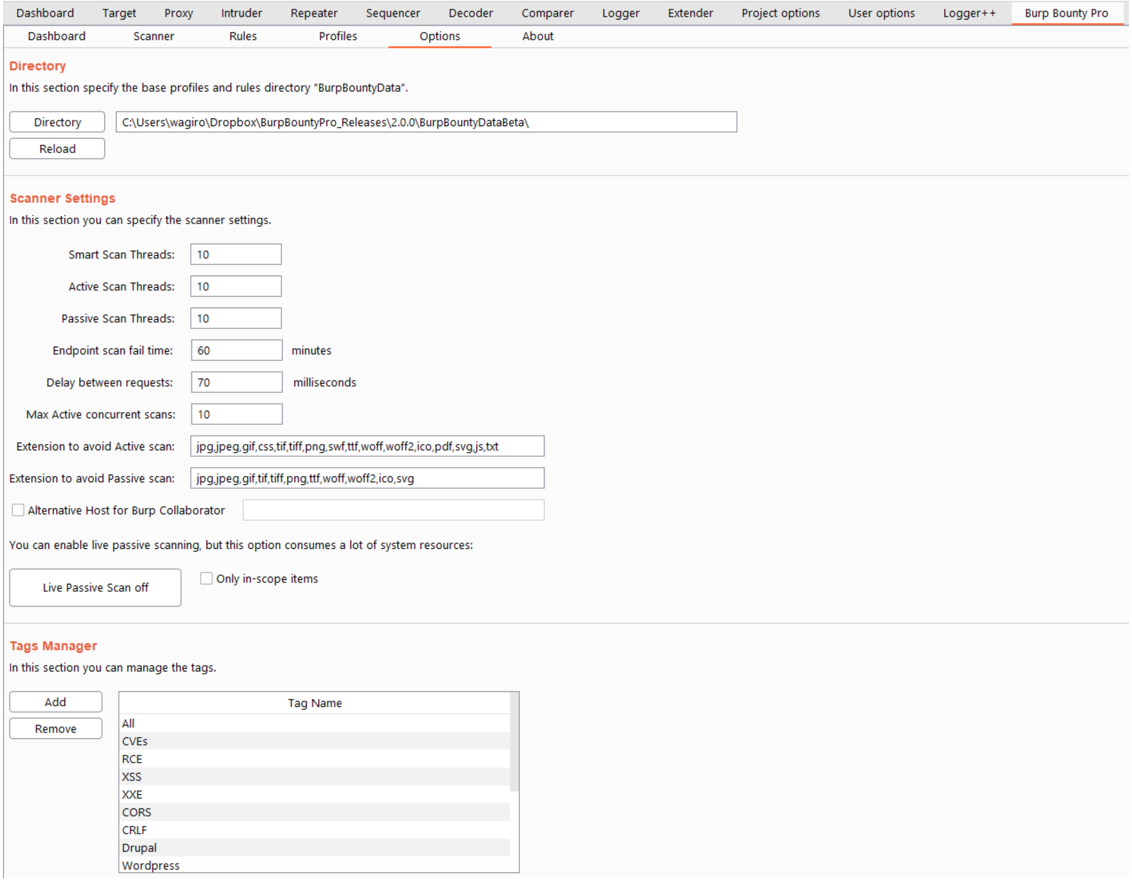
In this section you can manage the profiles.

Filter by Tag: All

Enabled	Profile Name	Tags
☑	Blind_RCE_Linux	All, RCE, Vulnerabilities
☑	Blind_XSS_append	All, XSS, Vulnerabilities
☑	Blind_XXE	All, XXE
☑	CORS Misconfiguration	All, CORS, Vulnerabilities, TEST
☑	CRLF_append	All, CRLF, Vulnerabilities
☑	Fuzzing_directories	All, Directories_fuzzer
☑	GitFinder	All, Directories_fuzzer, TEST
☑	Host_Header_Injection	All, Vulnerabilities
☑	OpenRedirect	All, OpenRedirect, Vulnerabilities
☑	OpenRedirect_SSRF_Collaborator	All, OpenRedirect, Vulnerabilities
☑	OpenRedirect-ParameterPollution	All, OpenRedirect, Vulnerabilities
☑	OpenRedirect-ParameterPollution_Path	All, OpenRedirect, Vulnerabilities, TEST
☑	RCE_Linux	All, RCE, Vulnerabilities
☑	RCE_Windows	All, RCE, Vulnerabilities
☑	Spring Boot Actuators	All, Directories_fuzzer
☑	SQLi	All, SQLi, Vulnerabilities
☑	SQLi_TimeBased_append	All, SQLi, Vulnerabilities
☑	SSTI	All, SSTI, Vulnerabilities
☑	Test_XSS_append	All, XSS, Vulnerabilities
☑	Test_XSS_append_encoded	All, XSS, Vulnerabilities
☑	Test_XSS_GET_POST	All, XSS, Vulnerabilities
☑	X-Headers-Collaborator	All, Vulnerabilities
☑	XSS	All, XSS, Vulnerabilities
☑	XXE_Windows	All, XXE, Vulnerabilities

Options

In this section you can specify different options for the extension.



Directory

In this section specify the base profiles and rules directory "BurpBountyData".

Directory: C:\Users\wagiro\Dropbox\BurpBountyPro_Releases\2.0.0\BurpBountyDataBeta\

Reload

Scanner Settings

In this section you can specify the scanner settings.

Smart Scan Threads: 10

Active Scan Threads: 10

Passive Scan Threads: 10

Endpoint scan fail time: 60 minutes

Delay between requests: 70 milliseconds

Max Active concurrent scans: 10

Extension to avoid Active scan: jpg,jpeg,gif,css,tif,tiff,png,swf,ttf,woff,woff2,ico,pdf,svg,js,txt

Extension to avoid Passive scan: jpg,jpeg,gif,tif,tiff,png,ttf,woff,woff2,ico,svg

☐ Alternative Host for Burp Collaborator

You can enable live passive scanning, but this option consumes a lot of system resources:

Live Passive Scan off ☐ Only in-scope items

Tags Manager

In this section you can manage the tags.

Add

Remove

Tag Name
All
CVEs
RCE
XSS
XXE
CORS
CRLF
Drupal
Wordpress

Directory: Here you can select de Burp Bounty Data folder (profiles and rules).

Scanner Settings:

- **Smart scan threads**: Here the threads that will be used in the active part of the smart scan are specified.
- **Active scan threads**: Here the threads that will be used in the active scanner are specified.
- **Passive scan threads**: Here the threads that will be used in the passive scanner are specified.
- **Endpoint scan fail time**: After the specified scan time has passed, the endpoint will go to the "failed" status and will continue with the next endpoint.
- **Delay between requests**: Delay between each request.
- **Max active concurrent scans**: This number specifies how many simultaneous endpoints will be scanned.
- **Extensions to avoid in the active scan**: Extensions that will not be scanned on the active scanner.

- **Extensions to avoid in the passive scan**: Extensions that will not be scanned on the passive scanner.
- **Alternative host for burp collaborator**: You can specify an alternative host to Burp collaborator, which will replace the token {BC}.
- **Live passive scan button**: Passive scanning can be started in live mode.
- **Only in-scope items**: The live passive scanner only takes into account the endpoints that are specified in the scope.

Tags Manager:

In this section you can add or delete Tags. If a Tag is deleted, it will be removed from all the profiles where it's assigned.

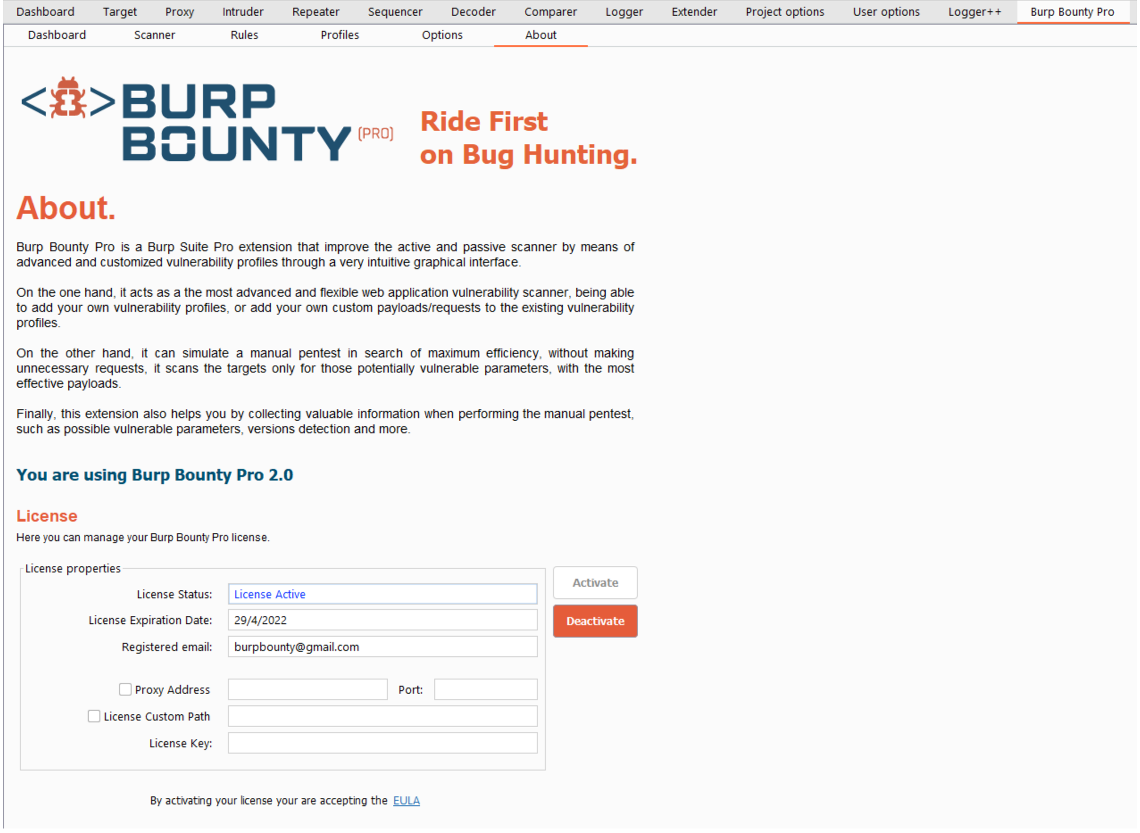
About

In this section you can view information about Burp Bounty Pro, as well as view the EULA and activate the license.

To activate the license you have to put the license number in the "License key" field and press the "Activate" button.

The "License Custom Path" field is for specifying the directory where the license.key file will be saved once it has been activated.

The "Proxy address" and "Port" field is to specify the IP address and port of the proxy to activate the license through proxy.



About.

Burp Bounty Pro is a Burp Suite Pro extension that improve the active and passive scanner by means of advanced and customized vulnerability profiles through a very intuitive graphical interface.

On the one hand, it acts as a the most advanced and flexible web application vulnerability scanner, being able to add your own vulnerability profiles, or add your own custom payloads/requests to the existing vulnerability profiles.

On the other hand, it can simulate a manual pentest in search of maximum efficiency, without making unnecessary requests, it scans the targets only for those potentially vulnerable parameters, with the most effective payloads.

Finally, this extension also helps you by collecting valuable information when performing the manual pentest, such as possible vulnerable parameters, versions detection and more.

You are using Burp Bounty Pro 2.0

License

Here you can manage your Burp Bounty Pro license.

License properties

License Status: License Active

License Expiration Date: 29/4/2022

Registered email: burpbounty@gmail.com

☐ Proxy Address: Port:

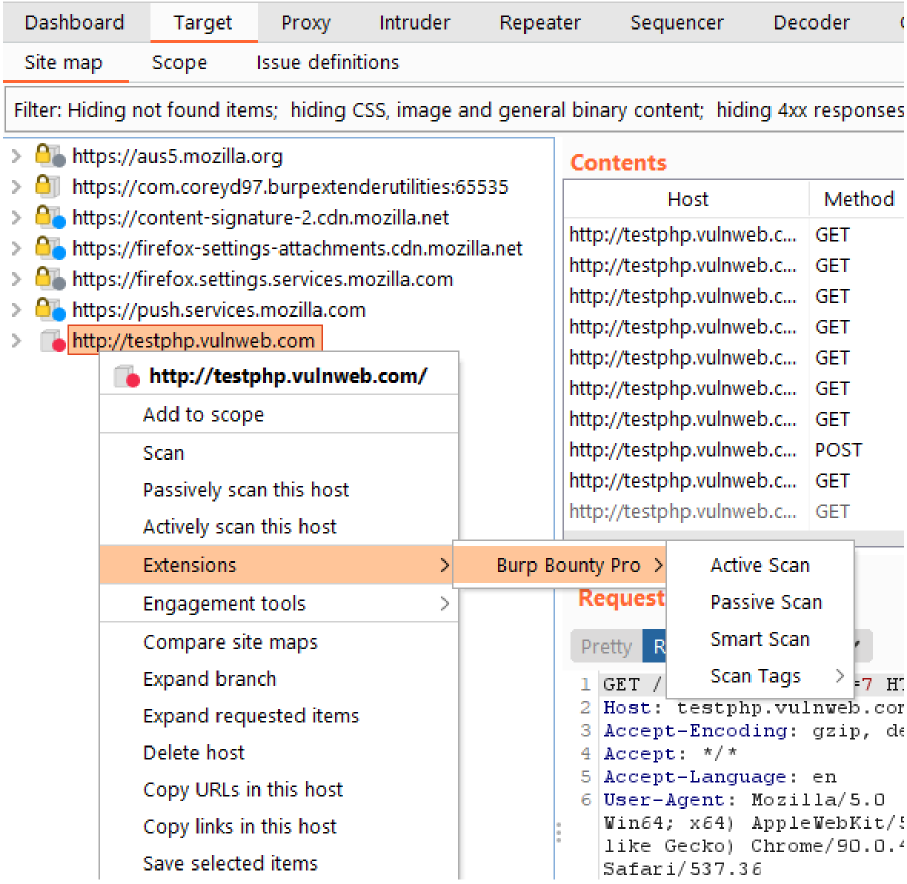
☐ License Custom Path:

License Key:

By activating your license your are accepting the EULA

2. Extension Usage

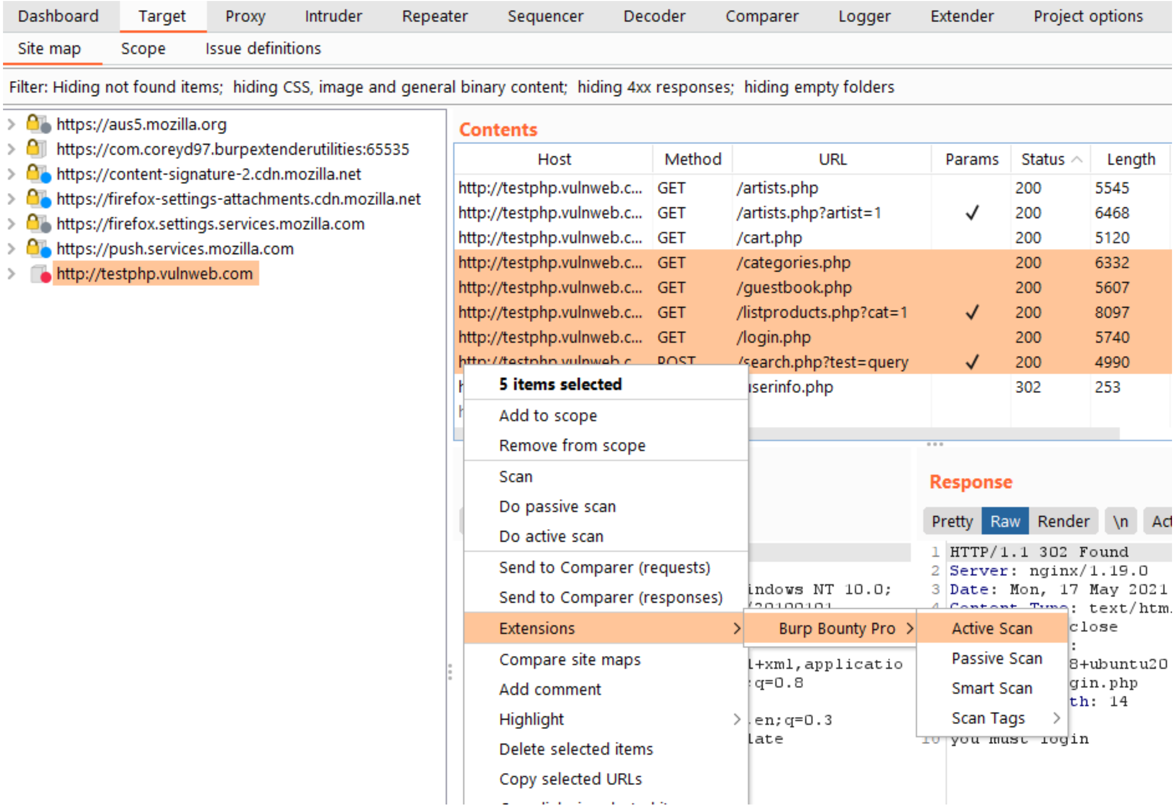
With Burp Bounty Pro 2 you can scan an entire domain in target:



Host	Method
http://testphp.vulnweb.c...	GET
http://testphp.vulnweb.c...	GET
http://testphp.vulnweb.c...	GET
http://testphp.vulnweb.c...	GET
http://testphp.vulnweb.c...	GET
http://testphp.vulnweb.c...	GET
http://testphp.vulnweb.c...	GET
http://testphp.vulnweb.c...	POST
http://testphp.vulnweb.c...	GET
http://testphp.vulnweb.c...	GET

```
GET /                    =7 HT
Host: testphp.vulnweb.cor
Accept-Encoding: gzip, de
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0
Win64; x64) AppleWebKit/5
like Gecko) Chrome/90.0.4
Safari/537.36
```

You can also scan several selected requests:



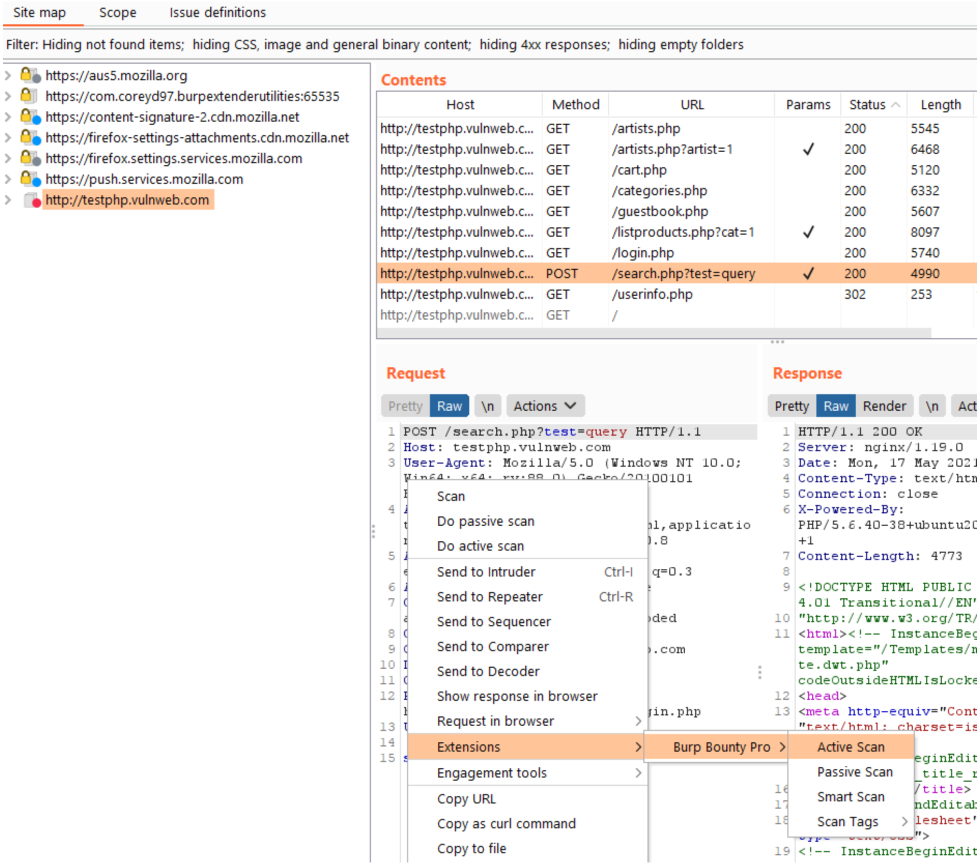
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://aus5.mozilla.org
- https://com.coreyd97.burpextenderutilities:65535
- https://content-signature-2.cdn.mozilla.net
- https://firefox-settings-attachments.cdn.mozilla.net
- https://firefox.settings.services.mozilla.com
- https://push.services.mozilla.com
- http://testphp.vulnweb.com

Host	Method	URL	Params	Status	Length
http://testphp.vulnweb.c...	GET	/artists.php		200	5545
http://testphp.vulnweb.c...	GET	/artists.php?artist=1	✓	200	6468
http://testphp.vulnweb.c...	GET	/cart.php		200	5120
http://testphp.vulnweb.c...	GET	/categories.php		200	6332
http://testphp.vulnweb.c...	GET	/guestbook.php		200	5607
http://testphp.vulnweb.c...	GET	/listproducts.php?cat=1	✓	200	8097
http://testphp.vulnweb.c...	GET	/login.php		200	5740
http://testphp.vulnweb.c...	POST	/search.php?test=query	✓	200	4990
		serinfo.php		302	253

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.19.0
3 Date: Mon, 17 May 2021
```

Or a simple request from Target, Repeater, History, etc:



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://aus5.mozilla.org
- https://com.coreyd97.burpextenderutilities:65535
- https://content-signature-2.cdn.mozilla.net
- https://firefox-settings-attachments.cdn.mozilla.net
- https://firefox.settings.services.mozilla.com
- https://push.services.mozilla.com
- http://testphp.vulnweb.com

Host	Method	URL	Params	Status	Length
http://testphp.vulnweb.c...	GET	/artists.php		200	5545
http://testphp.vulnweb.c...	GET	/artists.php?artist=1	✓	200	6468
http://testphp.vulnweb.c...	GET	/cart.php		200	5120
http://testphp.vulnweb.c...	GET	/categories.php		200	6332
http://testphp.vulnweb.c...	GET	/guestbook.php		200	5607
http://testphp.vulnweb.c...	GET	/listproducts.php?cat=1	✓	200	8097
http://testphp.vulnweb.c...	GET	/login.php		200	5740
http://testphp.vulnweb.c...	POST	/search.php?test=query	✓	200	4990
http://testphp.vulnweb.c...	GET	/userinfo.php		302	253
http://testphp.vulnweb.c...	GET	/			

```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0;
```

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 17 May 2021
Content-Type: text/htm
Connection: close
X-Powered-By:
PHP/5.6.40-38+ubuntu20
+1
Content-Length: 4773

<!DOCTYPE HTML PUBLIC
4.01 Transitional//EN"
"http://www.w3.org/TR/
<html><!-- InstanceBeg
template="/Templates/m
te.dwt.php"
codeOutsideHTMLIsLocke
<head>
<meta http-equiv="Cont
```

3. Scan methods

In the Burp Bounty Pro 2 version, nothing is scanned in live by default, now everything works through the right button.

1. Active Scan

Burp Bounty Pro gives you the ability to create your own vulnerability profiles to the active scanner.

The philosophy behind Burp Bounty's active profiles is simple:

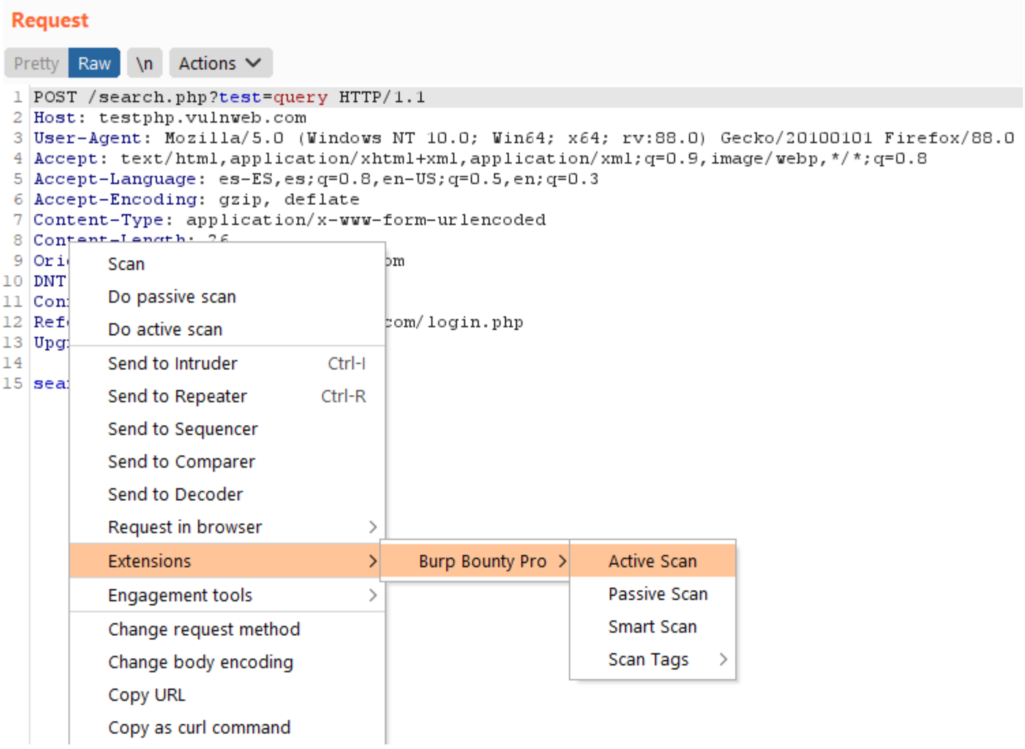
1. Profile payloads are inserted at the selected insertion points and the request is sent it to the server. Another option is use Raw request and sent it to the server.

2. In the HTTP response looks for a pattern (or patterns) with all the filtering options in the profiles.

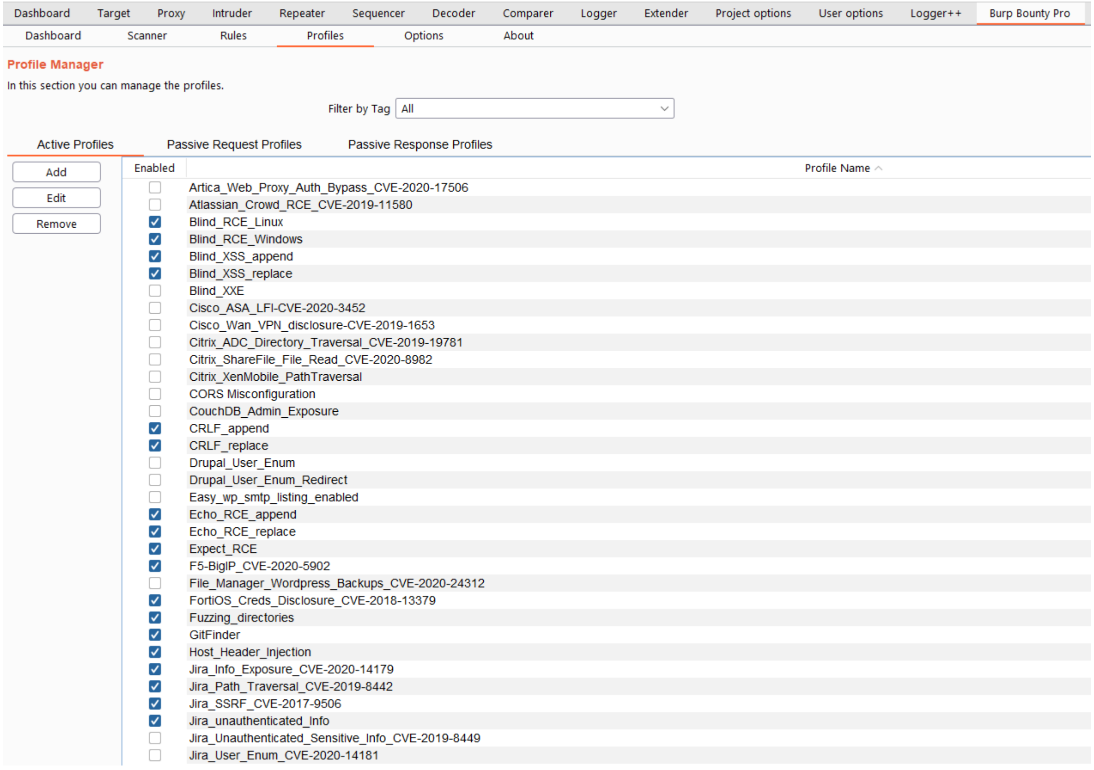
Operation:

1. The request insertion points are extracted.
2. All active profiles are executed.
3. If there is a vulnerability, it's reported.

If you scan one or multiple requests with the Active scan, you will launch against the request all the profiles that are active in the tab "Profiles-> Active Profiles"



```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Ori                                      om
DNT
Con
Ref                                      com/login.php
Upg

sea
```



Profile Manager

In this section you can manage the profiles.

Filter by Tag: All

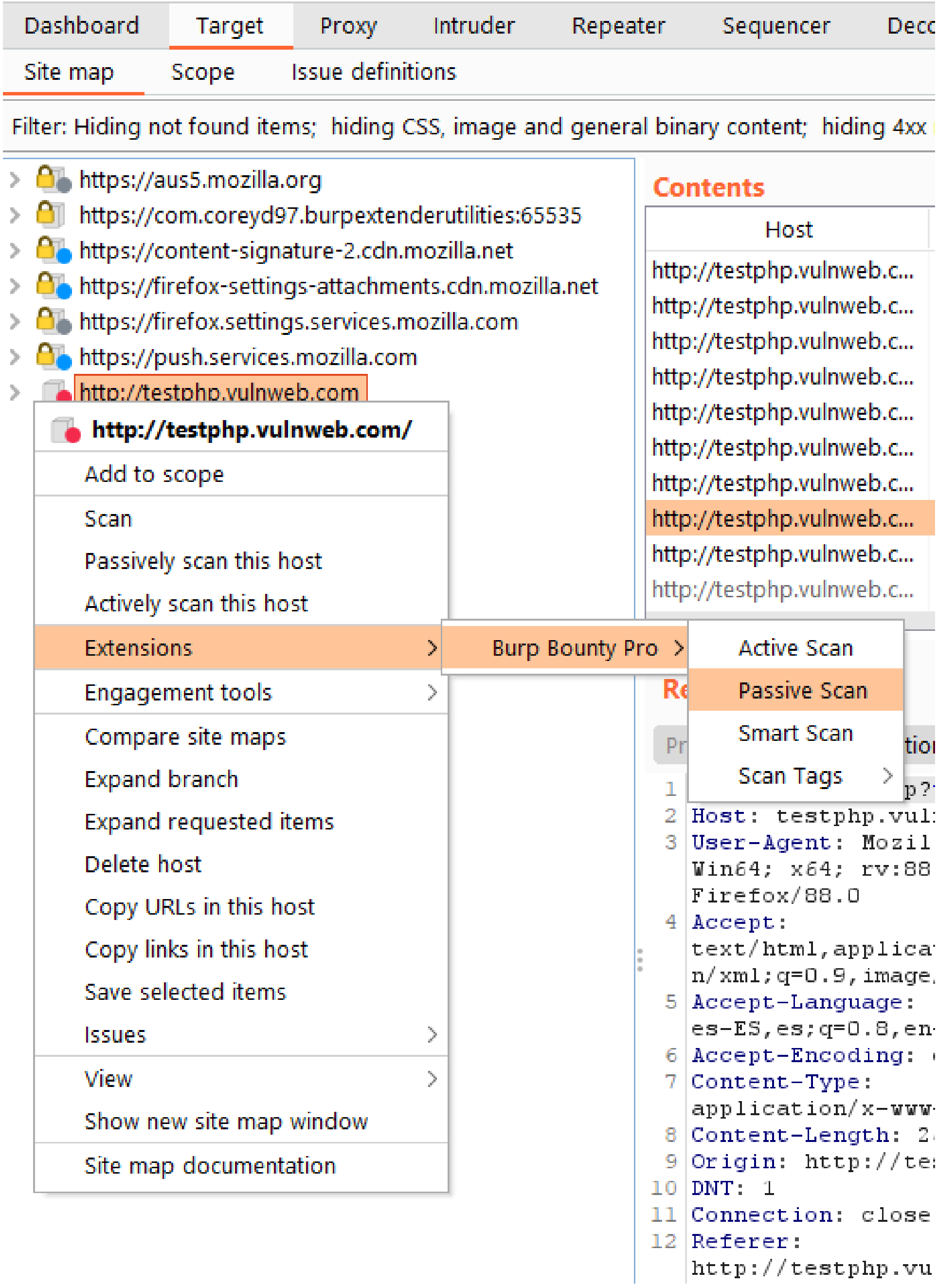
Enabled	Profile Name
□	Artica_Web_Proxy_Auth_Bypass_CVE-2020-17506
□	Atlassian_Crowd_RCE_CVE-2019-11580
☑	Blind_RCE_Linux
☑	Blind_RCE_Windows
☑	Blind_XSS_append
☑	Blind_XSS_replace
□	Blind_XXE
□	Cisco_ASA_LFI-CVE-2020-3452
□	Cisco_Wan_VPN_disclosure-CVE-2019-1653
□	Citrix_ADC_Directory_Traversal_CVE-2019-19781
□	Citrix_ShareFile_File_Read_CVE-2020-8982
□	Citrix_XenMobile_PathTraversal
□	CORS Misconfiguration
□	CouchDB_Admin_Exposure
☑	CRLF_append
☑	CRLF_replace
□	Drupal_User_Enum
□	Drupal_User_Enum_Redirect
□	Easy_wp_smtp_listing_enabled
☑	Echo_RCE_append
☑	Echo_RCE_replace
☑	Expect_RCE
☑	F5-BigIP_CVE-2020-5902
□	File_Manager_Wordpress_Backups_CVE-2020-24312
☑	FortiOS_Creds_Disclosure_CVE-2018-13379
☑	Fuzzing_directories
☑	GitFinder
☑	Host_Header_Injection
☑	Jira_Info_Exposure_CVE-2020-14179
☑	Jira_Path_Traversal_CVE-2019-8442
☑	Jira_SSRF_CVE-2017-9506
☑	Jira_unauthenticated_Info
□	Jira_Unauthenticated_Sensitive_Info_CVE-2019-8449
□	Jira_User_Enum_CVE-2020-14181

2. Passive Scan

The passive scanner doesn’t interact with HTTP traffic. Searches for patterns (or absence of them) in HTTP requests and responses.

A pattern is information detected through strings or a regular expression. If it detects a pattern, you get an alert.

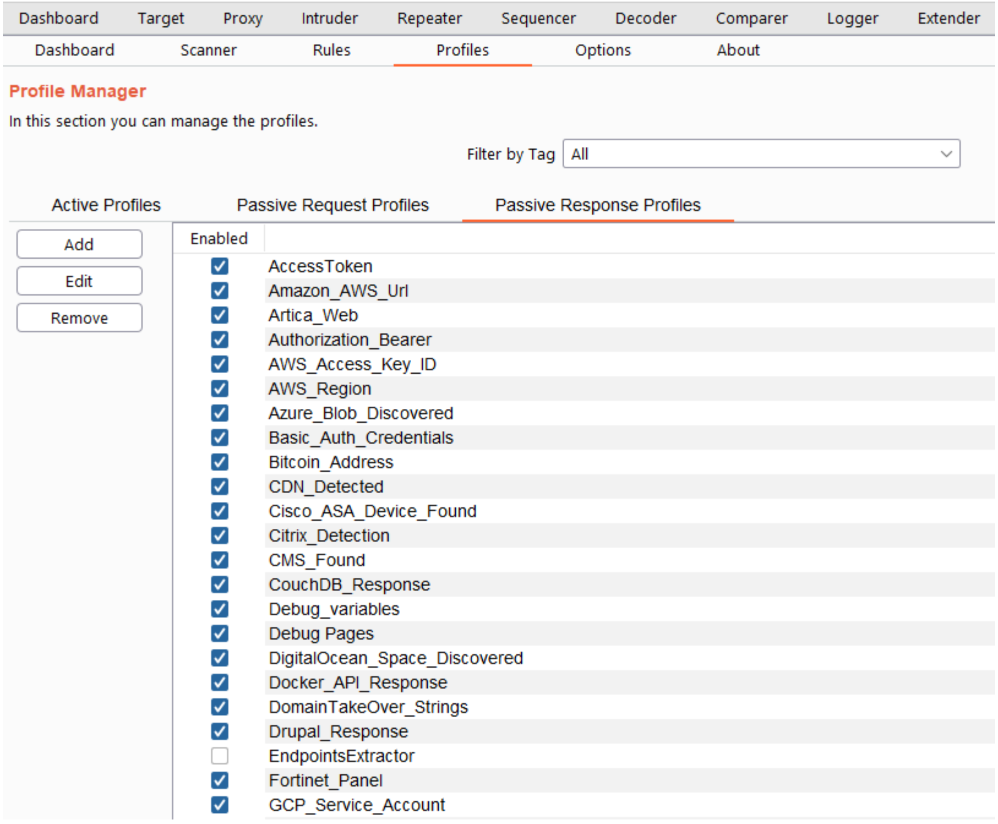
If you scan one or multiple requests with the Passive scan, you will launch against the request/response the profiles that are active in the tab "Profiles-> Passive Request Profiles" and "Profiles-> Passive Response Profiles". This scanner does not perform any request against the target, it only analyses the request/responses passively.



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx

Host
http://testphp.vulnweb.c...
http://testphp.vulnweb.c...
http://testphp.vulnweb.c...
http://testphp.vulnweb.c...
http://testphp.vulnweb.c...
http://testphp.vulnweb.c...
http://testphp.vulnweb.c...
http://testphp.vulnweb.c...
http://testphp.vulnweb.c...
http://testphp.vulnweb.c...

```
p?
Host: testphp.vul
User-Agent: Mozil
Win64; x64; rv:88
Firefox/88.0
Accept:
text/html,applica
n/xml;q=0.9,image,
Accept-Language:
es-ES,es;q=0.8,en
Accept-Encoding:
Content-Type:
application/x-www
Content-Length: 2
Origin: http://te
DNT: 1
Connection: close
Referer:
http://testphp.vu
```



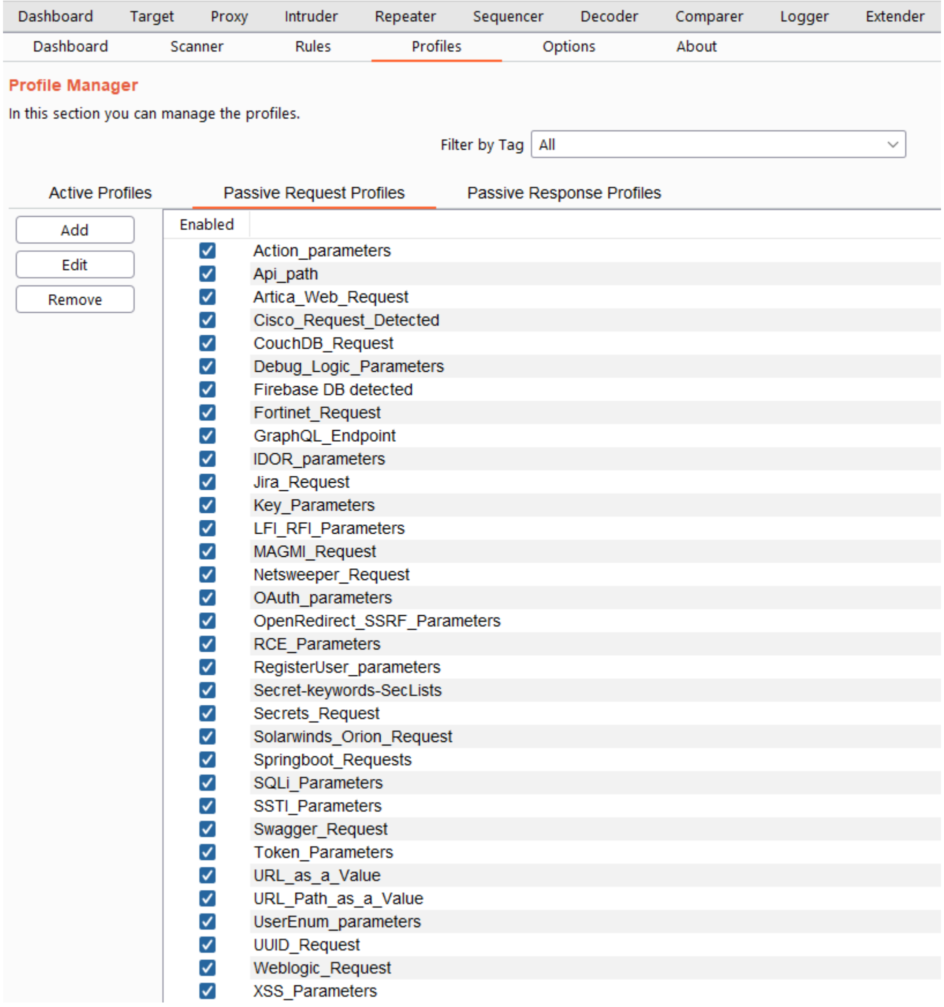
Profile Manager

In this section you can manage the profiles.

Filter by Tag: All

Enabled

- ☑ AccessToken
- ☑ Amazon_AWS_Url
- ☑ Artica_Web
- ☑ Authorization_Bearer
- ☑ AWS_Access_Key_ID
- ☑ AWS_Region
- ☑ Azure_Blob_Discovered
- ☑ Basic_Auth_Credentials
- ☑ Bitcoin_Address
- ☑ CDN_Detected
- ☑ Cisco_ASA_Device_Found
- ☑ Citrix_Detection
- ☑ CMS_Found
- ☑ CouchDB_Response
- ☑ Debug_variables
- ☑ Debug Pages
- ☑ DigitalOcean_Space_Discovered
- ☑ Docker_API_Response
- ☑ DomainTakeOver_Strings
- ☑ Drupal_Response
- □ EndpointsExtractor
- ☑ Fortinet_Panel
- ☑ GCP_Service_Account



Profile Manager

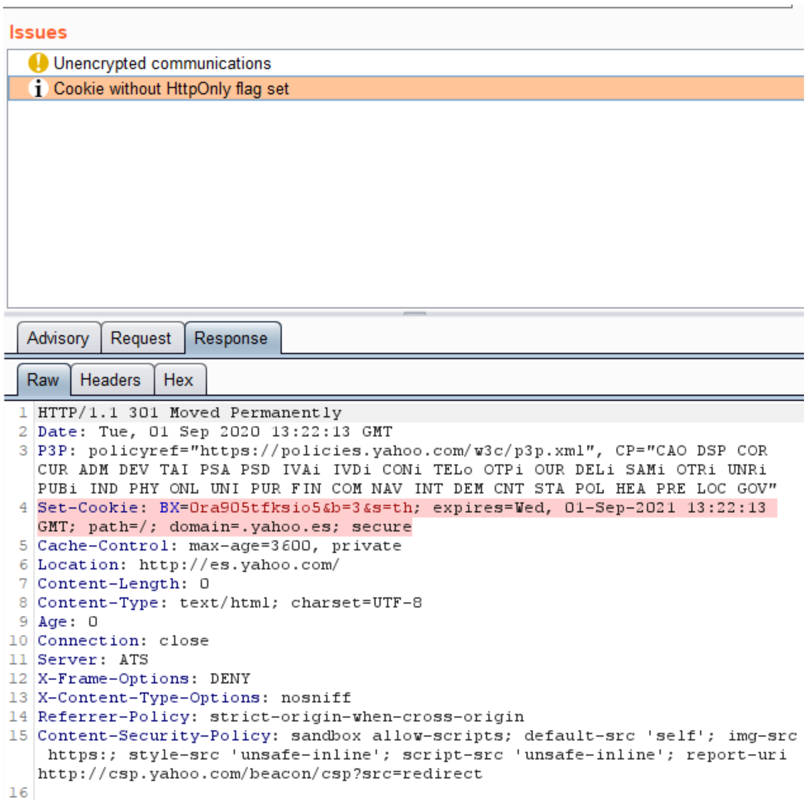
In this section you can manage the profiles.

Filter by Tag: All

Enabled

- ☑ Action_parameters
- ☑ Api_path
- ☑ Artica_Web_Request
- ☑ Cisco_Request_Detected
- ☑ CouchDB_Request
- ☑ Debug_Logic_Parameters
- ☑ Firebase DB detected
- ☑ Fortinet_Request
- ☑ GraphQL_Endpoint
- ☑ IDOR_parameters
- ☑ Jira_Request
- ☑ Key_Parameters
- ☑ LFI_RFI_Parameters
- ☑ MAGMI_Request
- ☑ Netsweeper_Request
- ☑ OAuth_parameters
- ☑ OpenRedirect_SSRF_Parameters
- ☑ RCE_Parameters
- ☑ RegisterUser_parameters
- ☑ Secret-keywords-SecLists
- ☑ Secrets_Request
- ☑ Solarwinds_Orion_Request
- ☑ Springboot_Requests
- ☑ SQLi_Parameters
- ☑ SSTI_Parameters
- ☑ Swagger_Request
- ☑ Token_Parameters
- ☑ URL_as_a_Value
- ☑ URL_Path_as_a_Value
- ☑ UserEnum_parameters
- ☑ UUID_Request
- ☑ Weblogic_Request
- ☑ XSS_Parameters

In this image you can see how an alert has been generated for the absence of a pattern. In this case, a Set cookie is detected, without HTTPOnly attribute set.

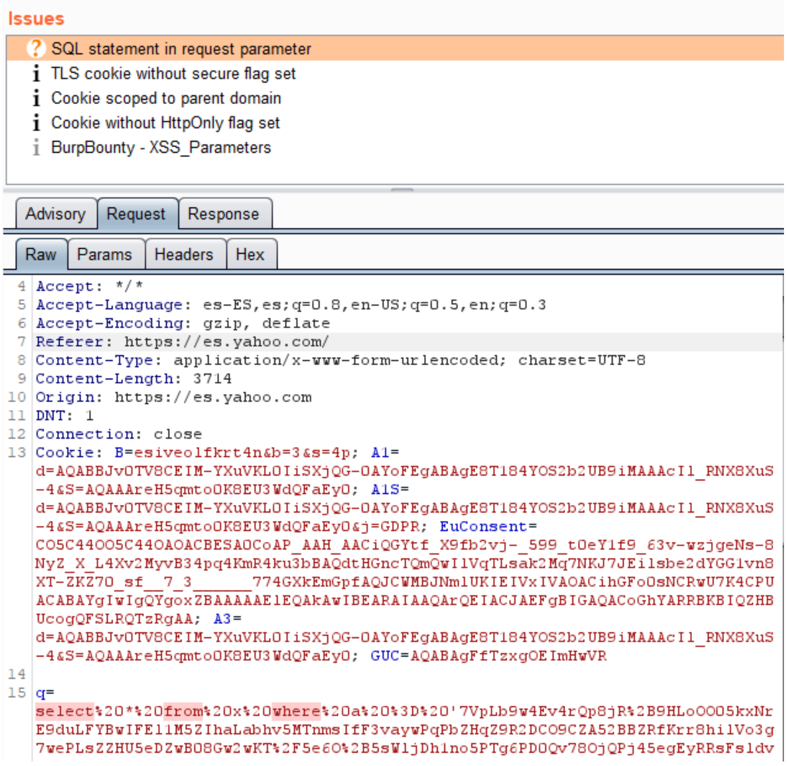


Issues

- Unencrypted communications
- Cookie without HttpOnly flag set

```
HTTP/1.1 301 Moved Permanently
Date: Tue, 01 Sep 2020 13:22:13 GMT
P3P: policyref="https://policies.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR
CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi
PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV"
Set-Cookie: BX=0ra905tfksio5&b=3&s=th; expires=Wed, 01-Sep-2021 13:22:13
GMT; path=/; domain=.yahoo.es; secure
Cache-Control: max-age=3600, private
Location: http://es.yahoo.com/
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Age: 0
Connection: close
Server: ATS
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Content-Security-Policy: sandbox allow-scripts; default-src 'self'; img-src
 https:; style-src 'unsafe-inline'; script-src 'unsafe-inline'; report-uri
http://csp.yahoo.com/beacon/csp?src=redirect

```

In next image, you can see how it detects an SQL statement in The HTTP Request. As you can see below, a "select" is detected followed by a "from" followed by "where".



Issues

- SQL statement in request parameter
- TLS cookie without secure flag set
- Cookie scoped to parent domain
- Cookie without HttpOnly flag set
- BurpBounty - XSS_Parameters

```
Accept: */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://es.yahoo.com/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 3714
Origin: https://es.yahoo.com
DNT: 1
Connection: close
Cookie: B=esiveolfkrt4n&b=3&s=4p; A1=
d=AQABBJvOTV8CEIM-YXuVKLOIiSXjQG-OAYoFEgABAgE8T184YOS2b2UB9iMAAAcIl_RNX8XuS
-4&S=AQAAAreH5qmtoOK8EU3WdQFaEy0; A1S=
d=AQABBJvOTV8CEIM-YXuVKLOIiSXjQG-OAYoFEgABAgE8T184YOS2b2UB9iMAAAcIl_RNX8XuS
-4&S=AQAAAreH5qmtoOK8EU3WdQFaEy0&j=GDPR; EuConsent=
CO5C44OO5C44OAOACBESAOCoAP_AAH_AACiQGYtf_X9fb2vj-_599_t0eY1f9_63v-wzjgeNs-8
NyZ_X_L4Xv2MyvB34pq4KmR4ku3bBAQdtHGncTQmQwIlVqTLsak2Mq7NKJ7JEilsbe2dYGG1vn8
XT-ZKZ70_sf__7_3______774GXkEmGpfAQJCWMBJNmlUKIEIVxIVAOACihGFoOsNCRwU7K4CPU
ACABAYgIwIgQYgoxZBAAAAAElEQAkAwIBEARAIAAQArQEIACJAEFgBIGAQACoGhYARRBKBIQZHB
UcogQFSLRQTzRgAA; A3=
d=AQABBJvOTV8CEIM-YXuVKLOIiSXjQG-OAYoFEgABAgE8T184YOS2b2UB9iMAAAcIl_RNX8XuS
-4&S=AQAAAreH5qmtoOK8EU3WdQFaEy0; GUC=AQABAgFfTzxgOEImHwVR

q=
select%20*%20from%20x%20where%20a%20%3D%20'7VpLb9w4Ev4rQp8jR%2B9HLoOO05kxNr
E9duLFYBwIFE11M5ZIhaLabhv5MTnmsIfF3vaywPqPbZHqZ9R2DCO9CZA52BBZRfKrr8hilVo3g
7wePLsZZHU5eDZwBO8Gw2wKT%2F5e60%2B5sWljDh1no5PTg6PDOQv78OjQPj45egEyRRsFsldv
```

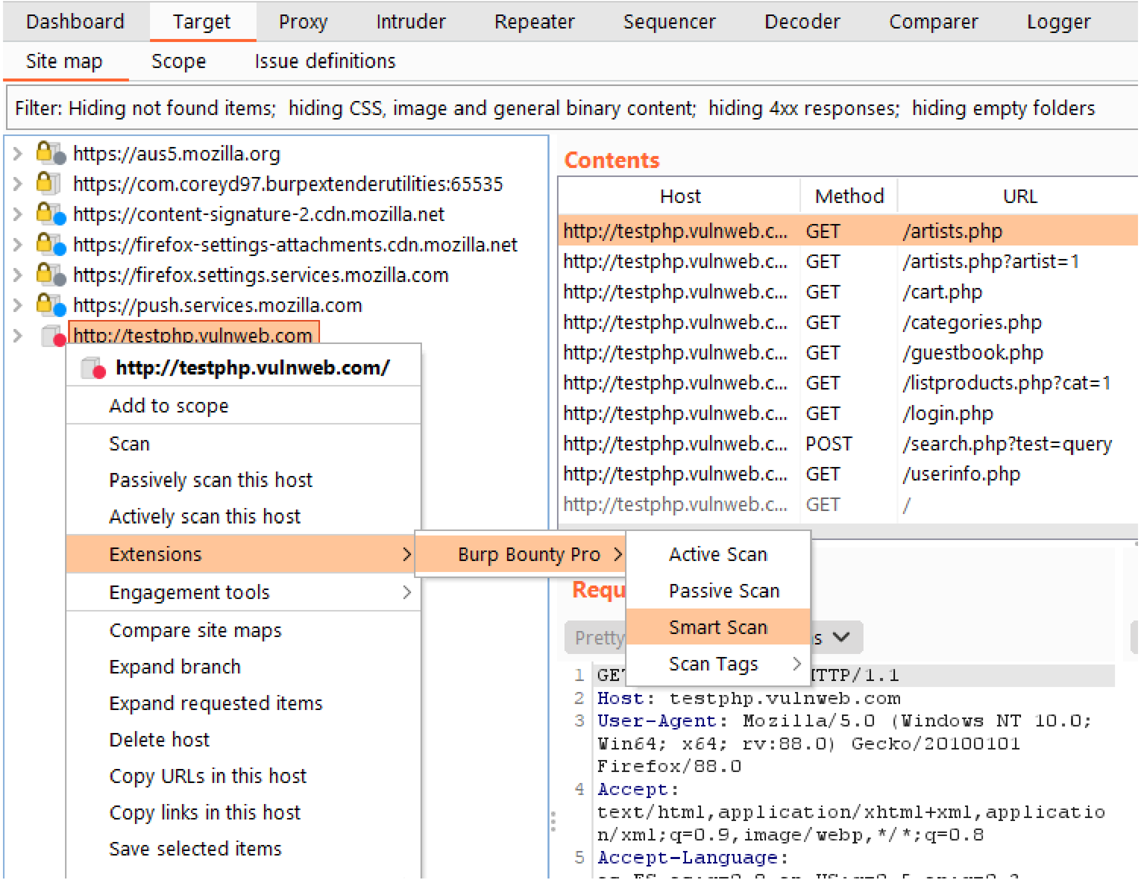
3. Smart Scan

If you scan a request or a domain with Smart Scan, attacks will be launched based on the enabled rules in the "Rules" section

The Smart Scan is a scanner that uses Burp Bounty Pro profiles to perform automatic attacks simulating the attacks that you would perform manually in a web application.

That is, if it detects an open redirect parameter, for example redirect_url, it will launch open redirect attacks only for that parameter.

You can create a rule to launch the automatic WordPress attacks, only when it has detected that the application you are analysing is a WordPress.



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

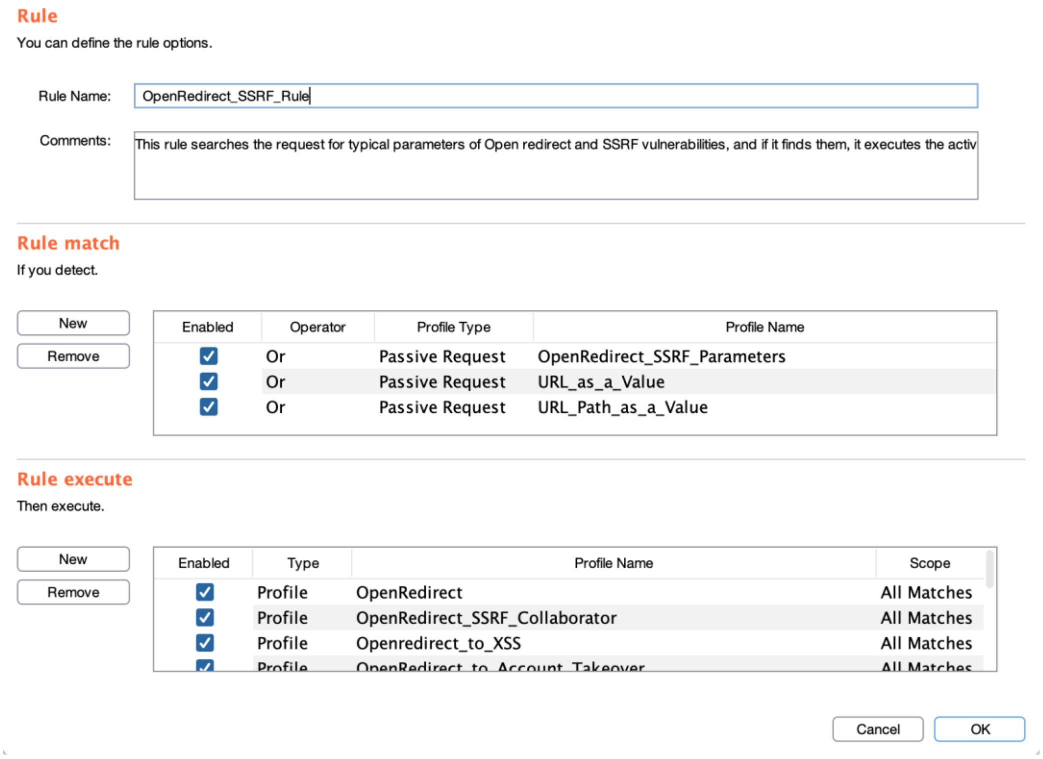
Host	Method	URL
http://testphp.vulnweb.c...	GET	/artists.php
http://testphp.vulnweb.c...	GET	/artists.php?artist=1
http://testphp.vulnweb.c...	GET	/cart.php
http://testphp.vulnweb.c...	GET	/categories.php
http://testphp.vulnweb.c...	GET	/guestbook.php
http://testphp.vulnweb.c...	GET	/listproducts.php?cat=1
http://testphp.vulnweb.c...	GET	/login.php
http://testphp.vulnweb.c...	POST	/search.php?test=query
http://testphp.vulnweb.c...	GET	/userinfo.php
http://testphp.vulnweb.c...	GET	/

```
GE  TTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept:
text/html,application/xhtml+xml,applicatio
n/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language:
```

The logic is simple:

1. You create a passive profile or several
2. You create an active profile or several
3. You create a rule, where you specify:
   - If you detect that Passive Profiles have generated an alert
   - Launches Active Profiles against the host that generated the alerts
   - If successful, it will generate an automatic alert

Create a rule:



Rule

You can define the rule options.

Rule Name: OpenRedirect_SSRF_Rule

Comments: This rule searches the request for typical parameters of Open redirect and SSRF vulnerabilities, and if it finds them, it executes the activ

Rule match

If you detect.

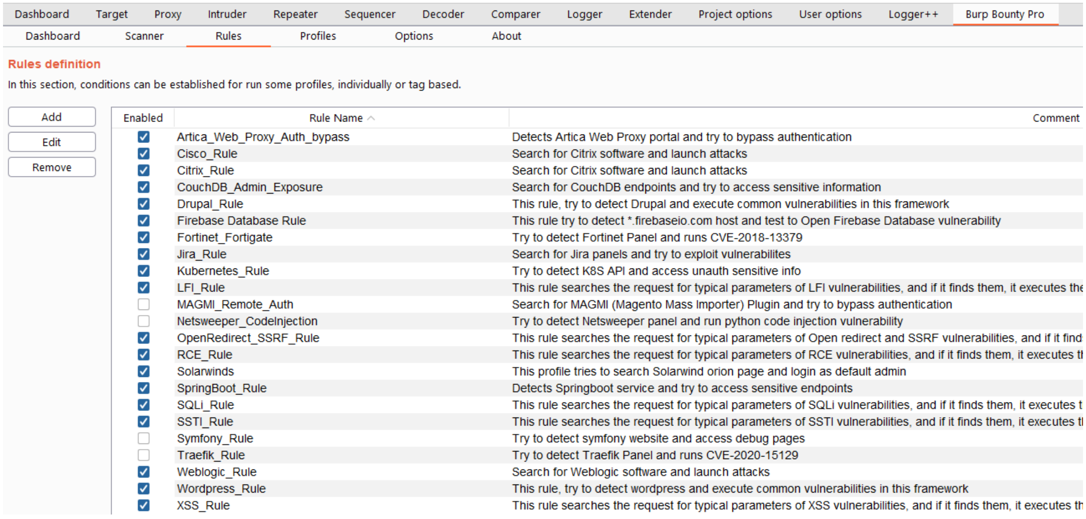
Enabled	Operator	Profile Type	Profile Name
☑	Or	Passive Request	OpenRedirect_SSRF_Parameters
☑	Or	Passive Request	URL_as_a_Value
☑	Or	Passive Request	URL_Path_as_a_Value

Rule execute

Then execute.

Enabled	Type	Profile Name	Scope
☑	Profile	OpenRedirect	All Matches
☑	Profile	OpenRedirect_SSRF_Collaborator	All Matches
☑	Profile	Openredirect_to_XSS	All Matches
☑	Profile	OpenRedirect_to_Account_Takeover	All Matches

Rules section:



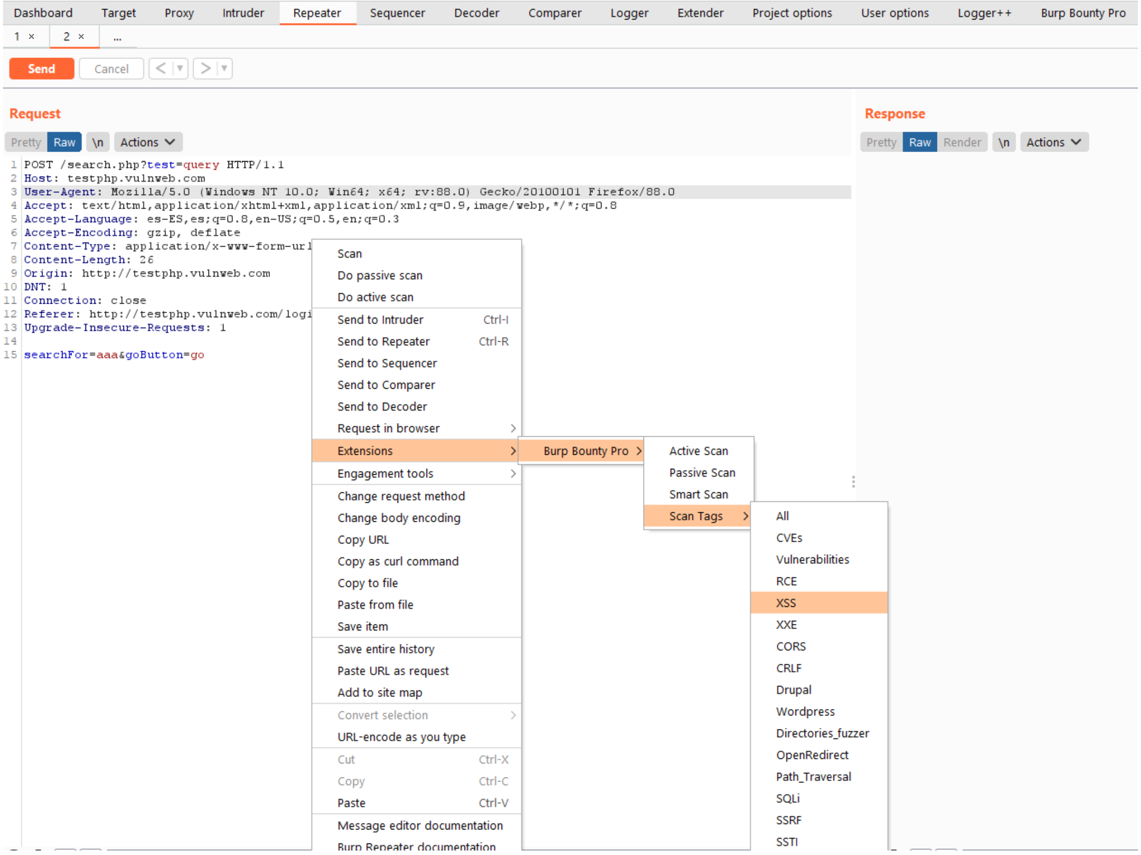
Rules definition

In this section, conditions can be established for run some profiles, individually or tag based.

Enabled	Rule Name	Comment
☑	Artica_Web_Proxy_Auth_bypass	Detects Artica Web Proxy portal and try to bypass authentication
☑	Cisco_Rule	Search for Citrix software and launch attacks
☑	Citrix_Rule	Search for Citrix software and launch attacks
☑	CouchDB_Admin_Exposure	Search for CouchDB endpoints and try to access sensitive information
☑	Drupal_Rule	This rule, try to detect Drupal and execute common vulnerabilities in this framework
☑	Firebase Database Rule	This rule try to detect *.firebaseio.com host and test to Open Firebase Database vulnerability
☑	Fortinet_Fortigate	Try to detect Fortinet Panel and runs CVE-2018-13379
☑	Jira_Rule	Search for Jira panels and try to exploit vulnerabilites
☑	Kubernetes_Rule	Try to detect K8S API and access unauth sensitive info
☑	LFI_Rule	This rule searches the request for typical parameters of LFI vulnerabilities, and if it finds them, it executes the
☐	MAGMI_Remote_Auth	Search for MAGMI (Magento Mass Importer) Plugin and try to bypass authentication
☐	Netsweeper_CodeInjection	Try to detect Netsweeper panel and run python code injection vulnerability
☑	OpenRedirect_SSRF_Rule	This rule searches the request for typical parameters of Open redirect and SSRF vulnerabilities, and if it find
☑	RCE_Rule	This rule searches the request for typical parameters of RCE vulnerabilities, and if it finds them, it executes t
☑	Solarwinds	This profile tries to search Solarwind orion page and login as default admin
☑	SpringBoot_Rule	Detects Springboot service and try to access sensitive endpoints
☑	SQLi_Rule	This rule searches the request for typical parameters of SQLi vulnerabilities, and if it finds them, it executes t
☑	SSTI_Rule	This rule searches the request for typical parameters of SSTI vulnerabilities, and if it finds them, it executes t
☐	Symfony_Rule	Try to detect symfony website and access debug pages
☐	Traefik_Rule	Try to detect Traefik Panel and runs CVE-2020-15129
☑	Weblogic_Rule	Search for Weblogic software and launch attacks
☑	Wordpress_Rule	This rule, try to detect wordpress and execute common vulnerabilities in this framework
☑	XSS_Rule	This rule searches the request for typical parameters of XSS vulnerabilities, and if it finds them, it executes th

4. Scan Tags

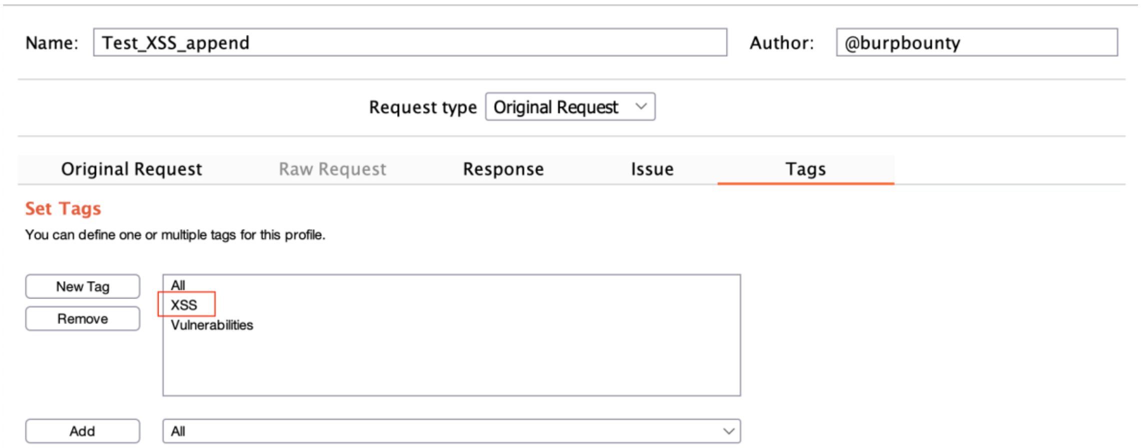
If you scan a request, several request or one entire domain with “Scan Tags->Some TAG”, the profiles that are tagged with "Some TAG" will be launched on that request/requests. For example, if you scan with Scan Tags->XSS, the profiles tagged with the XSS tag will be launched on the request/requests.



```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-url
Content-Length: 26
Origin: http://testphp.vulnweb.com
DNT: 1
Connection: close
Referer: http://testphp.vulnweb.com/logi
Upgrade-Insecure-Requests: 1

searchFor=aaa&goButton=go
```

Right click and “Scan tags->XSS”

The profiles with the Tag “XSS” will be launched. For example, the “Test XSS append” and “XSS” profiles.



Name: Test_XSS_append

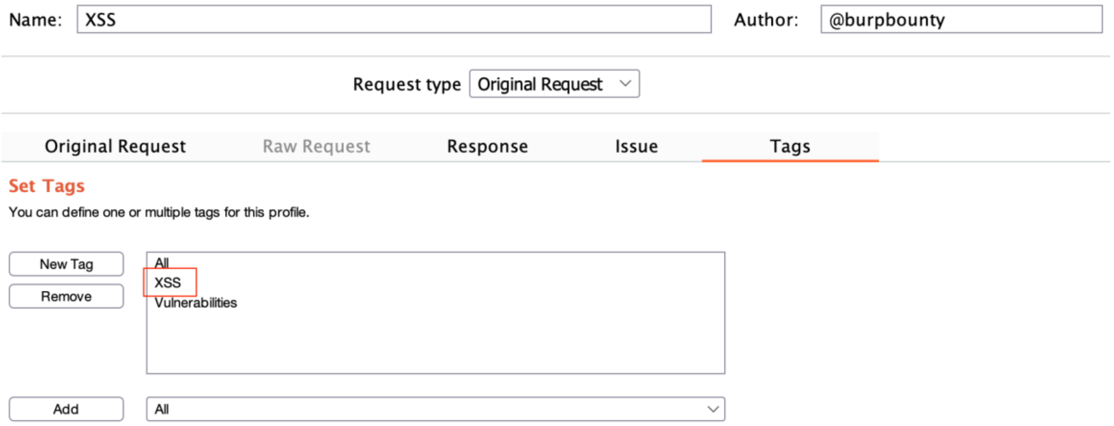
Author: @burpbounty

Request type: Original Request

Set Tags

You can define one or multiple tags for this profile.

All
XSS
Vulnerabilities



Name: XSS

Author: @burpbounty

Request type: Original Request

Set Tags

You can define one or multiple tags for this profile.

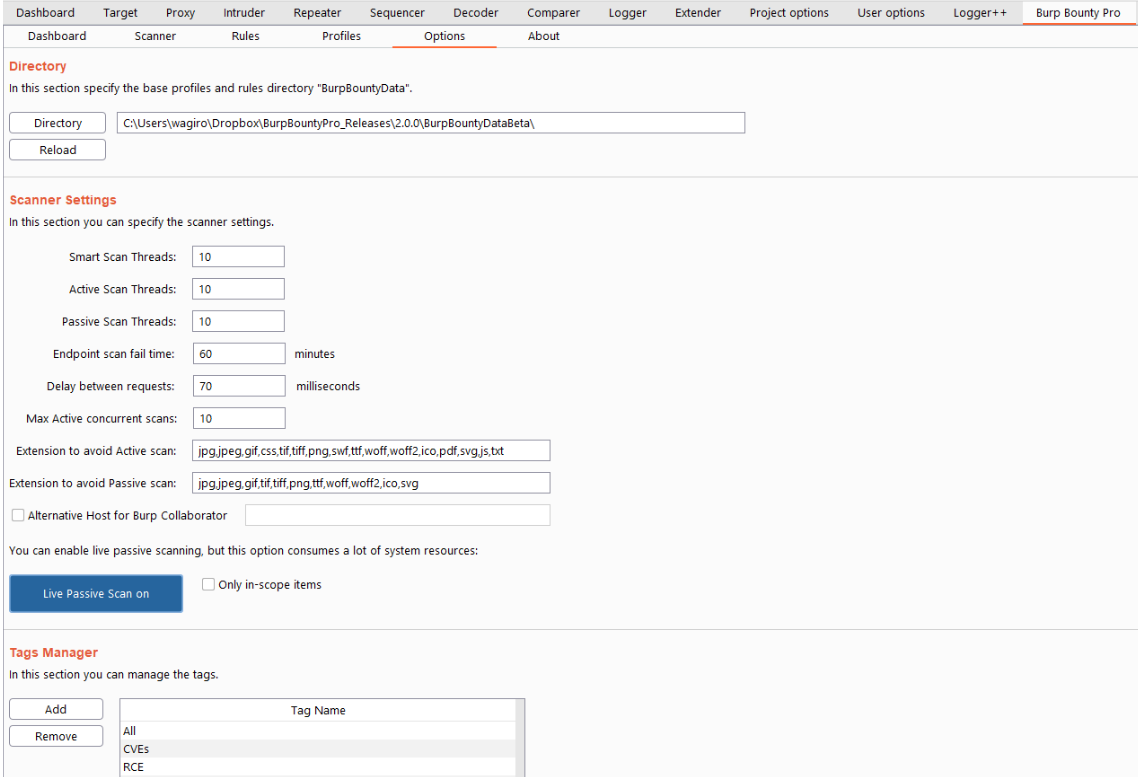
All
XSS
Vulnerabilities

All

You can create new tags and create your own profiles groups for be launched to a target.

5. Live Passive Scan

if you want to activate the live passive scanner by default, you can do it through the "Options" tab with “Live Passive Scan” button.



Directory

In this section specify the base profiles and rules directory "BurpBountyData".

Directory: C:\Users\wagiro\Dropbox\BurpBountyPro_Releases\2.0.0\BurpBountyDataBeta\

Reload

Scanner Settings

In this section you can specify the scanner settings.

Smart Scan Threads: 10

Active Scan Threads: 10

Passive Scan Threads: 10

Endpoint scan fail time: 60 minutes

Delay between requests: 70 milliseconds

Max Active concurrent scans: 10

Extension to avoid Active scan: jpg,jpeg,gif,css,tif,tiff,png,swf,ttf,woff,woff2,ico,pdf,svg,js,txt

Extension to avoid Passive scan: jpg,jpeg,gif,tif,tiff,png,ttf,woff,woff2,ico,svg

□ Alternative Host for Burp Collaborator

You can enable live passive scanning, but this option consumes a lot of system resources:

Live Passive Scan on

□ Only in-scope items

Tags Manager

In this section you can manage the tags.

Add

Remove

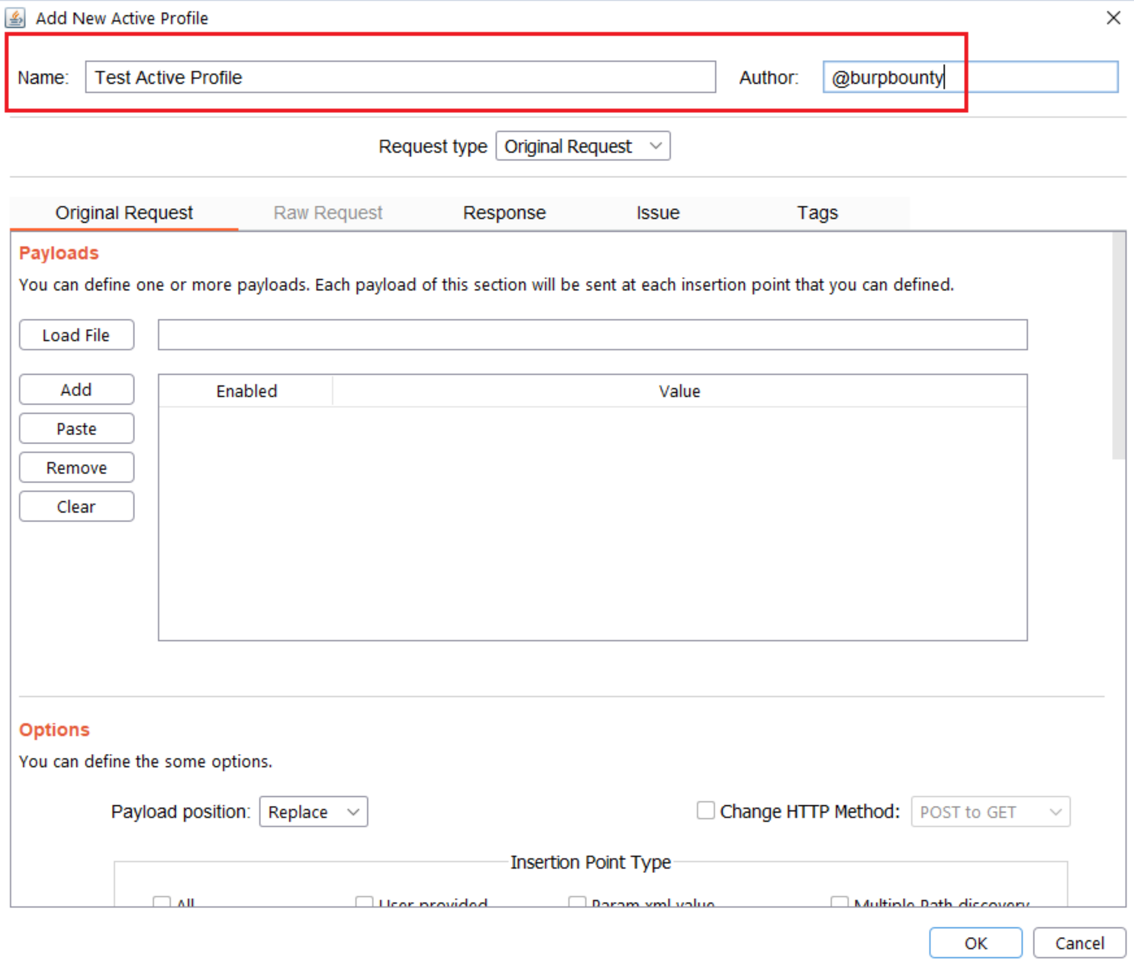
Tag Name
All
CVEs
RCE

4. Profiles

Active Profiles

Burp Bounty Pro gives you the ability to create your own vulnerability profiles to the active scanner.

Step 1 (Required): The name and author of the profile are first set.



Add New Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Payloads

You can define one or more payloads. Each payload of this section will be sent at each insertion point that you can defined.

Options

You can define the some options.

Payload position: Replace

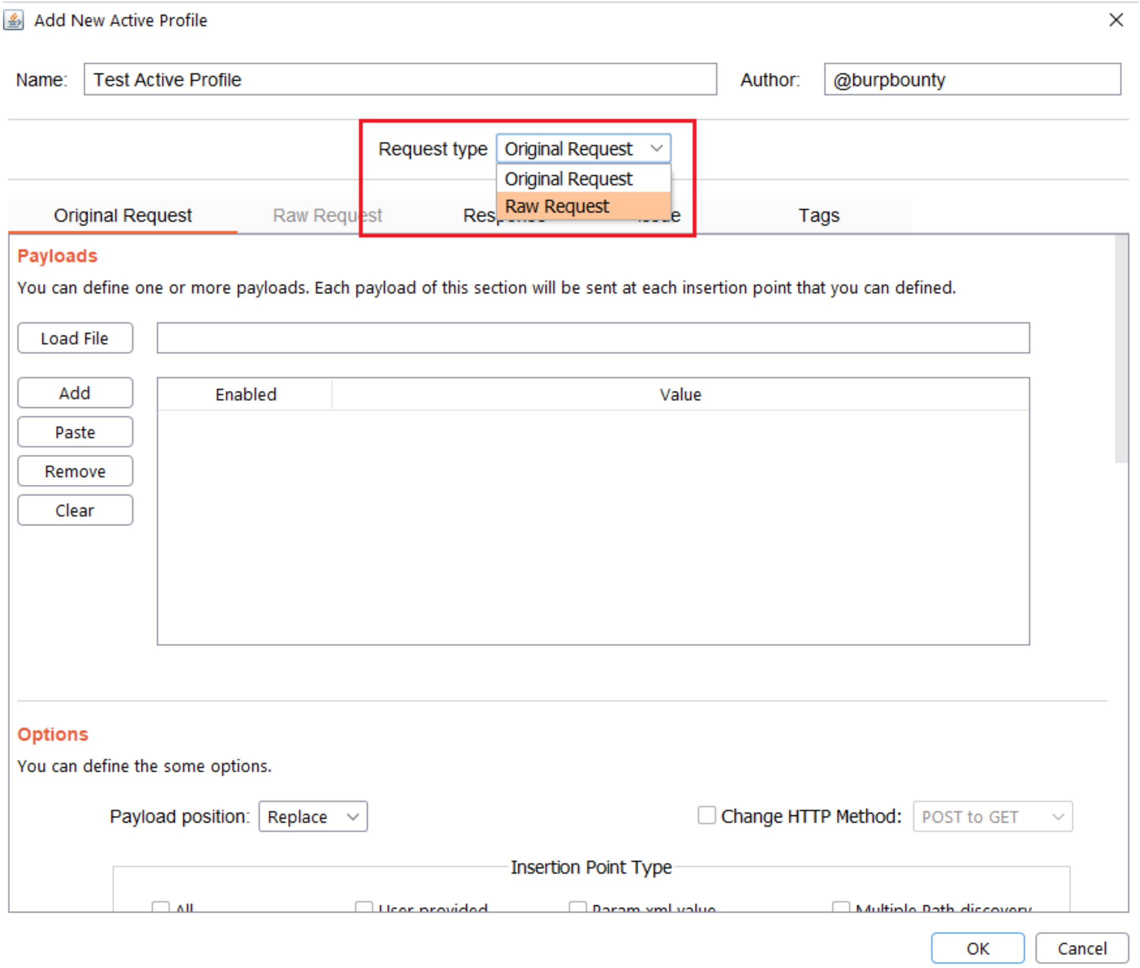
□ Change HTTP Method: POST to GET

Insertion Point Type

□ All □ User provided □ Param xml value □ Multiple Path discovery

Step 2 (Required): Here you can choose the request type:

- **Original Request**: The extension get the original request that is sended to the scanner, extract insertion points, put the payloads in the selected insertion points, makes the necessary modifications and sends it to the server.
- **Raw Request**: You specify a new request, inheriting fields from the original request.



Add New Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Payloads

You can define one or more payloads. Each payload of this section will be sent at each insertion point that you can defined.

Options

You can define the some options.

Payload position: Replace

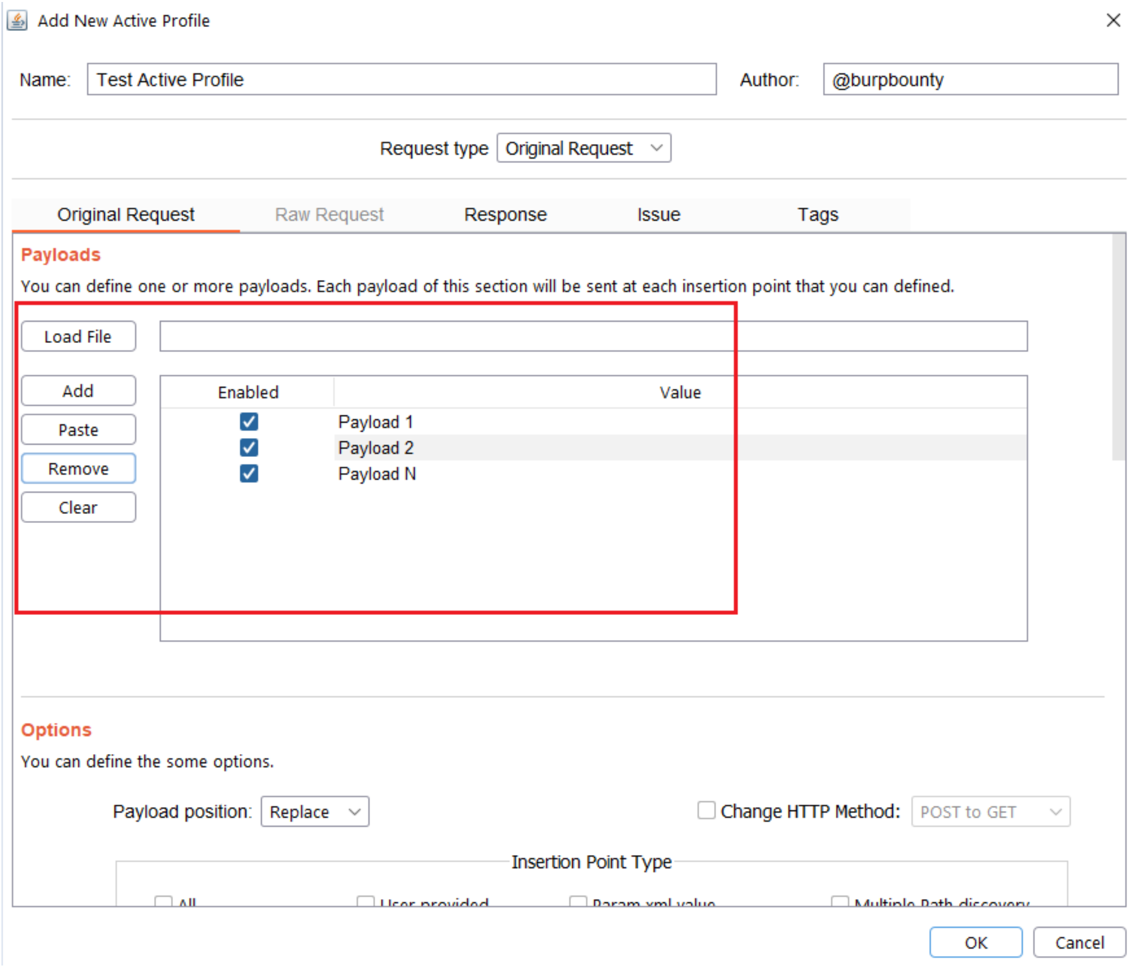
□ Change HTTP Method: POST to GET

Insertion Point Type

□ All □ User provided □ Param xml value □ Multiple Path discovery

Step 2.1 (Required)- Original Request -> Payloads: It sets the payload or payloads that will be sent in the selected request insertion points.

- You can add the Payload by click on the "add" button and modifying the value, or by pasting it directly with the "Paste" button if you already have it in the clipboard.
- You can also load a payloads file (one per line) with the "Load file" button.



Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Payloads

You can define one or more payloads. Each payload of this section will be sent at each insertion point that you can defined.

Enabled	Value
☑	Payload 1
☑	Payload 2
☑	Payload N

Options

You can define the some options.

Payload position: Replace

□ Change HTTP Method: POST to GET

Insertion Point Type

□ All □ User provided □ Param xml value □ Multiple Path discovery

Step 2.2 (Required)- Original Request -> Payload Position:

The Payload position field is to specify where each of the payloads defined in the profiles will be established. For example in a request:

```
GET /listproducts.php?cat=123456 HTTP/1.1
Host: testphp.vulnweb.com
```

Suppose that we have specified the Insertion point type is Param url value (123456). If we have the **'-alert(1)-'** as a payload, the Payload position can be the following:

Replace: the original value is replaced.

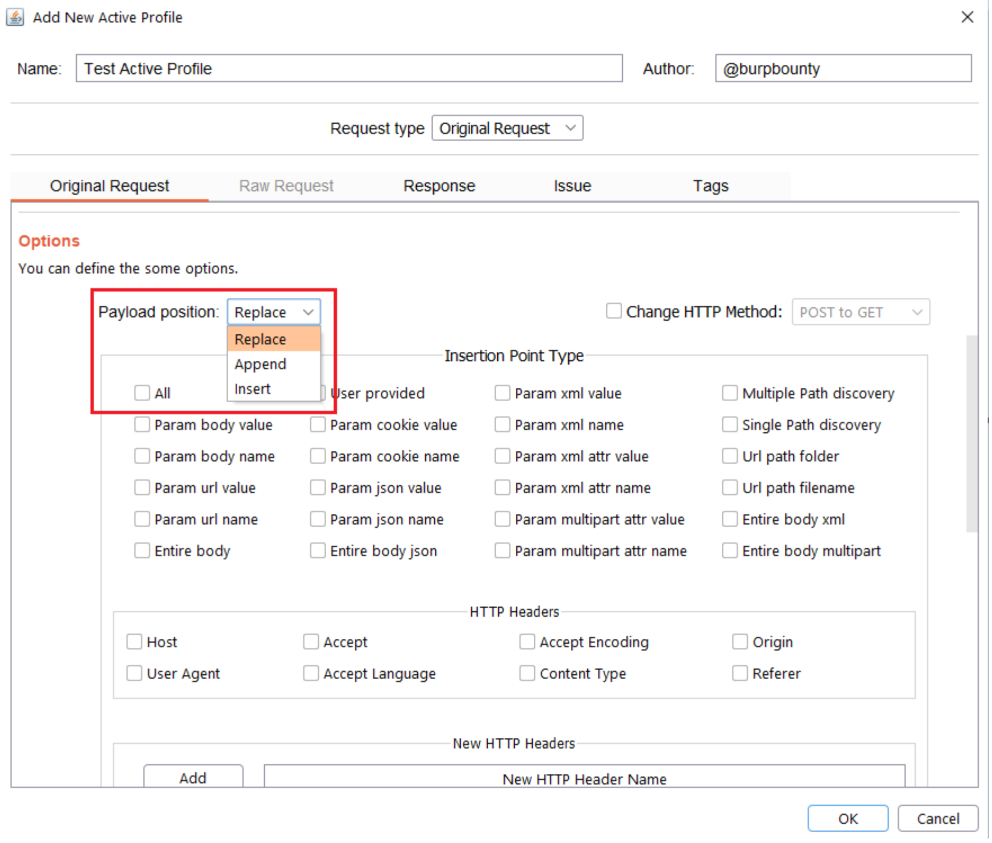
```
GET /listproducts.php?cat='-alert(1)-' HTTP/1.1
Host: testphp.vulnweb.com
```

Append: The value of the payload is added to the original value.

```
GET /listproducts.php?cat=123456'-alert(1)-' HTTP/1.1
Host: testphp.vulnweb.com
```

Insert: The value of the payload is inserted in the middle of the original value.

```
GET /listproducts.php?cat=123'-alert(1)-'456 HTTP/1.1
Host: testphp.vulnweb.com
```



Add New Active Profile

Name: Test Active Profile   Author: @burpbounty

Request type: Original Request

Original Request | Raw Request | Response | Issue | Tags

Options

You can define the some options.

Payload position: Replace

□ Change HTTP Method: POST to GET

Insertion Point Type

□ All   □ User provided   □ Param xml value   □ Multiple Path discovery
□ Param body value   □ Param cookie value   □ Param xml name   □ Single Path discovery
□ Param body name   □ Param cookie name   □ Param xml attr value   □ Url path folder
□ Param url value   □ Param json value   □ Param xml attr name   □ Url path filename
□ Param url name   □ Param json name   □ Param multipart attr value   □ Entire body xml
□ Entire body   □ Entire body json   □ Param multipart attr name   □ Entire body multipart

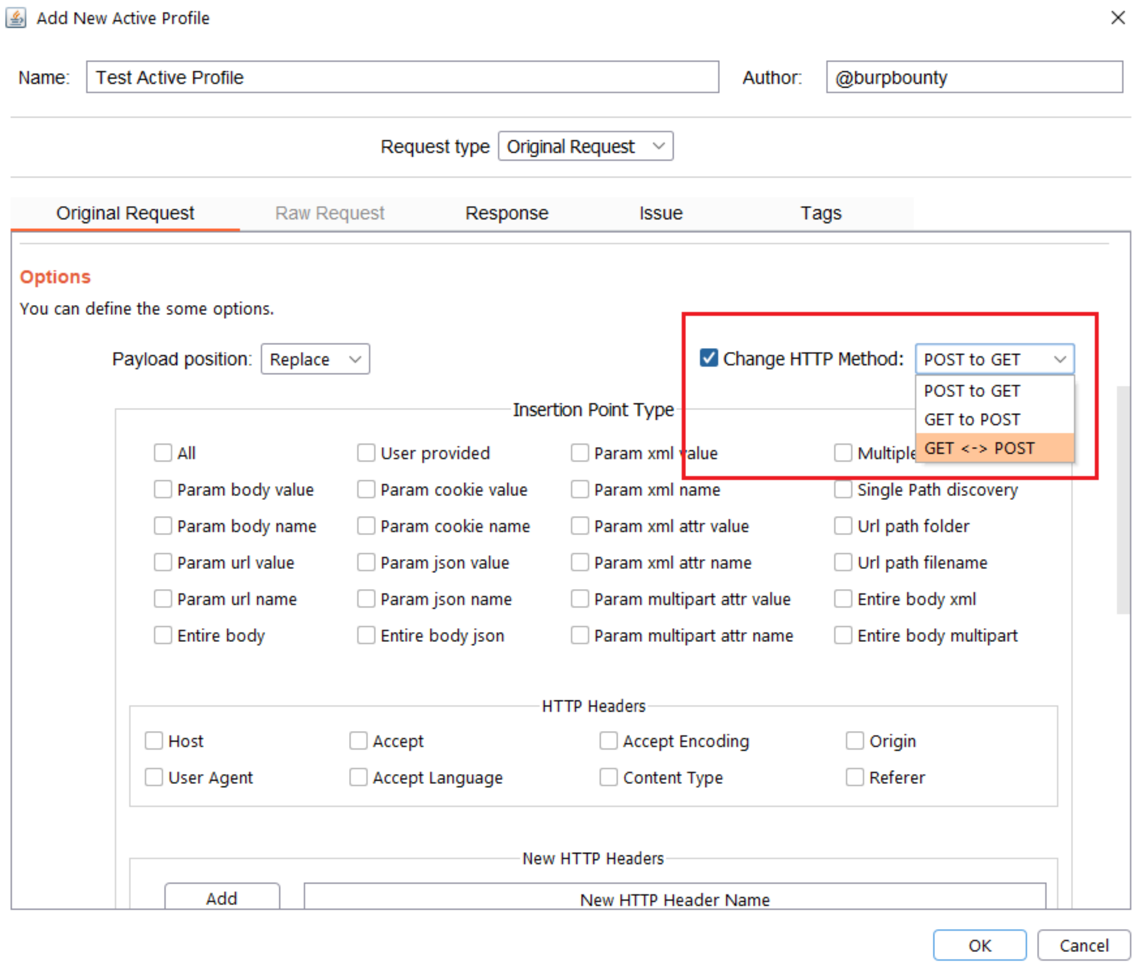
HTTP Headers

□ Host   □ Accept   □ Accept Encoding   □ Origin
□ User Agent   □ Accept Language   □ Content Type   □ Referer

New HTTP Headers

Step 2.3 (Optional)- Original Request -> Change HTTP Method:

- **POST to GET**: If this option is selected, when scanning a POST HTTP request with this profile, it will first change the request method to GET and then do the tests.
- **GET to POST**: If this option is selected, when scanning a GET HTTP request with this profile, it will first change the request method to POST and then do the tests.
- **GET <-> POST**: If this option is selected, when scanning a GET HTTP request with this profile, it will first change the request method to POST and then do the tests. On the other hand, when scanning a POST HTTP request with this profile, it will first change the request method to GET and then do the tests.



Add New Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Options

You can define the some options.

Payload position: Replace

☑ Change HTTP Method: POST to GET

Step 2.4 (Required)- Original Request -> Insertion Point Type:

Here you can select the insertion points where you want the payloads to be sent.

The insertion points are the zones of the HTTP request where the specified payload will be placed. For example in this HTTP request:

```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

If the payload **<script>alert (1)</script>** is specified and the insertion point "Param body value" is selected, the HTTP requests that Burp Bounty Pro will make will be:

1. Change “test” value for the payload:

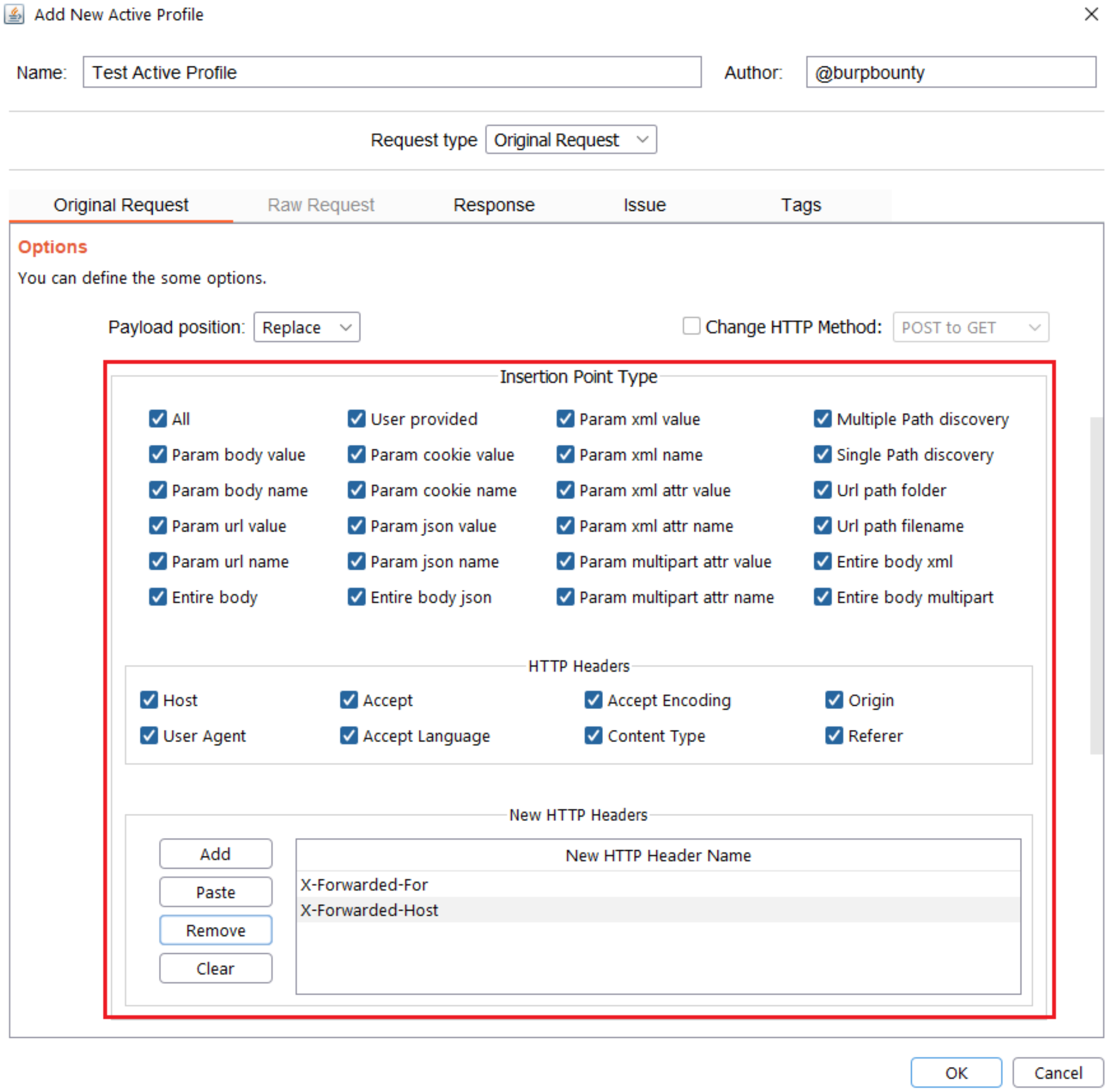
```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=<script>alert (1)</script>&goButton=go
```

2. Change “go” value, for the payload:

```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
```

```
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=<script>alert (1)</script>
```

Below you can see in detail each insertion point type.



Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Options

You can define the some options.

Payload position: Replace

□ Change HTTP Method: POST to GET

Insertion Point Type

☑ All	☑ User provided	☑ Param xml value	☑ Multiple Path discovery
☑ Param body value	☑ Param cookie value	☑ Param xml name	☑ Single Path discovery
☑ Param body name	☑ Param cookie name	☑ Param xml attr value	☑ Url path folder
☑ Param url value	☑ Param json value	☑ Param xml attr name	☑ Url path filename
☑ Param url name	☑ Param json name	☑ Param multipart attr value	☑ Entire body xml
☑ Entire body	☑ Entire body json	☑ Param multipart attr name	☑ Entire body multipart

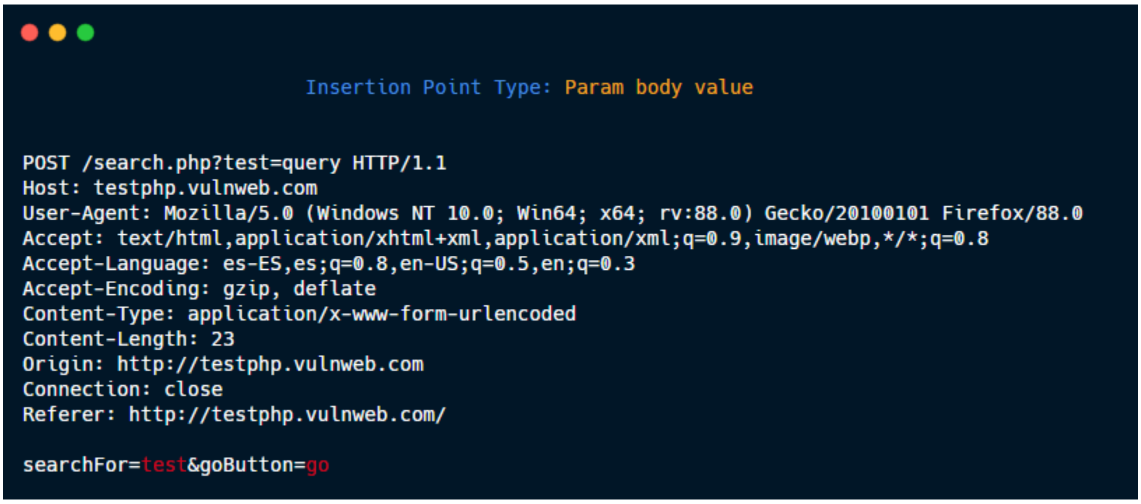
HTTP Headers

☑ Host	☑ Accept	☑ Accept Encoding	☑ Origin
☑ User Agent	☑ Accept Language	☑ Content Type	☑ Referer

New HTTP Headers

New HTTP Header Name
X-Forwarded-For
X-Forwarded-Host

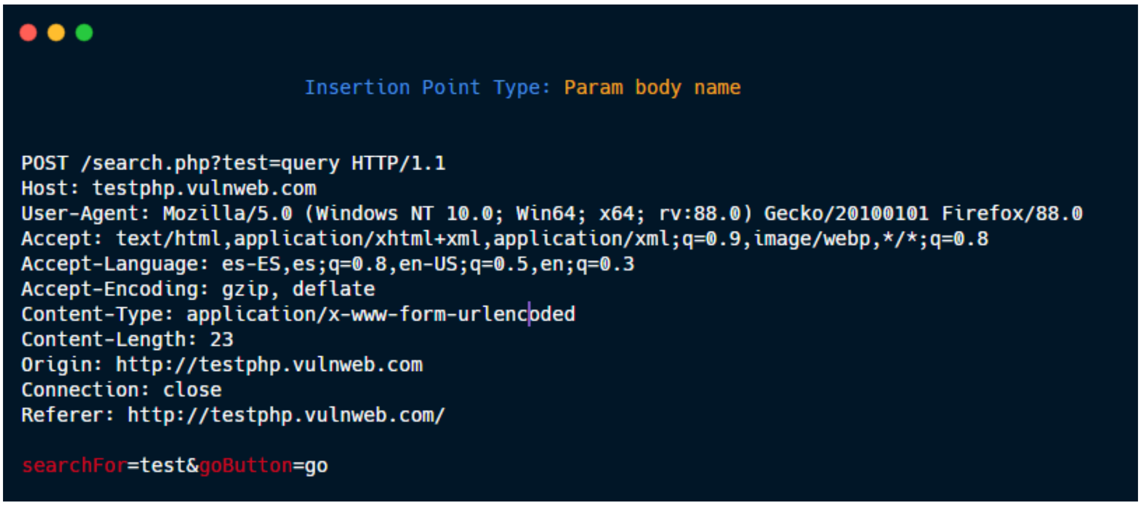
Param body value.



Insertion Point Type: Param body value

```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

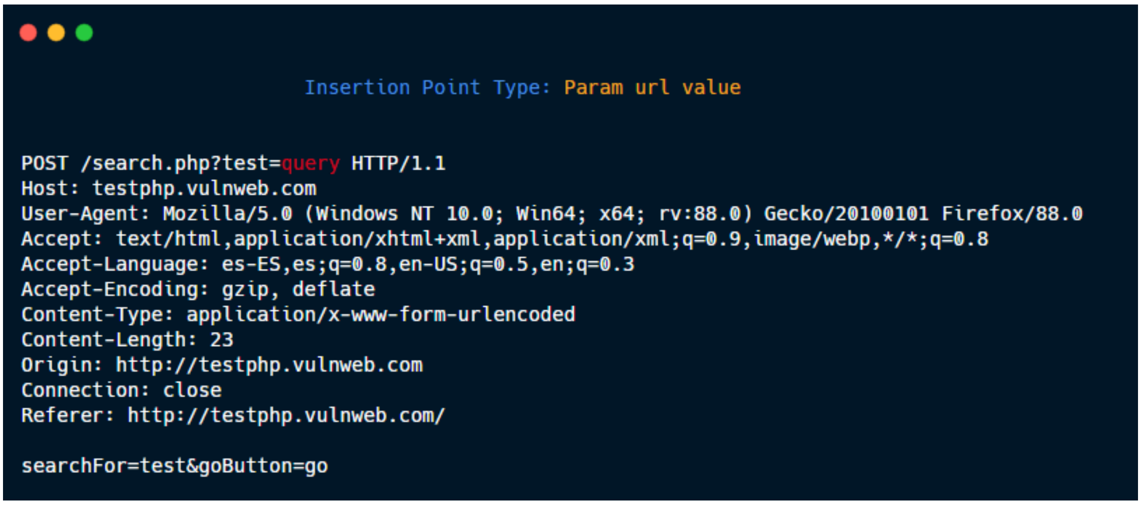
Param body name.



Insertion Point Type: Param body name

```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

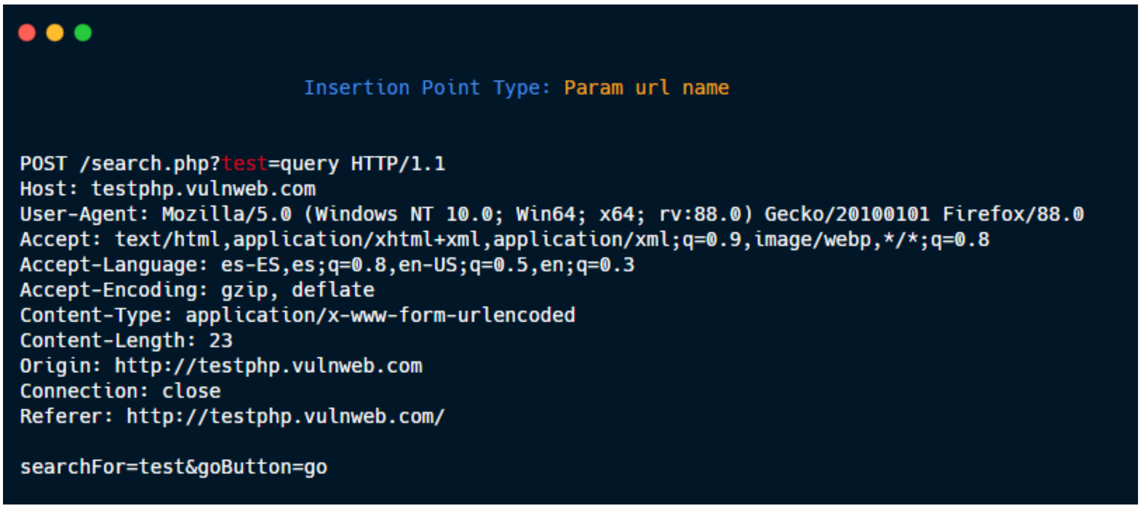
Param URL value.



Insertion Point Type: Param url value

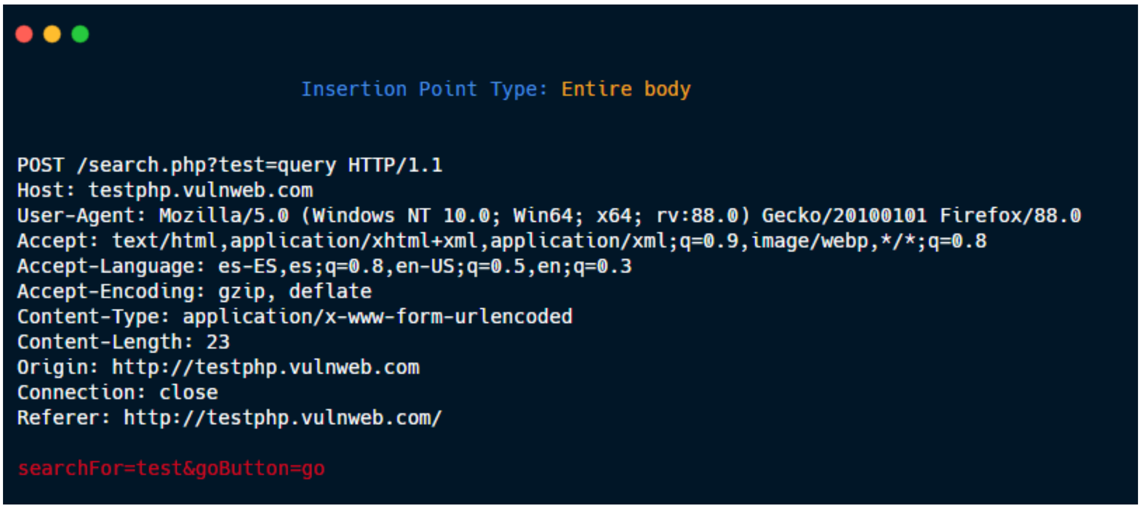
```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

Param URL name.



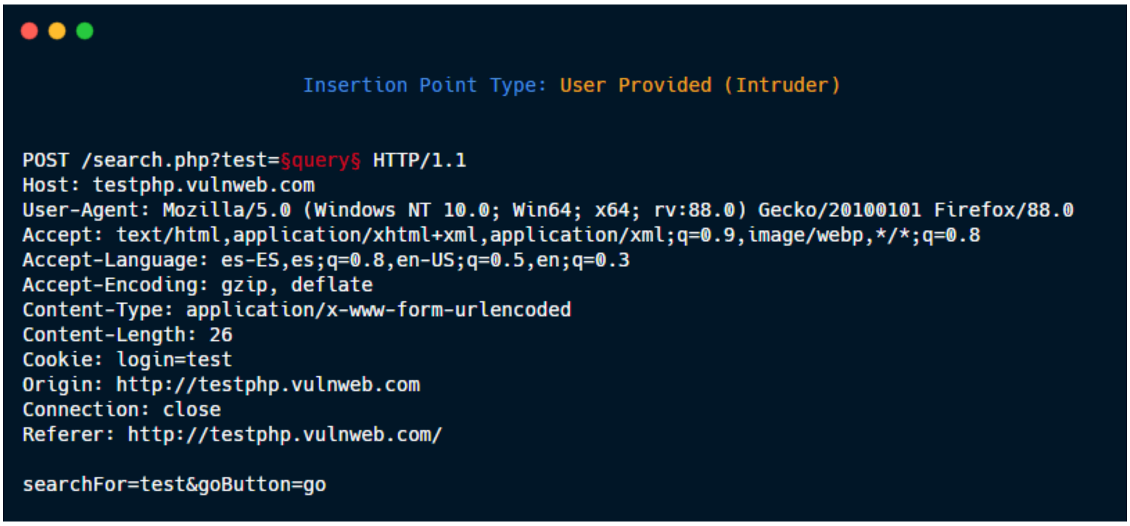
```
                    Insertion Point Type: Param url name

POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

Entire body.



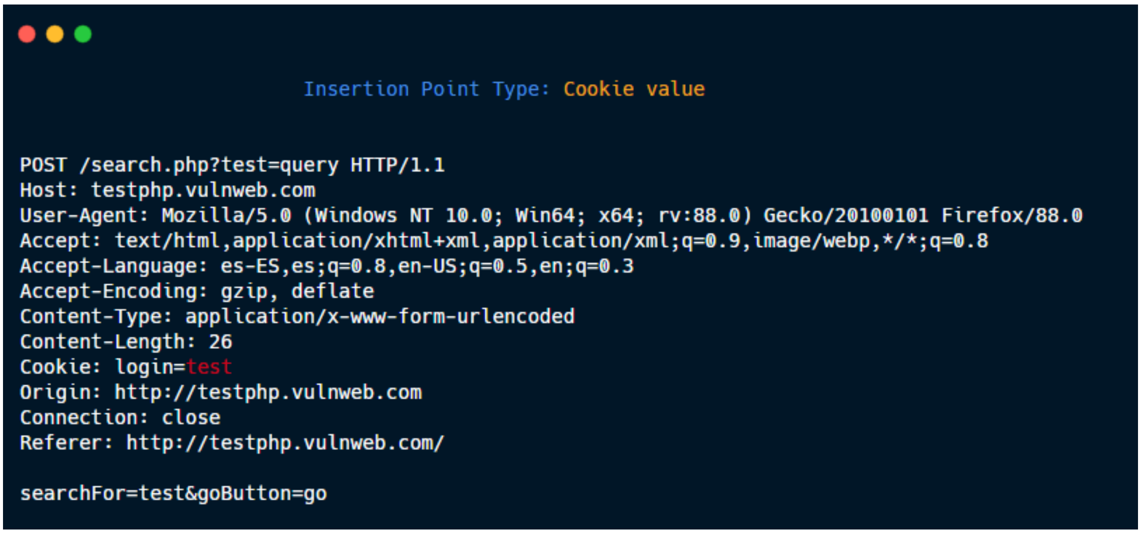
```
                    Insertion Point Type: Entire body

POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

User provided: Defined by the user in the Intruder tab.



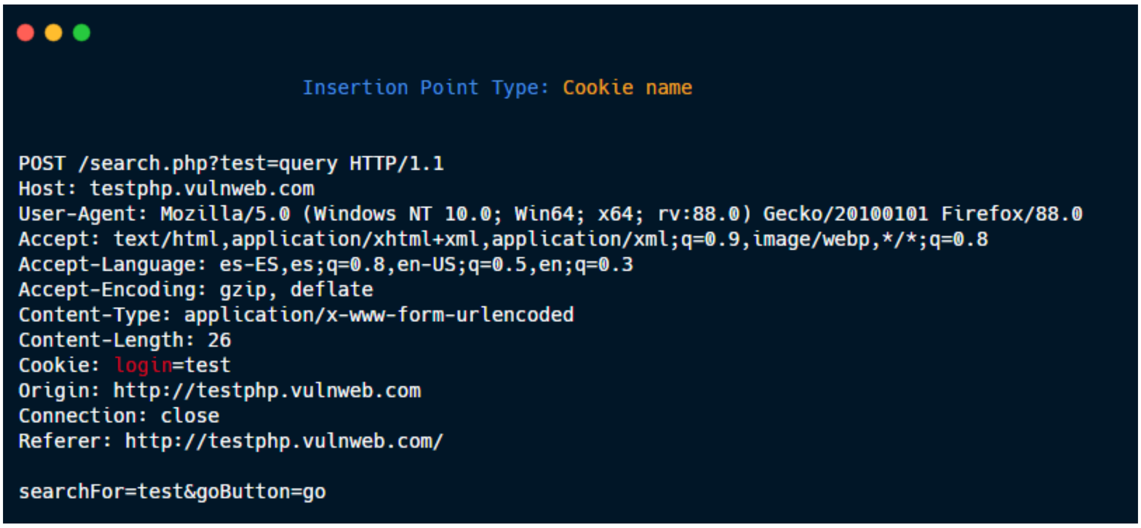
```
                    Insertion Point Type: User Provided (Intruder)

POST /search.php?test=§query§ HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

Cookie value.



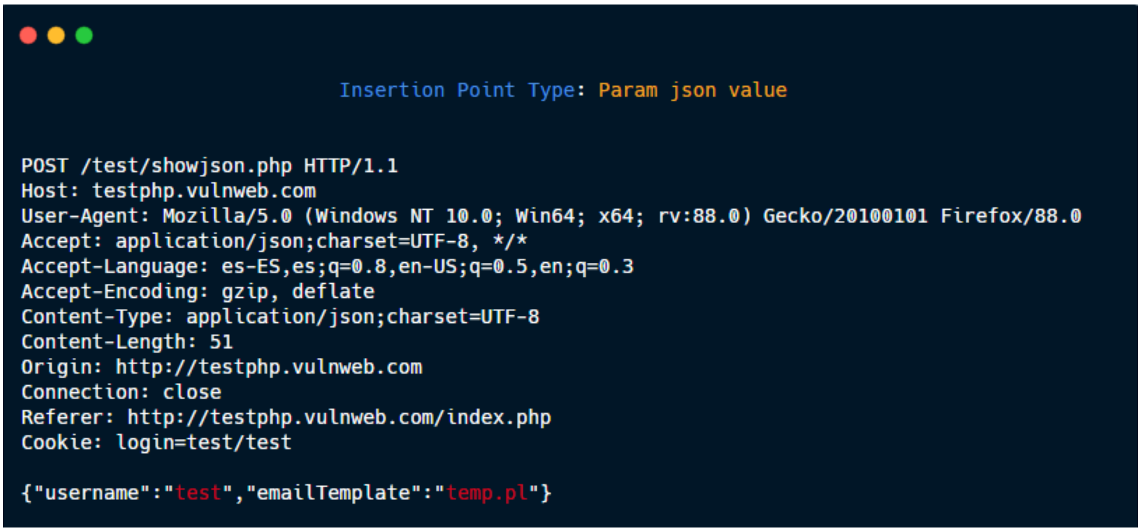
```
                         Insertion Point Type: Cookie value

POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

Cookie name.



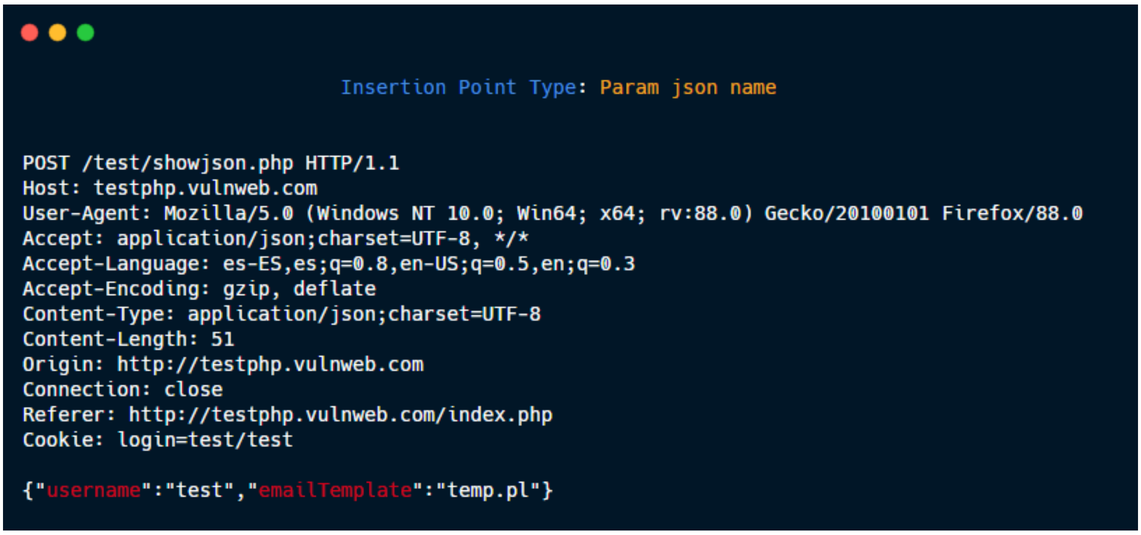
```
                         Insertion Point Type: Cookie name

POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

Param json value.



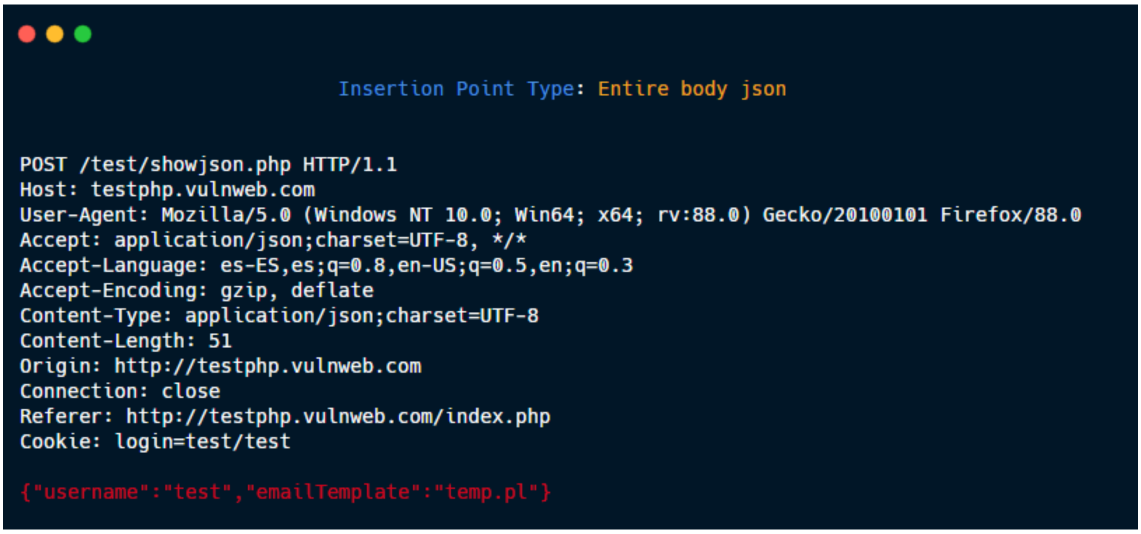
```
                            Insertion Point Type: Param json value

POST /test/showjson.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: application/json;charset=UTF-8, */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=UTF-8
Content-Length: 51
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/index.php
Cookie: login=test/test

{"username":"test","emailTemplate":"temp.pl"}
```

Param json name.



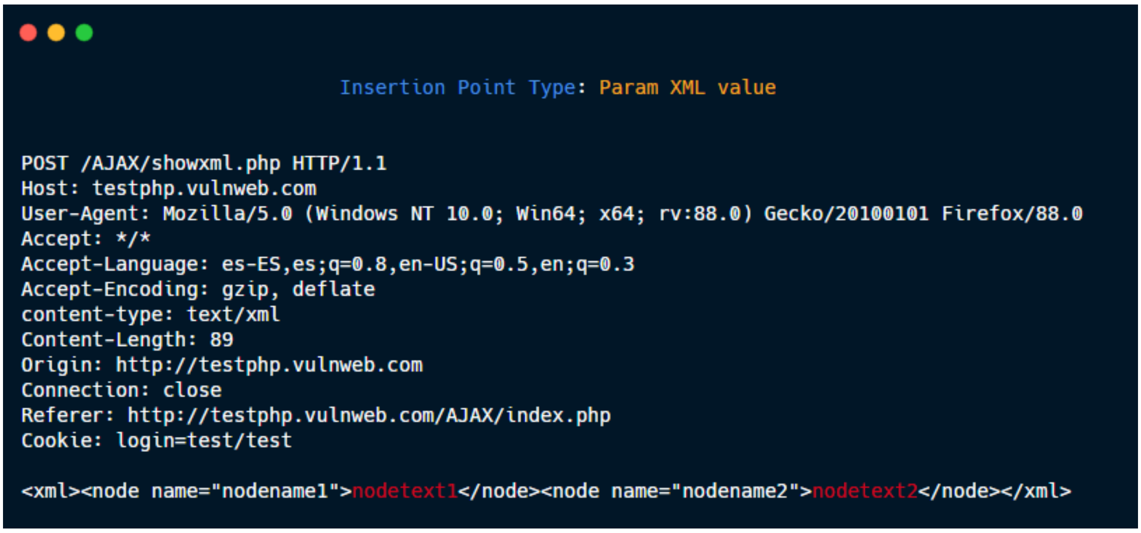
```
Insertion Point Type: Param json name

POST /test/showjson.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: application/json;charset=UTF-8, */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=UTF-8
Content-Length: 51
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/index.php
Cookie: login=test/test

{"username":"test","emailTemplate":"temp.pl"}
```

Entire body json.



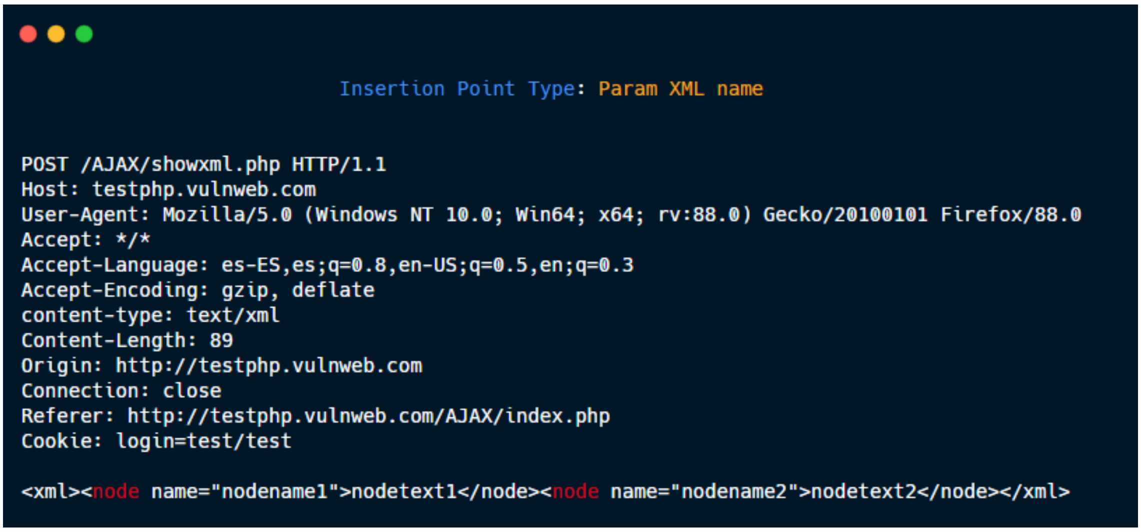
```
Insertion Point Type: Entire body json

POST /test/showjson.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: application/json;charset=UTF-8, */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=UTF-8
Content-Length: 51
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/index.php
Cookie: login=test/test

{"username":"test","emailTemplate":"temp.pl"}
```

Param XML value.



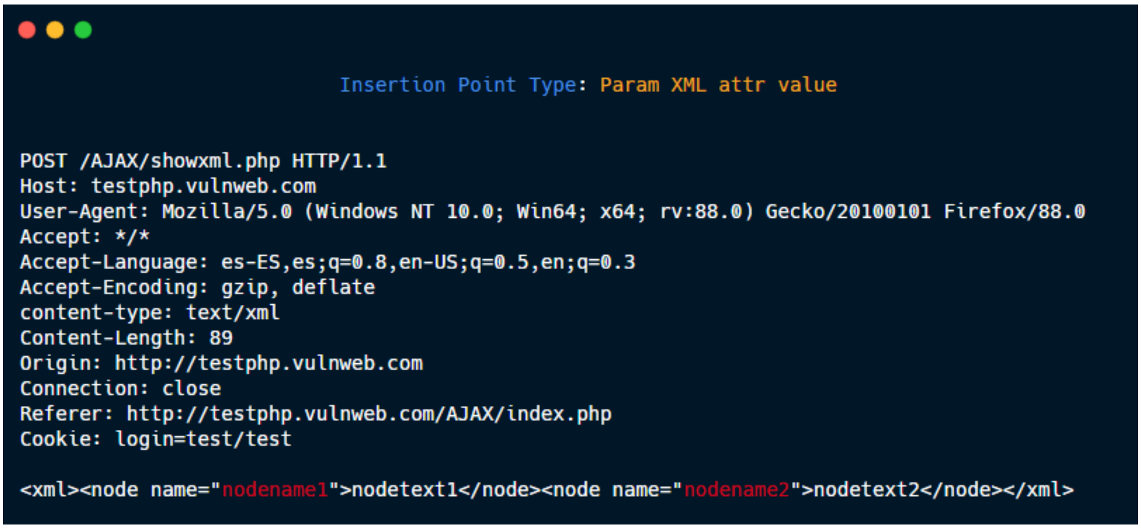
```
Insertion Point Type: Param XML value

POST /AJAX/showxml.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
content-type: text/xml
Content-Length: 89
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/AJAX/index.php
Cookie: login=test/test

<xml><node name="nodename1">nodetext1</node><node name="nodename2">nodetext2</node></xml>
```

Param XML name.



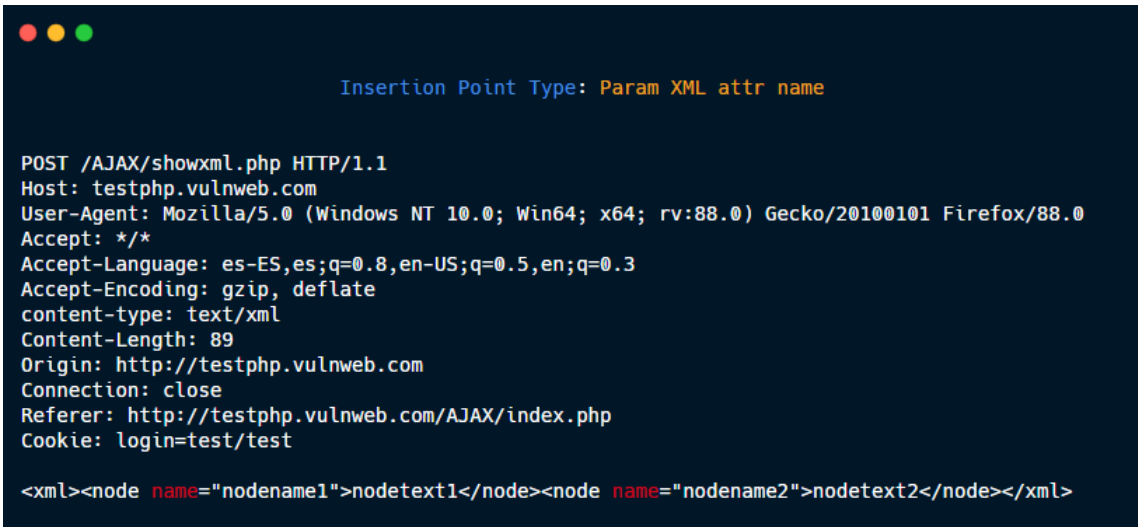
```
Insertion Point Type: Param XML name

POST /AJAX/showxml.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
content-type: text/xml
Content-Length: 89
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/AJAX/index.php
Cookie: login=test/test

<xml><node name="nodename1">nodetext1</node><node name="nodename2">nodetext2</node></xml>
```

Param XML attr value.



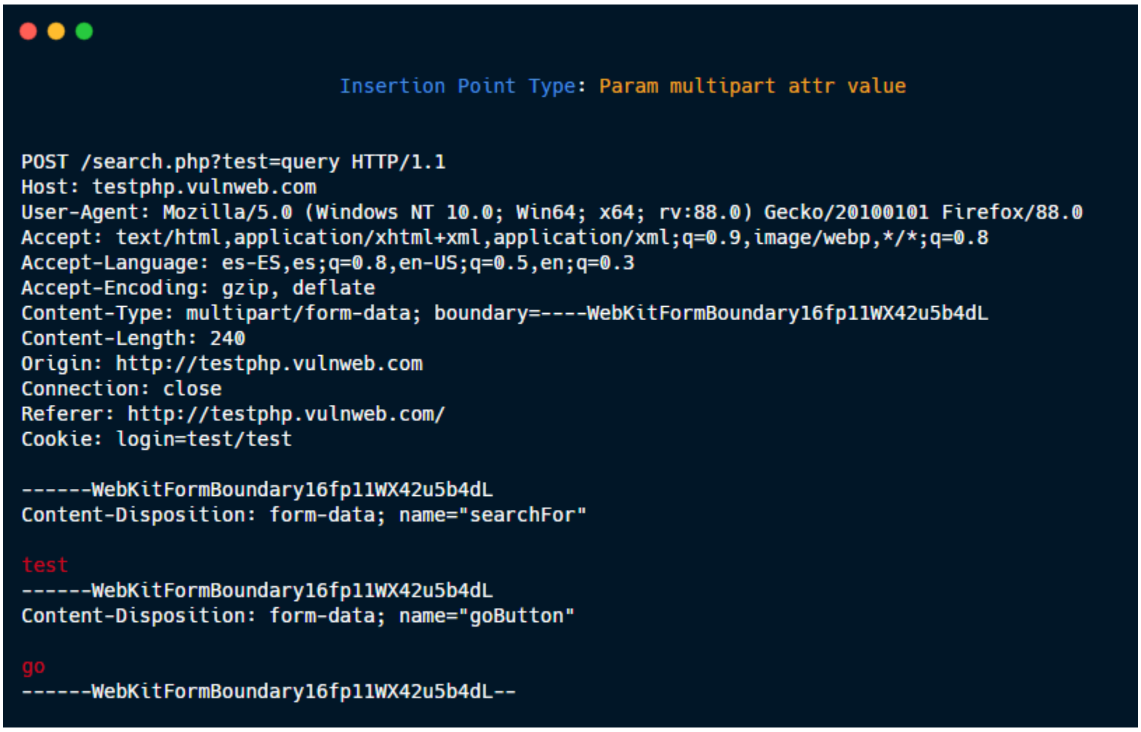
```
Insertion Point Type: Param XML attr value

POST /AJAX/showxml.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
content-type: text/xml
Content-Length: 89
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/AJAX/index.php
Cookie: login=test/test

<xml><node name="nodename1">nodetext1</node><node name="nodename2">nodetext2</node></xml>
```

Param XML attr name.



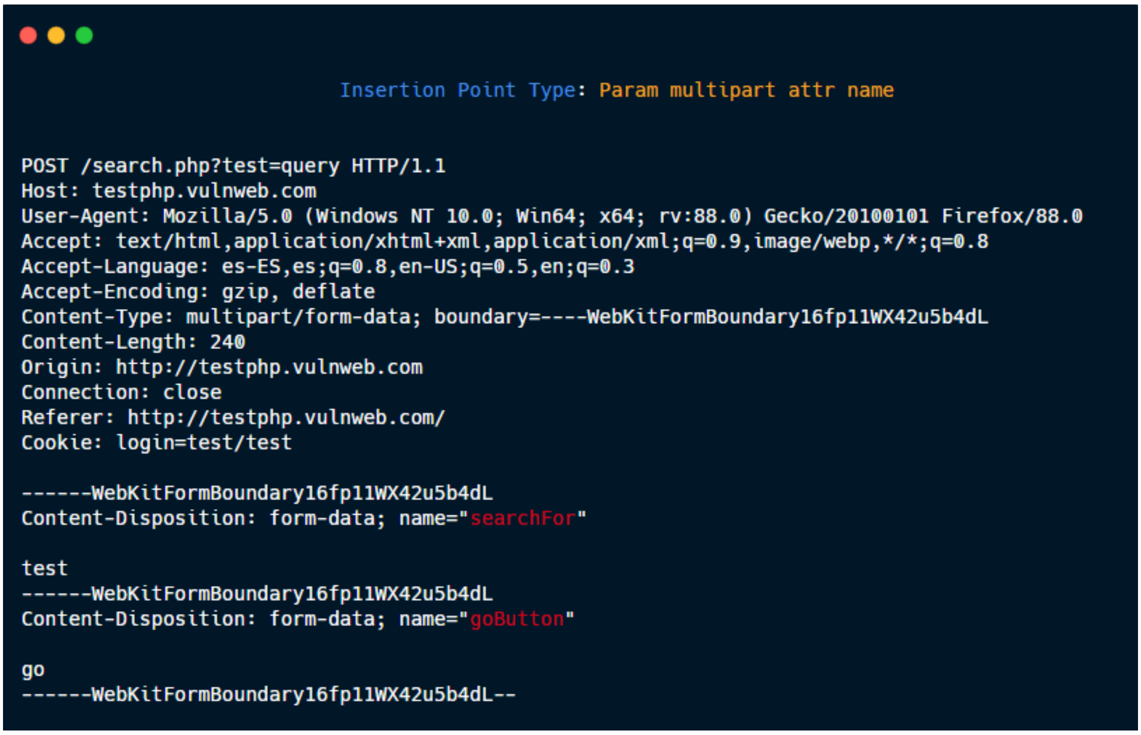
```
Insertion Point Type: Param XML attr name

POST /AJAX/showxml.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
content-type: text/xml
Content-Length: 89
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/AJAX/index.php
Cookie: login=test/test

<xml><node name="nodename1">nodetext1</node><node name="nodename2">nodetext2</node></xml>
```

Param multipart attr value.



```
                    Insertion Point Type: Param multipart attr value


POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary16fp11WX42u5b4dL
Content-Length: 240
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/
Cookie: login=test/test

------WebKitFormBoundary16fp11WX42u5b4dL
Content-Disposition: form-data; name="searchFor"

test
------WebKitFormBoundary16fp11WX42u5b4dL
Content-Disposition: form-data; name="goButton"

go
------WebKitFormBoundary16fp11WX42u5b4dL--
```

Param multipart attr name.



```
                    Insertion Point Type: Param multipart attr name


POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary16fp11WX42u5b4dL
Content-Length: 240
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/
Cookie: login=test/test

------WebKitFormBoundary16fp11WX42u5b4dL
Content-Disposition: form-data; name="searchFor"

test
------WebKitFormBoundary16fp11WX42u5b4dL
Content-Disposition: form-data; name="goButton"

go
------WebKitFormBoundary16fp11WX42u5b4dL--
```

Multiple Path discovery: These insertions point type are added to the requests to discover hidden files and directories:

GET /dir1/dir2/file.php?param=value HTTP/1.1

Generate three new Insertion points:

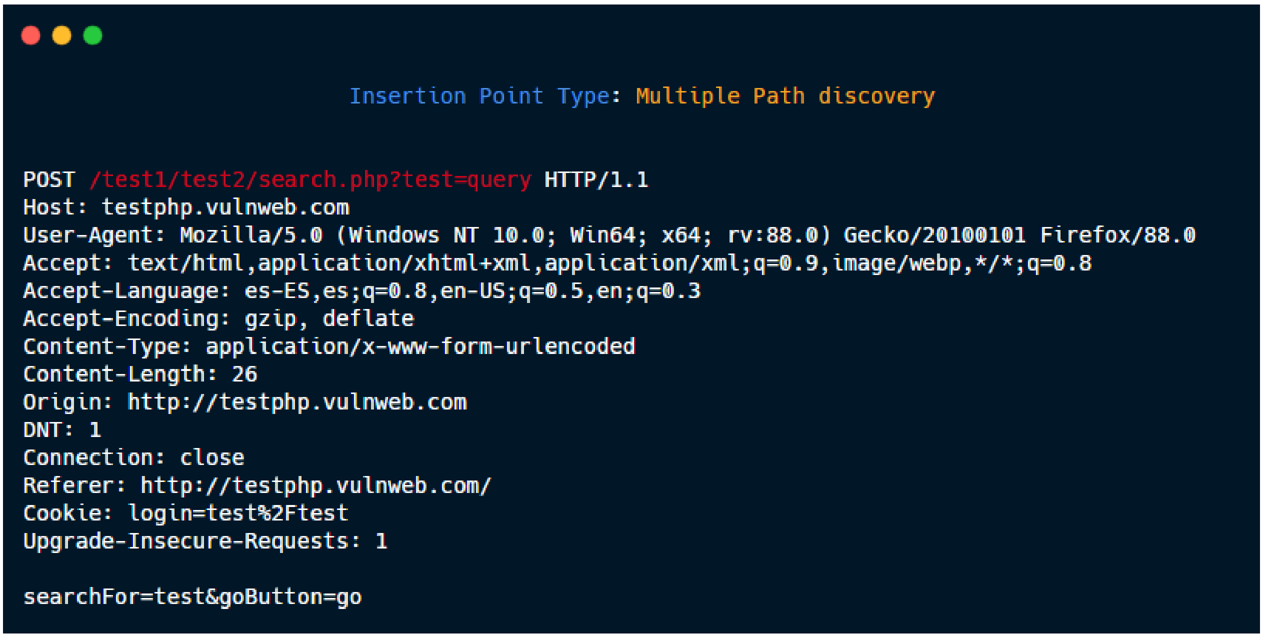
1- GET **{HERE}** HTTP/1.1
2- GET /dir1**{HERE}** HTTP/1.1
3- GET /dir1/dir2**{HERE}** HTTP/1.1

Then, if you put in payload /.git/HEAD, the three new request are:

1- GET /.git/HEAD HTTP/1.1
2- GET /dir1/.git/HEAD HTTP/1.1
3- GET /dir1/dir2/.git/HEAD HTTP/1.1

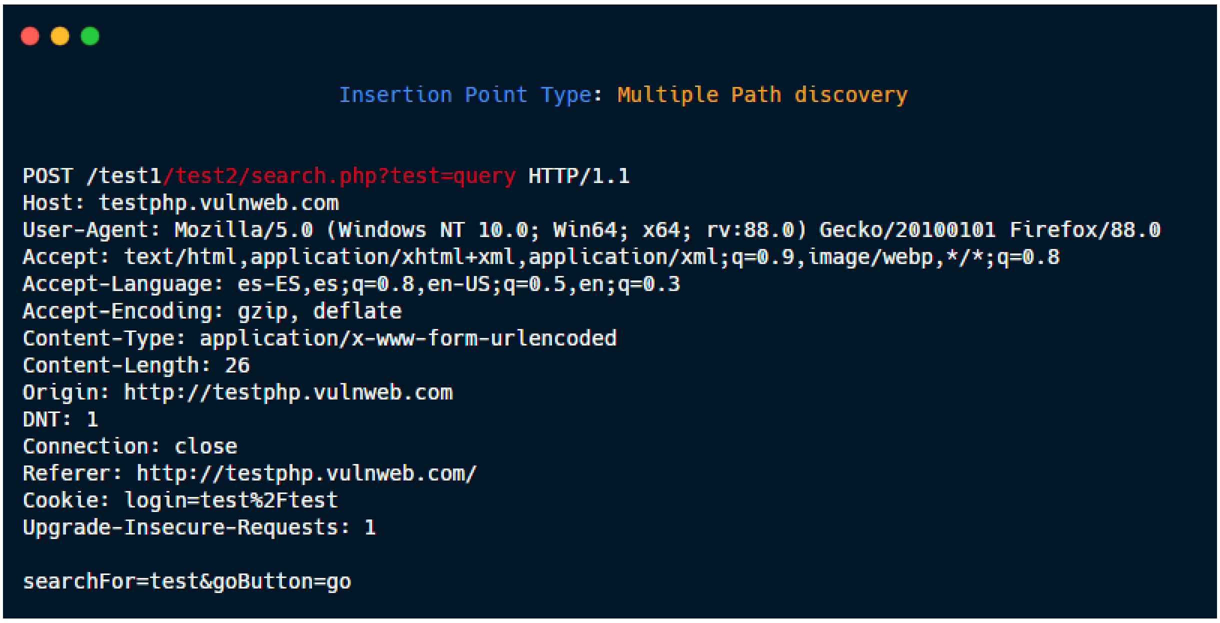
without param=value.

Multiple Path discovery 1.



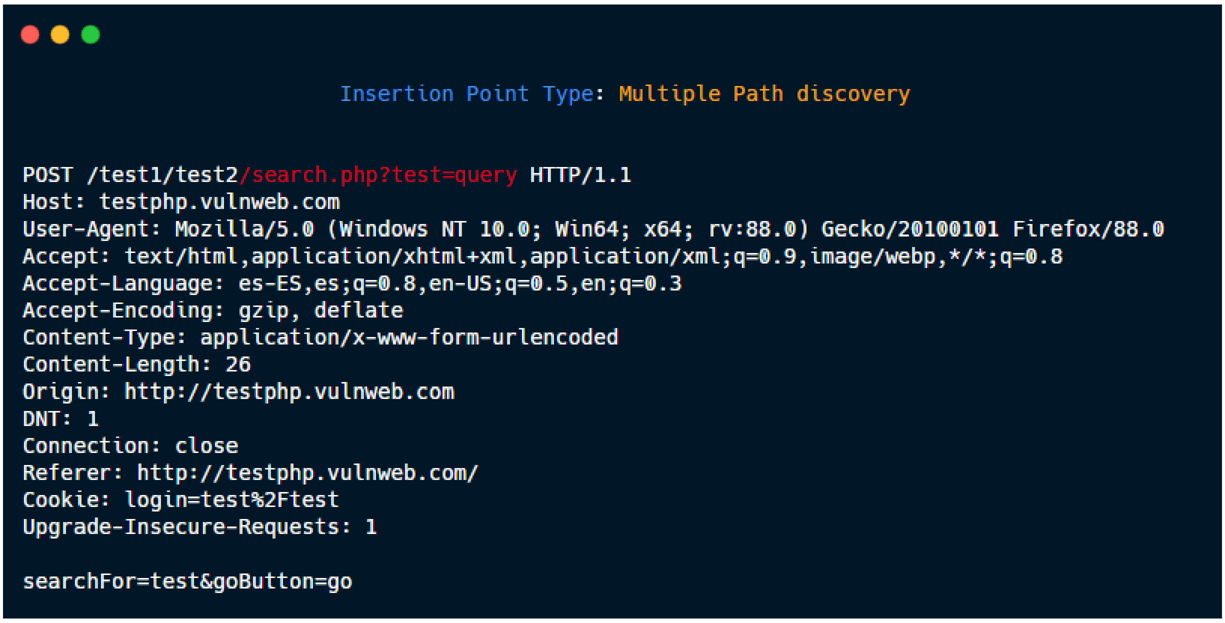
```
                    Insertion Point Type: Multiple Path discovery


POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://testphp.vulnweb.com
DNT: 1
Connection: close
Referer: http://testphp.vulnweb.com/
Cookie: login=test%2Ftest
Upgrade-Insecure-Requests: 1

searchFor=test&goButton=go
```

Multiple Path discovery 2.



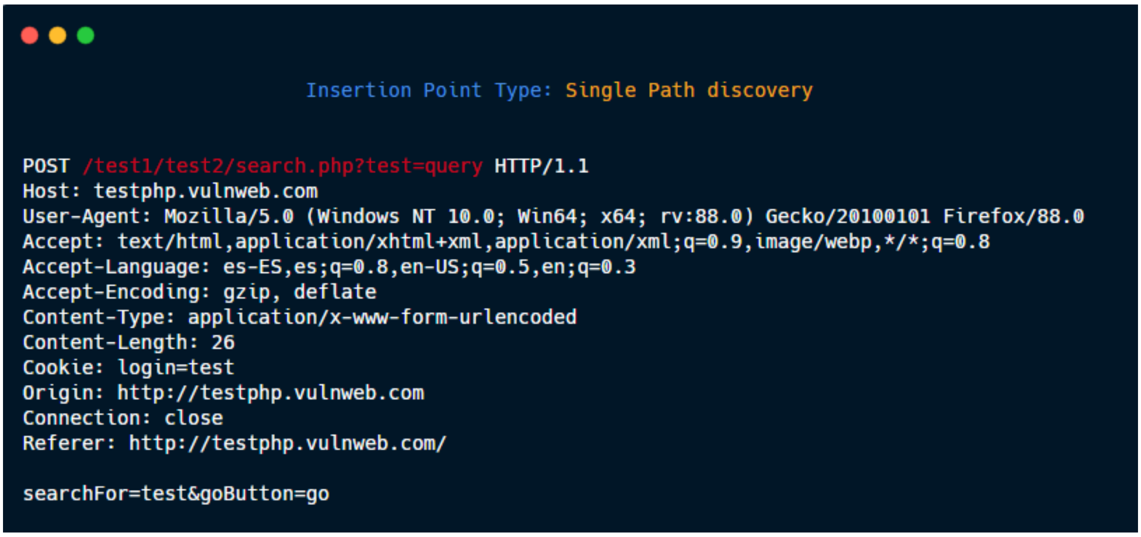
```
Insertion Point Type: Multiple Path discovery

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://testphp.vulnweb.com
DNT: 1
Connection: close
Referer: http://testphp.vulnweb.com/
Cookie: login=test%2Ftest
Upgrade-Insecure-Requests: 1

searchFor=test&goButton=go
```

Multiple Path discovery 3.



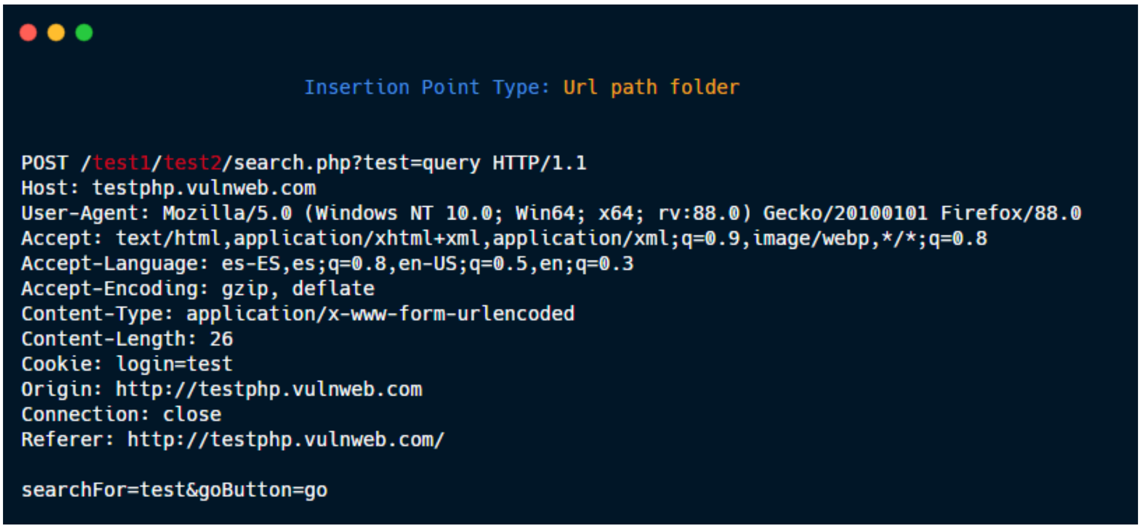
```
Insertion Point Type: Multiple Path discovery

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://testphp.vulnweb.com
DNT: 1
Connection: close
Referer: http://testphp.vulnweb.com/
Cookie: login=test%2Ftest
Upgrade-Insecure-Requests: 1

searchFor=test&goButton=go
```

Single Path discovery.



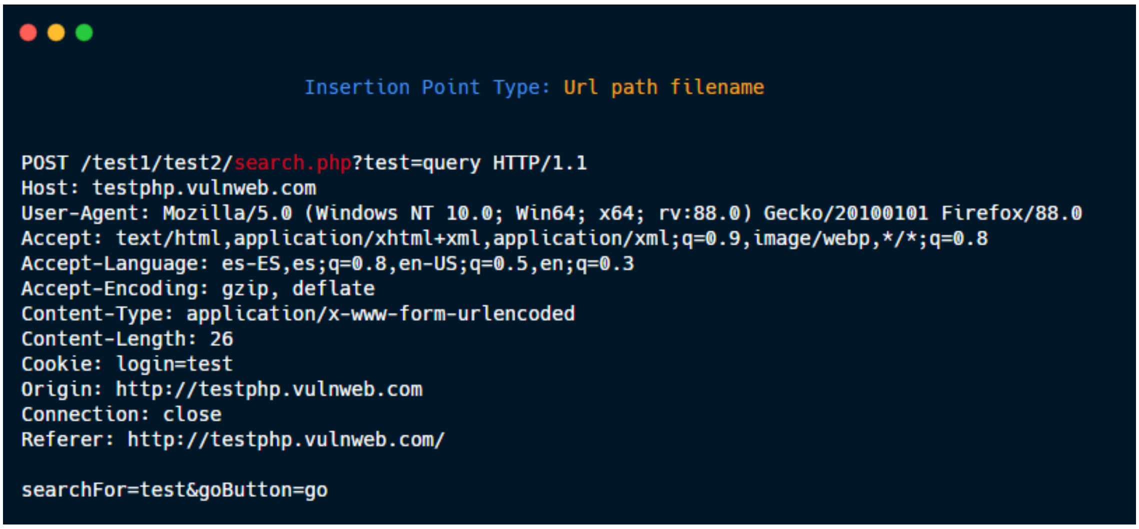
```
                              Insertion Point Type: Single Path discovery


POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

Url path folder.



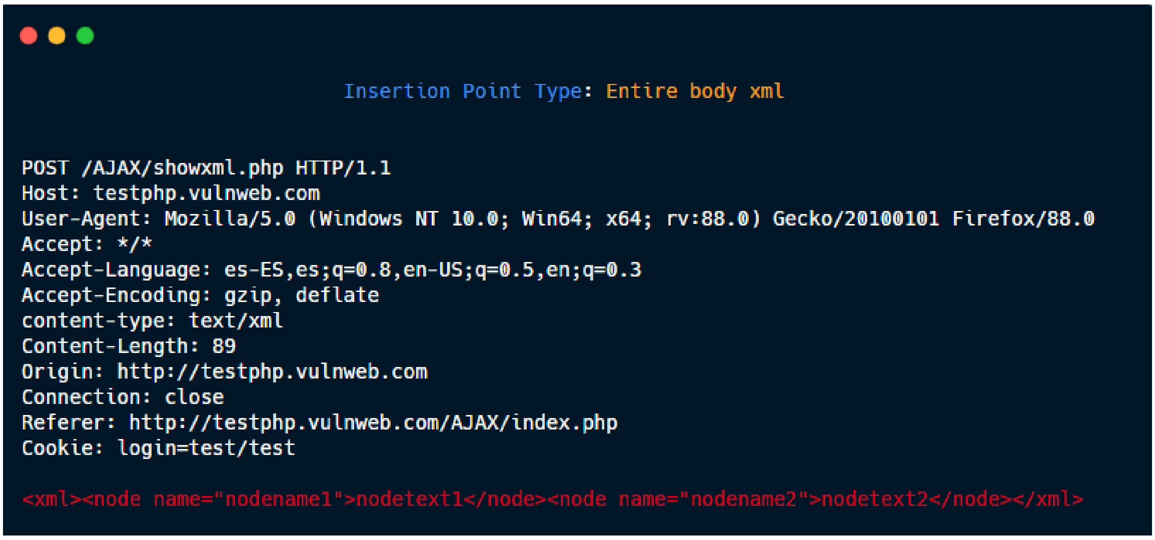
```
                              Insertion Point Type: Url path folder


POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

Url path filename.



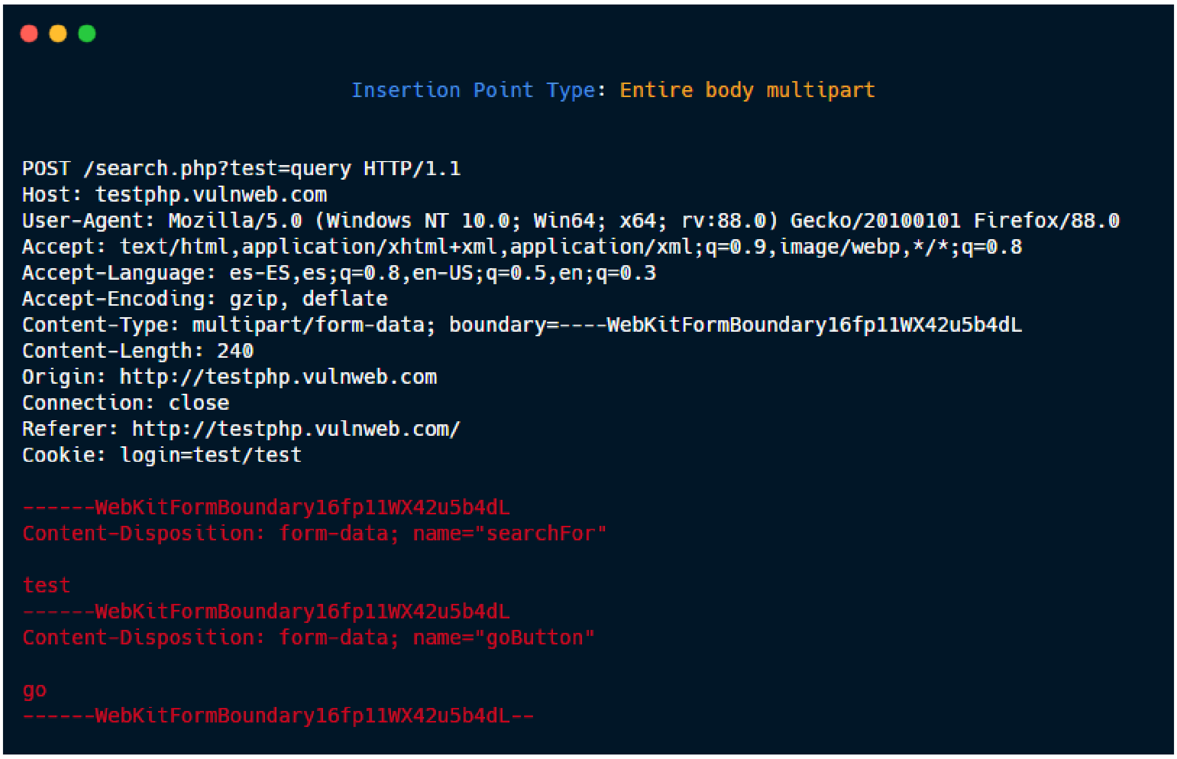
```
                              Insertion Point Type: Url path filename


POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

Entire body xml.



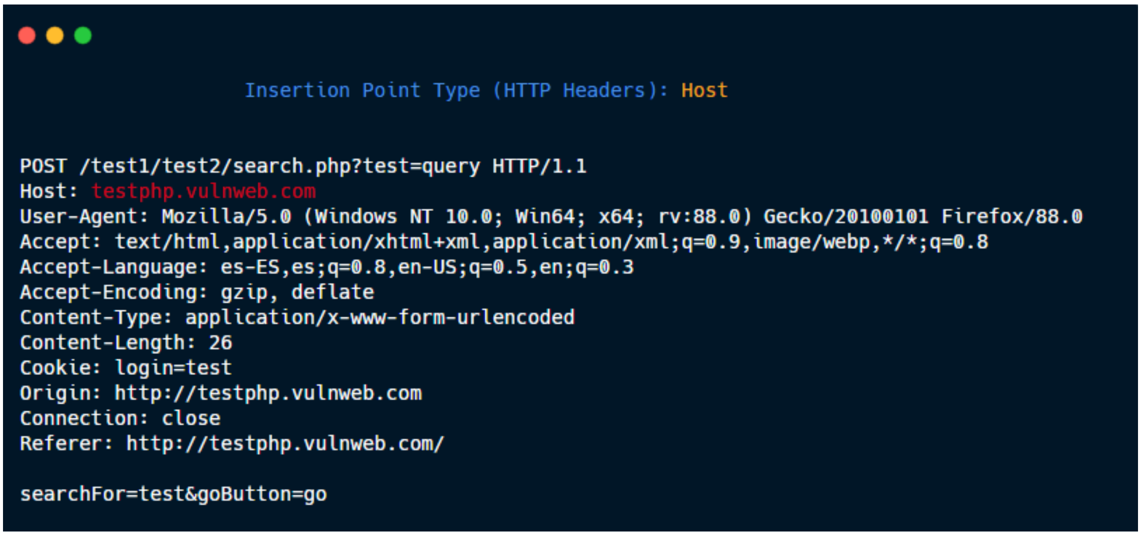
```
Insertion Point Type: Entire body xml

POST /AJAX/showxml.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
content-type: text/xml
Content-Length: 89
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/AJAX/index.php
Cookie: login=test/test

<xml><node name="nodename1">nodetext1</node><node name="nodename2">nodetext2</node></xml>
```

Entire body multipart.



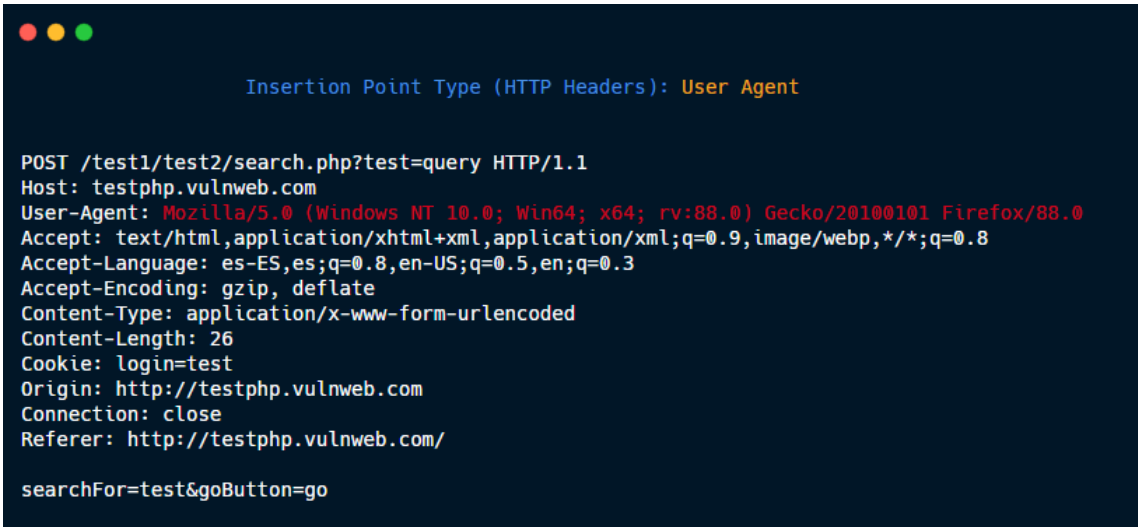
```
Insertion Point Type: Entire body multipart

POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary16fp11WX42u5b4dL
Content-Length: 240
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/
Cookie: login=test/test

------WebKitFormBoundary16fp11WX42u5b4dL
Content-Disposition: form-data; name="searchFor"

test
------WebKitFormBoundary16fp11WX42u5b4dL
Content-Disposition: form-data; name="goButton"

go
------WebKitFormBoundary16fp11WX42u5b4dL--
```

HTTP Headers: Host



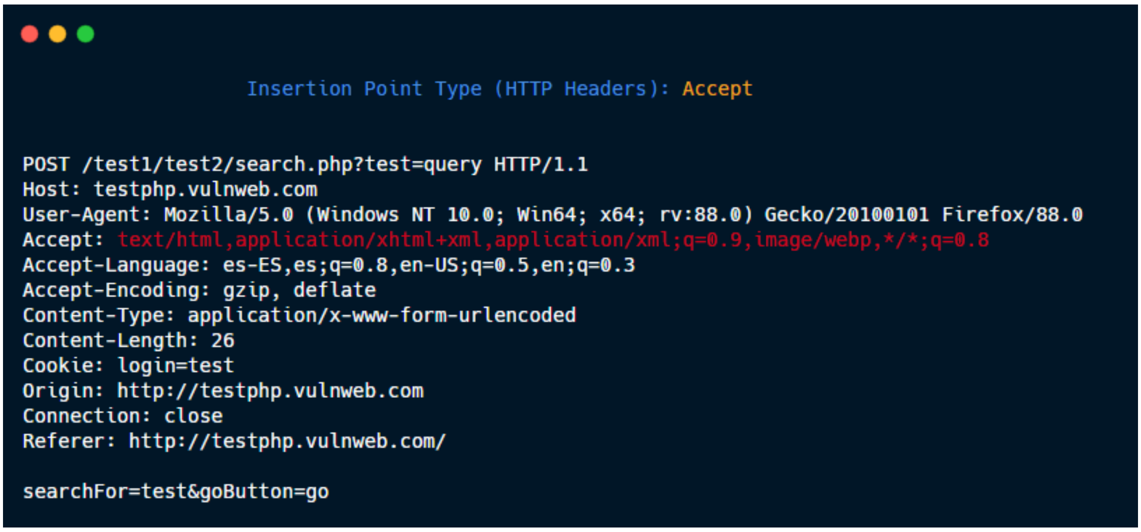
```
                    Insertion Point Type (HTTP Headers): Host

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

HTTP Headers: User agent



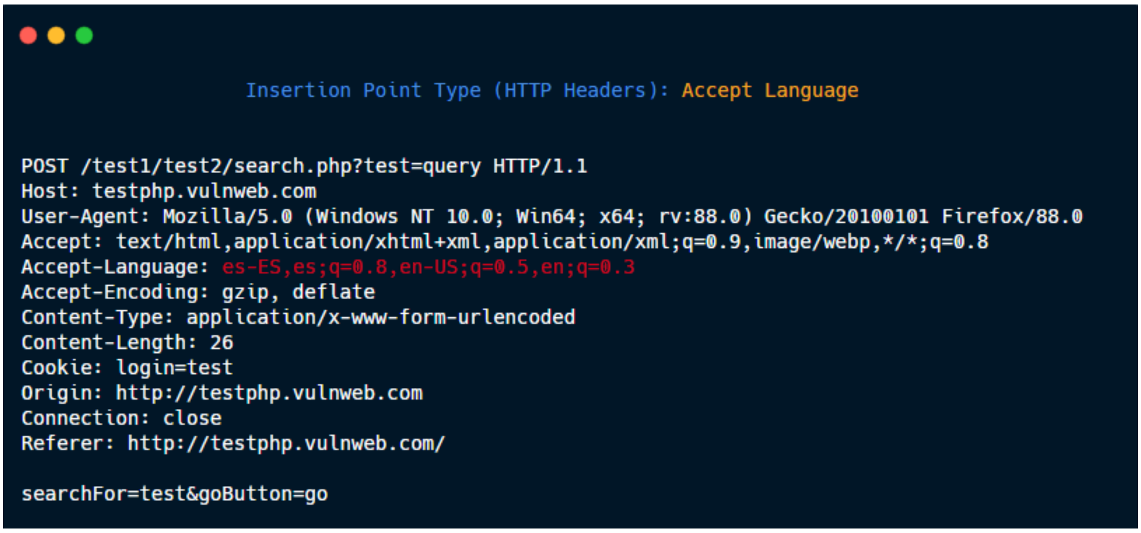
```
                    Insertion Point Type (HTTP Headers): User Agent

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

HTTP Headers: Accept



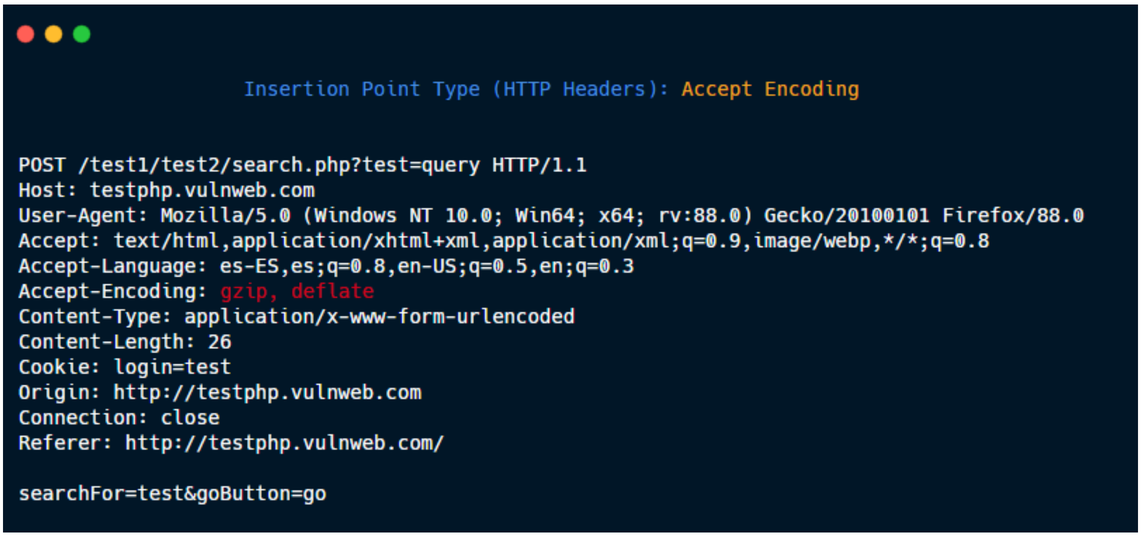
```
                    Insertion Point Type (HTTP Headers): Accept

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

HTTP Headers: Accept Language



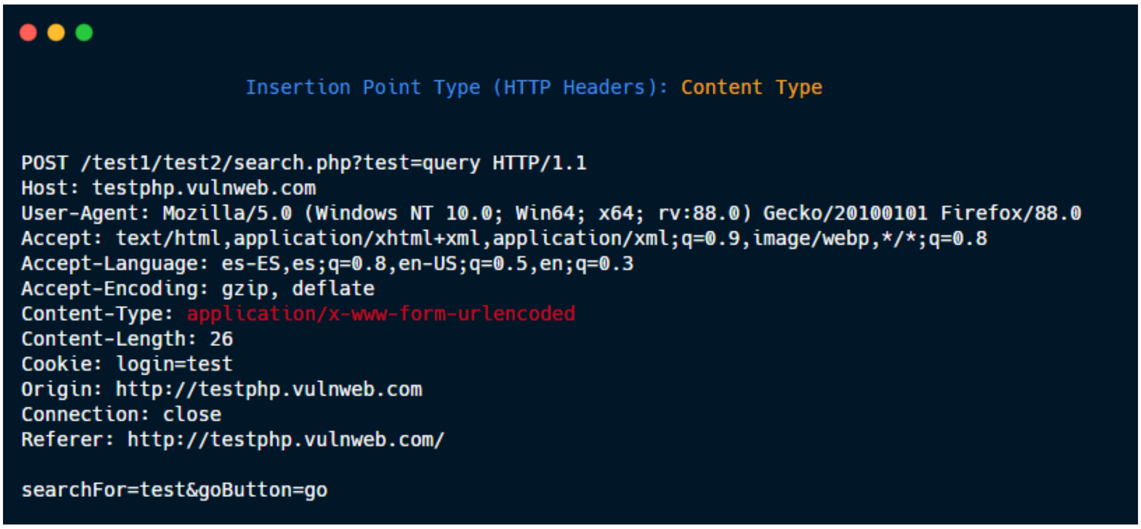
```
                    Insertion Point Type (HTTP Headers): Accept Language

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

HTTP Headers: Accept Encoding



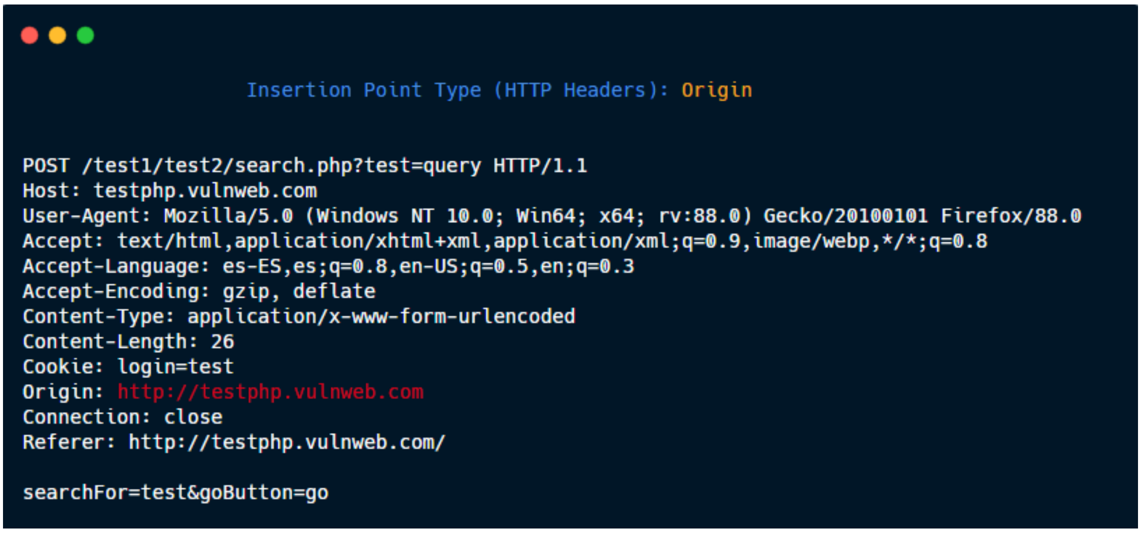
```
                    Insertion Point Type (HTTP Headers): Accept Encoding

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

HTTP Headers: Content Type



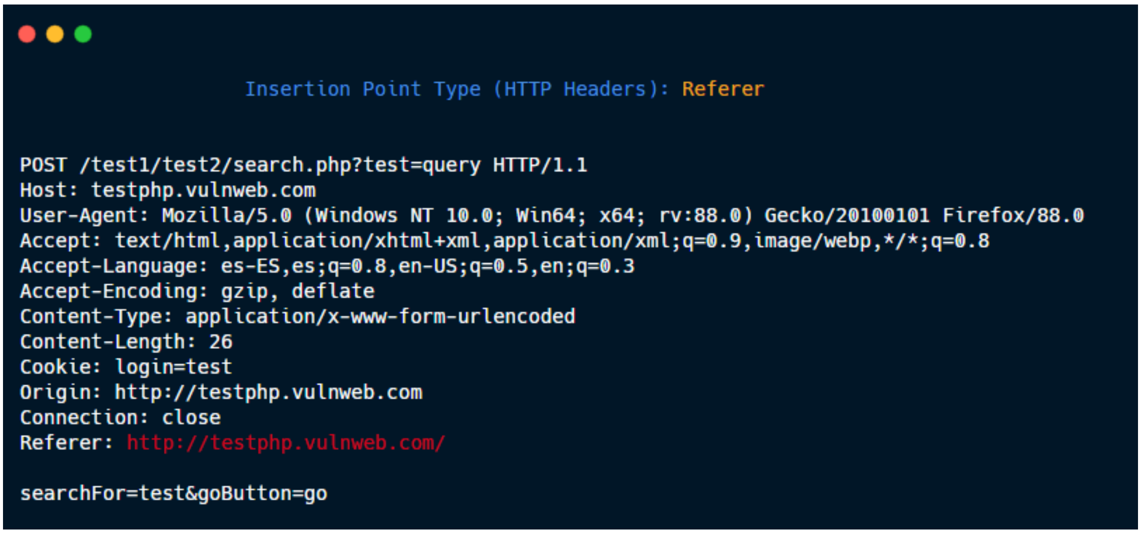
```
                    Insertion Point Type (HTTP Headers): Content Type

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

HTTP Headers: Origin



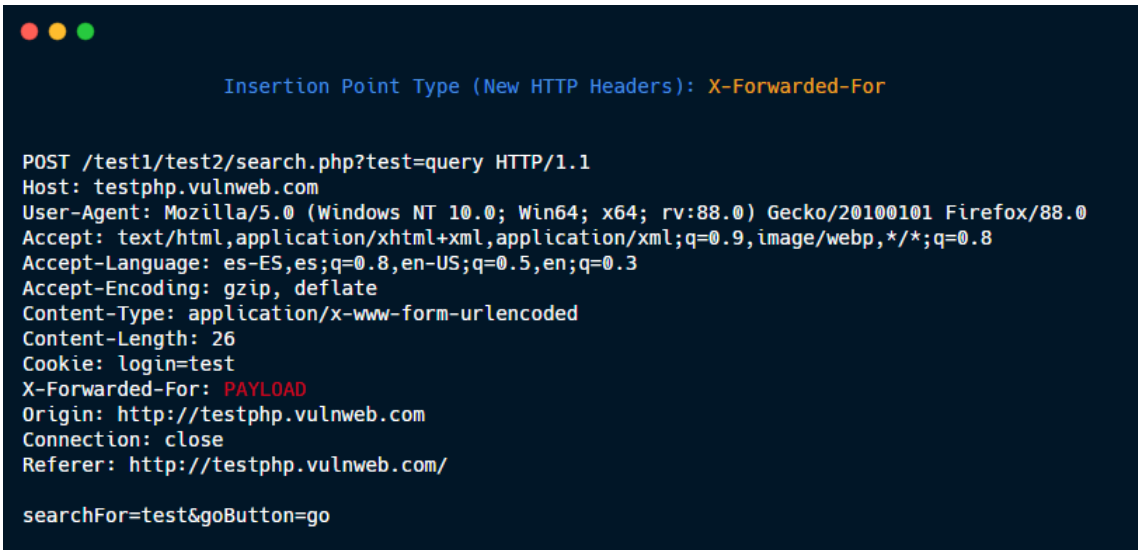
```
Insertion Point Type (HTTP Headers): Origin

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

HTTP Headers: Referer



```
Insertion Point Type (HTTP Headers): Referer

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

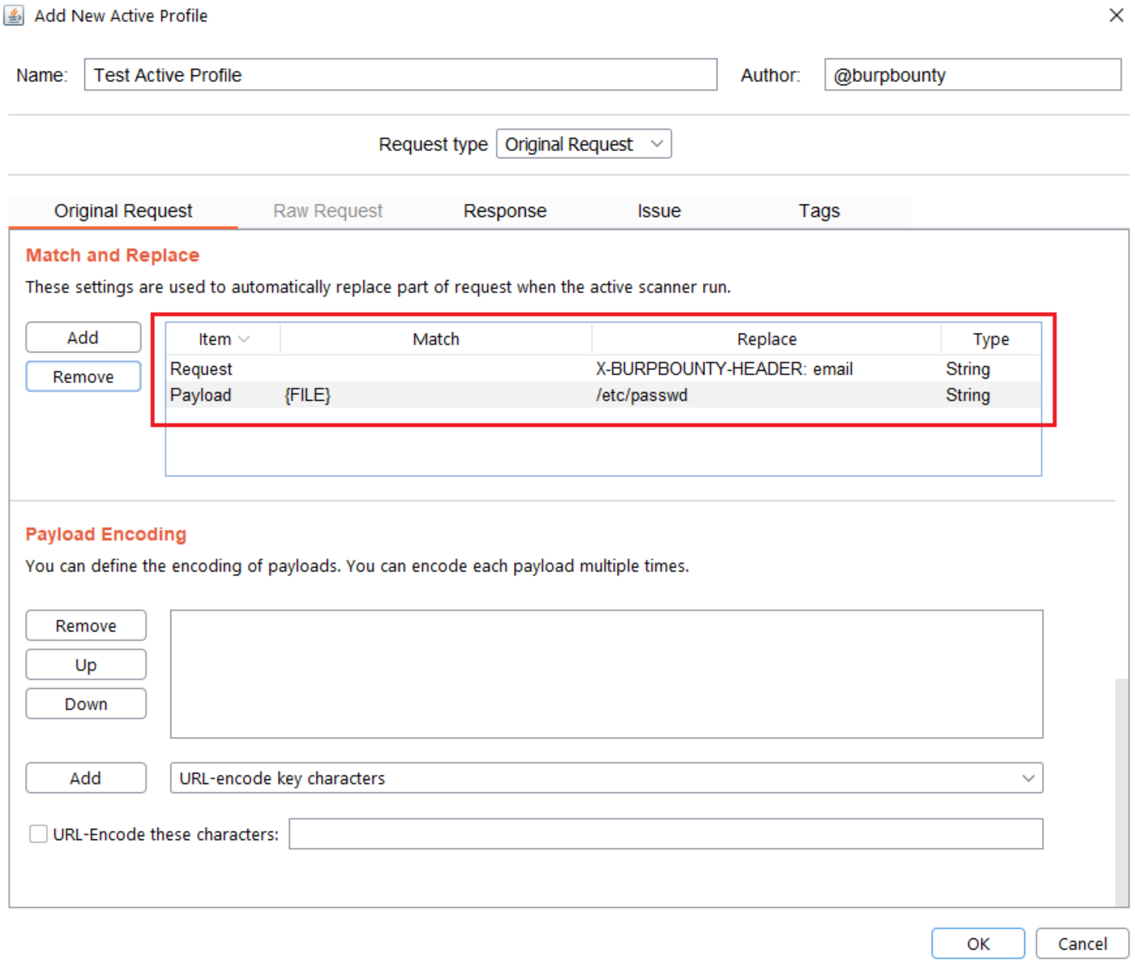
New HTTP Headers: X-Forwarded-For (or whichever that you specify)



```
Insertion Point Type (New HTTP Headers): X-Forwarded-For

POST /test1/test2/search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: login=test
X-Forwarded-For: PAYLOAD
Origin: http://testphp.vulnweb.com
Connection: close
Referer: http://testphp.vulnweb.com/

searchFor=test&goButton=go
```

Step 2.5 (Optional)- Original Request -> Match and Replace:

In this section you can replace values in the payload/request or you can insert new fields in the HTTP request.



Add New Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Match and Replace

These settings are used to automatically replace part of request when the active scanner run.

Item	Match	Replace	Type
Request		X-BURPBOUNTY-HEADER: email	String
Payload	{FILE}	/etc/passwd	String

Payload Encoding

You can define the encoding of payloads. You can encode each payload multiple times.

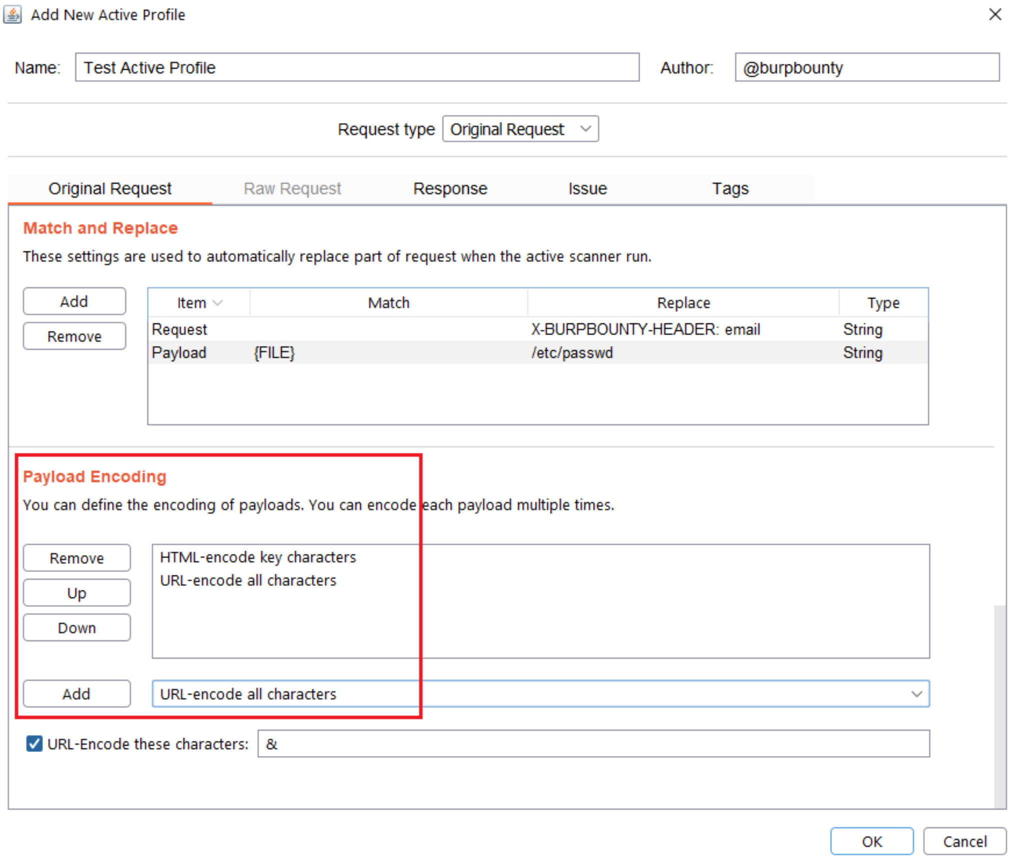
URL-encode key characters

□ URL-Encode these characters:

Step 2.6 (Optional)- Original Request -> Payload encoding:

In this section you can use one or more encodings that will be applied to the payloads before being sent in the HTTP request. You can choose between:

- URL-encode key characters
- URL-encode all characters
- URL-encode all characters (Unicode)
- HTML-encode key characters
- HTML-encode all characters
- Base64-encode



Add New Active Profile

Name: Test Active Profile Author: @burpbounty

Request type: Original Request

Match and Replace

These settings are used to automatically replace part of request when the active scanner run.

Item	Match	Replace	Type
Request		X-BURPBOUNTY-HEADER: email	String
Payload	{FILE}	/etc/passwd	String

Payload Encoding

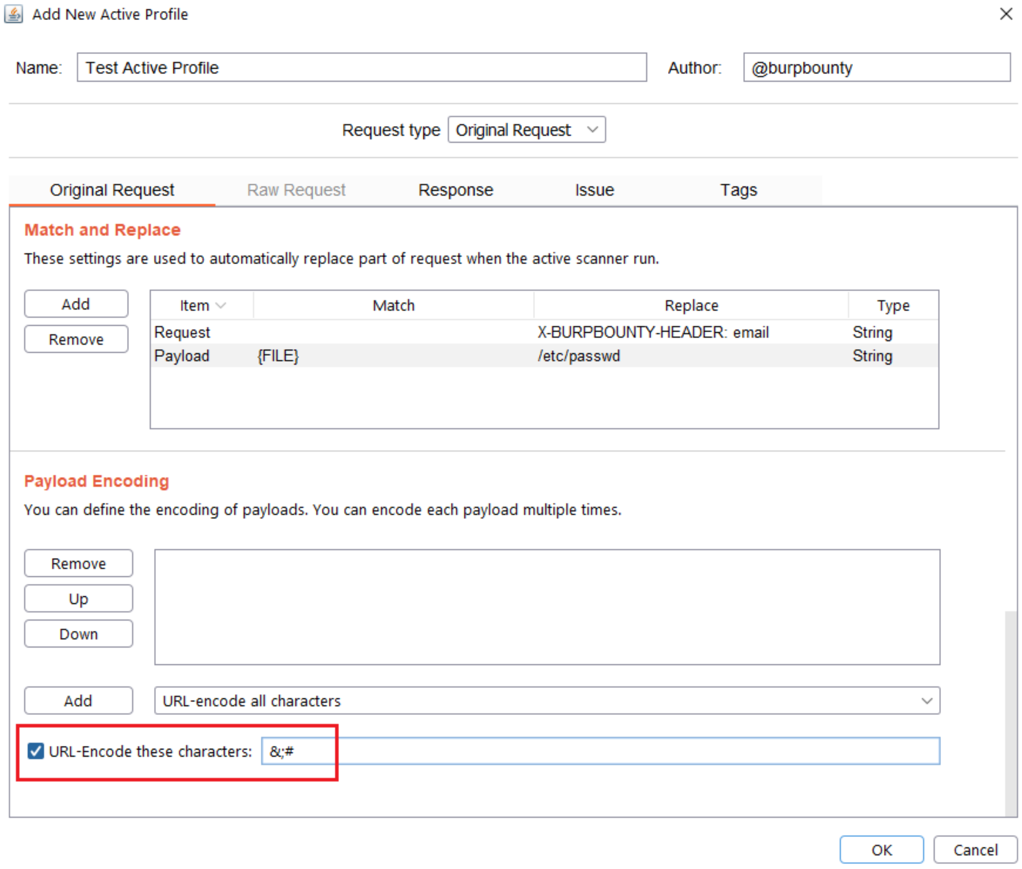
You can define the encoding of payloads. You can encode each payload multiple times.

HTML-encode key characters
URL-encode all characters

URL-encode all characters

☑ URL-Encode these characters: &

In this section, you can also encode in "URL encode" only the payload characters that you choose:



Add New Active Profile

Name: Test Active Profile Author: @burpbounty

Request type: Original Request

Match and Replace

These settings are used to automatically replace part of request when the active scanner run.

Item	Match	Replace	Type
Request		X-BURPBOUNTY-HEADER: email	String
Payload	{FILE}	/etc/passwd	String

Payload Encoding

You can define the encoding of payloads. You can encode each payload multiple times.

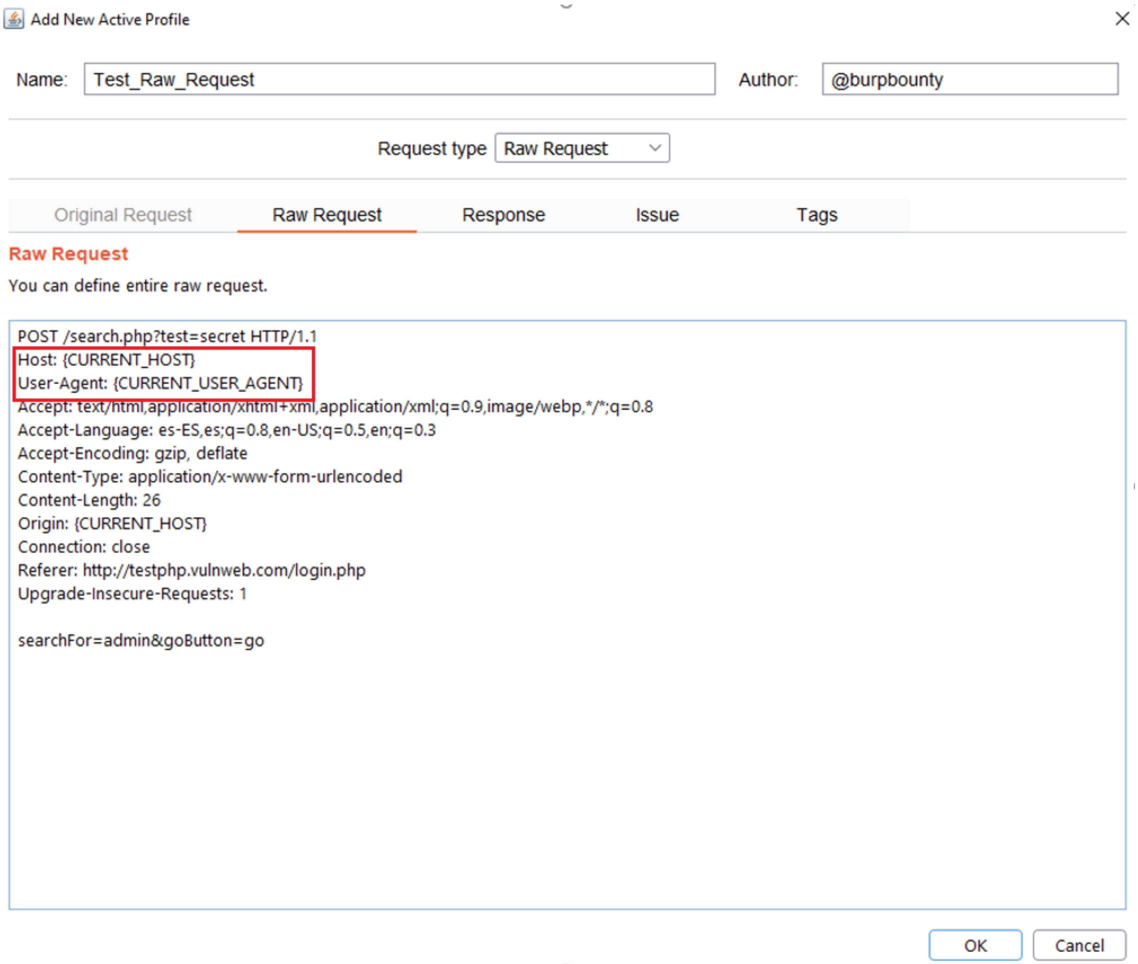
URL-encode all characters

☑ URL-Encode these characters: &;#

Step 3 (Required if you choose raw request option)- Raw Request:

Another new improvement of Burp Bounty Pro 2 is the possibility of sending Raw requests inheriting attributes of the request that is being scanned.

This means that when a HTTP request or domain is scanned, this custom RAW Request will be sent to the system that you are attacking.



Name: Test_Raw_Request
Author: @burpbounty
Request type: Raw Request

Raw Request

You can define entire raw request.

```
POST /search.php?test=secret HTTP/1.1
Host: {CURRENT_HOST}
User-Agent: {CURRENT_USER_AGENT}
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: {CURRENT_HOST}
Connection: close
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

searchFor=admin&goButton=go
```

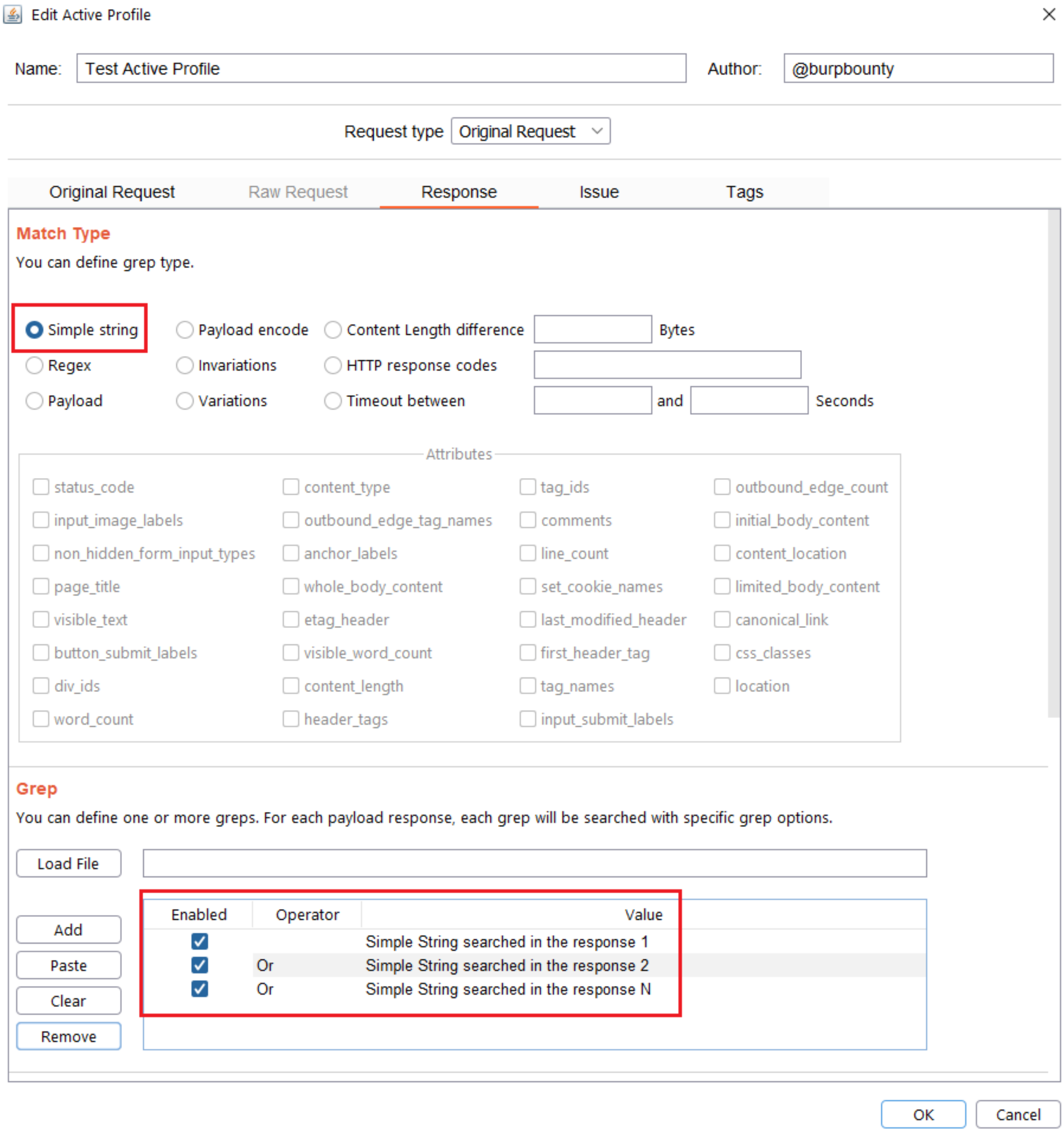
You can insert these attributes wherever you want in the Raw Request. The available attributes are:

{CURRENT_INSERTION_POINT_NAME}
{CURRENT_INSERTION_POINT_VALUE}
{CURRENT_URL}
{CURRENT_PORT}
{CURRENT_PATH}
{CURRENT_HOST}
{CURRENT_METHOD}
{CURRENT_QUERY}
{CURRENT_FILE}

{CURRENT_PROTOCOL}
{CURRENT_USER_AGENT}
{CURRENT_REFERER}
{CURRENT_ORIGIN}
{CURRENT_CONTENT_TYPE}
{CURRENT_ACCEPT}
{CURRENT_ACCEPT_LANGUAGE}
{CURRENT_ACCEPT_ENCODING}
{CURRENT_CONTENT_LENGTH}

Step 4 (Required)- Response->Match Type: In this section we must specify how we will look for the pattern in the HTTP response.

- **Simple string**: Search for a simple string in the HTTP Response that you specify in the "Grep" section.



Edit Active Profile

Name: Test Active Profile   Author: @burpbounty

Request type: Original Request

Match Type

You can define grep type.

● Simple string ○ Payload encode ○ Content Length difference ____ Bytes
○ Regex ○ Invariations ○ HTTP response codes ____
○ Payload ○ Variations ○ Timeout between ____ and ____ Seconds

Attributes

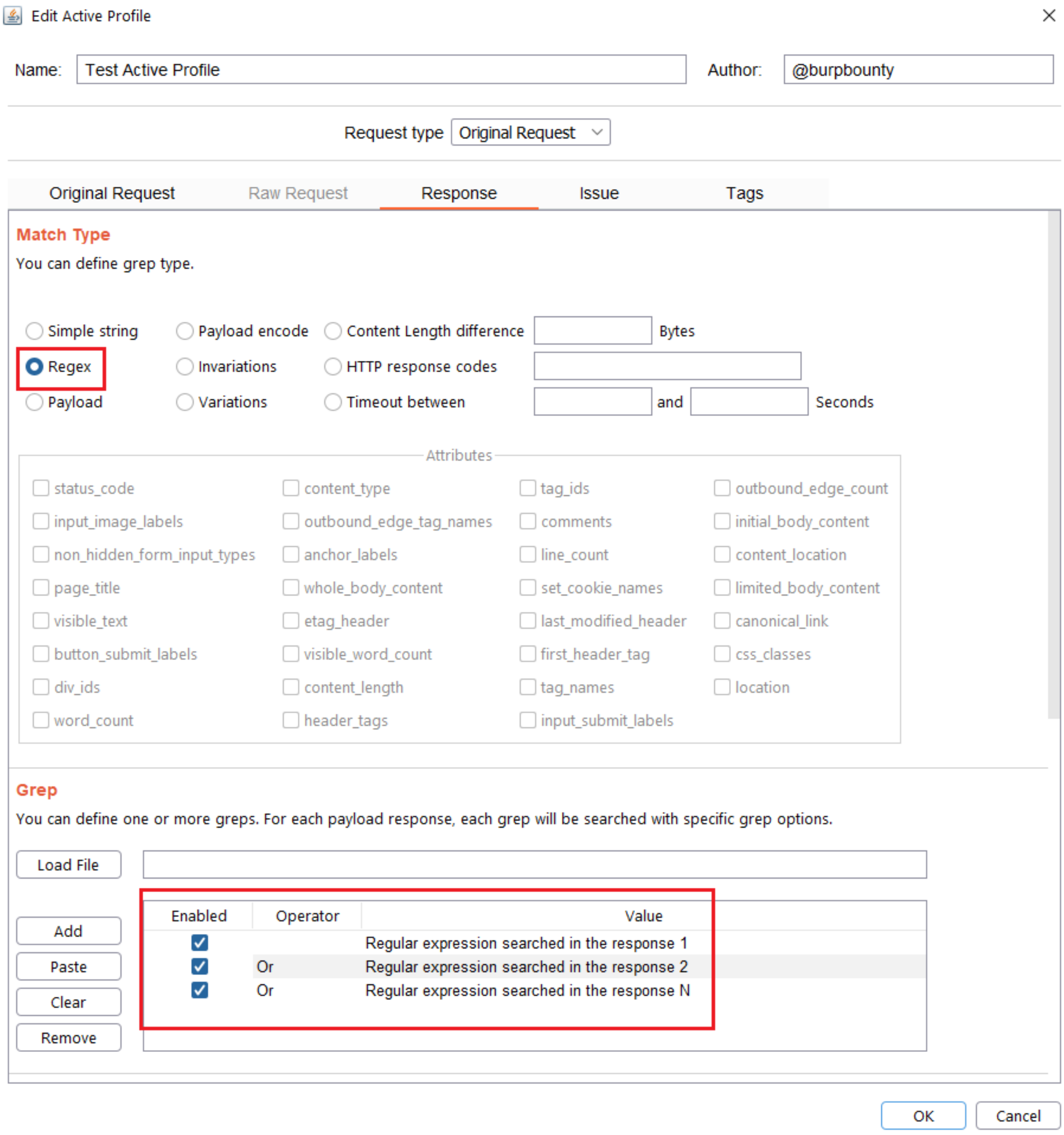
□ status_code □ content_type □ tag_ids □ outbound_edge_count
□ input_image_labels □ outbound_edge_tag_names □ comments □ initial_body_content
□ non_hidden_form_input_types □ anchor_labels □ line_count □ content_location
□ page_title □ whole_body_content □ set_cookie_names □ limited_body_content
□ visible_text □ etag_header □ last_modified_header □ canonical_link
□ button_submit_labels □ visible_word_count □ first_header_tag □ css_classes
□ div_ids □ content_length □ tag_names □ location
□ word_count □ header_tags □ input_submit_labels

Grep

You can define one or more greps. For each payload response, each grep will be searched with specific grep options.

Enabled	Operator	Value
☑		Simple String searched in the response 1
☑	Or	Simple String searched in the response 2
☑	Or	Simple String searched in the response N

- **Regex**: Search for a regular expression in the HTTP Response that you specify in the "Grep" section.



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Match Type

You can define grep type.

○ Simple string ○ Payload encode ○ Content Length difference Bytes

● Regex ○ Invariations ○ HTTP response codes

○ Payload ○ Variations ○ Timeout between and Seconds

Attributes

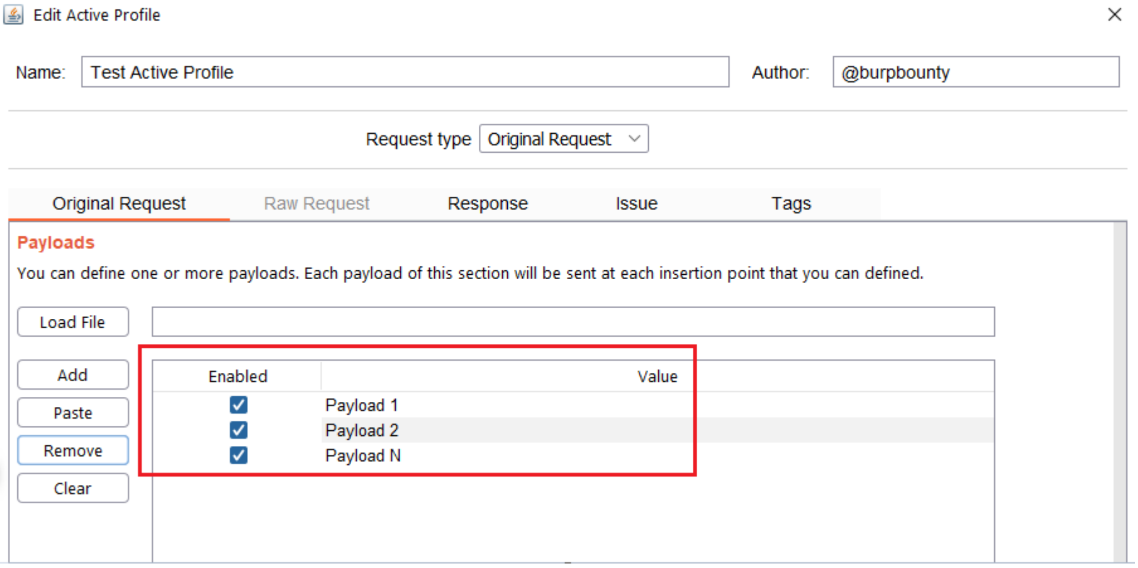
□ status_code
□ input_image_labels
□ non_hidden_form_input_types
□ page_title
□ visible_text
□ button_submit_labels
□ div_ids
□ word_count
□ content_type
□ outbound_edge_tag_names
□ anchor_labels
□ whole_body_content
□ etag_header
□ visible_word_count
□ content_length
□ header_tags
□ tag_ids
□ comments
□ line_count
□ set_cookie_names
□ last_modified_header
□ first_header_tag
□ tag_names
□ input_submit_labels
□ outbound_edge_count
□ initial_body_content
□ content_location
□ limited_body_content
□ canonical_link
□ css_classes
□ location

Grep

You can define one or more greps. For each payload response, each grep will be searched with specific grep options.

Enabled	Operator	Value
☑		Regular expression searched in the response 1
☑	Or	Regular expression searched in the response 2
☑	Or	Regular expression searched in the response N

- **Payload**: Search for a Payload (that have been specified in the Original Request->Payloads section) in the HTTP response.



Name: Test Active Profile

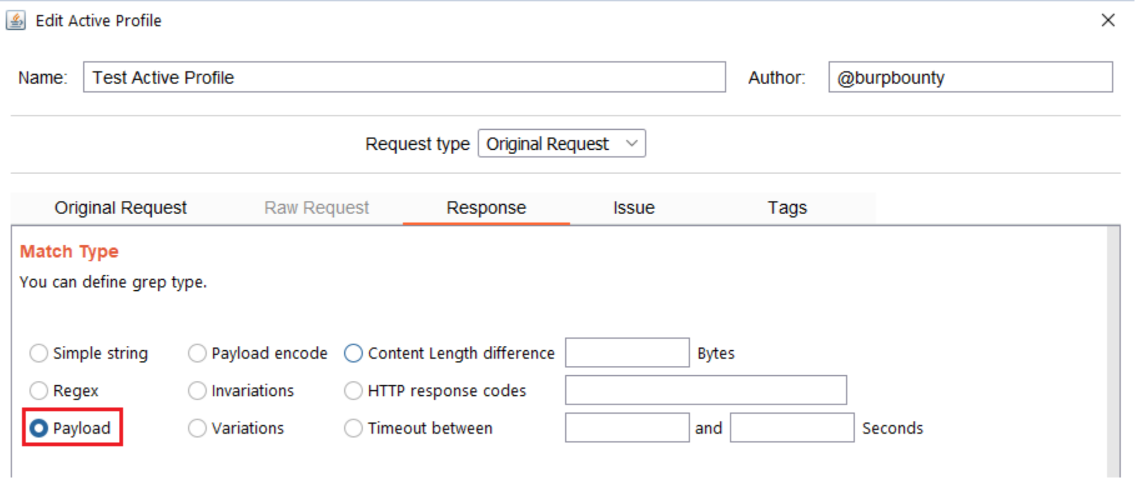
Author: @burpbounty

Request type: Original Request

Payloads

You can define one or more payloads. Each payload of this section will be sent at each insertion point that you can defined.

Enabled	Value
☑	Payload 1
☑	Payload 2
☑	Payload N



Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Match Type

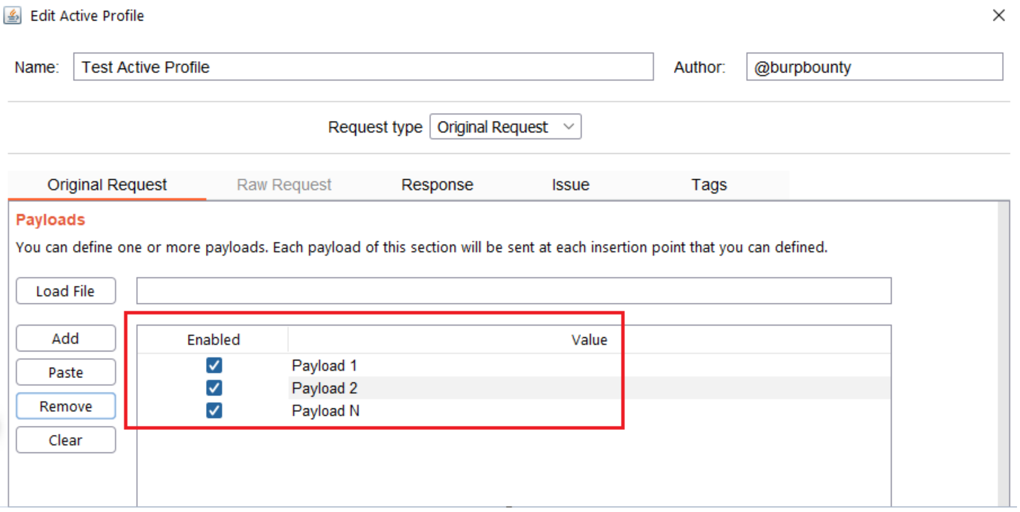
You can define grep type.

○ Simple string ○ Payload encode ○ Content Length difference

○ Regex ○ Invariations ○ HTTP response codes

● Payload ○ Variations ○ Timeout between

- **Payload encode**: If you have encoded the payload with the original request functionalities, here you look for the value of the payload before it's encoded, in the HTTP response. In this case you look for "Payload 1…Payload N" in the HTTP Response.



Edit Active Profile

Name: Test Active Profile

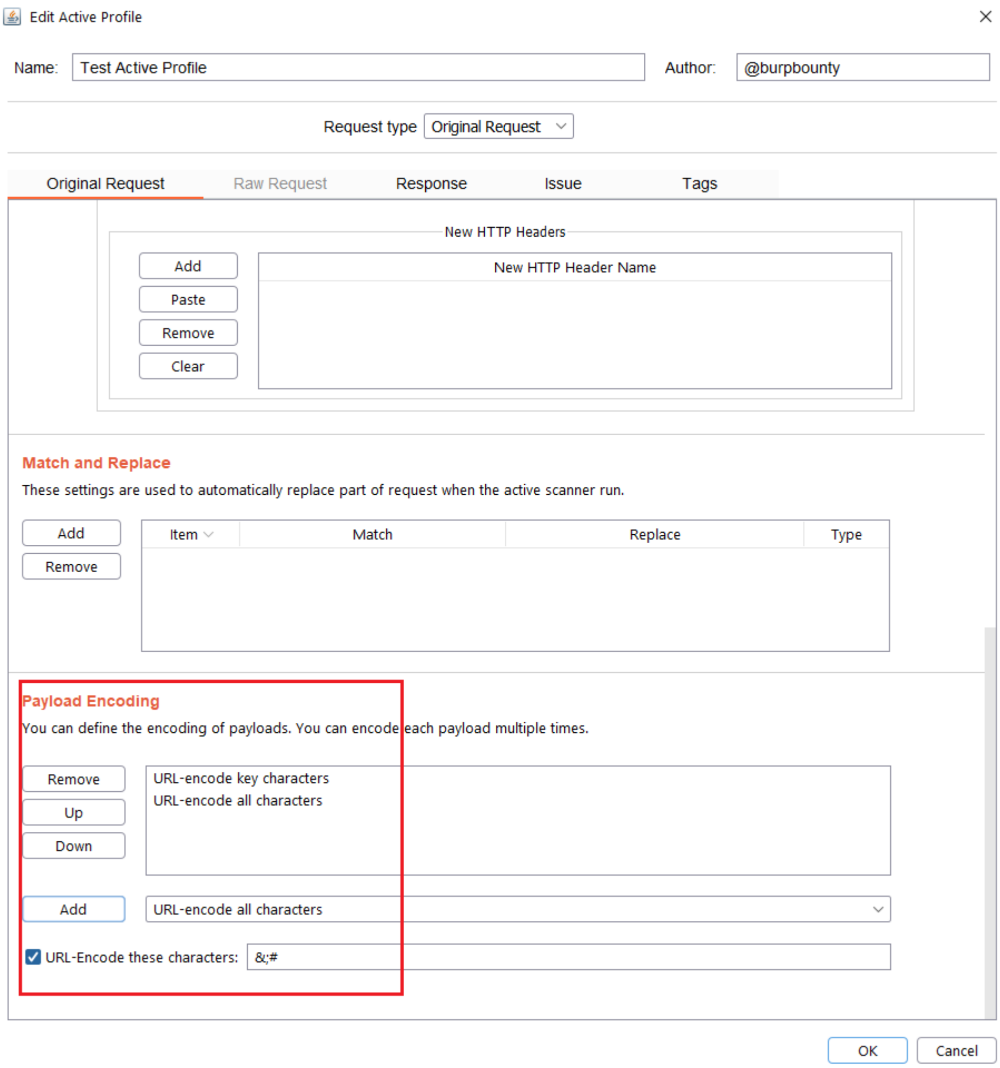
Author: @burpbounty

Request type: Original Request

Payloads

You can define one or more payloads. Each payload of this section will be sent at each insertion point that you can defined.

Enabled	Value
☑	Payload 1
☑	Payload 2
☑	Payload N



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Match and Replace

These settings are used to automatically replace part of request when the active scanner run.

Item	Match	Replace	Type

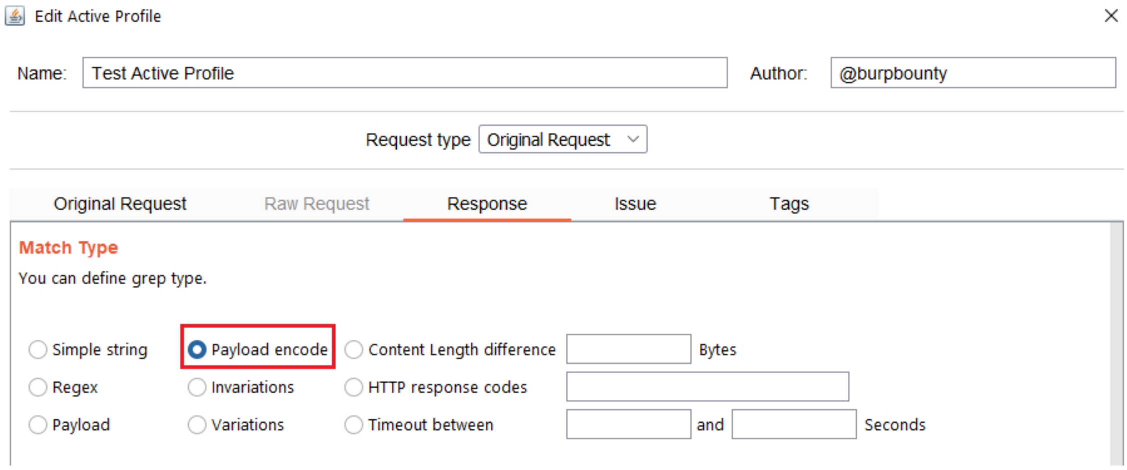
Payload Encoding

You can define the encoding of payloads. You can encode each payload multiple times.

URL-encode key characters
URL-encode all characters

URL-encode all characters

☑ URL-Encode these characters: &;#



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Match Type

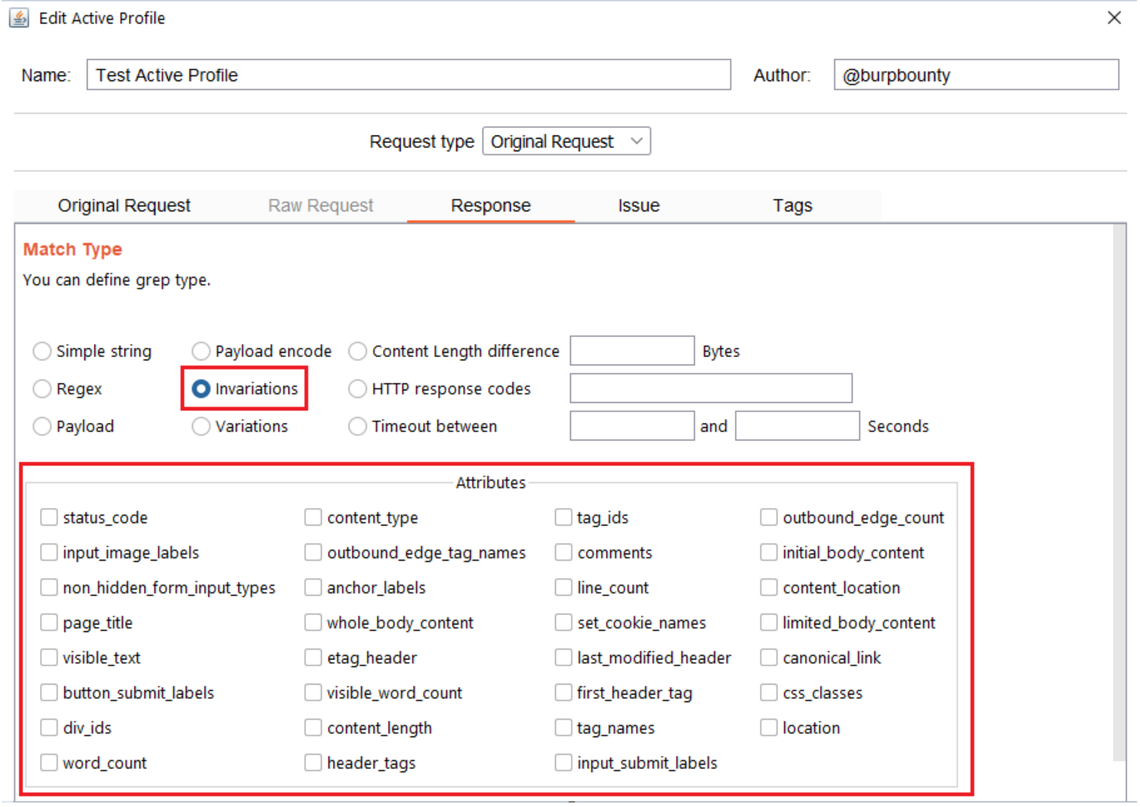
You can define grep type.

○ Simple string ● Payload encode ○ Content Length difference ______ Bytes

○ Regex ○ Invariations ○ HTTP response codes ______

○ Payload ○ Variations ○ Timeout between ______ and ______ Seconds

- **Invariations**: This option looks for the NO difference in the attributes marked in the "Attributes" section between the response of the original HTTP request and the responses of the HTTP requests modified with the payloads.



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Match Type

You can define grep type.

○ Simple string ○ Payload encode ○ Content Length difference ______ Bytes

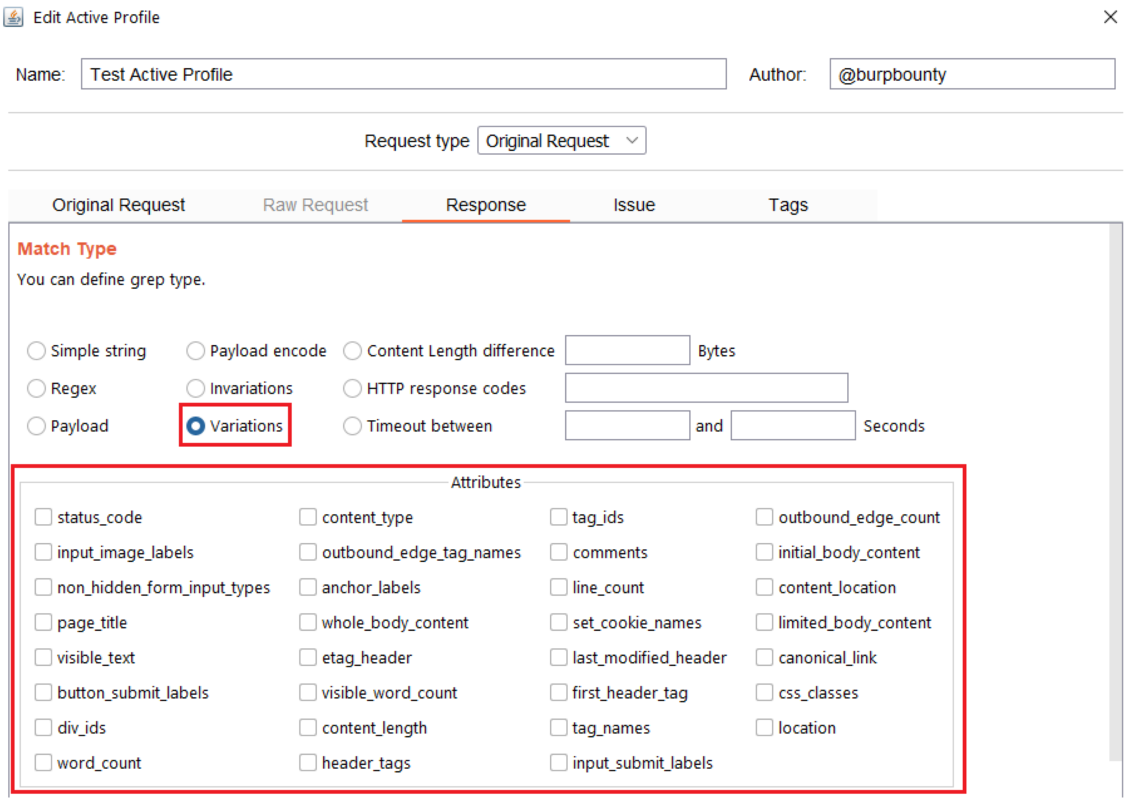
○ Regex ● Invariations ○ HTTP response codes ______

○ Payload ○ Variations ○ Timeout between ______ and ______ Seconds

Attributes

□ status_code	□ content_type	□ tag_ids	□ outbound_edge_count
□ input_image_labels	□ outbound_edge_tag_names	□ comments	□ initial_body_content
□ non_hidden_form_input_types	□ anchor_labels	□ line_count	□ content_location
□ page_title	□ whole_body_content	□ set_cookie_names	□ limited_body_content
□ visible_text	□ etag_header	□ last_modified_header	□ canonical_link
□ button_submit_labels	□ visible_word_count	□ first_header_tag	□ css_classes
□ div_ids	□ content_length	□ tag_names	□ location
□ word_count	□ header_tags	□ input_submit_labels	

- **Variations**: This option looks for the difference in the attributes marked in the "Attributes" section between the response of the original HTTP request and the responses of the requests modified with the payloads.



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Original Request | Raw Request | Response | Issue | Tags

Match Type

You can define grep type.

○ Simple string ○ Payload encode ○ Content Length difference [ ] Bytes

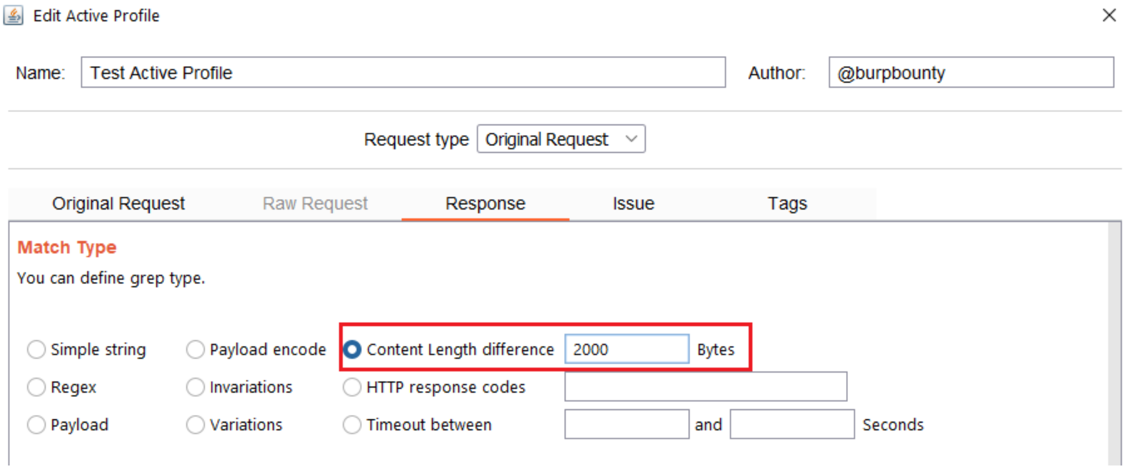
○ Regex ○ Invariations ○ HTTP response codes [ ]

○ Payload ● Variations ○ Timeout between [ ] and [ ] Seconds

Attributes

□ status_code
□ input_image_labels
□ non_hidden_form_input_types
□ page_title
□ visible_text
□ button_submit_labels
□ div_ids
□ word_count
□ content_type
□ outbound_edge_tag_names
□ anchor_labels
□ whole_body_content
□ etag_header
□ visible_word_count
□ content_length
□ header_tags
□ tag_ids
□ comments
□ line_count
□ set_cookie_names
□ last_modified_header
□ first_header_tag
□ tag_names
□ input_submit_labels
□ outbound_edge_count
□ initial_body_content
□ content_location
□ limited_body_content
□ canonical_link
□ css_classes
□ location

- **Content length difference**: This option finds the difference between the content length (in bytes) of the response of the original HTTP request and the responses of the requests modified with the payloads.



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Original Request | Raw Request | Response | Issue | Tags

Match Type

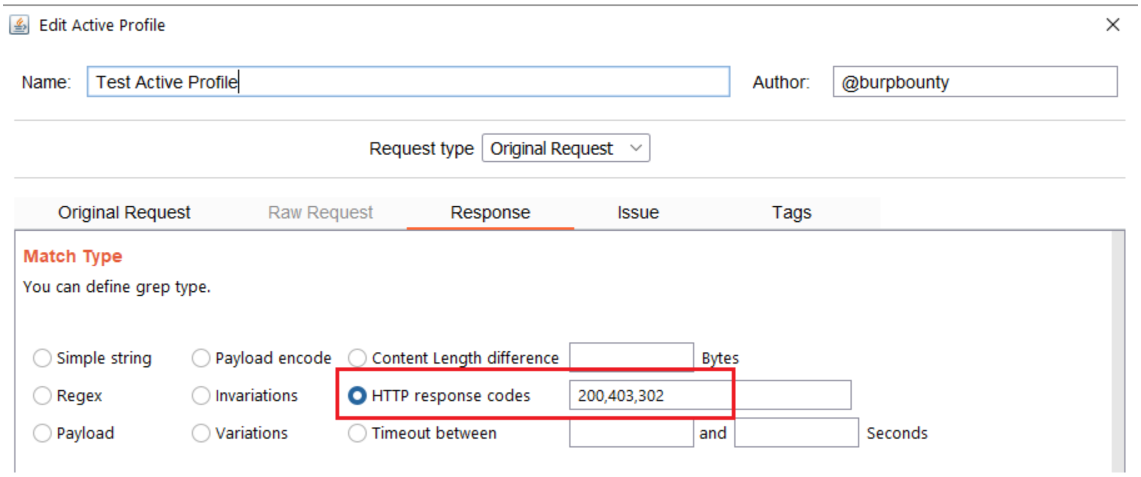
You can define grep type.

○ Simple string ○ Payload encode ● Content Length difference 2000 Bytes

○ Regex ○ Invariations ○ HTTP response codes [ ]

○ Payload ○ Variations ○ Timeout between [ ] and [ ] Seconds

- **HTTP Response codes**: This option looks for the HTTP response codes. The following example will search for:
    - HTTP 200 OK
    - HTTP 403 Forbidden
    - HTTP 302 Found



Edit Active Profile

Name: Test Active Profile | Author: @burpbounty

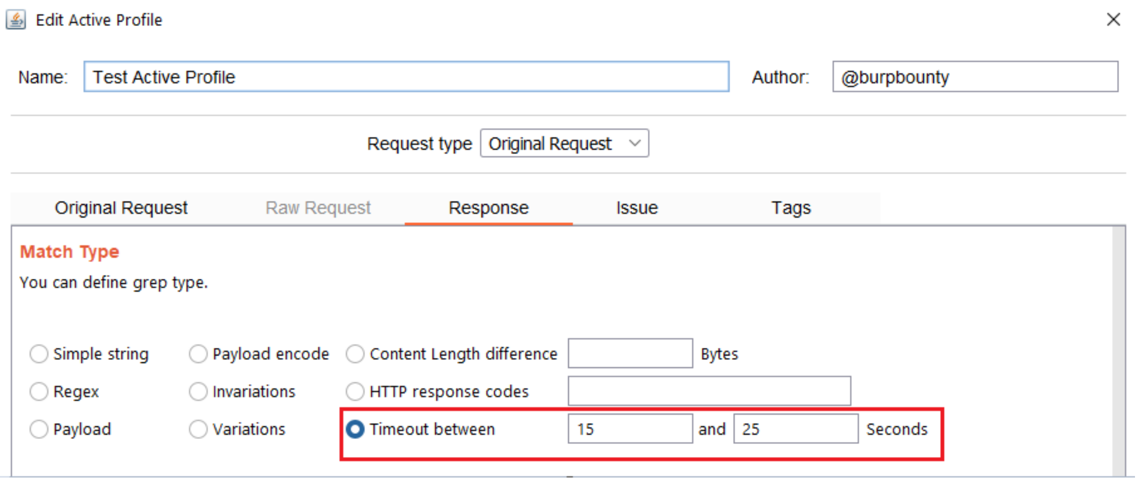
Request type: Original Request

Match Type

You can define grep type.

○ Simple string ○ Payload encode ○ Content Length difference Bytes
○ Regex ○ Invariations ● HTTP response codes 200,403,302
○ Payload ○ Variations ○ Timeout between and Seconds

- **Timeout between**: This option searches in the HTTP responses for a time delay in seconds in a range that can be specified. The following example looks for a HTTP response to take between 15 seconds and 25 seconds to respond.



Edit Active Profile

Name: Test Active Profile | Author: @burpbounty

Request type: Original Request

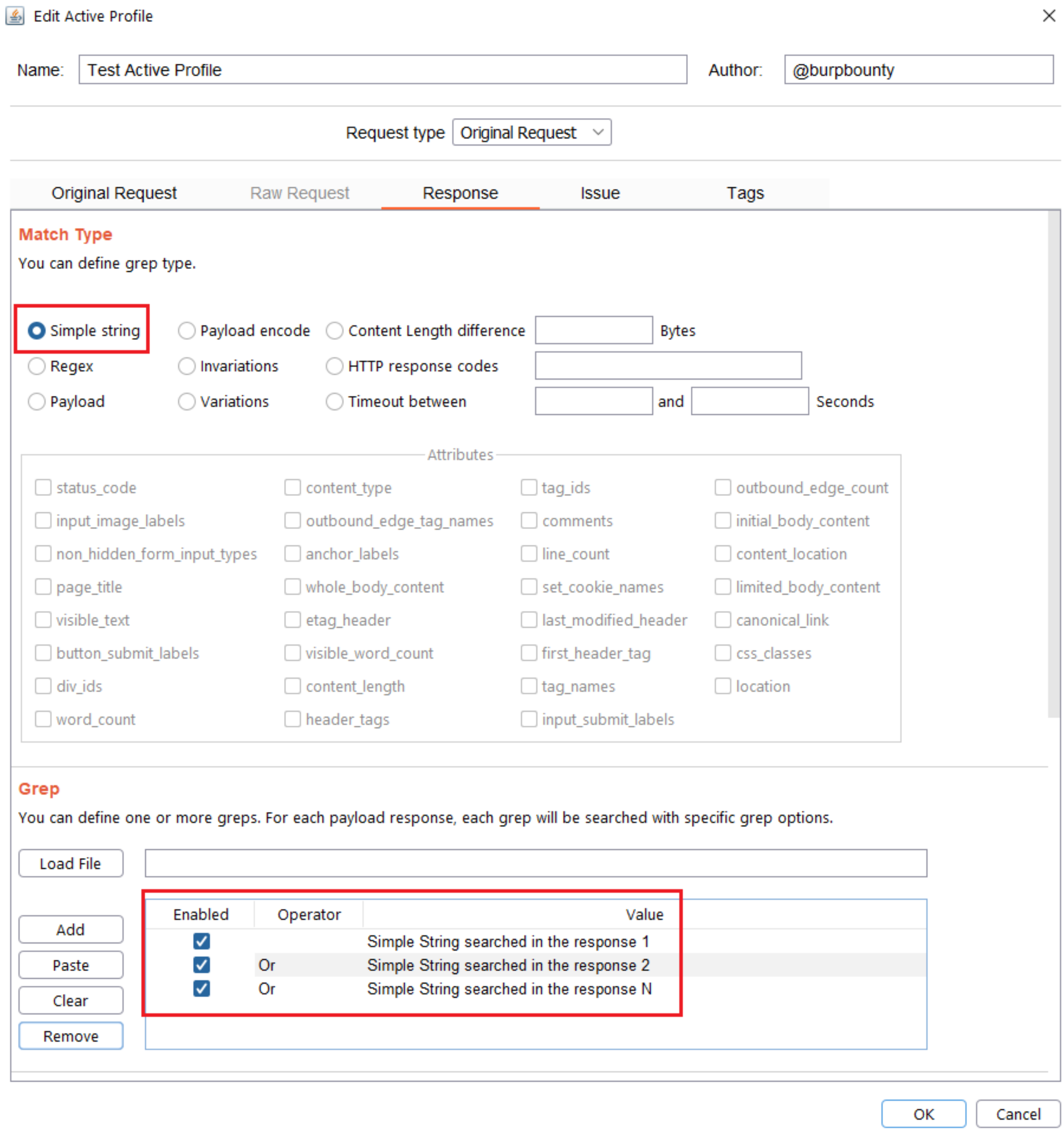
Match Type

You can define grep type.

○ Simple string ○ Payload encode ○ Content Length difference Bytes
○ Regex ○ Invariations ○ HTTP response codes
○ Payload ○ Variations ● Timeout between 15 and 25 Seconds

Step 5 (Required if you choose Simple string or Regex match type)-Response->Grep: In this section we must specify what we will look for in the HTTP response.

Simple String: What "Simple string" we will look for in the response. In this case we will look for three simple strings, "Simple String searched in the response 1", "Simple String searched in the response 2", "Simple String searched in the response N".



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Match Type

You can define grep type.

● Simple string
○ Regex
○ Payload
○ Payload encode
○ Invariations
○ Variations
○ Content Length difference ___ Bytes
○ HTTP response codes ___
○ Timeout between ___ and ___ Seconds

Attributes

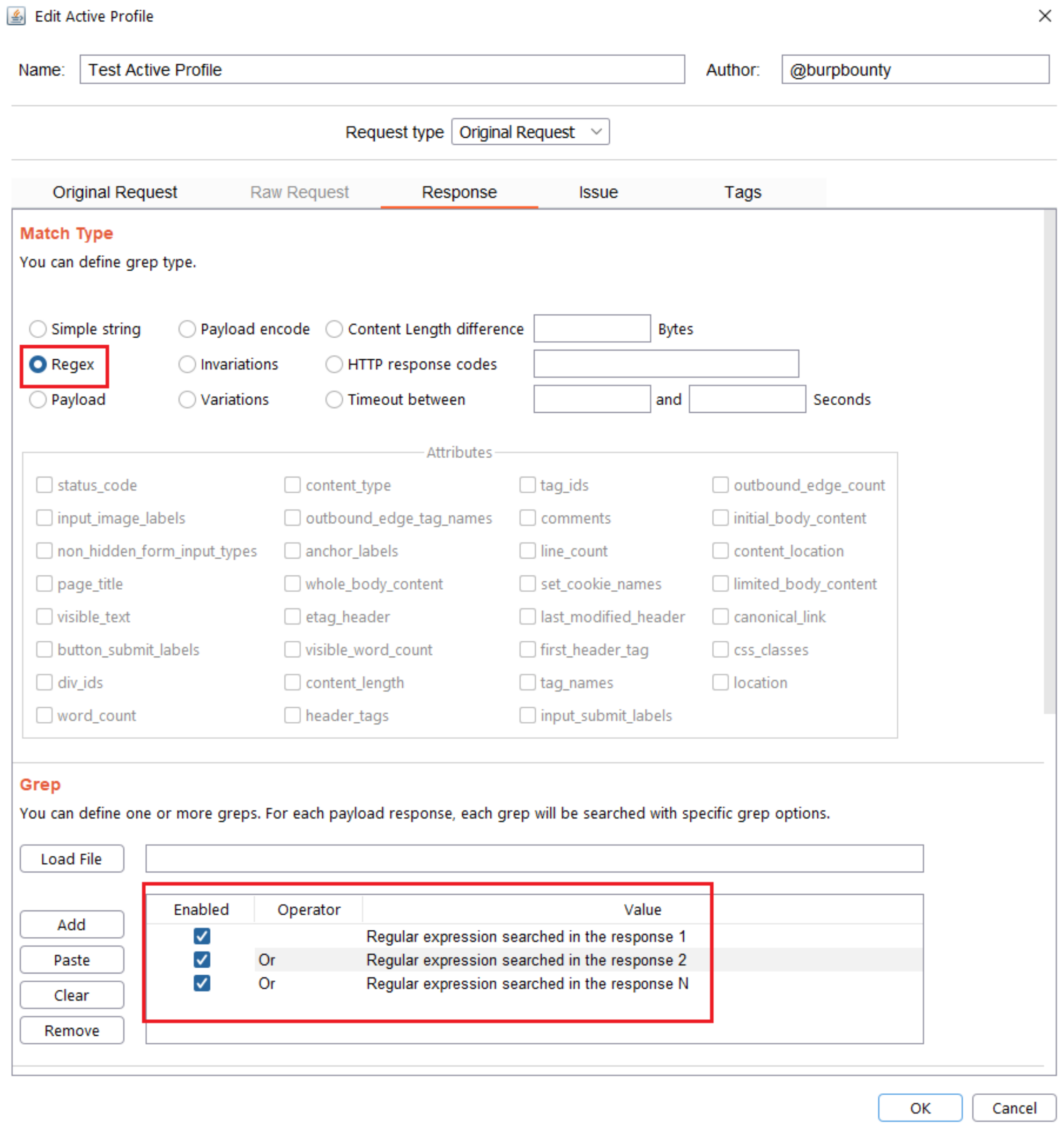
□ status_code
□ input_image_labels
□ non_hidden_form_input_types
□ page_title
□ visible_text
□ button_submit_labels
□ div_ids
□ word_count
□ content_type
□ outbound_edge_tag_names
□ anchor_labels
□ whole_body_content
□ etag_header
□ visible_word_count
□ content_length
□ header_tags
□ tag_ids
□ comments
□ line_count
□ set_cookie_names
□ last_modified_header
□ first_header_tag
□ tag_names
□ input_submit_labels
□ outbound_edge_count
□ initial_body_content
□ content_location
□ limited_body_content
□ canonical_link
□ css_classes
□ location

Grep

You can define one or more greps. For each payload response, each grep will be searched with specific grep options.

Enabled	Operator	Value
☑		Simple String searched in the response 1
☑	Or	Simple String searched in the response 2
☑	Or	Simple String searched in the response N

Regex: What regular expression we will look for in the response. In this case we will look for three regular expressions, "Regular expression searched in the response 1", "Regular expression searched in the response 2", "Regular expression searched in the response N".



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Match Type

You can define grep type.

○ Simple string ○ Payload encode ○ Content Length difference Bytes

● Regex ○ Invariations ○ HTTP response codes

○ Payload ○ Variations ○ Timeout between and Seconds

Attributes

□ status_code □ content_type □ tag_ids □ outbound_edge_count

□ input_image_labels □ outbound_edge_tag_names □ comments □ initial_body_content

□ non_hidden_form_input_types □ anchor_labels □ line_count □ content_location

□ page_title □ whole_body_content □ set_cookie_names □ limited_body_content

□ visible_text □ etag_header □ last_modified_header □ canonical_link

□ button_submit_labels □ visible_word_count □ first_header_tag □ css_classes

□ div_ids □ content_length □ tag_names □ location

□ word_count □ header_tags □ input_submit_labels

Grep

You can define one or more greps. For each payload response, each grep will be searched with specific grep options.

Enabled	Operator	Value
☑		Regular expression searched in the response 1
☑	Or	Regular expression searched in the response 2
☑	Or	Regular expression searched in the response N

Step 6 (Optional)- Response->Grep Options: In this section you can specify more options to create more accurate profiles and obtain fewer false positives. This options only are disponible for the Match types:

- Simple string
- Regex
- Payload
- Payload Encode

Each of the options will be detailed below:

- **Negative match**: It will show you the alert, if the pattern you have set is not present in the HTTP response.

- **Case sensitive**: The pattern will be searched in the HTTP response considering that it’s case sensitive.

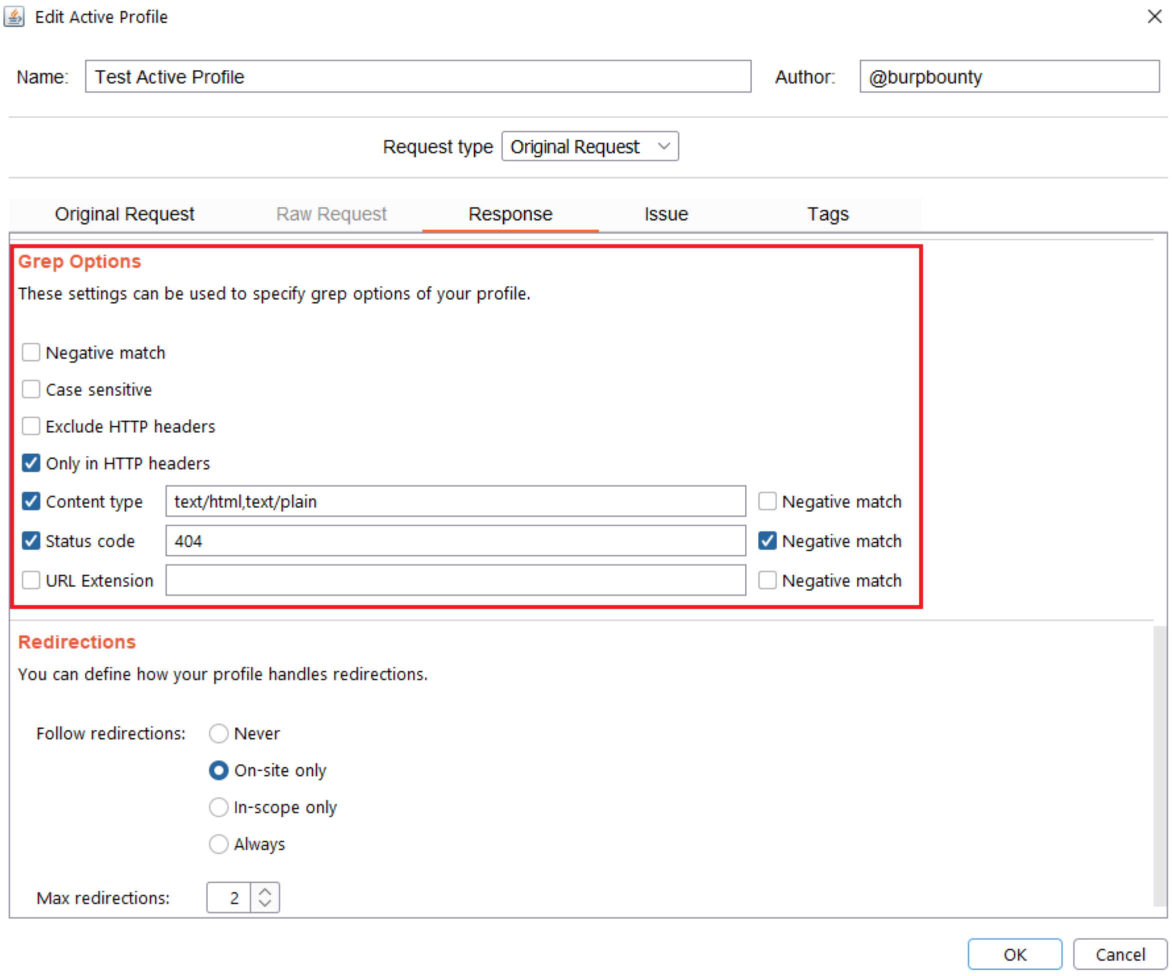
- **Exclude HTTP headers**: The pattern will NOT be searched in the HTTP headers. (Only in the body of the HTTP response)

- **Only in HTTP header**: The pattern will ONLY be searched in the HTTP headers.

- **Content type**: The pattern will only be searched in the HTTP response if the content type of the HTTP response is equal to the "content type" field. You can specify multiple content types separated by commas. You can also specify that ONLY look for the pattern in the HTTP response if the content type is NOT equal to this field, marking the "negative match" checkbox.

- **Status code**: The pattern will only be searched in the HTTP response if the Status code of the HTTP response is equal to the "status code" field. You can specify multiple status code separated by commas. You can also specify that ONLY look for the pattern in the HTTP response if the status code is NOT equal to this field, marking the "negative match" checkbox.

- **URL Extension**: It will only search for patterns if the extension of the URL to which the request is made, matches the extension or extensions specified in this field (for example, php or jsp, etc) or if it doesn’t match (negative match checkbox)



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Grep Options

These settings can be used to specify grep options of your profile.

☐ Negative match

☐ Case sensitive

☐ Exclude HTTP headers

☑ Only in HTTP headers

☑ Content type: text/html,text/plain ☐ Negative match

☑ Status code: 404 ☑ Negative match

☐ URL Extension: ☐ Negative match

Redirections

You can define how your profile handles redirections.

Follow redirections:
○ Never
● On-site only
○ In-scope only
○ Always

Max redirections: 2

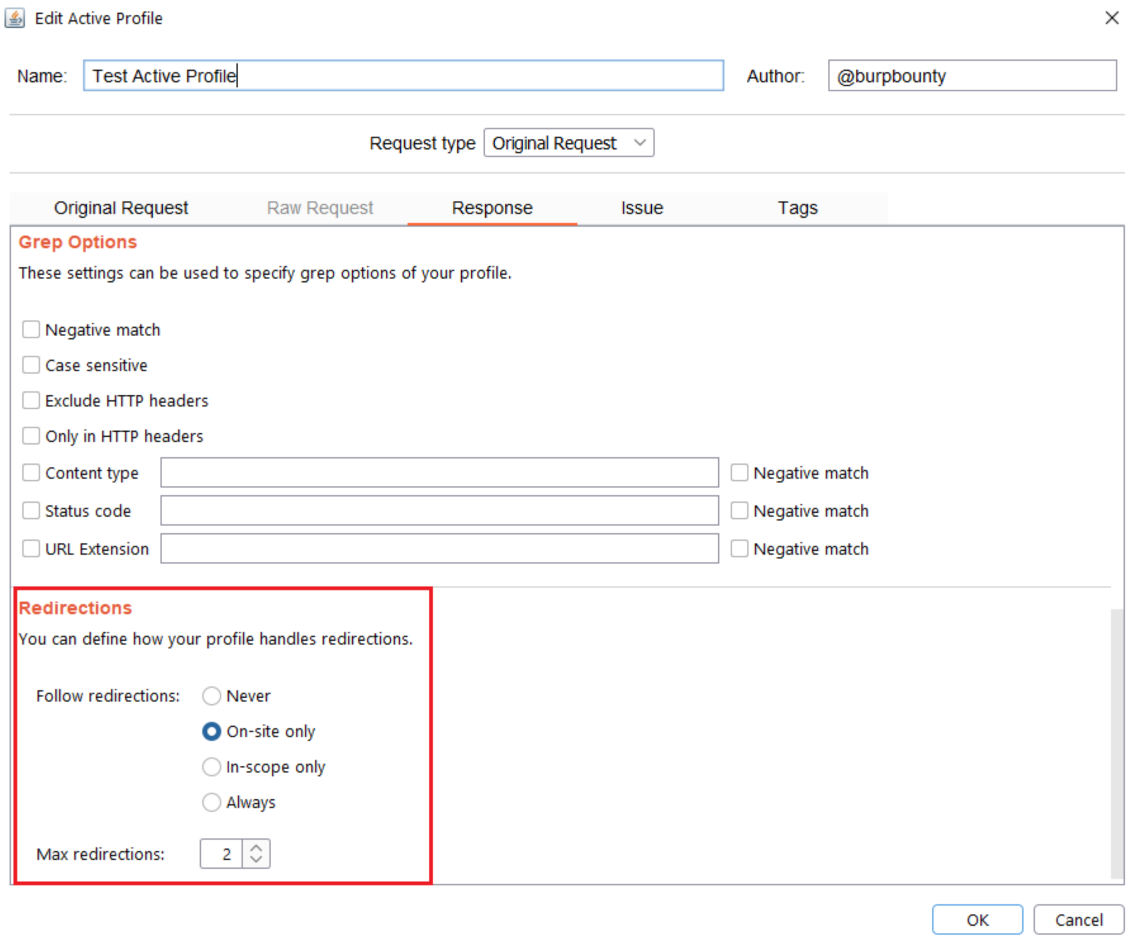
Step 7 (Optional)- Response->Redirections: In this section you can specify the redirection options. This options only are disponible for the Match types:

- Simple string
- Regex
- Payload
- Payload Encode

Each of the options will be detailed below:

- **Never:** As the name suggests, no redirect will be followed.
- **On-site only:** It will only follow the redirects that lead to the same site of origin.
- **In-scope only:** It will only follow redirects that lead to a domain that is in scope.
- **Always:** As the name suggests, it will follow all redirects.

Max redirections: In this field the maximum number of redirects that will follow is indicated.



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Original Request | Raw Request | Response | Issue | Tags

Grep Options

These settings can be used to specify grep options of your profile.

□ Negative match
□ Case sensitive
□ Exclude HTTP headers
□ Only in HTTP headers
□ Content type □ Negative match
□ Status code □ Negative match
□ URL Extension □ Negative match

Redirections

You can define how your profile handles redirections.

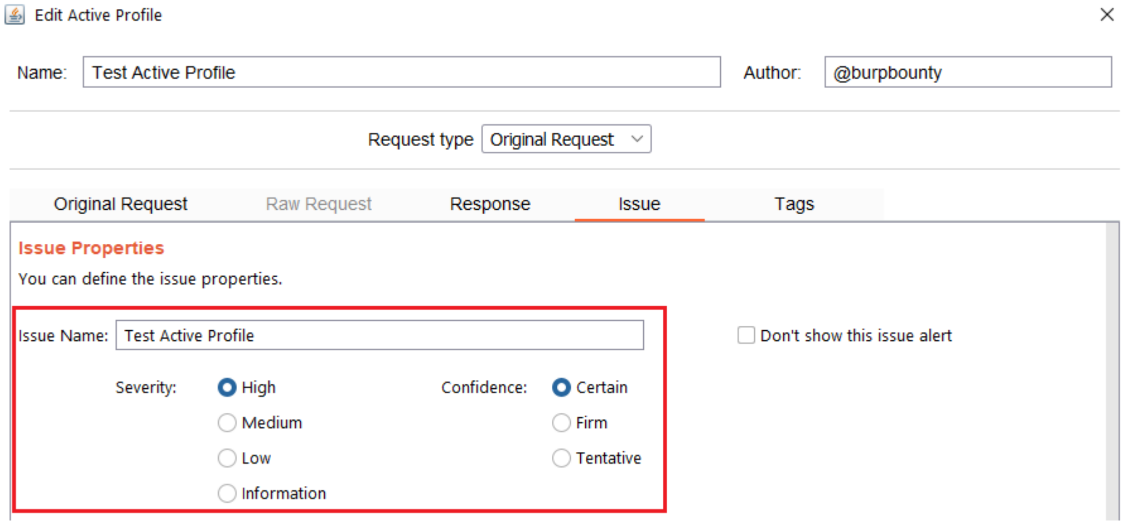
Follow redirections: ○ Never ● On-site only ○ In-scope only ○ Always

Max redirections: 2

Step 8 (Required)- Issue: It specifies the name that will appear in the alert and the criticality of that alert.

It's necessary for the issue to appear, give it a "Issue Name" and complete the two fields, both the "severity" and the "confidence". The issue descriptions are optional.

If you check the option "Don't show this issue alert" the alert will not be shown in the dashboard, it will only be used for the Smart Scan.



Edit Active Profile

Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Issue Properties

You can define the issue properties.

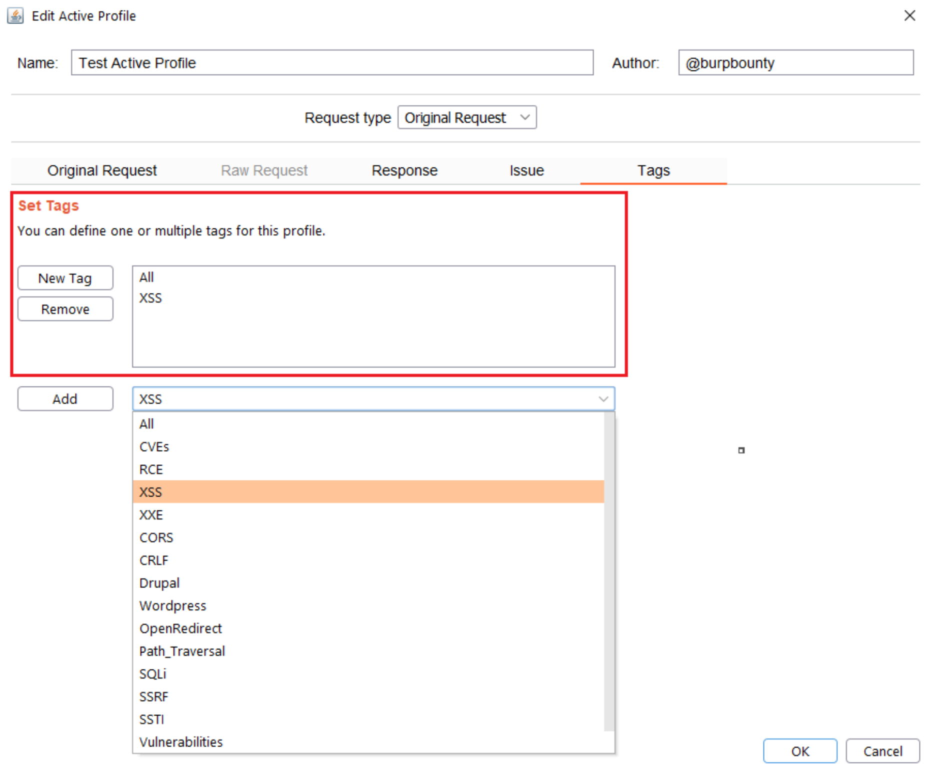
Issue Name: Test Active Profile

Severity: ● High ○ Medium ○ Low ○ Information

Confidence: ● Certain ○ Firm ○ Tentative

□ Don't show this issue alert

Step 9 (Optional): A tag is created and assigned to the profile. These tags can be used to launch the "Scan Tags" scanner.



Edit Active Profile

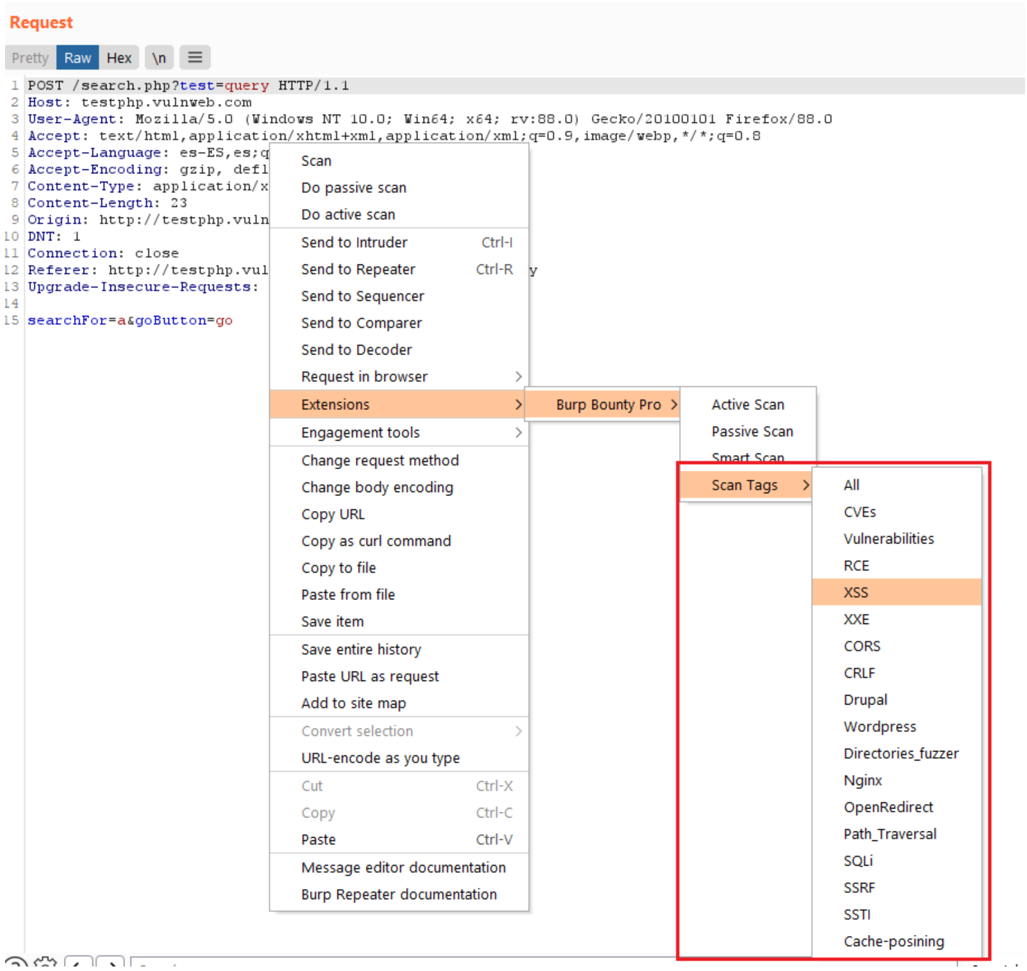
Name: Test Active Profile

Author: @burpbounty

Request type: Original Request

Set Tags

You can define one or multiple tags for this profile.



Request

```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q
Accept-Encoding: gzip, defl
Content-Type: application/x
Content-Length: 23
Origin: http://testphp.vuln
DNT: 1
Connection: close
Referer: http://testphp.vul                        y
Upgrade-Insecure-Requests:

searchFor=a&goButton=go
```

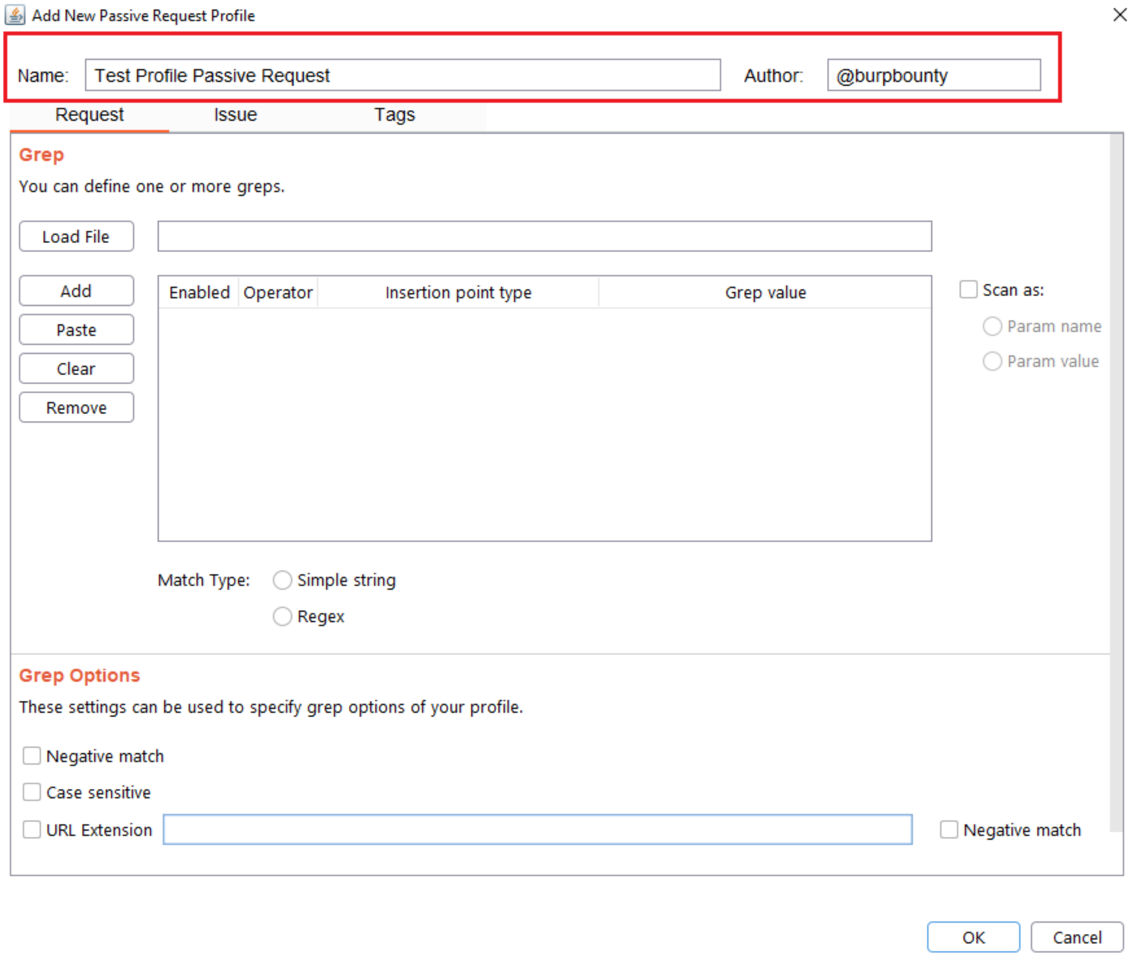
Passive Request Profiles

Burp Bounty Pro gives you the ability to create your own vulnerability profiles to the passive scanner.

- Passive Request Scanner: Look for strings/regex (or the absence of them) in HTTP requests.

Next let's see how passive request profiles are created to look for something (or the absence of it) in the **HTTP** request.

Step 1 (Required): The name and author of the profile are first set.



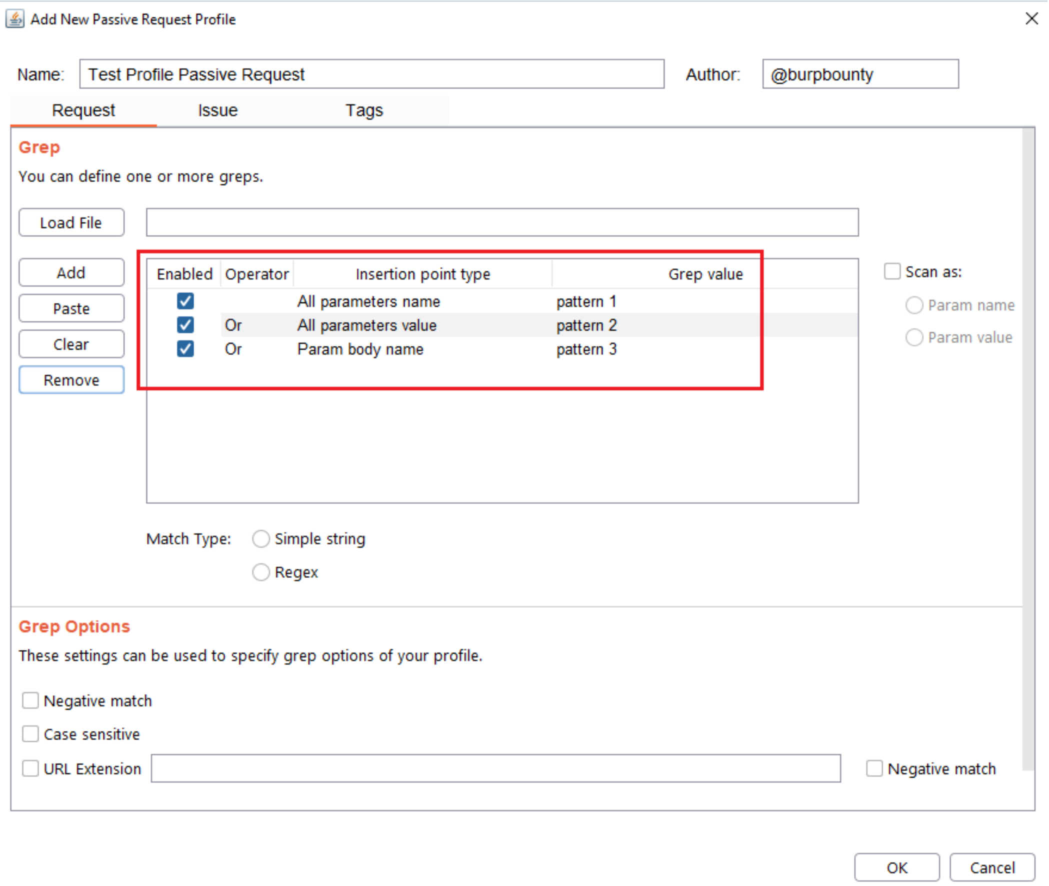
Add New Passive Request Profile

Name: Test Profile Passive Request

Author: @burpbounty

Step 2 (Required): Specifies the pattern or patterns to search in the request.

- You can add the pattern by click on the "add" button and modifying the value, or by pasting it directly with the "Paste" button if you already have it in the clipboard.
- You can also load a patterns file (one per line) with the "Load file" button.



Add New Passive Request Profile

Name: Test Profile Passive Request

Author: @burpbounty

Grep

You can define one or more greps.

Enabled	Operator	Insertion point type	Grep value
☑		All parameters name	pattern 1
☑	Or	All parameters value	pattern 2
☑	Or	Param body name	pattern 3

□ Scan as:

○ Param name

○ Param value

Match Type: ○ Simple string ○ Regex

Grep Options

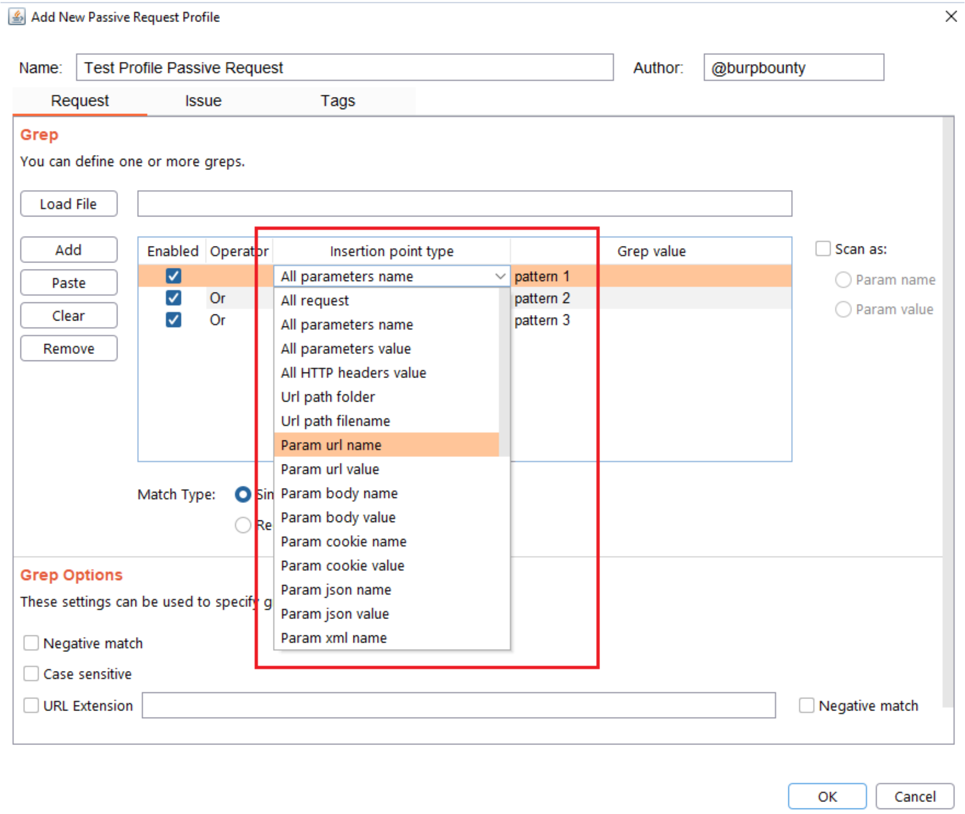
These settings can be used to specify grep options of your profile.

□ Negative match

□ Case sensitive

□ URL Extension □ Negative match

In this section you can choose in which insertion point you want to search for the pattern.



Add New Passive Request Profile

Name: Test Profile Passive Request Author: @burpbounty

Request Issue Tags

Grep

You can define one or more greps.

Enabled	Operator	Insertion point type	Grep value
☑		All parameters name	pattern 1
☑	Or		pattern 2
☑	Or		pattern 3

Match Type: ● Sin… ○ Re…

□ Scan as: ○ Param name ○ Param value

Grep Options

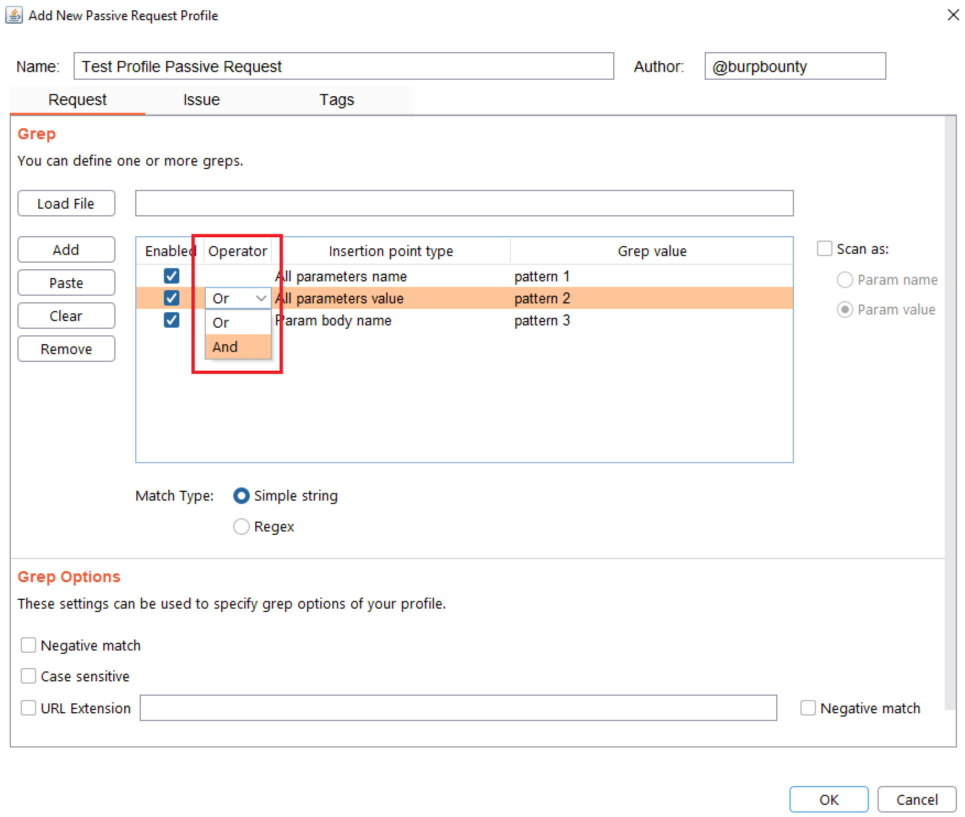
These settings can be used to specify g…

□ Negative match

□ Case sensitive

□ URL Extension □ Negative match

At the same time, the logical AND operator can be used when searching for a value. This allows us to further refine the profile and avoid false positives.



Add New Passive Request Profile

Name: Test Profile Passive Request Author: @burpbounty

Request Issue Tags

Grep

You can define one or more greps.

Enabled	Operator	Insertion point type	Grep value
☑		All parameters name	pattern 1
☑	Or	All parameters value	pattern 2
☑		Param body name	pattern 3

Match Type: ● Simple string ○ Regex

□ Scan as: ○ Param name ● Param value

Grep Options

These settings can be used to specify grep options of your profile.

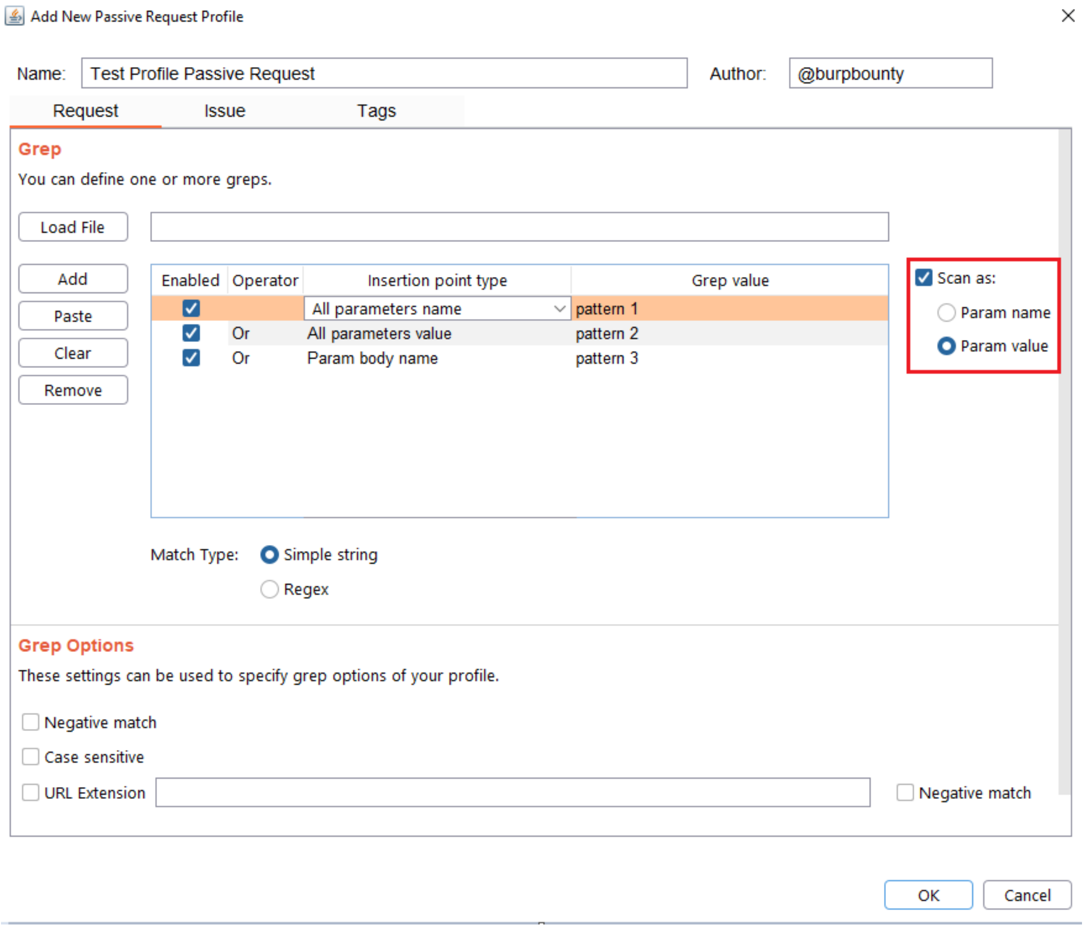
□ Negative match

□ Case sensitive

□ URL Extension □ Negative match

Step 3 (Optional): The passive request profile can be used for the Smart Scan. Two types of options:

- **Param name:** the insertion point type name will be scanned with the active profiles selected in a rule.
- **Param value:** the insertion point type value will be scanned with the active profiles selected in a rule.



Add New Passive Request Profile

Name: Test Profile Passive Request

Author: @burpbounty

Grep

You can define one or more greps.

Enabled	Operator	Insertion point type	Grep value
☑		All parameters name	pattern 1
☑	Or	All parameters value	pattern 2
☑	Or	Param body name	pattern 3

☑ Scan as:

○ Param name

● Param value

Match Type: ● Simple string ○ Regex

Grep Options

These settings can be used to specify grep options of your profile.

□ Negative match

□ Case sensitive

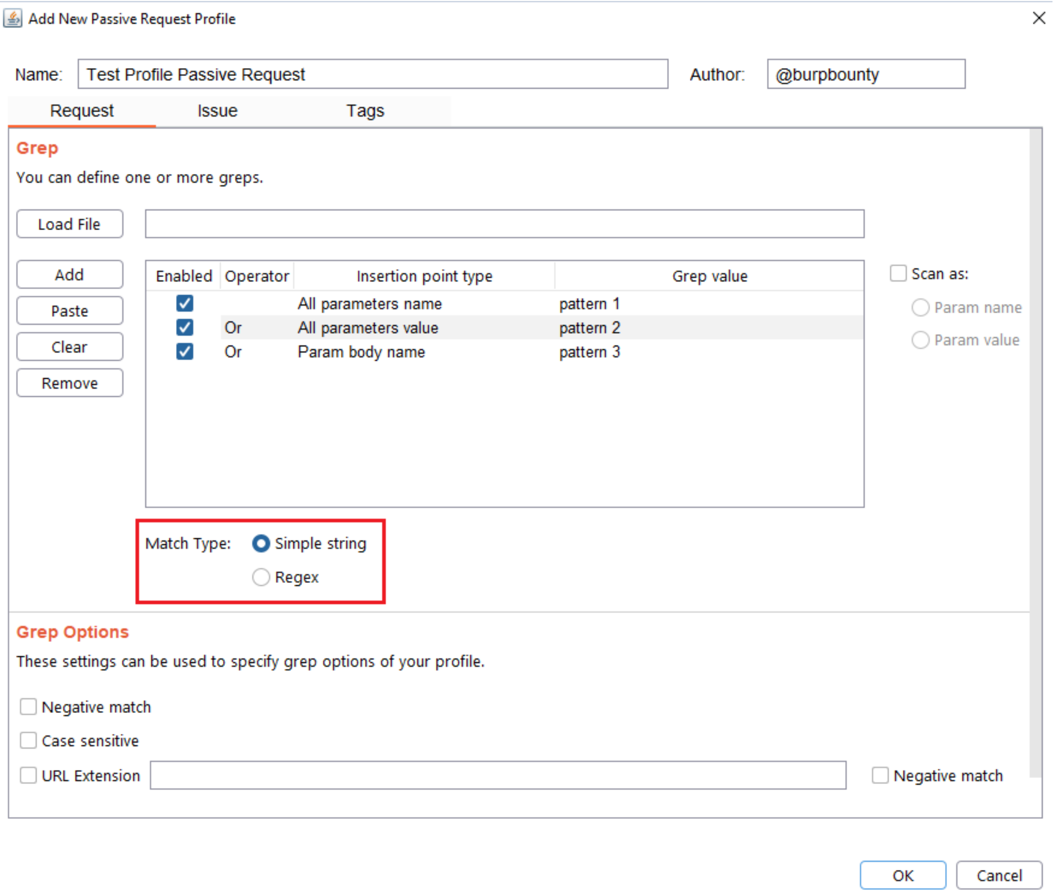
□ URL Extension □ Negative match

Note, that this step is not necessary if you only want to look for a pattern in the request and that it shows you an alert.

Step 4 (Required): Specifies which type of pattern to search in the insertion point.

- Simple string
- Regular expression

In this section you specify, if in the insertion point you want to search for a simple string or a regular expression.



Add New Passive Request Profile

Name: Test Profile Passive Request

Author: @burpbounty

Grep

You can define one or more greps.

Enabled	Operator	Insertion point type	Grep value
☑		All parameters name	pattern 1
☑	Or	All parameters value	pattern 2
☑	Or	Param body name	pattern 3

□ Scan as:

○ Param name

○ Param value

Match Type: ● Simple string ○ Regex

Grep Options

These settings can be used to specify grep options of your profile.

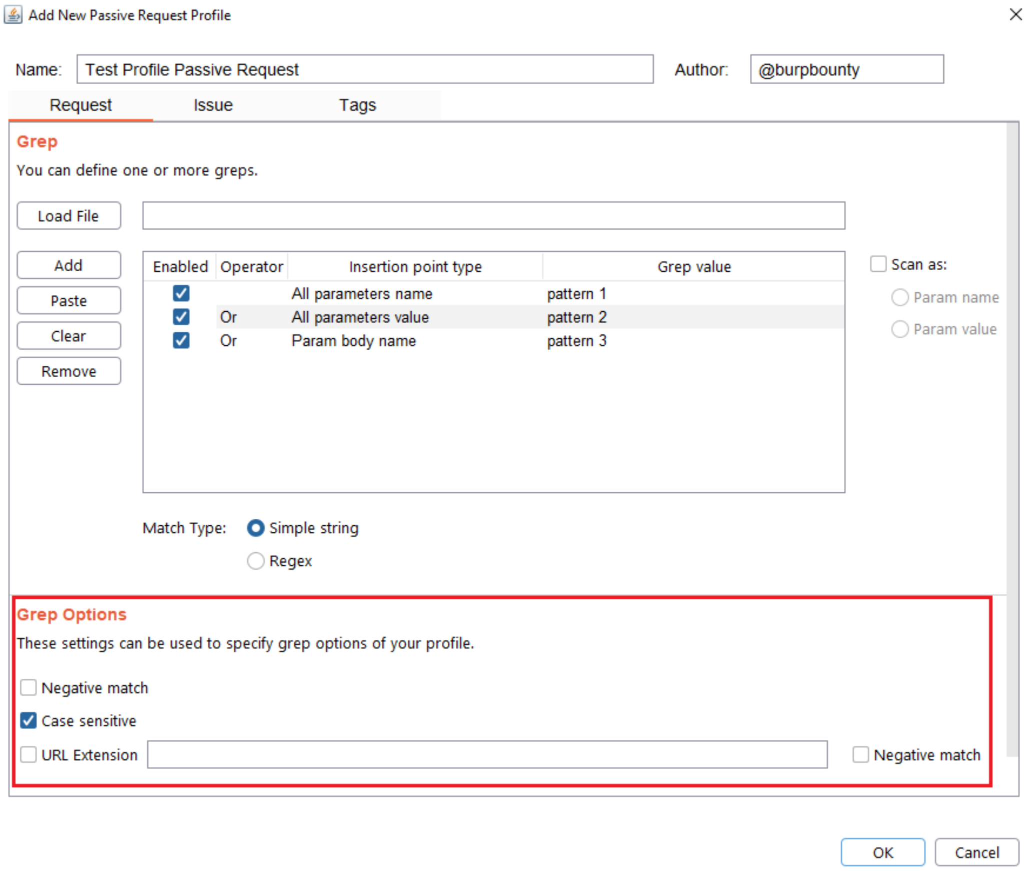
□ Negative match

□ Case sensitive

□ URL Extension □ Negative match

Step 5 (Optional): Grep options are specified**.**

- **Negative match**: It will show you the alert, if the pattern you have set is not present in the insertion point that you have chosen.
- **Case sensitive**: The pattern will be searched in the insertion point considering that it's case sensitive.
- **URL Extension**: It will only search for patterns if the extension of the URL to which the request is made, matches the extension or extensions specified in this field (for example, php or jsp, etc) or if it doesn't match (negative match checkbox)



Name: Test Profile Passive Request

Author: @burpbounty

Grep

You can define one or more greps.

Enabled	Operator	Insertion point type	Grep value
☑		All parameters name	pattern 1
☑	Or	All parameters value	pattern 2
☑	Or	Param body name	pattern 3

□ Scan as:
○ Param name
○ Param value

Match Type: ● Simple string ○ Regex

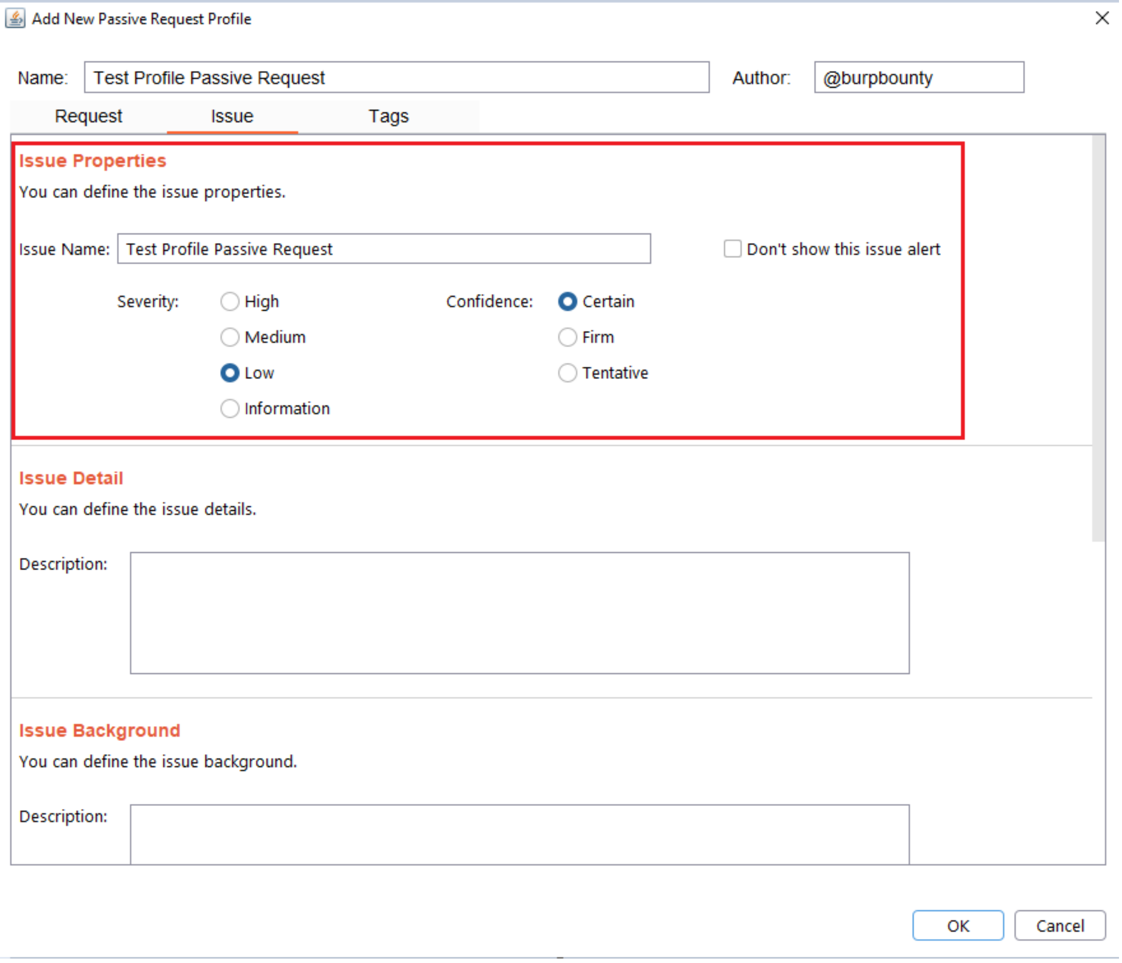
Grep Options

These settings can be used to specify grep options of your profile.

□ Negative match
☑ Case sensitive
□ URL Extension □ Negative match

Step 6 (Required): It specifies the name that will appear in the alert and the criticality of that alert.

It's necessary for the issue to appear, give it a "Issue Name" and complete the two fields, both the "severity" and the "confidence". The issue descriptions are optional.



Name: Test Profile Passive Request

Author: @burpbounty

Issue Properties

You can define the issue properties.

Issue Name: Test Profile Passive Request

□ Don't show this issue alert

Severity: ○ High ○ Medium ● Low ○ Information

Confidence: ● Certain ○ Firm ○ Tentative

Issue Detail

You can define the issue details.

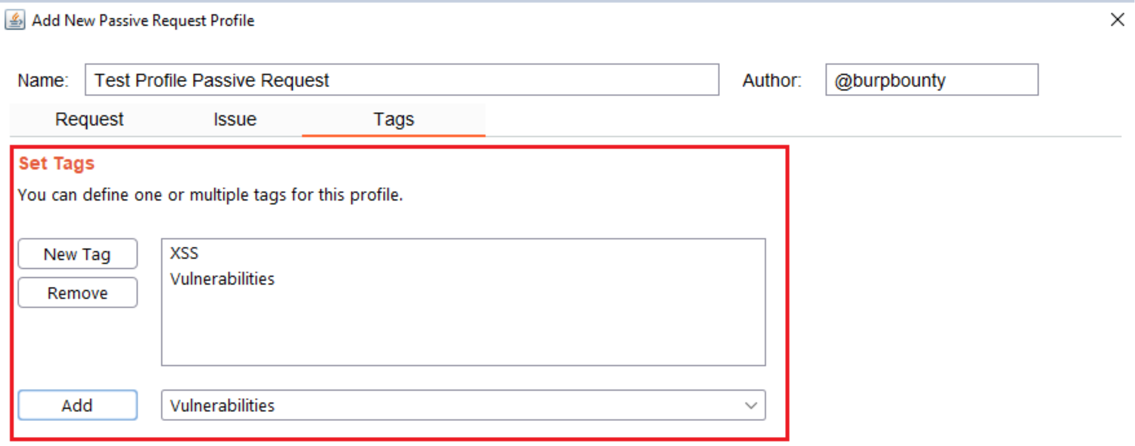
Description:

Issue Background

You can define the issue background.

Description:

Step 7 (Optional): A tag is created and assigned to the profile. This is useful for better organization of profiles.



Add New Passive Request Profile

Name: Test Profile Passive Request

Author: @burpbounty

Set Tags

You can define one or multiple tags for this profile.

XSS
Vulnerabilities

Vulnerabilities

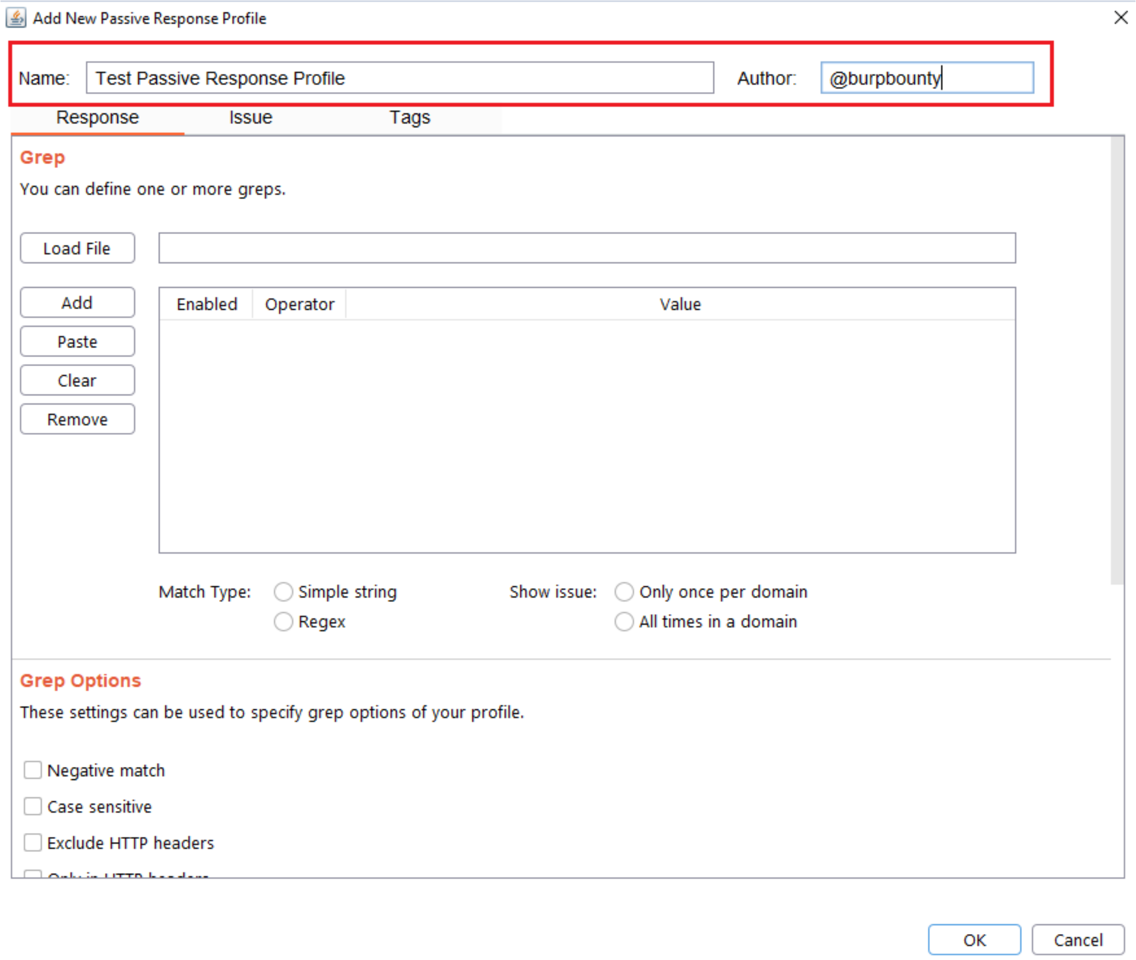
Passive Response Profiles

Burp Bounty Pro gives you the ability to create your own vulnerability profiles to the passive scanner.

- Passive Response Scanner: Look for strings/regex (or the absence of them) in HTTP response

Next let's see how passive response profiles are created to look for something (or the absence of it) in the **HTTP** response.

Step 1 (Required): The name and author of the profile are first set.



Add New Passive Response Profile

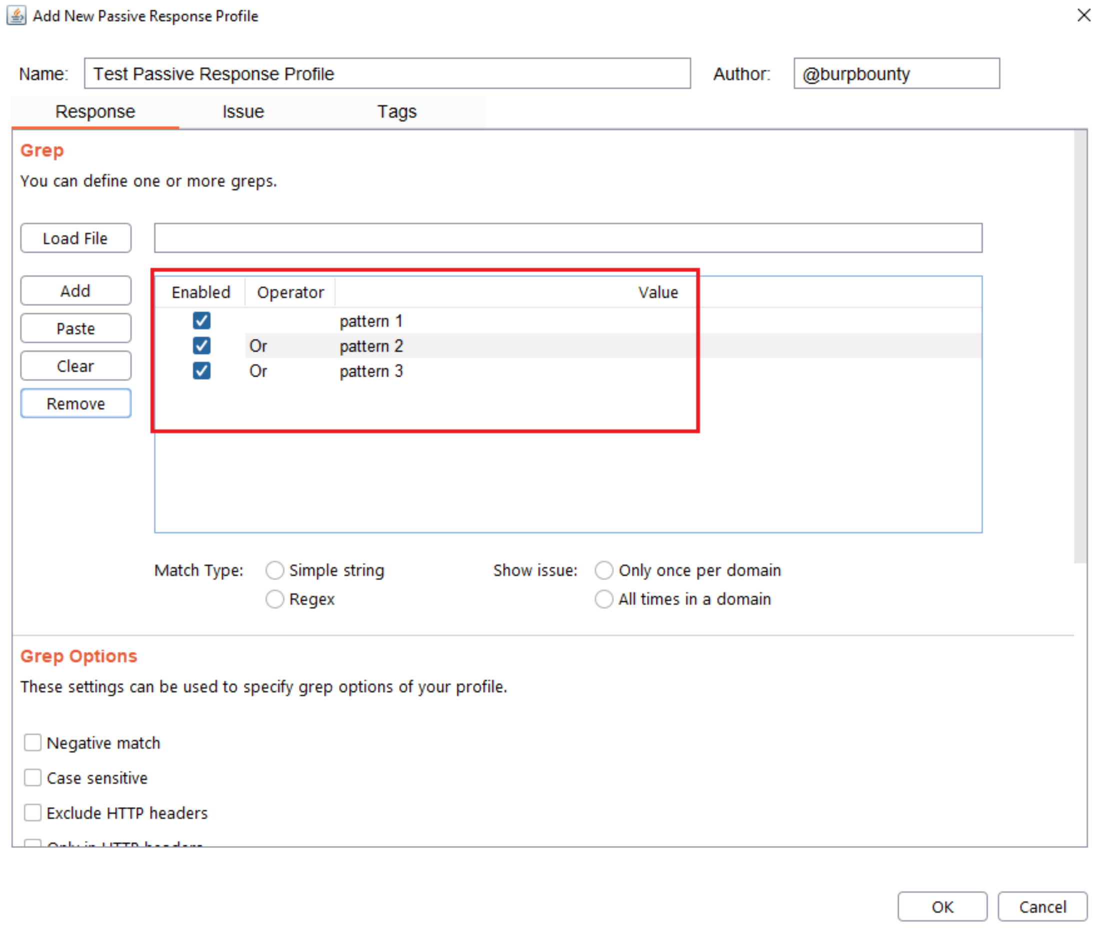
Name: Test Passive Response Profile

Author: @burpbounty

Response
Issue
Tags
Grep
You can define one or more greps.
Load File
Add
Paste
Clear
Remove
Enabled
Operator
Value
Match Type: ○ Simple string ○ Regex
Show issue: ○ Only once per domain ○ All times in a domain
Grep Options
These settings can be used to specify grep options of your profile.
□ Negative match
□ Case sensitive
□ Exclude HTTP headers
OK
Cancel

Step 2 (Required): It specifies the pattern or patterns to look for in the HTTP response.

- You can add the pattern by click on the "add" button and modifying the value, or by pasting it directly with the "Paste" button if you already have it in the clipboard.
- You can also load a patterns file (one per line) with the "Load file" button.
- At the same time, the logical AND operator can be used when searching for a value. This allows us to further refine the profile and avoid false positives.



Add New Passive Response Profile

Name: Test Passive Response Profile

Author: @burpbounty

Grep

You can define one or more greps.

Enabled	Operator	Value
☑		pattern 1
☑	Or	pattern 2
☑	Or	pattern 3

Match Type: ○ Simple string ○ Regex

Show issue: ○ Only once per domain ○ All times in a domain

Grep Options

These settings can be used to specify grep options of your profile.

☐ Negative match

☐ Case sensitive

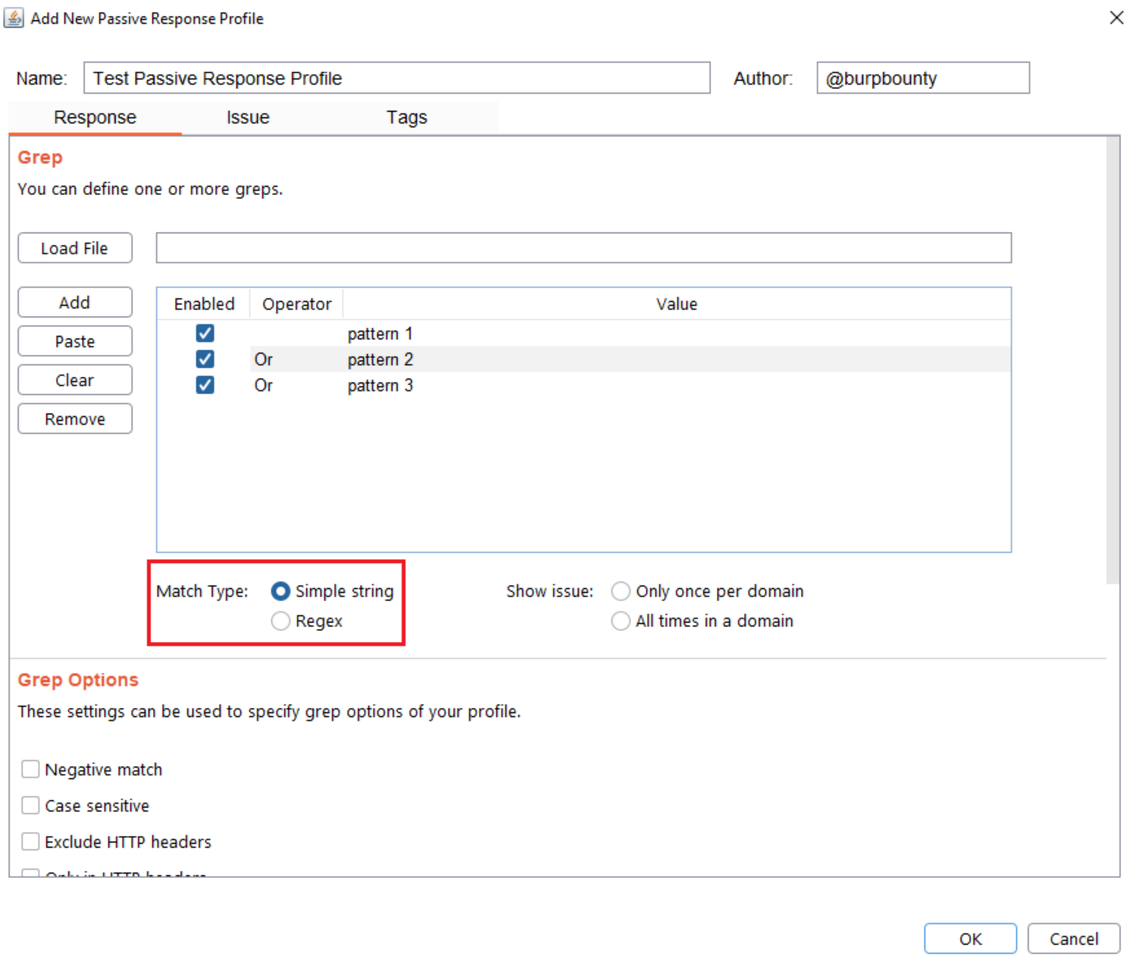
☐ Exclude HTTP headers

☐ Only in HTTP headers

Step 3 (Required): Specifies which type of pattern to search in the response.

- Simple string
- Regular expression

In this section you specify, if in the insertion point you want to search for a simple string or a regular expression.



Add New Passive Response Profile

Name: Test Passive Response Profile

Author: @burpbounty

Grep

You can define one or more greps.

Enabled	Operator	Value
☑		pattern 1
☑	Or	pattern 2
☑	Or	pattern 3

Match Type: ● Simple string ○ Regex

Show issue: ○ Only once per domain ○ All times in a domain

Grep Options

These settings can be used to specify grep options of your profile.

□ Negative match

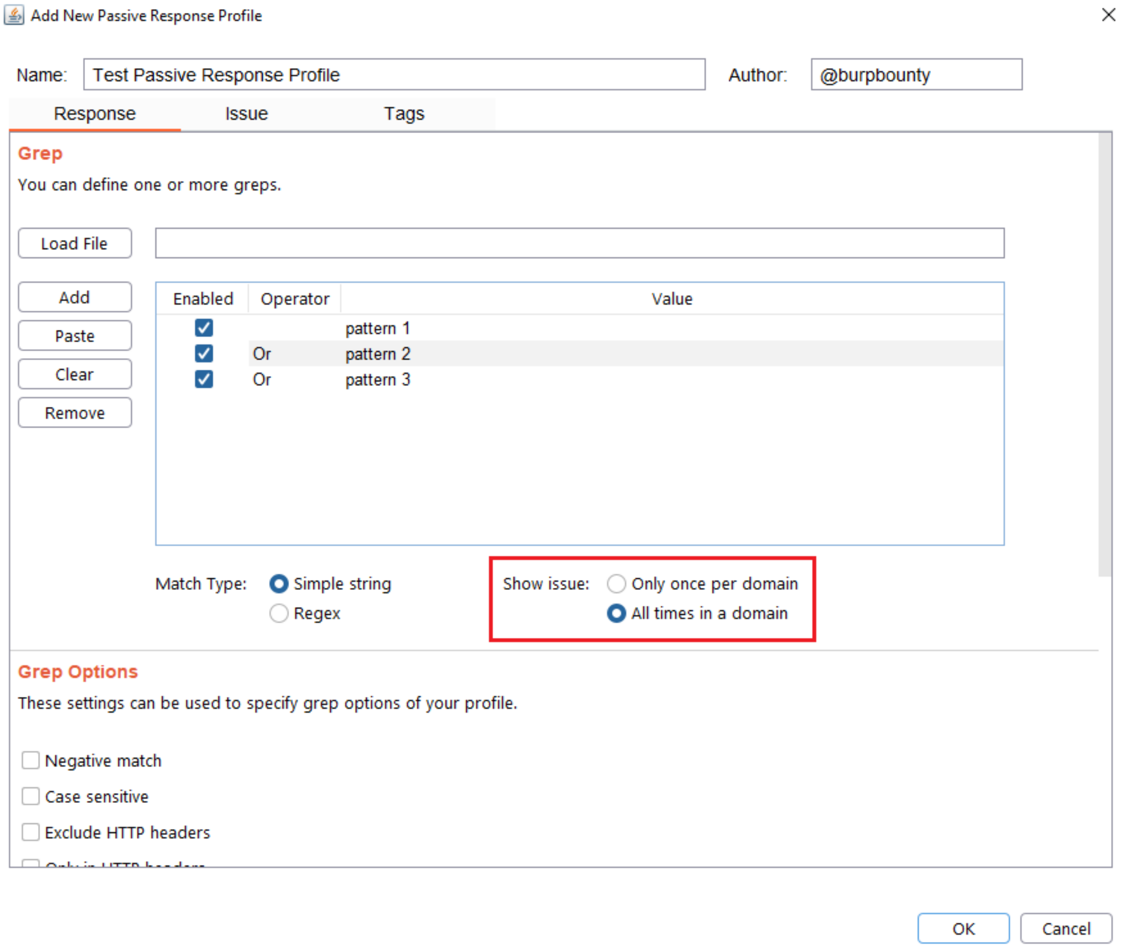
□ Case sensitive

□ Exclude HTTP headers

□ Only in HTTP headers

Step 4 (Optional): Specify how many times this issue will be displayed for one domain.

- **Only once per domain**: Only once time for all HTTP responses in one domain.
- **All times in a domain**: Every time that the pattern is detected in the domain HTTP responses.



Add New Passive Response Profile

Name: Test Passive Response Profile

Author: @burpbounty

Response | Issue | Tags

Grep

You can define one or more greps.

Enabled	Operator	Value
☑		pattern 1
☑	Or	pattern 2
☑	Or	pattern 3

Match Type: ● Simple string ○ Regex

Show issue: ○ Only once per domain ● All times in a domain

Grep Options

These settings can be used to specify grep options of your profile.

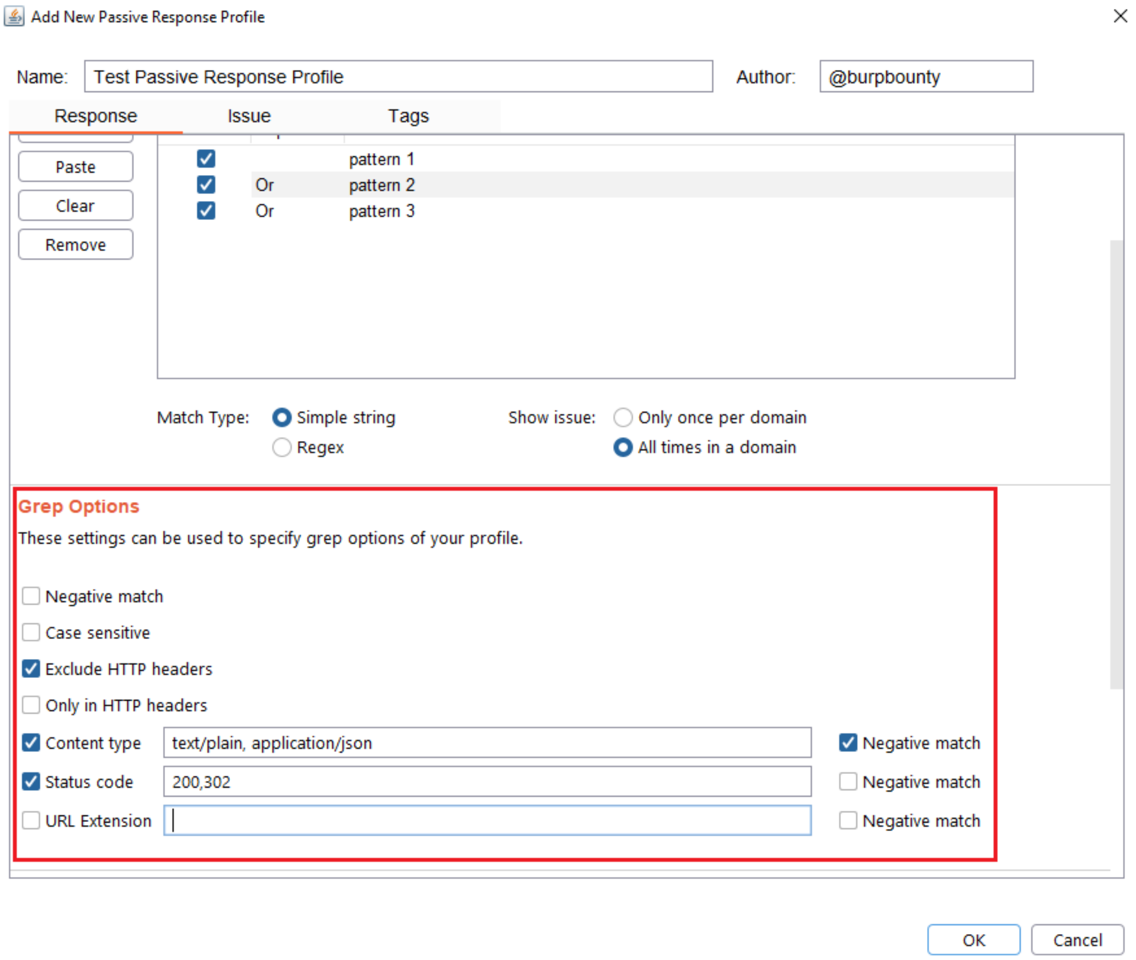
☐ Negative match

☐ Case sensitive

☐ Exclude HTTP headers

☐ Only in HTTP headers

Step 5 (Optional): Grep options are specified.



Add New Passive Response Profile

Name: Test Passive Response Profile

Author: @burpbounty

☑ pattern 1

☑ Or pattern 2

☑ Or pattern 3

Match Type: ● Simple string ○ Regex

Show issue: ○ Only once per domain ● All times in a domain

Grep Options

These settings can be used to specify grep options of your profile.

□ Negative match

□ Case sensitive

☑ Exclude HTTP headers

□ Only in HTTP headers

☑ Content type: text/plain, application/json ☑ Negative match

☑ Status code: 200,302 □ Negative match

□ URL Extension: □ Negative match

- **Negative match**: It will show you the alert, if the pattern you have set is not present in the HTTP response.

- **Case sensitive**: The pattern will be searched in the HTTP response considering that it’s case sensitive.

- **Exclude HTTP headers**: The pattern will NOT be searched in the HTTP headers. (Only in the body of the HTTP response)

- **Only in HTTP header**: The pattern will ONLY be searched in the HTTP headers.

- **Content type**: The pattern will only be searched in the HTTP response if the content type of the HTTP response is equal to the "content type" field. You can specify multiple content types separated by commas. You can also specify that ONLY look for the pattern in the HTTP response if the content type is NOT equal to this field, marking the "negative match" checkbox.

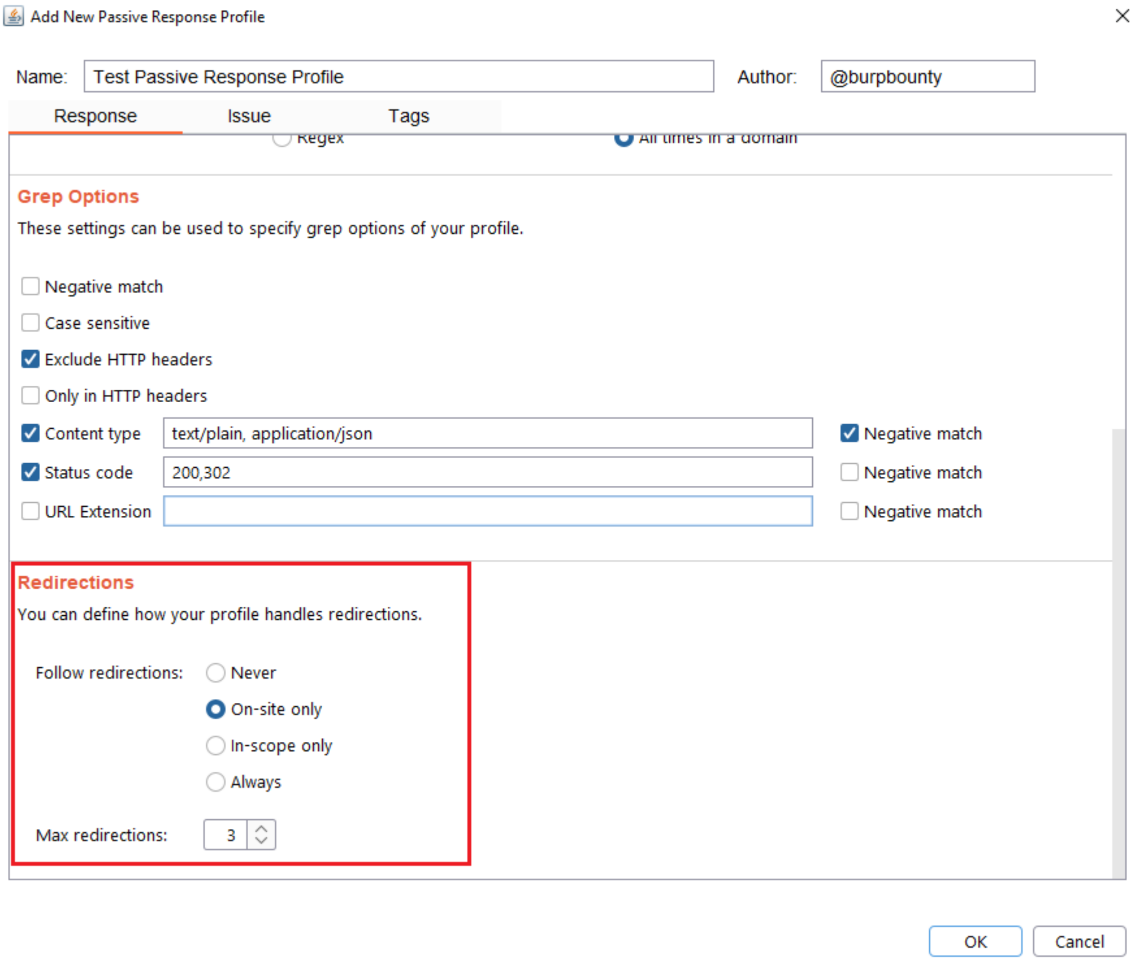
- **Status code**: The pattern will only be searched in the HTTP response if the Status code of the HTTP response is equal to the "status code" field. You can specify multiple status code separated by commas. You can also specify that ONLY look for the pattern in the HTTP response if the status code is NOT equal to this field, marking the "negative match" checkbox.

- **URL Extension**: It will only search for patterns if the extension of the URL to which the request is made, matches the extension or extensions specified in this field (for example, php or jsp, etc) or if it doesn't match (negative match checkbox)

Step 6 (Optional): Redirection options are specified. You can choose between the following options:

- **Never:** As the name suggests, no redirect will be followed.
- **On-site only:** It will only follow the redirects that lead to the same site of origin.
- **In-scope only:** It will only follow redirects that lead to a domain that is in scope.
- **Always:** As the name suggests, it will follow all redirects.

Max redirections: In this field the maximum number of redirects that will follow is indicated.



Add New Passive Response Profile

Name: Test Passive Response Profile   Author: @burpbounty

Grep Options

These settings can be used to specify grep options of your profile.

☐ Negative match
☐ Case sensitive
☑ Exclude HTTP headers
☐ Only in HTTP headers
☑ Content type: text/plain, application/json   ☑ Negative match
☑ Status code: 200,302   ☐ Negative match
☐ URL Extension: ☐ Negative match

Redirections

You can define how your profile handles redirections.

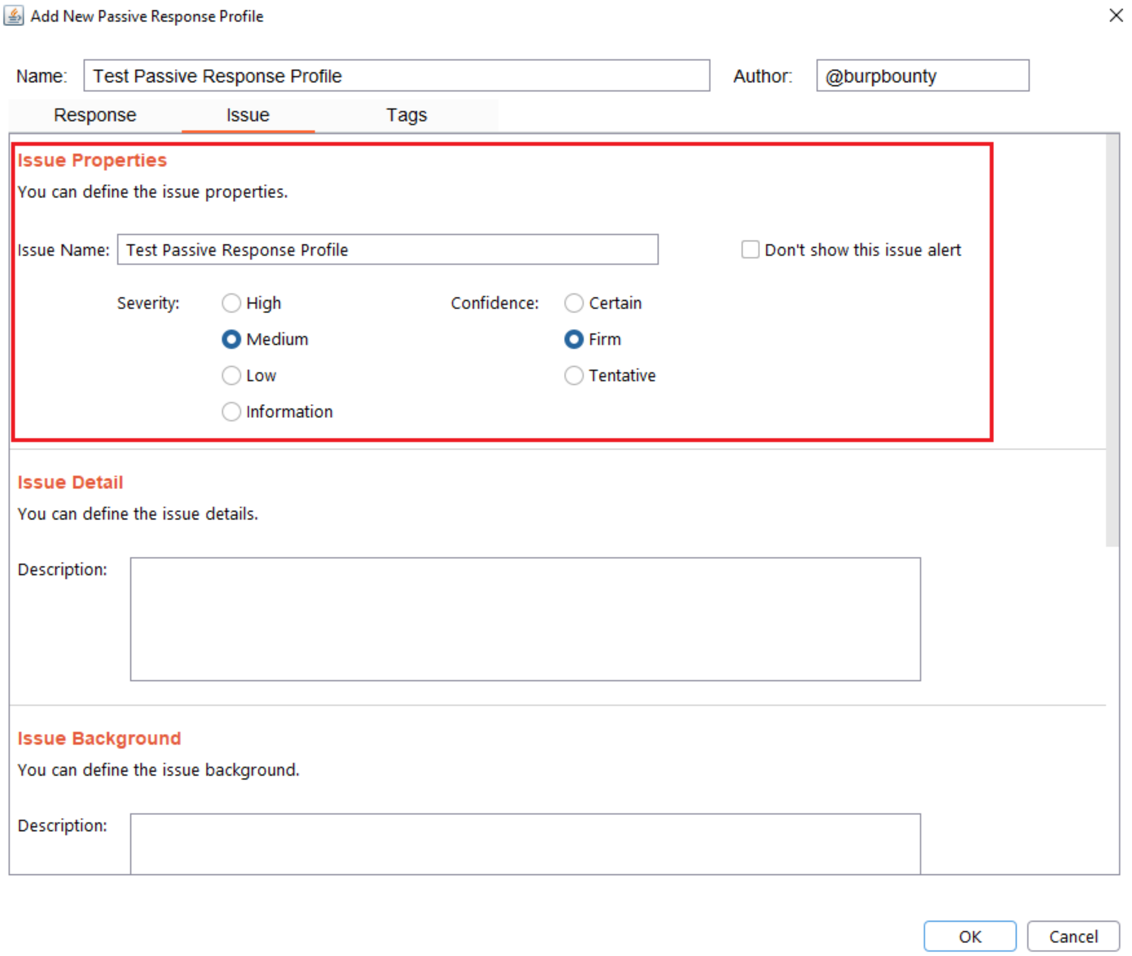
Follow redirections: ○ Never ● On-site only ○ In-scope only ○ Always

Max redirections: 3

Step 7 (Required): It specifies the name that will appear in the alert and the criticality of that alert.

It's necessary for the issue to appear, give it a "Issue Name" and complete the two fields, both the "severity" and the "confidence". The issue descriptions are optional.

If you check the option "Don't show this issue alert" the alert will not be shown in the dashboard, it will only be used for the Smart Scan.



Add New Passive Response Profile

Name: Test Passive Response Profile

Author: @burpbounty

Issue Properties

You can define the issue properties.

Issue Name: Test Passive Response Profile

□ Don't show this issue alert

Severity: ○ High ● Medium ○ Low ○ Information

Confidence: ○ Certain ● Firm ○ Tentative

Issue Detail

You can define the issue details.

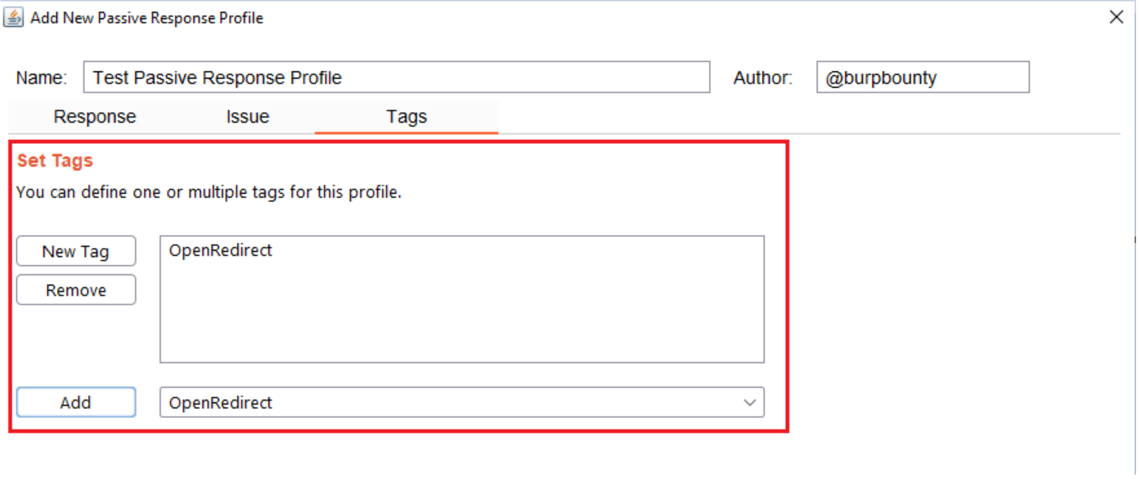
Description:

Issue Background

You can define the issue background.

Description:

Step 8 (Optional): A tag is created and assigned to the profile. This is useful for better organization of profiles.



Add New Passive Response Profile

Name: Test Passive Response Profile

Author: @burpbounty

Set Tags

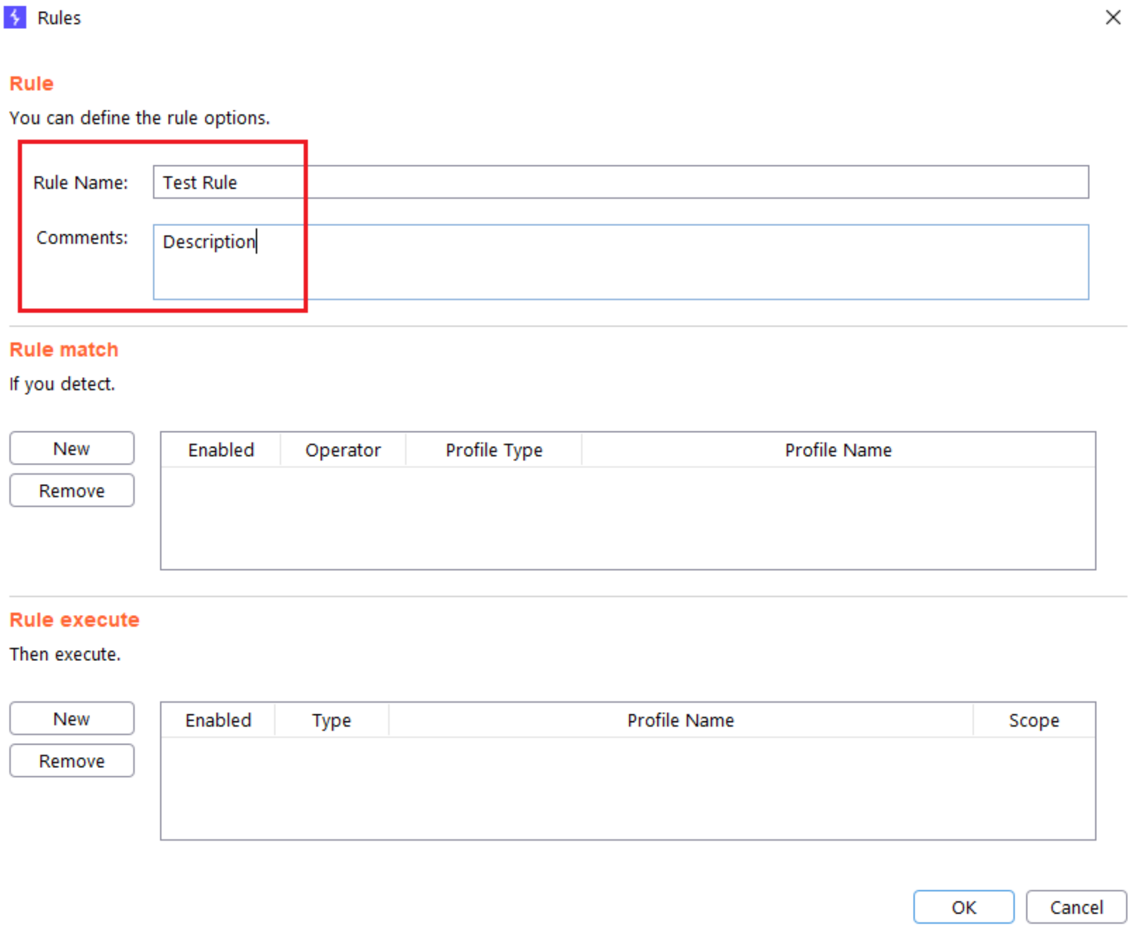
You can define one or multiple tags for this profile.

OpenRedirect

OpenRedirect

5. Rules

Step 1 (Required): The name of the rule is specified. The Comments field is optional.



Rules

Rule

You can define the rule options.

Rule Name: Test Rule

Comments: Description

Rule match

If you detect.

Enabled	Operator	Profile Type	Profile Name

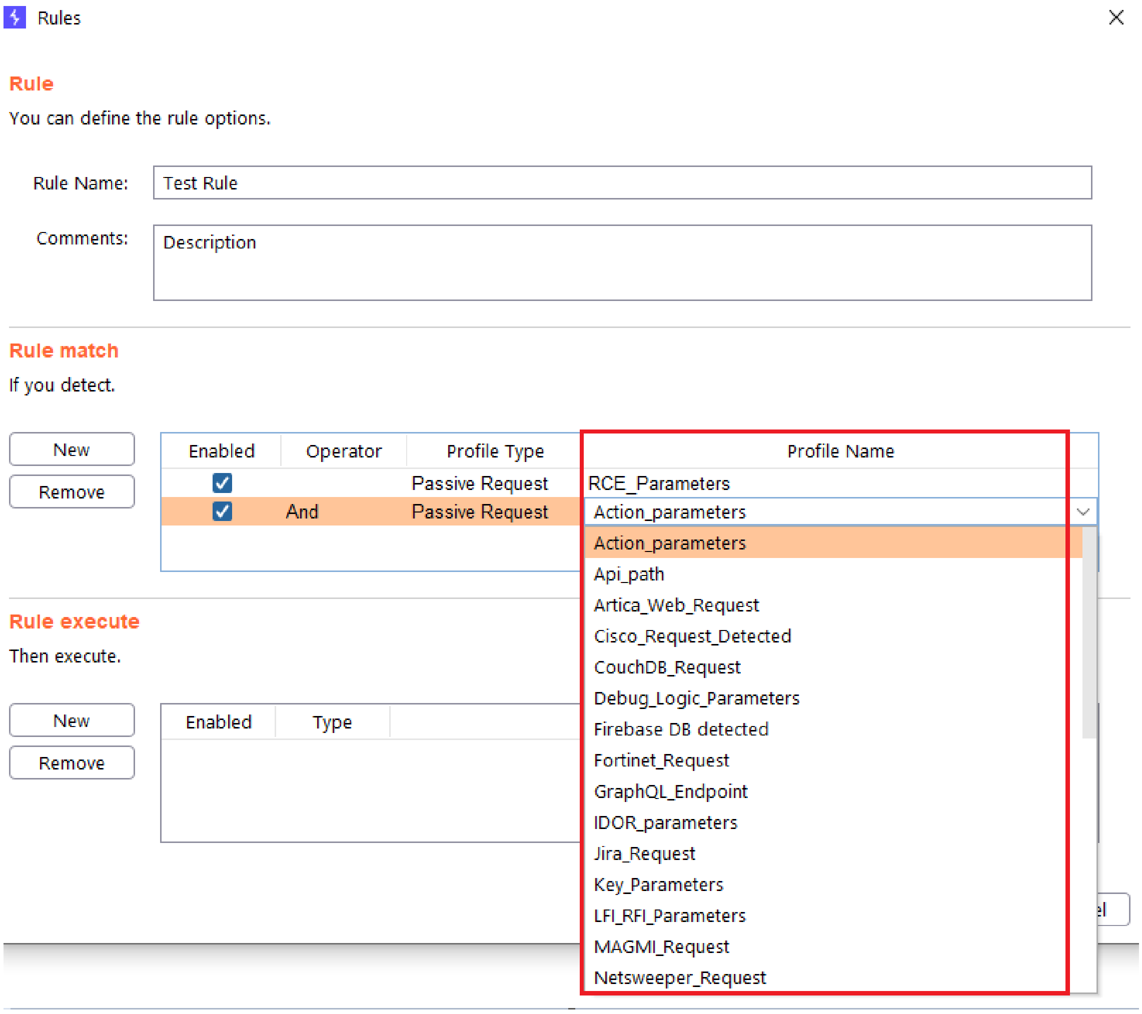
Rule execute

Then execute.

Enabled	Type	Profile Name	Scope

Step 2 (Required): You specify the passive profile(s) you want to be detected before launching the attacks.

- **Enabled**: Here you can enable or disable the profile in the rule.
- **Operator**: You can choose between "And" or "Or" logical operator.
- **Profile type**: You can choose between "Passive Request" and "Passive Response" profiles type.
- **Profile Name**: You can choose the passive profile that you want to be detected before launching the attacks.



Rule

You can define the rule options.

Rule Name: Test Rule

Comments: Description

Rule match

If you detect.

Enabled	Operator	Profile Type	Profile Name
☑		Passive Request	RCE_Parameters
☑	And	Passive Request	Action_parameters

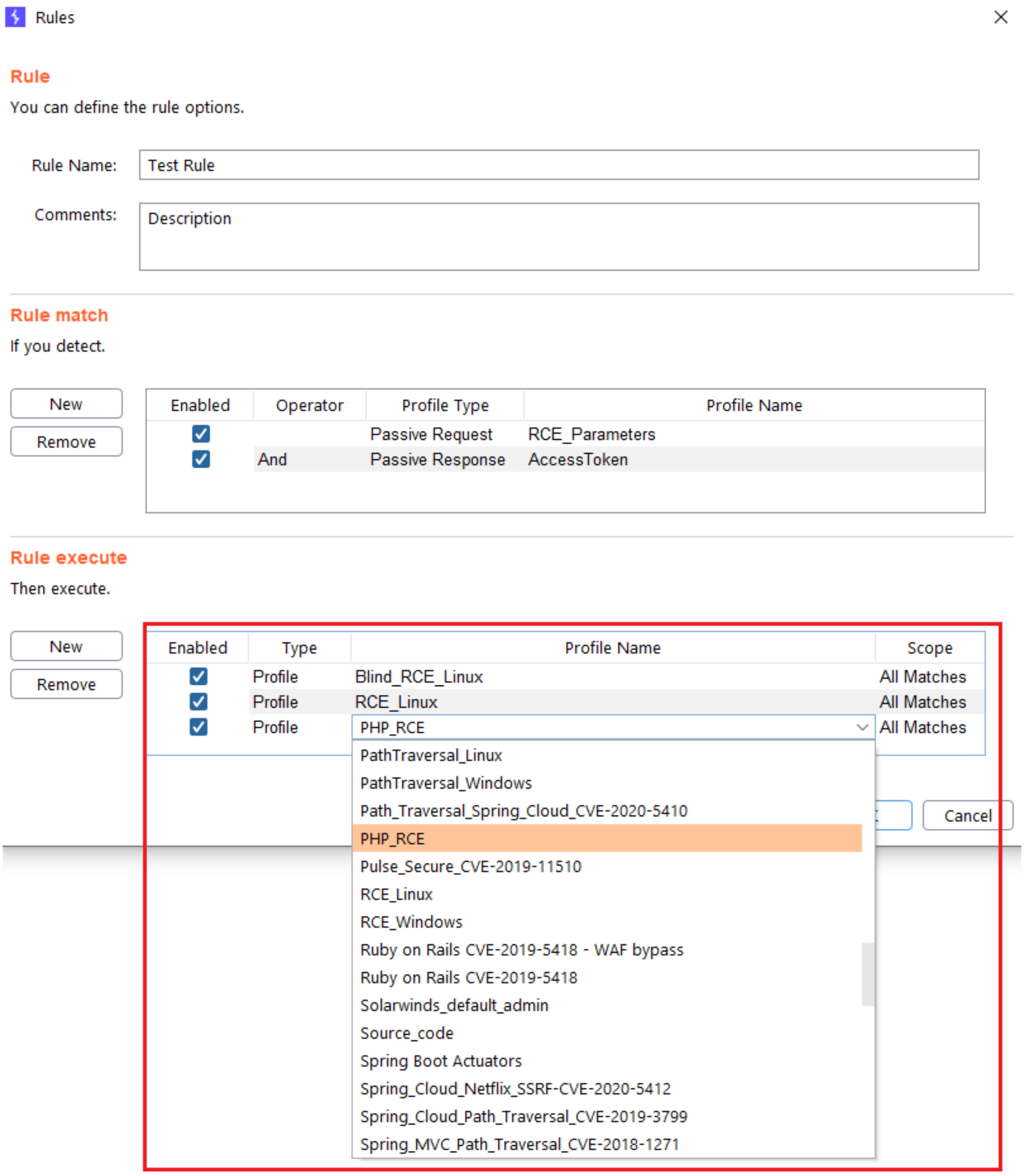
Rule execute

Then execute.

Enabled	Type

Step 5 (Required): You specify the active profile(s) that you want to be launched against the domain that has generated the passive alerts.

In "Type" column you can choose whether you want a profile to be launched or all the profiles that contain a Tag.



Rule

You can define the rule options.

Rule Name: Test Rule

Comments: Description

Rule match

If you detect.

Enabled	Operator	Profile Type	Profile Name
☑		Passive Request	RCE_Parameters
☑	And	Passive Response	AccessToken

Rule execute

Then execute.

Enabled	Type	Profile Name	Scope
☑	Profile	Blind_RCE_Linux	All Matches
☑	Profile	RCE_Linux	All Matches
☑	Profile	PHP_RCE	All Matches

PathTraversal_Linux
PathTraversal_Windows
Path_Traversal_Spring_Cloud_CVE-2020-5410
PHP_RCE
Pulse_Secure_CVE-2019-11510
RCE_Linux
RCE_Windows
Ruby on Rails CVE-2019-5418 - WAF bypass
Ruby on Rails CVE-2019-5418
Solarwinds_default_admin
Source_code
Spring Boot Actuators
Spring_Cloud_Netflix_SSRF-CVE-2020-5412
Spring_Cloud_Path_Traversal_CVE-2019-3799
Spring_MVC_Path_Traversal_CVE-2018-1271

At the "Scope" columns you can specify if you want that the profile to be launched in all the detections, or only once per domain.

6. More Documentation resources

For now, there are more resources on how the Burp Bounty Pro extension works. In this documentation you will mainly find how version 1.6 works, but the creation of profiles and rules is the same in 1.6 as in 2. In version 2 the use has been improved making it easier, and the power, increasing the functionalities in the profiles.

You can find more documentation in the URLs:

- https://burpbounty.net/burp-bounty-ekoparty-2020/
- https://vimeo.com/493308580
- https://burpbounty.net/faq/

Or on our YouTube channel:

- https://www.youtube.com/channel/UCSq4R2o9_nGIMHWZ4H98GkQ/videos