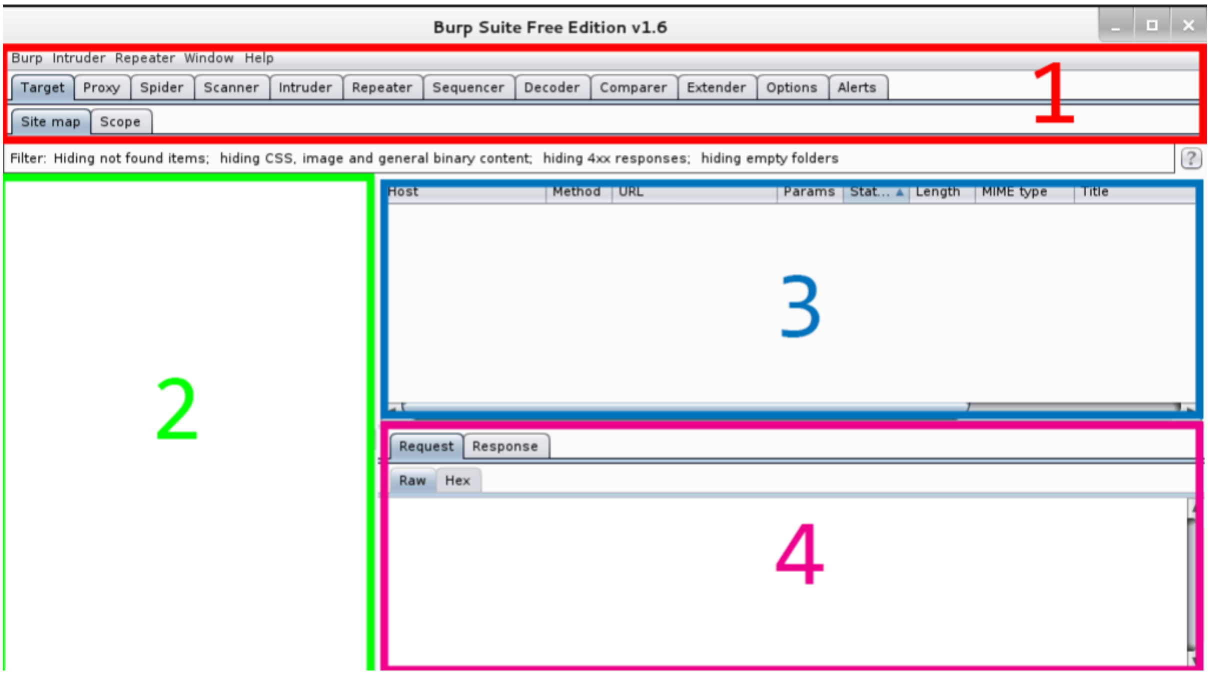
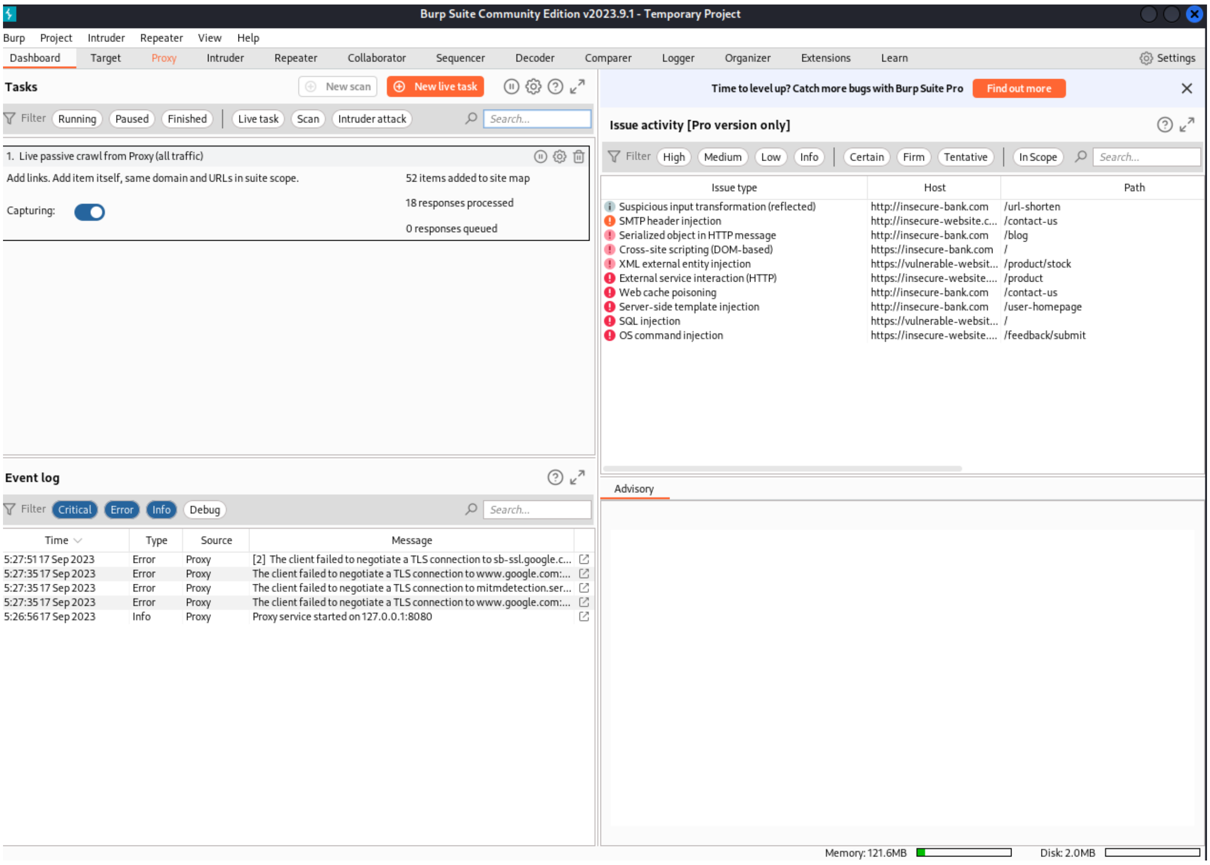
SHIVANSHU TIWARI 21BDS0191 ASSIGNMENT-4

Aim- We have to prepare a document about usage and exploration of various features of burp suite tool.

Burp suite community edition- Burp Suite is a popular cybersecurity tool used for web application security testing and vulnerability assessment. It provides a wide range of features and capabilities to help security professionals identify and mitigate vulnerabilities in web applications.


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Host Method URL Params Stat... Length MIME type Title
Request Response
Raw Hex
1
2
3
4


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Search...
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Filter High Medium Low Info Certain Firm Tentative In Scope
Search...
Event log
Filter Critical Error Info Debug
Search...
Advisory
Memory: 121.6MB
Disk: 2.0MB

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

52 items added to site map

18 responses processed

0 responses queued

Issue activity [Pro version only]

Issue type	Host	Path
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.c...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/product/stock
External service interaction (HTTP)	https://insecure-website....	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepage
SQL injection	https://vulnerable-websit...	/
OS command injection	https://insecure-website....	/feedback/submit

Time	Type	Source	Message
5:27:51 17 Sep 2023	Error	Proxy	[2] The client failed to negotiate a TLS connection to sb-ssl.google.c...
5:27:35 17 Sep 2023	Error	Proxy	The client failed to negotiate a TLS connection to www.google.com:...
5:27:35 17 Sep 2023	Error	Proxy	The client failed to negotiate a TLS connection to mitmdetection.ser...
5:27:35 17 Sep 2023	Error	Proxy	The client failed to negotiate a TLS connection to www.google.com:...
5:26:56 17 Sep 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080

Here we can see the burp suite community edition dashboard interface-

Proxy: Burp Suite acts as a proxy server that intercepts and logs HTTP and HTTPS traffic between a web browser and a web server. This allows users to inspect and modify requests and responses, making it a valuable tool for manual testing and analysis.

Scanner: Burp includes an automated scanner that can identify various vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and more. It can help automate the vulnerability assessment process.

Spider: The spider tool can crawl a website to discover and map out its content and functionality. This is useful for identifying hidden pages and potential attack surfaces.

Intruder: Burp Intruder is a powerful tool for performing automated attacks on web applications, such as brute-force attacks, fuzzing, and payload manipulation. It helps identify vulnerabilities that may not be apparent through manual testing.

Repeater: This tool allows security professionals to manually modify and replay HTTP requests to observe how a web application responds. It's helpful for identifying vulnerabilities and testing the impact of different inputs.

Sequencer: Burp Sequencer analyses the quality of randomness in tokens and session identifiers, which can help identify potential session management vulnerabilities.

Decoder: It provides various encoding and decoding tools for working with different data formats, such as URL encoding, Base64, and more.

Comparer: Burp Suite's comparer helps identify differences between two HTTP responses or requests, which can be useful for detecting potential security issues.

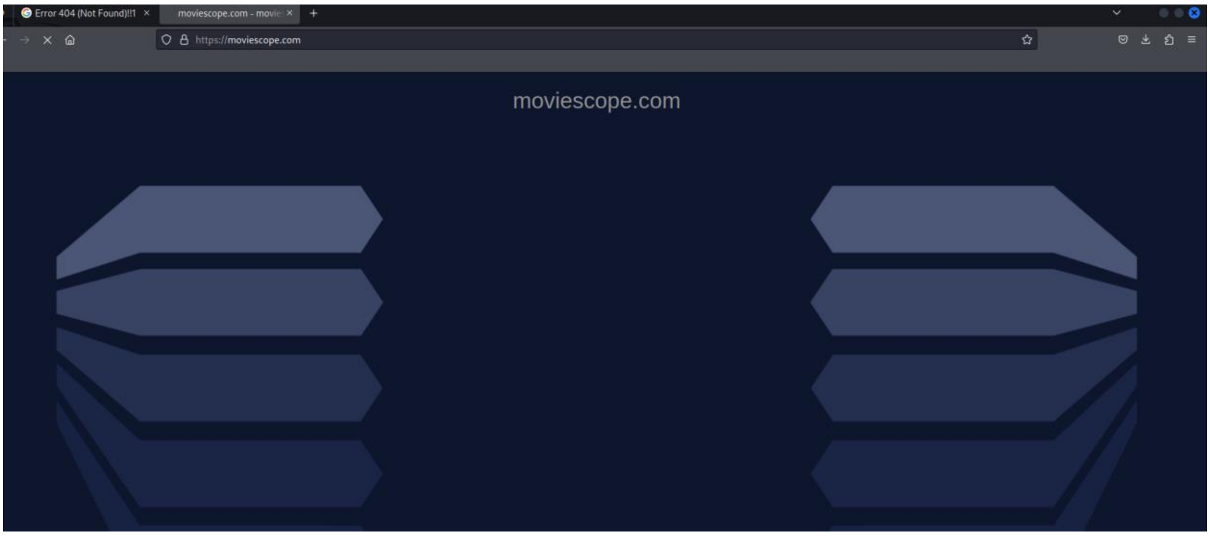
Extensibility: Burp Suite can be extended using its extensive API. Security professionals and developers can create custom extensions, plugins, and scripts to enhance its functionality and integrate it with other tools and systems.

Target Scope: Users can define the scope of their testing by specifying which parts of a website or web application should be included or excluded from the scan or testing.

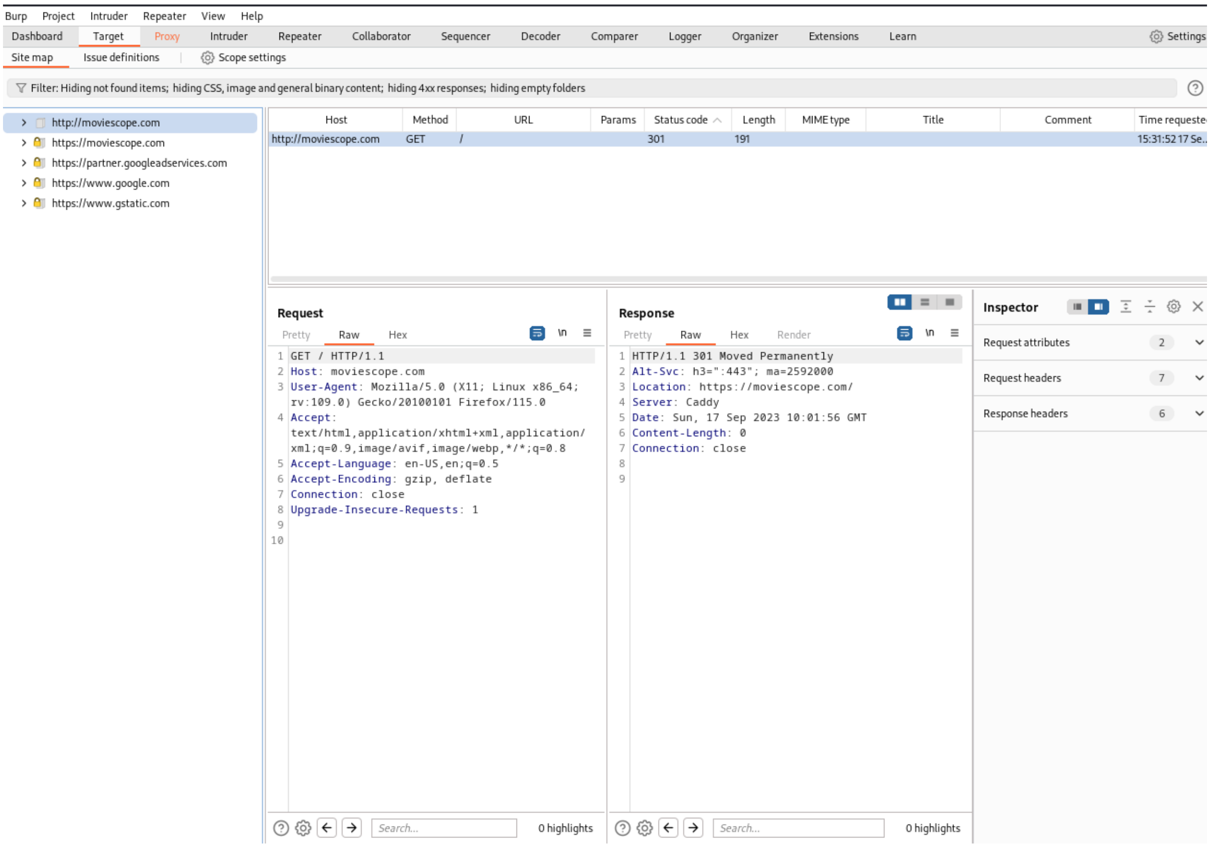
Collaborator: Burp Collaborator helps detect out-of-band vulnerabilities by providing a unique domain that can be used to trigger interactions with the target application, revealing potential security weaknesses.

Session Handling: Burp Suite allows you to manage and manipulate sessions, cookies, and authentication tokens during testing, enabling a more comprehensive assessment of web application security.

Reporting: It offers customizable reporting capabilities to generate detailed reports of identified vulnerabilities and testing results.



Here we can see that www.moviescope.com website is opened in our web browser



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

- http://moviescope.com
- https://moviescope.com
- https://partner.googleadservices.com
- https://www.google.com
- https://www.gstatic.com

Host	Method	URL	Params	Status code	Length	MIME type	Title	Comment	Time requeste
http://moviescope.com	GET	/		301	191				15:31:52 17 Se..

Request

```
GET / HTTP/1.1
Host: moviescope.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/
xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1


```

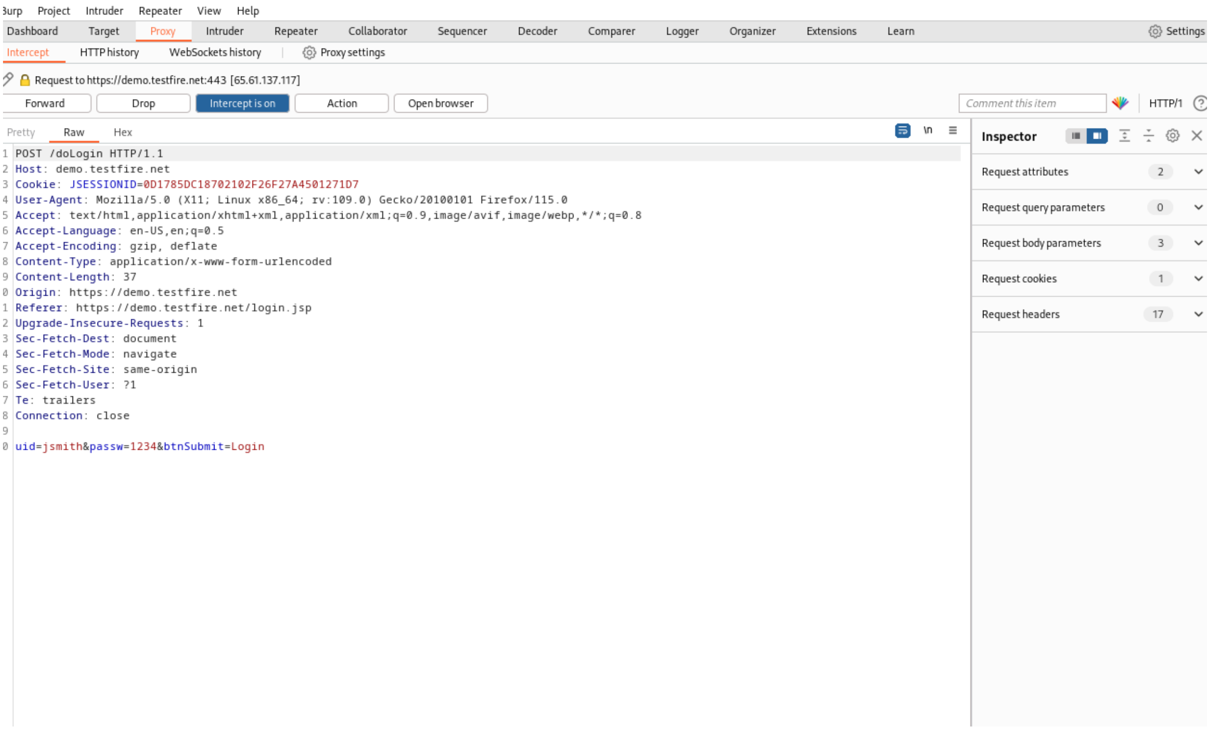
Response

```
HTTP/1.1 301 Moved Permanently
Alt-Svc: h3=":443"; ma=2592000
Location: https://moviescope.com/
Server: Caddy
Date: Sun, 17 Sep 2023 10:01:56 GMT
Content-Length: 0
Connection: close


```

Inspector	
Request attributes	2
Request headers	7
Response headers	6

Here we can see our website our web browser and burp suite are linked with manual proxy 127.0.0.1 and port 8080   we can see the websites incoming requests get and post, in this way we can intercept the following websites and perform man in the middle attack.



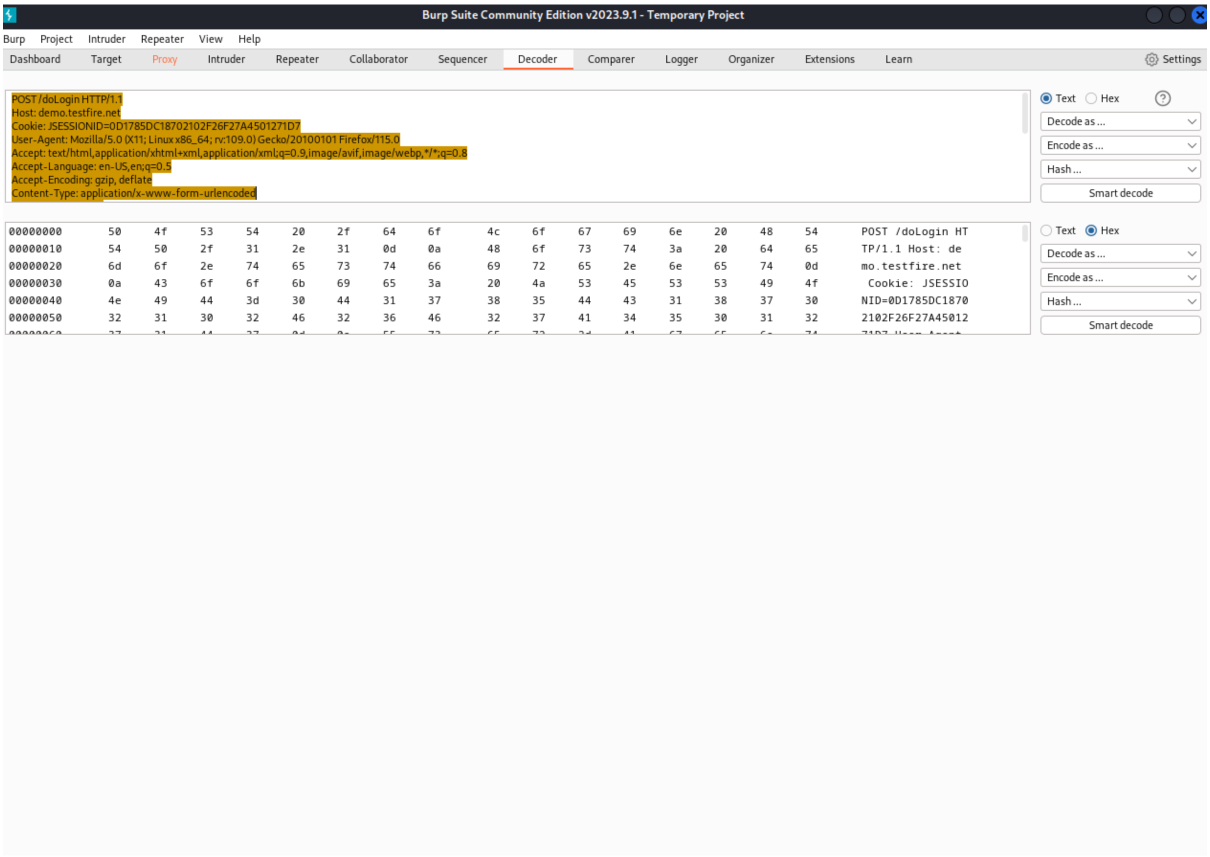
Request to https://demo.testfire.net:443 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=0D1785DC18702102F26F27A4501271D7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: https://demo.testfire.net
Referer: https://demo.testfire.net/login.jsp
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

uid=jsmith&passw=1234&btnSubmit=Login
```

Here we can see that when we login in our website, burp suite has captured the login details ,it has also captured cookie id, j session id,

By poisoning them we can perform session hijacking attack as well as man in the middle attack.

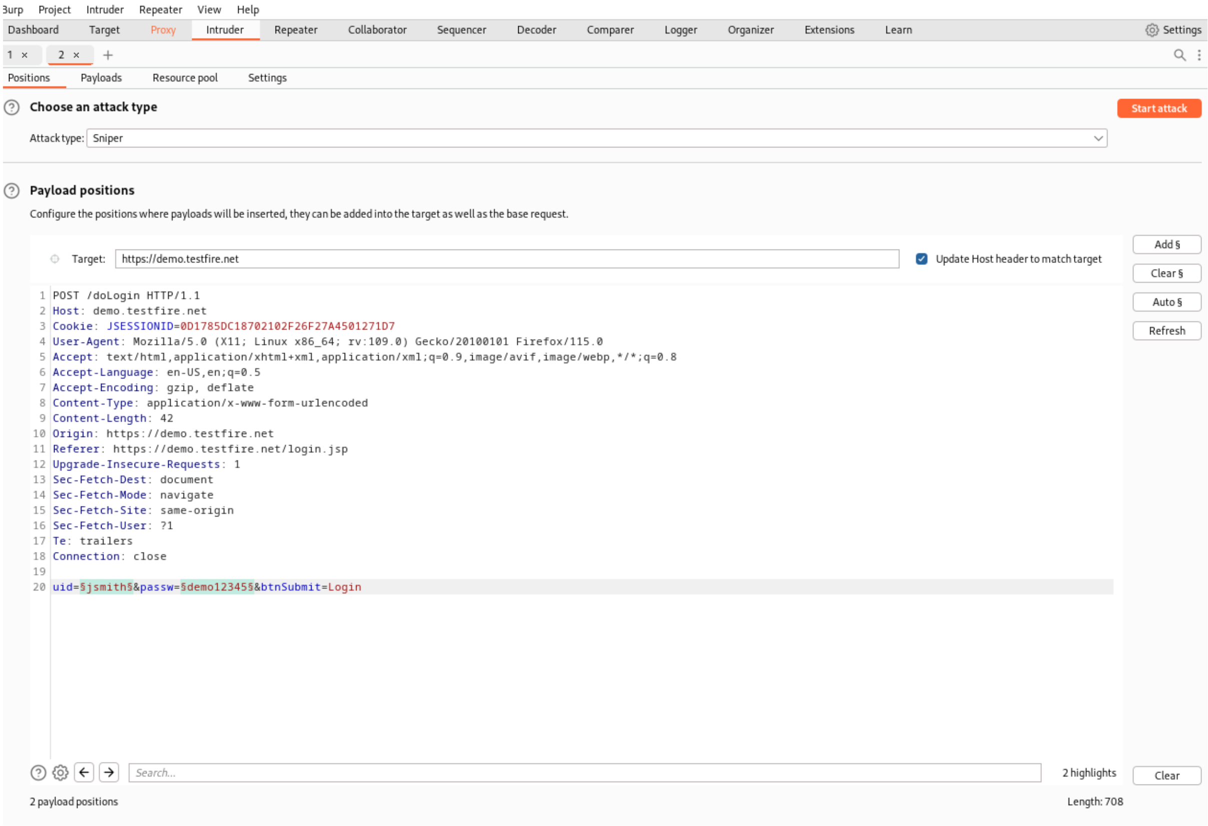


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
○ Text ● Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=0D1785DC18702102F26F27A4501271D7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
```

```
00000000   50 4f 53 54 20 2f 64 6f   4c 6f 67 69 6e 20 48 54   POST /doLogin HT
00000010   54 50 2f 31 2e 31 0d 0a   48 6f 73 74 3a 20 64 65   TP/1.1 Host: de
00000020   6d 6f 2e 74 65 73 74 66   69 72 65 2e 6e 65 74 0d   mo.testfire.net
00000030   0a 43 6f 6f 6b 69 65 3a   20 4a 53 45 53 53 49 4f    Cookie: JSESSIO
00000040   4e 49 44 3d 30 44 31 37   38 35 44 43 31 38 37 30   NID=0D1785DC1870
00000050   32 31 30 32 46 32 36 46   32 37 41 34 35 30 31 32   2102F26F27A45012
```

We can see decoder section which helps us to decode our back end code, we can decode it in many forms and in hex format as well.



Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 × 2 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Search...
Clear

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://demo.testfire.net

☑ Update Host header to match target

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=0D1785DC18702102F26F27A4501271D7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: https://demo.testfire.net
Referer: https://demo.testfire.net/login.jsp
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

uid=§jsmith§&passw=§demo12345§&btnSubmit=Login
```

2 highlights

2 payload positions

Length: 708

By sending our captured data to intruder we can perform brute force attack, we have four types of options as attack in this:

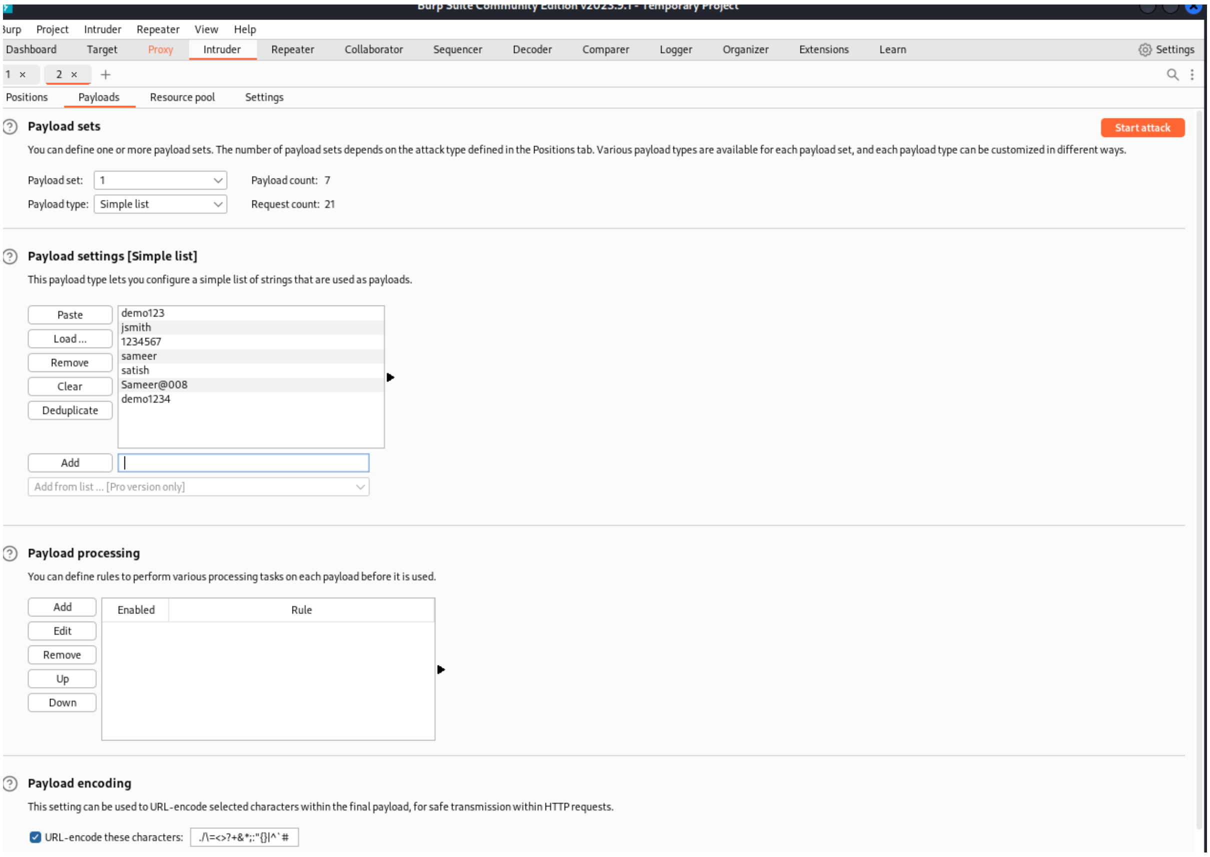
1-Sniper attack-it is used when there is generally one payloads.

2-battering ram-it used single set of payloads which iterates all the payloads while interchanging the payloads.

3-Pitch forks-this type of attack use multiple sets of payloads

Attacker iterate through each set of payloads simultaneously.

4-Cluster bomb-This attack iterates through a different payload set for each defined position. Payloads are placed from each set in turn, so that all payload combinations are tested.


Burp Suite Community Edition v2023.5.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Positions Payloads Resource pool Settings
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down
Enabled
Rule

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 7

Payload type: Simple list

Request count: 21

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
demo123
jsmith
1234567
sameer
satish
Sameer@008
demo1234
```

Payload processing

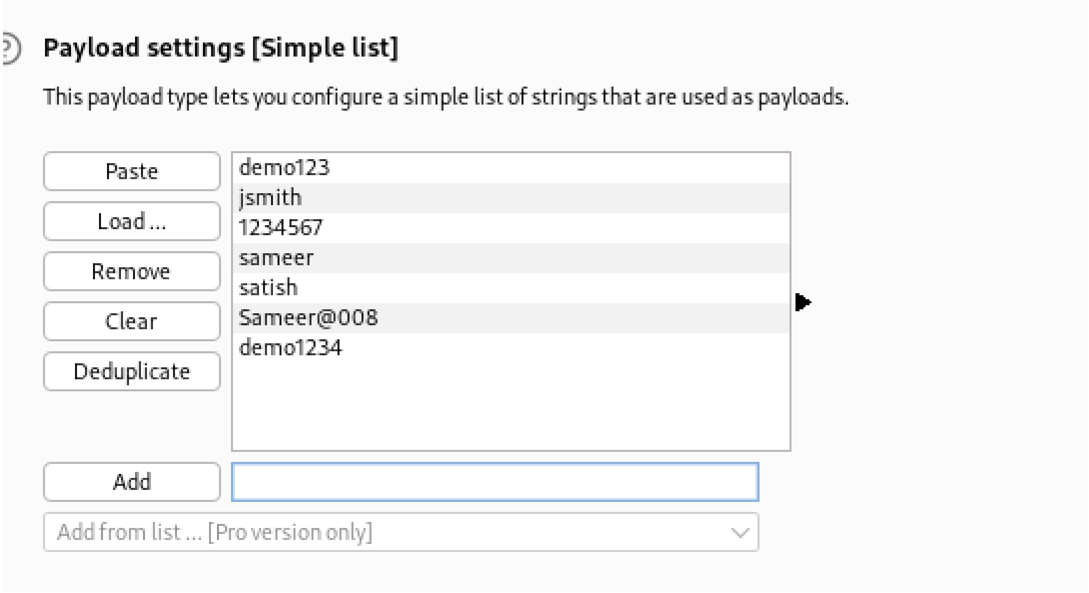
You can define rules to perform various processing tasks on each payload before it is used.

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

In this section we can set payloads and add customize dictionary for password attacks

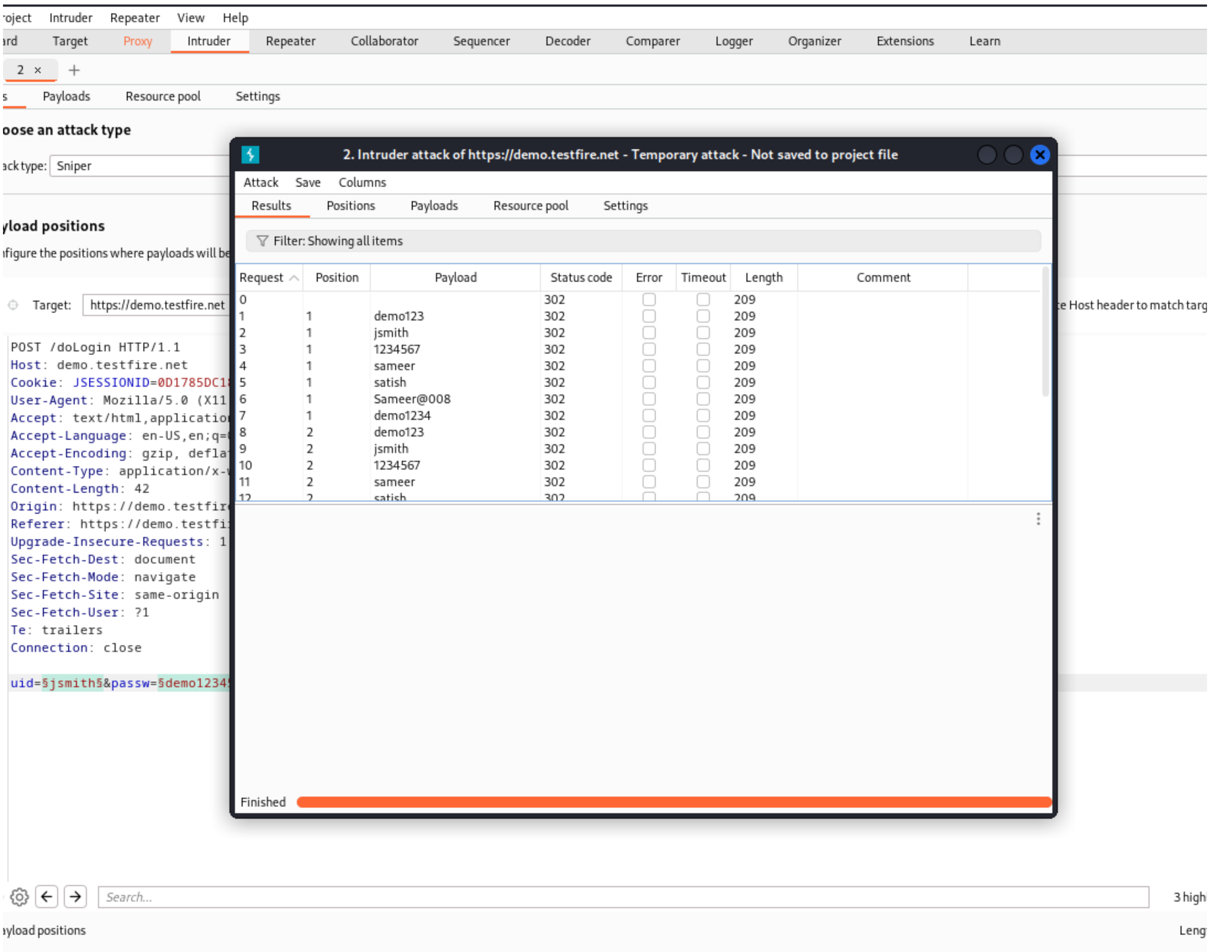


Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
demo123
jsmith
1234567
sameer
satish
Sameer@008
demo1234
```

Here we can see I added some wordlists to my payload in burp suite manually:


roject Intruder Repeater View Help
ard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
2 × +
s Payloads Resource pool Settings
oose an attack type
ack type: Sniper
yload positions
figure the positions where payloads will be
e Host header to match targ
2. Intruder attack of https://demo.testfire.net - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Finished
Search...
3 high
yload positions
Leng

Target: https://demo.testfire.net

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=0D1785DC1
User-Agent: Mozilla/5.0 (X11
Accept: text/html,applicatio
Accept-Language: en-US,en;q=
Accept-Encoding: gzip, defla
Content-Type: application/x-
Content-Length: 42
Origin: https://demo.testfir
Referer: https://demo.testfi
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

uid=§jsmith§&passw=§demo1234
```

Request	Position	Payload	Status code	Error	Timeout	Length	Comment
0			302	☐	☐	209	
1	1	demo123	302	☐	☐	209	
2	1	jsmith	302	☐	☐	209	
3	1	1234567	302	☐	☐	209	
4	1	sameer	302	☐	☐	209	
5	1	satish	302	☐	☐	209	
6	1	Sameer@008	302	☐	☐	209	
7	1	demo1234	302	☐	☐	209	
8	2	demo123	302	☐	☐	209	
9	2	jsmith	302	☐	☐	209	
10	2	1234567	302	☐	☐	209	
11	2	sameer	302	☐	☐	209	
12	2	satish	302	☐	☐	209	

As we can see our brute force attack is going on with the help of burp suite tool.

Spoofing your IP address using Burp Proxy match and replace:

Burp suite allows you to configure match and replace rules that automatically modify your requests and responses while you explore the target application as normal using Burp's browser. This enables you to add, remove, or modify headers in requests or responses, for example.

There are a number of uses for this, including potentially spoofing your IP address. In some cases, this may allow you to trick a server into believing that you belong to its local network, which could enable you to communicate with internal infrastructure that is otherwise inaccessible.

Burp Suite: Good Tool For Vulnerability Scanning:

It is a very good tool that you we can use to carry out vulnerability scanning on your web applications or websites.

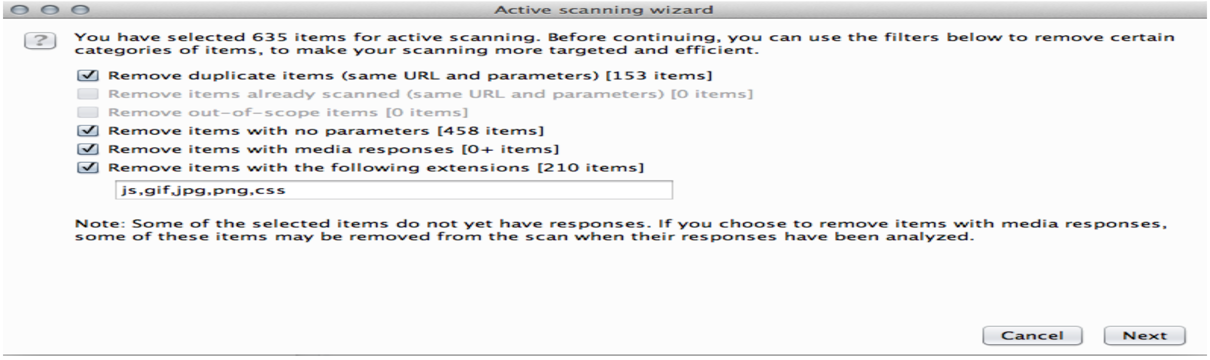
This is an automation process that helps the pen-tester to finish a testing task because sometimes the pen-tester may not have enough time to test all parameters of a web request. This will invariably make the pen-tester to be effective and efficient in achieving his target after going through a rigorous process of penetration testing.

It has the capacity to analyse every detail during the scanning process and it will notify you when a vulnerability has been discover.

Automated Scanning:

I like to do the passive scan first because it doesn't send any traffic to the target server. Alternatively you can configure Burp Suite to passively analyse requests and responses automatically in the "Live scanning" sub-tab. You can also do this for Active Scanning but I do not recommend it.

When doing an active scan I like to use the following settings.



Active scanning wizard

You have selected 635 items for active scanning. Before continuing, you can use the filters below to remove certain categories of items, to make your scanning more targeted and efficient.

- ☑ Remove duplicate items (same URL and parameters) [153 items]
- □ Remove items already scanned (same URL and parameters) [0 items]
- □ Remove out-of-scope items [0 items]
- ☑ Remove items with no parameters [458 items]
- ☑ Remove items with media responses [0+ items]
- ☑ Remove items with the following extensions [210 items]

js,gif,jpg,png,css

Note: Some of the selected items do not yet have responses. If you choose to remove items with media responses, some of these items may be removed from the scan when their responses have been analyzed.

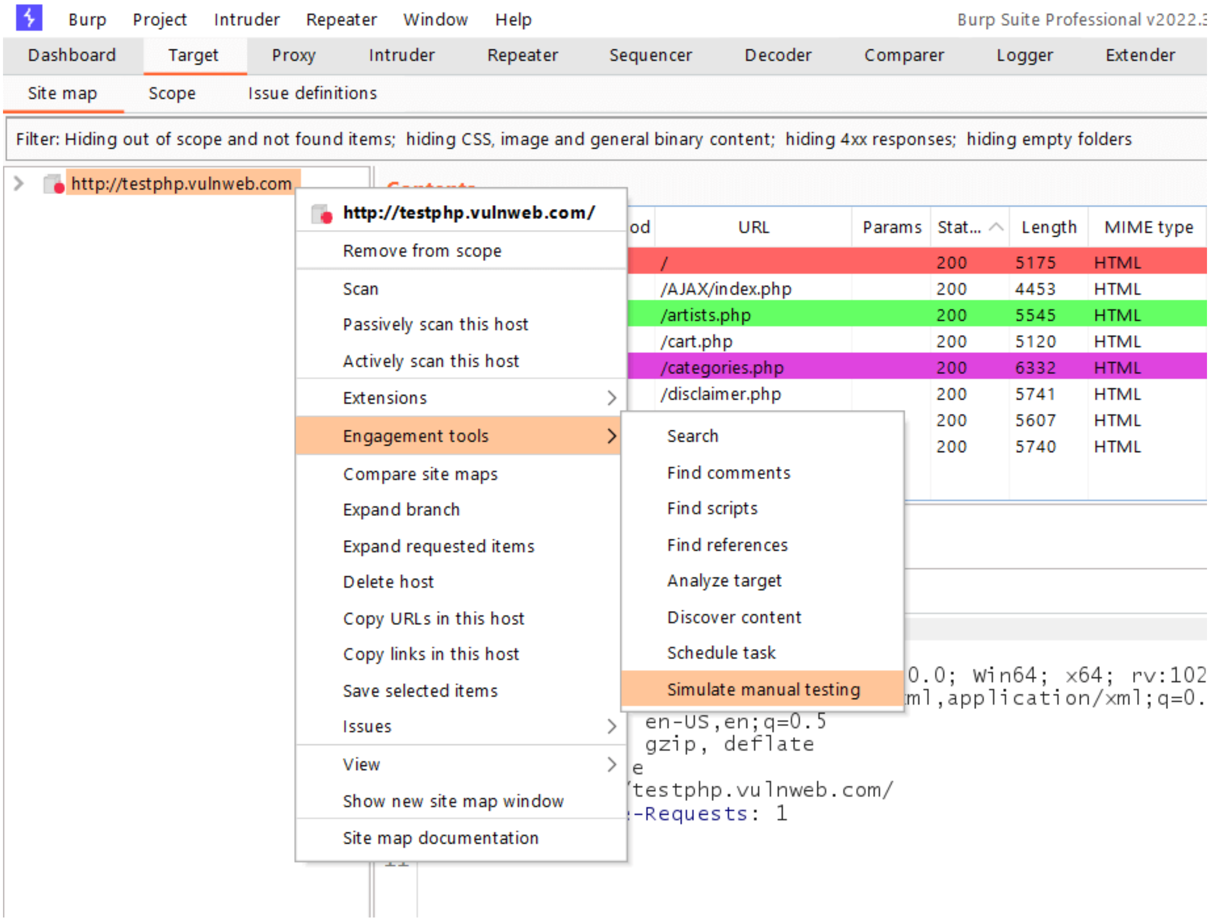
Spidering a Website:

A web crawler is a bot program that systematically browses the pages of a website for the purpose of indexing. Precisely a web crawler maps the structure of a website by browsing all its inner pages. The crawler is also referred to as a spider or automatic indexer.

Burp Suite has got its own spider called the burp spider. The burp spider is a program that crawls into all the pages of a target specified in the scope. Before starting the burp spider, the Burp suite has to be configured to intercept the HTTP traffic.

Simulate Manual Testing:

To simulate manual penetration testing traffic, the function sends common test payloads to random URLs and parameters at irregular intervals.
Its sole purpose is to allow you to take a break from testing while remaining active in the server's logs. Only the items from the site map that you selected will be requested.



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

od	URL	Params	Stat...	Length	MIME type
	/		200	5175	HTML
	/AJAX/index.php		200	4453	HTML
	/artists.php		200	5545	HTML
	/cart.php		200	5120	HTML
	/categories.php		200	6332	HTML
	/disclaimer.php		200	5741	HTML
			200	5607	HTML
			200	5740	HTML

```
0.0; Win64; x64; rv:102
ml,application/xml;q=0.
en-US,en;q=0.5
gzip, deflate
e
/testphp.vulnweb.com/
-Requests: 1
```

Conclusion: We noted the use of burp suite and explored different features of the tool