

AI FOR CYBER SECURITY

ASSIGNMENT-4

Name: Nikhil Sri Harsha

Reg.no: 21BCE8711

BURPSUITE

What is Burp Suite?

Burp Suite is a comprehensive set of cybersecurity tools designed for web application security testing and vulnerability assessment. It is developed by PortSwigger, a UK-based software company. Burp Suite is widely used by security professionals, penetration testers, and ethical hackers to identify and mitigate security vulnerabilities in web applications.

Why is Burp Suite used?

Burp Suite is used for several important purposes in the field of cybersecurity:

1. **Web Application Security Testing:** Burp Suite helps security professionals assess the security of web applications by identifying vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and more.
2. **Vulnerability Assessment:** It scans web applications to detect potential security weaknesses, misconfigurations, and other issues that could be exploited by attackers.
3. **Penetration Testing:** Ethical hackers and penetration testers use Burp Suite to simulate attacks on web applications, uncover vulnerabilities, and provide recommendations for remediation.
4. **Security Research:** Researchers use Burp Suite to analyse and study web application security, helping to improve the overall security of web applications.
5. **Web Application Development:** Developers can use Burp Suite to test their own applications during development to catch and fix security issues before they reach production.

Features of Burp Suite:

Burp Suite offers a wide range of features to support web application security testing:

1. **Proxy:** Allows intercepting and modifying HTTP/S requests and responses between the client and server, making it possible to analyse and manipulate web traffic.
2. **Scanner:** Automatically scans web applications for common vulnerabilities, such as SQL injection, XSS, and more, providing detailed reports.
3. **Intruder:** Facilitates automated and customizable attacks on web applications to discover vulnerabilities and weak points.
4. **Repeater:** Allows manual modification and resending of individual HTTP/S requests to observe how the application responds, aiding in vulnerability discovery and testing.
5. **Sequencer:** Analyses the randomness of tokens and session identifiers to assess the strength of session management and authentication mechanisms.
6. **Spider:** Crawls and maps the structure of a web application, helping testers understand its functionality and potential attack surfaces.
7. **Decoder:** Provides tools to decode and encode data in various formats, such as Base64 and

URL encoding.

8. Collaborator: Assists in detecting out-of-band vulnerabilities by creating unique payloads that trigger external interactions and reporting the results.

9. Extensibility: Burp Suite supports the development of custom extensions and plugins, allowing users to add additional functionality.

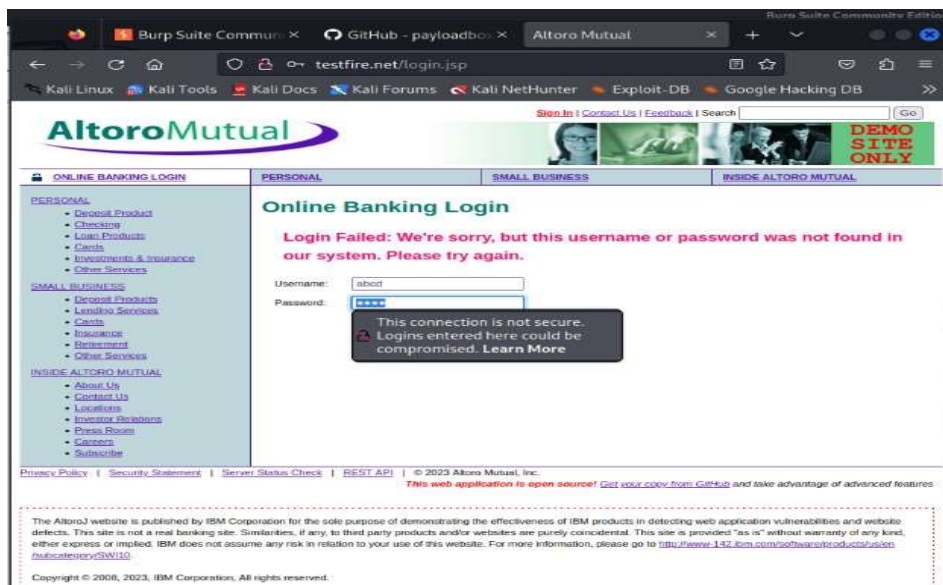
10. Reporting: Generates detailed reports with vulnerability findings and recommendations for remediation.

11. Target Scope Control: Allows users to define the scope of testing by specifying which parts of a web application should be included or excluded.

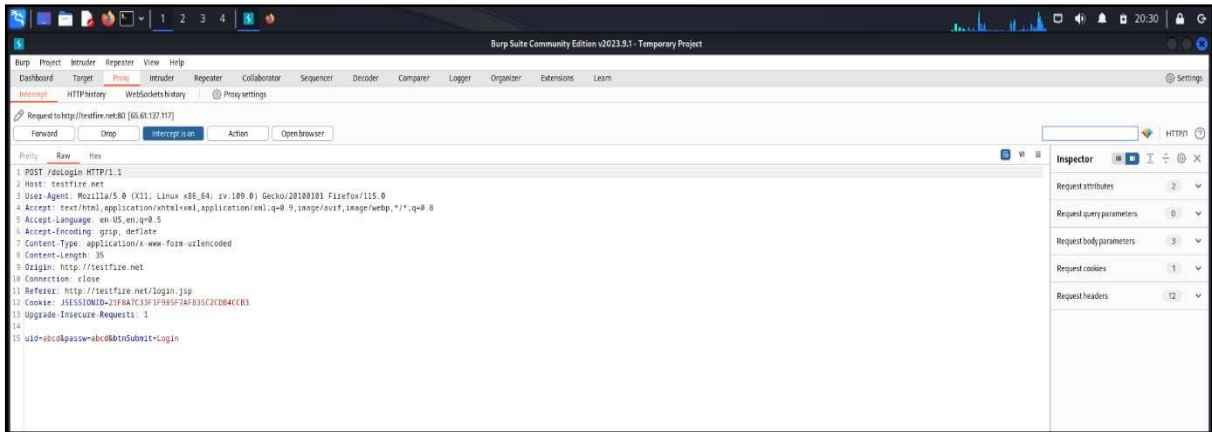
12. Session Handling: Manages and maintains user sessions to test authentication and authorization mechanisms thoroughly.

These features collectively make Burp Suite a powerful tool for identifying and mitigating web vulnerabilities of testfire.net website

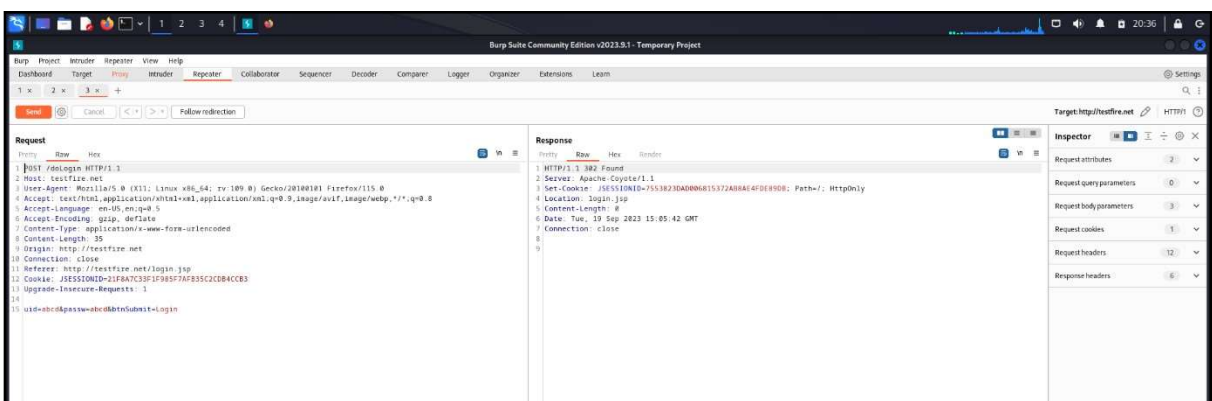
First, the website is opened and credentials are entered.



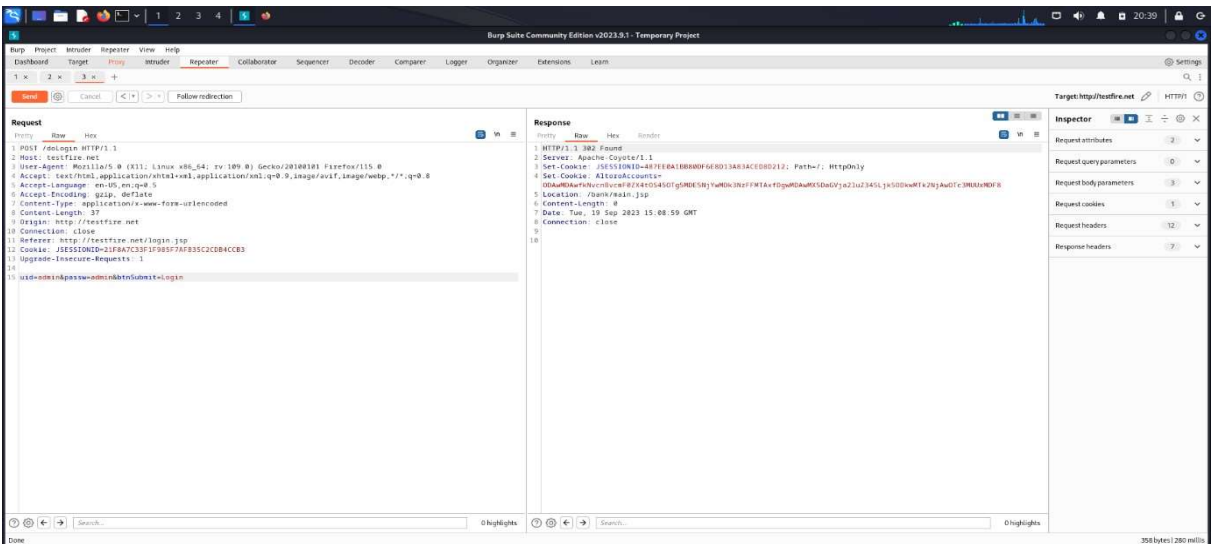
Next, the intercept in the proxy section of Burpsuite is turned on. After that, login button is clicked. After this, the below details are sent to repeater.



Here, as wrong credentials were entered, error is found.

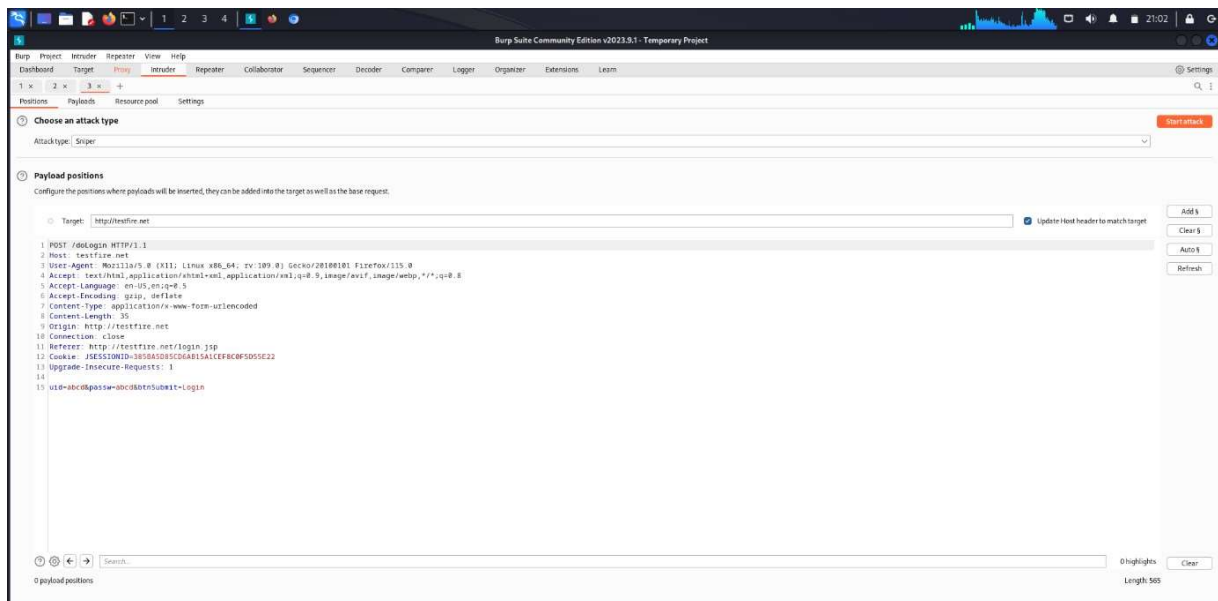


After entering the correct details, we got the source of the information below.

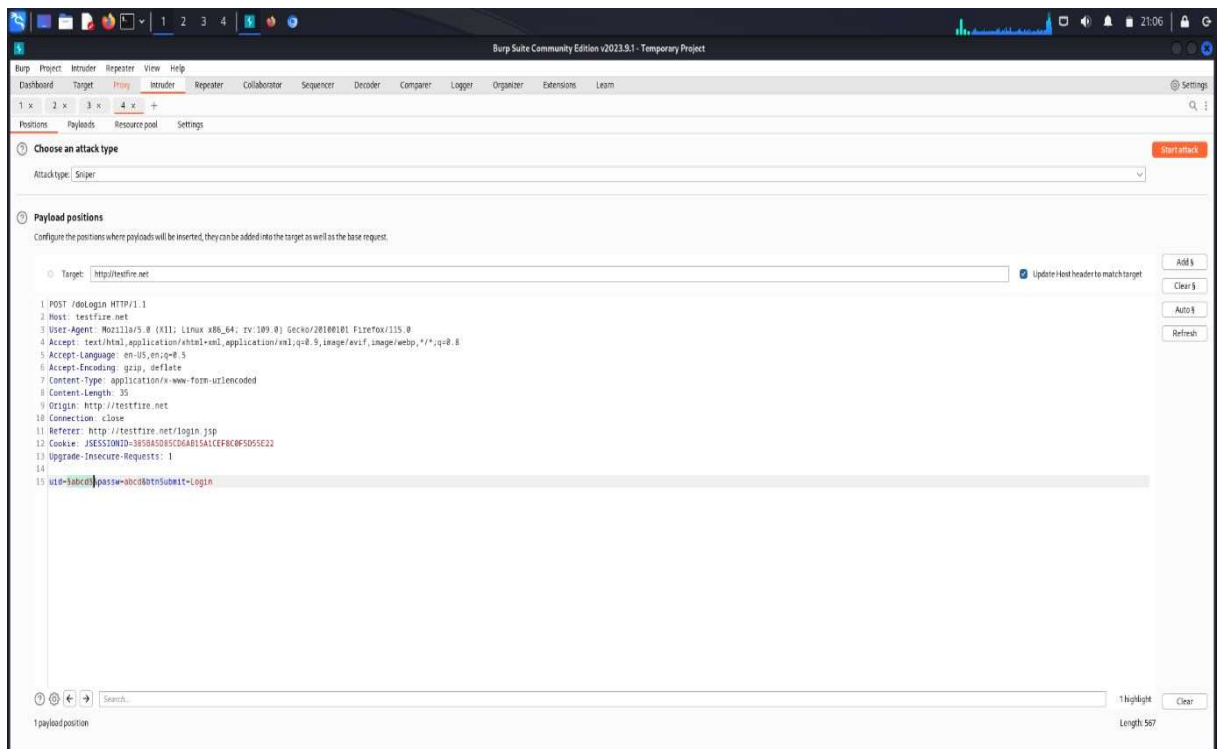


SQL INJECTION

SQL injection is a technique where a malicious code is injected in a website which leads to hacking of a web page and destroying of database of the website.

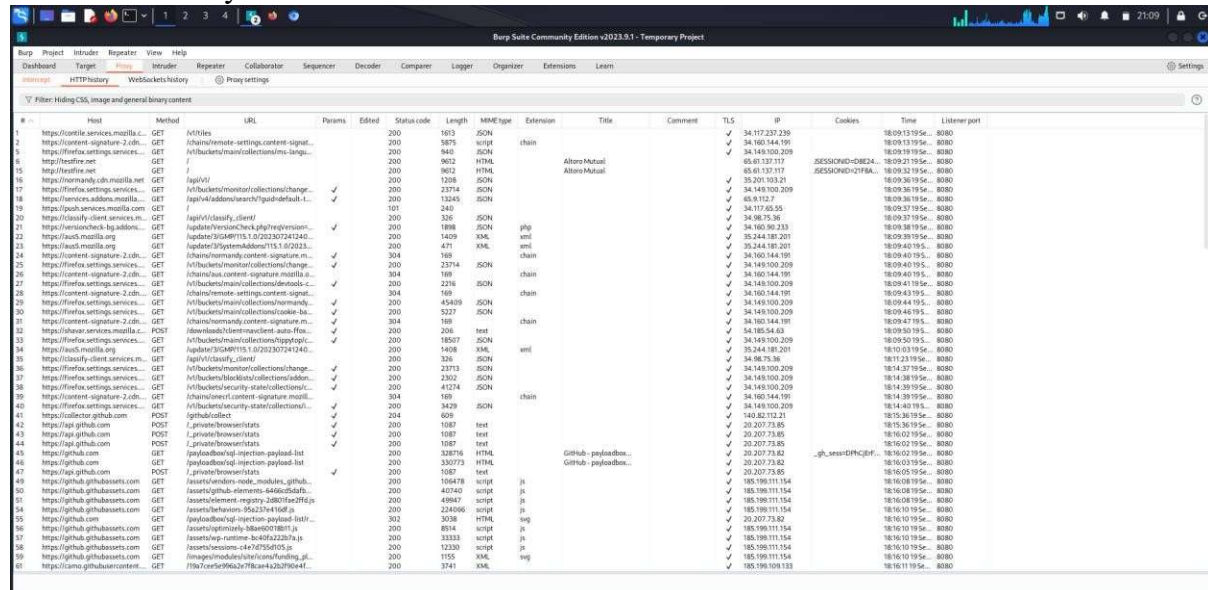


SQL injection attack is performed in the intruder tab. For this, the above code was used. The username is added as an element.



In the payloads section, paste the payload code which was copied from github. After this, click on start attack button.

This is the history of the websites searched.

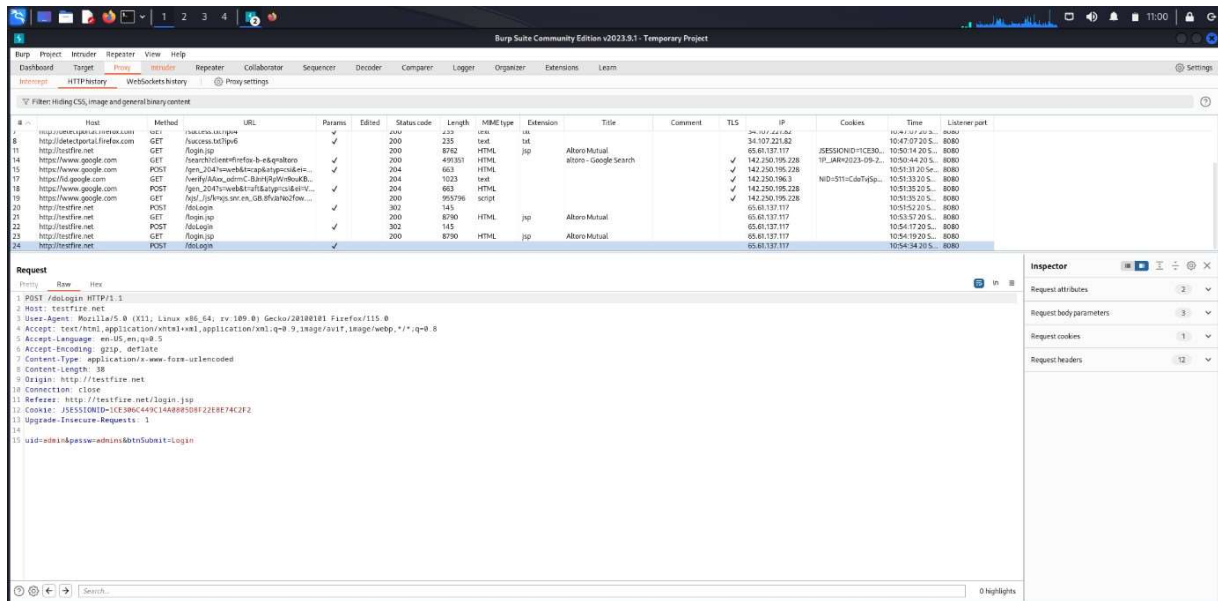


#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	https://content-signature-2.dh...	GET	/v1/beta			200	1913	JSON				✓	34.172.207.239		18:09:13 19 Se...	8080
2	https://content-signature-2.dh...	GET	/churn/metadata-settings/content-signat...			200	5875	script	chain			✓	34.160.144.191		18:09:13 19 Se...	8080
3	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/ms-lang...			200	940	JSON				✓	34.143.100.209		18:09:19 19 Se...	8080
4	https://ffox.settings.services.m...	GET	/			200	9652	HTML		Altare Mutual		✓	65.41.137.117	SESSIONID=0824...	18:09:21 19 Se...	8080
5	https://ffox.settings.services.m...	GET	/			200	9652	HTML		Altare Mutual		✓	65.41.137.117	SESSIONID=2F8A...	18:09:32 19 Se...	8080
6	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1208	JSON				✓	35.201.103.21		18:09:36 19 Se...	8080
7	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	23714	JSON				✓	34.143.100.209		18:09:36 19 Se...	8080
8	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	13243	JSON				✓	65.41.137.1		18:09:36 19 Se...	8080
9	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	101	245				✓	34.177.65.55		18:09:37 19 Se...	8080
10	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1888	JSON				✓	34.160.144.191		18:09:37 19 Se...	8080
11	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1409	KML	xml			✓	35.244.181.201		18:09:39 19 Se...	8080
12	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	471	KML	xml			✓	35.244.181.201		18:09:40 19 Se...	8080
13	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	169	KML	xml			✓	34.160.144.191		18:09:40 19 Se...	8080
14	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	23714	JSON				✓	34.143.100.209		18:09:40 19 Se...	8080
15	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	384	169	chain			✓	34.160.144.191		18:09:40 19 Se...	8080
16	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	2216	JSON				✓	34.143.100.209		18:09:41 19 Se...	8080
17	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	18507	JSON				✓	34.160.144.191		18:09:43 19 Se...	8080
18	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	45409	JSON				✓	34.143.100.209		18:09:44 19 Se...	8080
19	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	5227	JSON				✓	34.143.100.209		18:09:44 19 Se...	8080
20	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	384	169	chain			✓	34.160.144.191		18:09:47 19 Se...	8080
21	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	206	test				✓	34.160.144.191		18:09:50 19 Se...	8080
22	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	18507	JSON				✓	34.143.100.209		18:09:50 19 Se...	8080
23	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1408	KML	xml			✓	35.244.181.201		18:10:03 19 Se...	8080
24	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	326	JSON				✓	34.160.144.191		18:10:03 19 Se...	8080
25	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	23713	JSON				✓	34.143.100.209		18:10:03 19 Se...	8080
26	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	2302	JSON				✓	34.143.100.209		18:10:03 19 Se...	8080
27	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	41274	JSON				✓	34.143.100.209		18:10:03 19 Se...	8080
28	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	169	chain				✓	34.160.144.191		18:10:03 19 Se...	8080
29	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	3429	JSON				✓	34.143.100.209		18:10:03 19 Se...	8080
30	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
31	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
32	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
33	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
34	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
35	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
36	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
37	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
38	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
39	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
40	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
41	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
42	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
43	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
44	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
45	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
46	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
47	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
48	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
49	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
50	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
51	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
52	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
53	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
54	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
55	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
56	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
57	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
58	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
59	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
60	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080
61	https://ffox.settings.services.m...	GET	/v1/buckets/main/collections/change...			200	1087	test				✓	20.207.73.85		18:10:03 19 Se...	8080

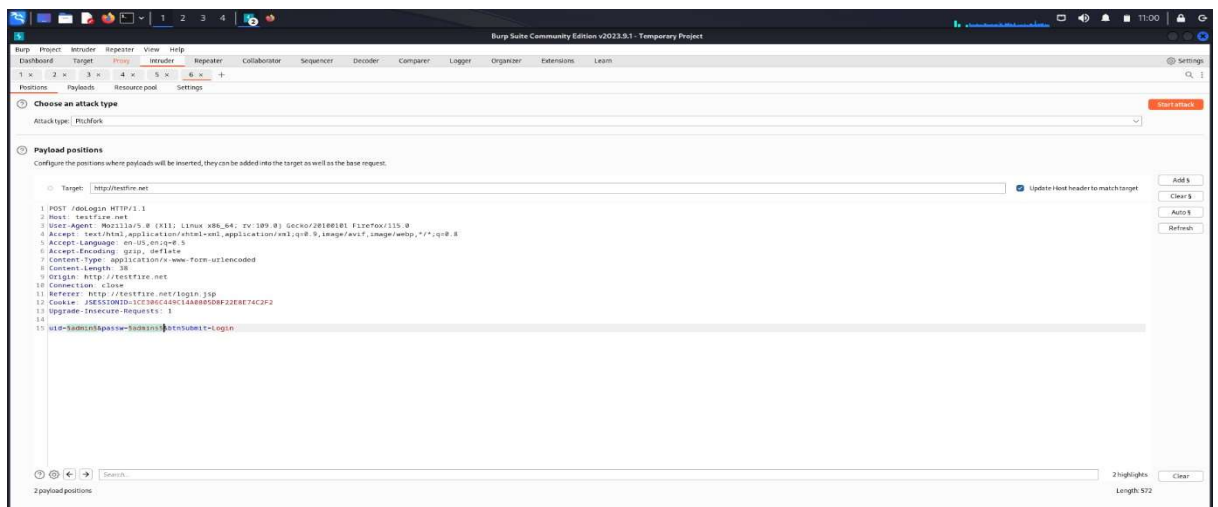
CREDENTIAL BYPASSING

Credential bypassing is an attack where the attacker does not have the credentials but enters the website by cracking the credentials.

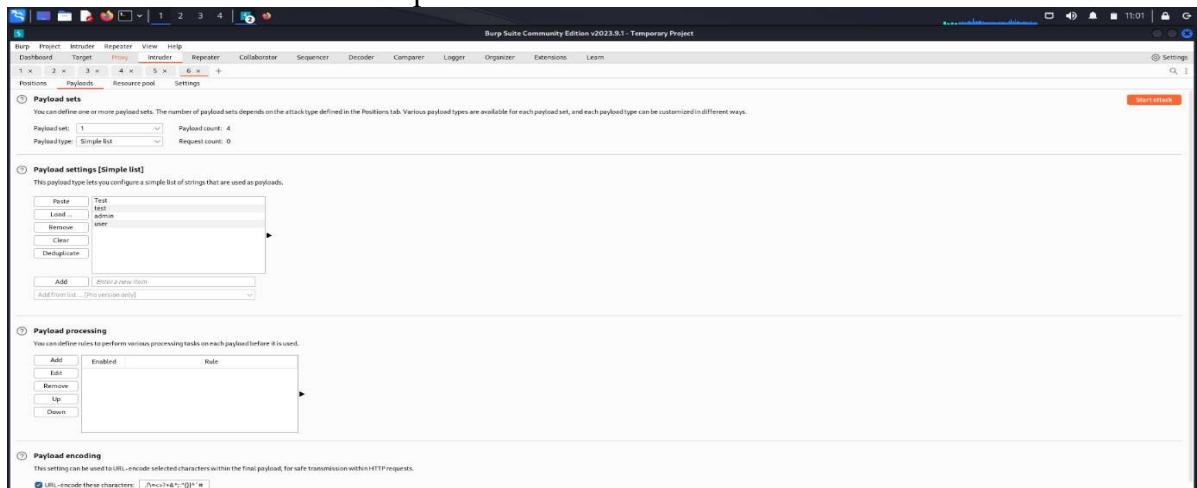
First of all, go to the desired website and turn on the intercept in burpsuite under proxy tab. Under HTTP history, we can see what all websites we have searched for. Right click on the code and send it to the intruder.



Under intruder tab, select the attack type as pitchfork. Then add the username and password as elements.



Insert the list of usernames and passwords and start the attack.



Among the 4 credentials entered, only one credential has the length of 264 which means it is the correct one.

The screenshot shows the Burp Suite interface with a 'Temporary attack' window open. The window displays a table of 4 requests with their payloads and status codes. The 4th request, with payload 'user', has a status code of 302 and a length of 264. The 'Request' tab shows the raw HTTP request details.

Request	Payload1	Payload2	Status code	Error	Timeout	Length	Comment
0			302			126	
1	test	test	302			126	
2	test	test	302			126	
3	admin	admin	302			264	
4	user	user	302			126	

The 'Request' tab shows the raw HTTP request details:

```
POST /api/login HTTP/1.1
Host: testfire.net
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: 33
Origin: http://testfire.net
Connection: keep-alive
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=1CE36C440C1A48895D8F2229B74C2F2
Upgrade-Insecure-Requests: 1
uid=admin&pass=wrong&nextSubst=1&login
```

application security vulnerabilities.

