Experiment No. 10

Title: BURP - Demonstrate Target,Proxy, Scanner Tab

Roll No.: 16010420075 **Experiments No.: 10**

Aim: To demonstrate target, proxy and scanner tab using BURP.

\

Resources: Virtual Box

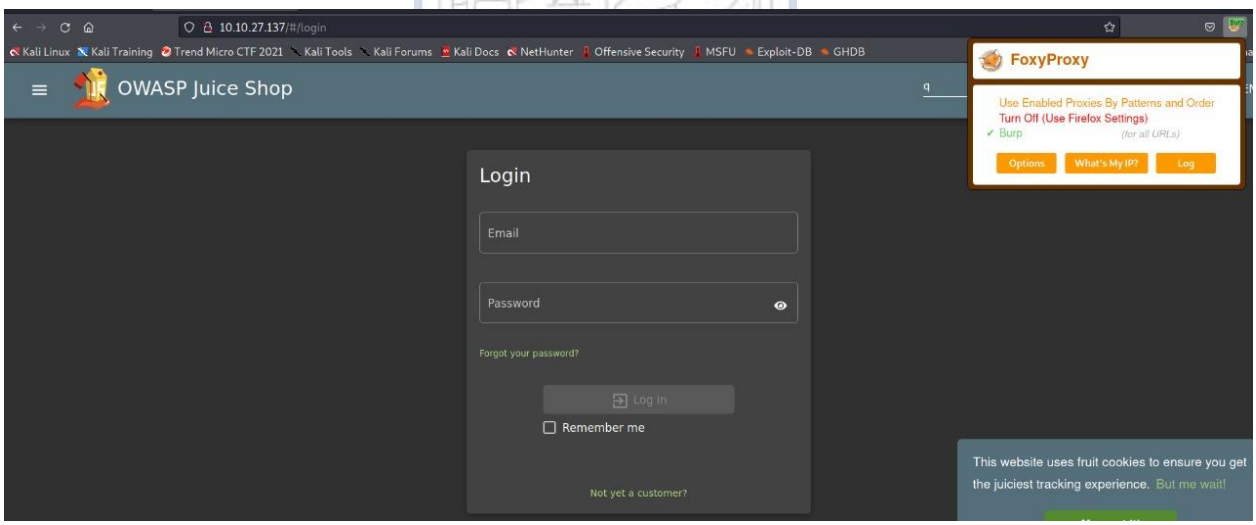
Theory

Burp Suite Enterprise Edition is a web-based programme that lets you leverage Burp Scanner's cutting-edge web scanning logic to find dozens of different vulnerabilities. It's made for large-scale automated scanning and integration with software development processes.

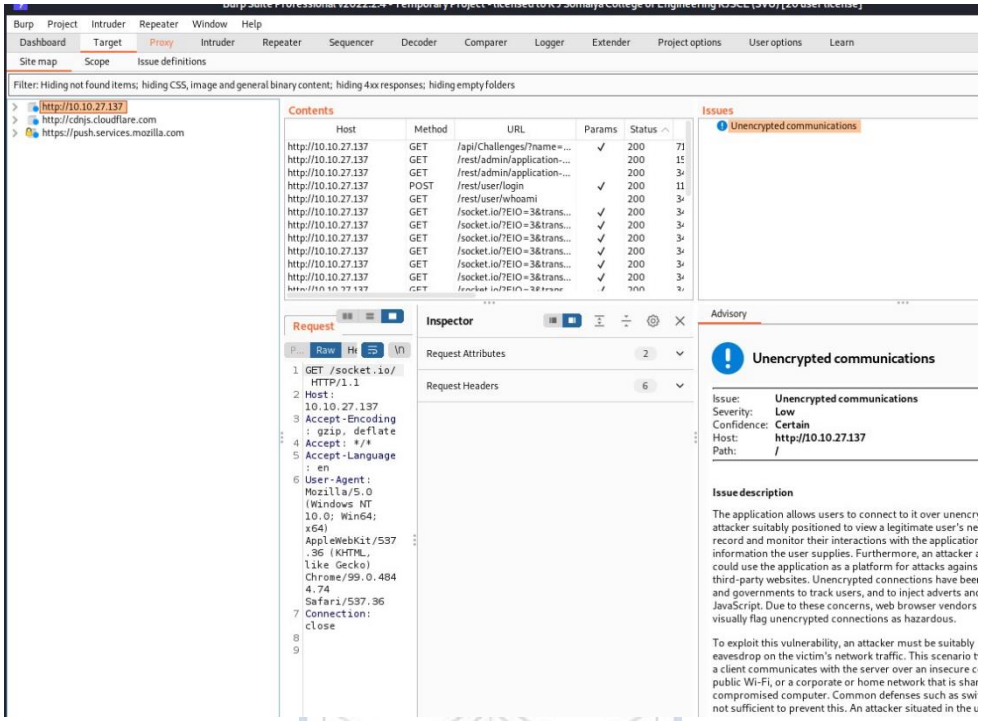
IMPLEMENTATION AND RESULTS:

Step 1: Getting Access to Login Page

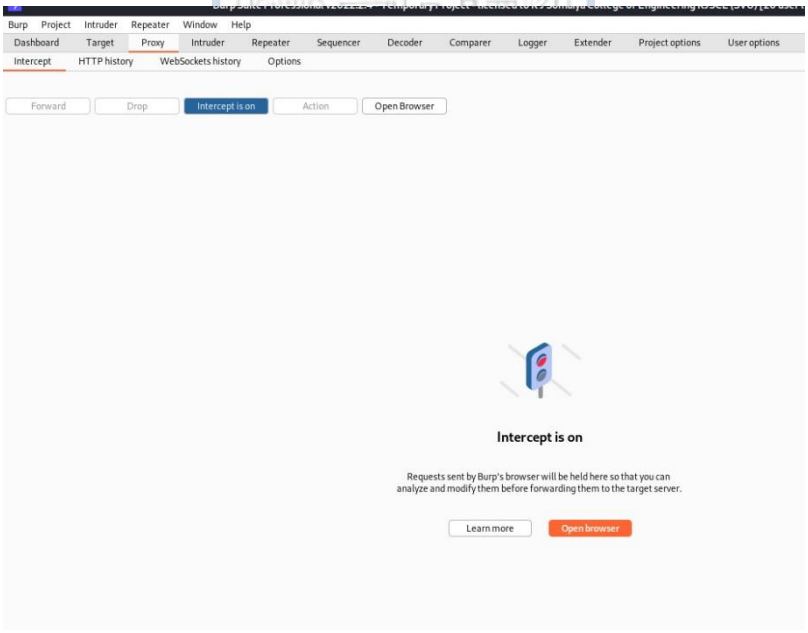
Step 2: Turning on burp proxy on browser to route requests to burp network



Step 3: Checking our target



Step 4: Switching on Intercept Mode

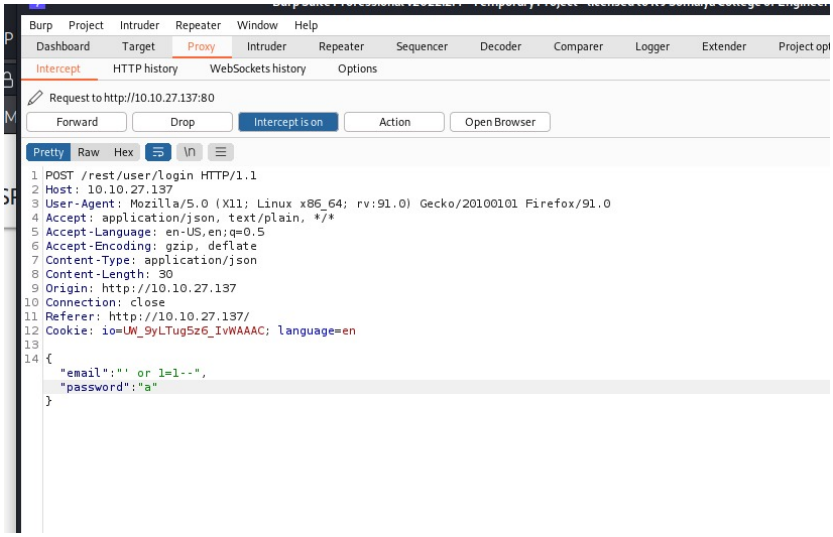


Step 5: Sending request from login page by inserting test values i.e random values

Step 6: Catching the request on Burp Suite

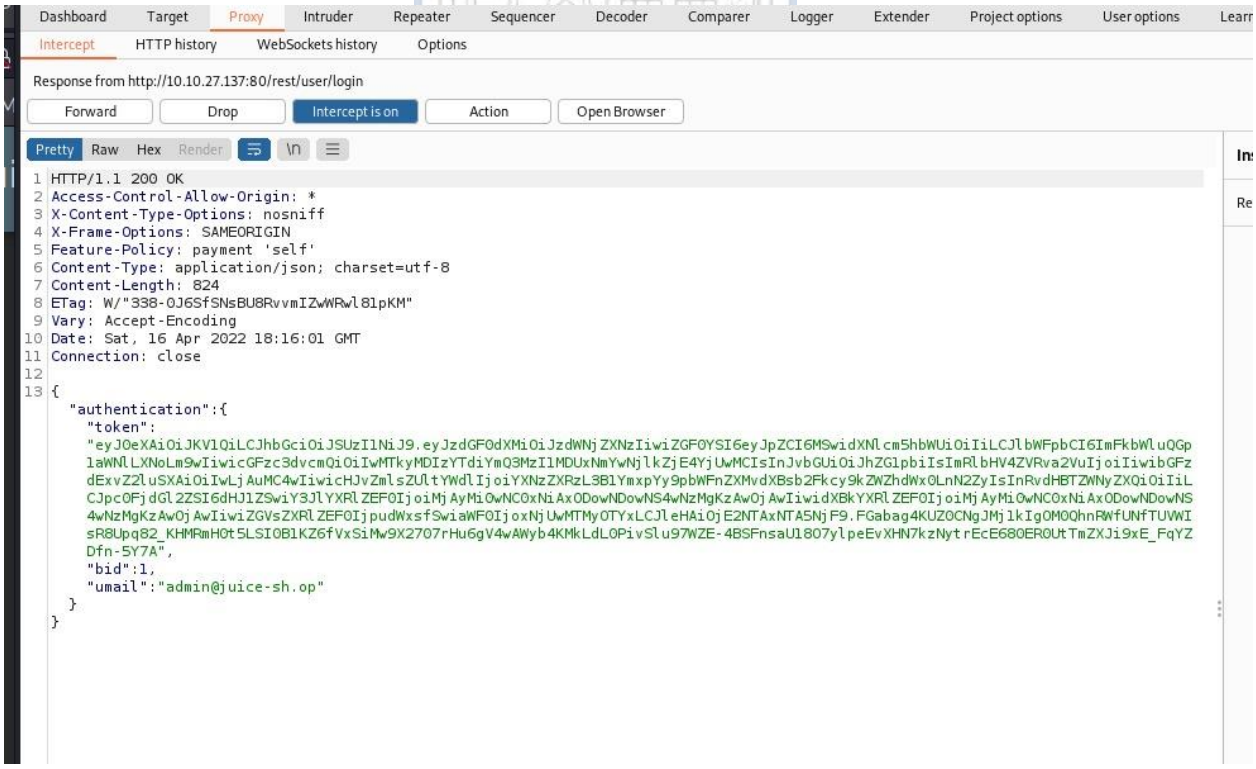
Step 7: Changing email field to→ ‘ or 1=1- -
Simple SQL injection to tell the server give details of admin

Let password be →test value→"a"

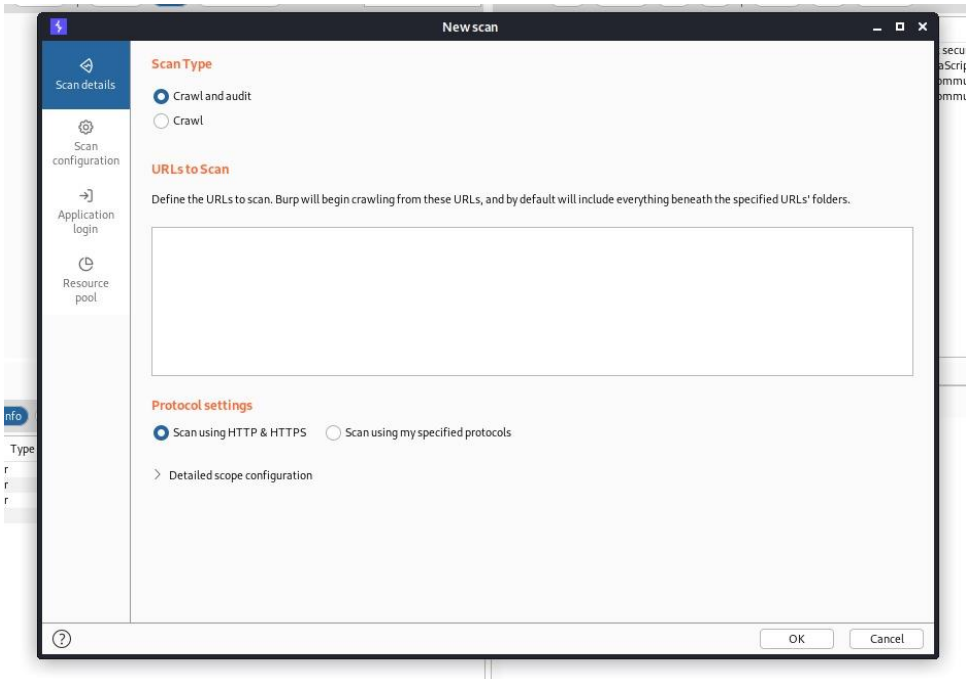


Step 8: Go to Dropdown and select option "Response to this request" on Burp Suite

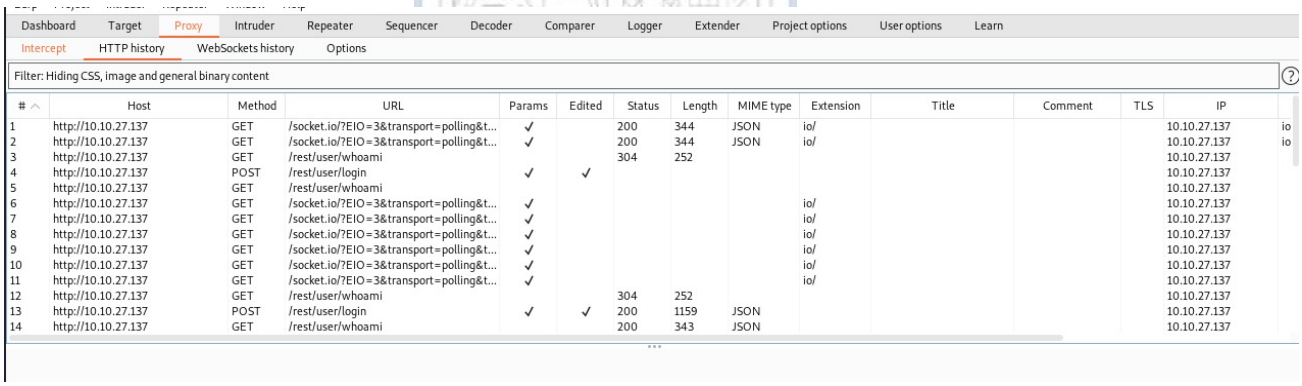
Step 9: Click on forward request button until the login is bypassed
And you get the authentication token



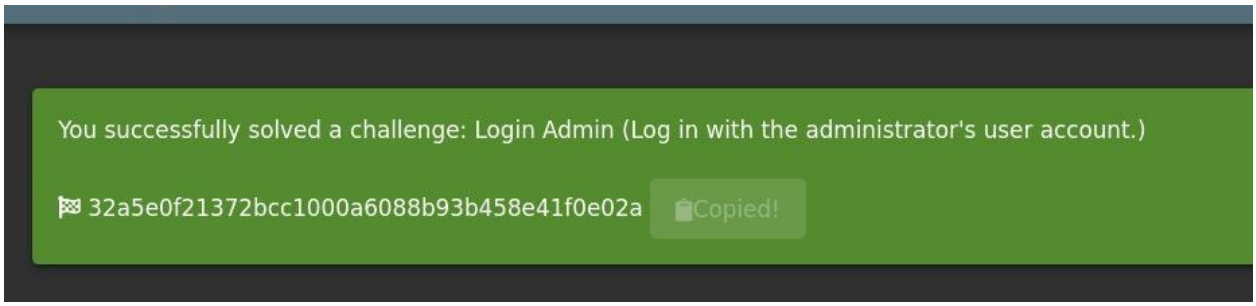
Step10: We can initiate scans from burp for further website inspection



Step 11: We can also check the HTTP history from burp Proxy tab to see the details of each request sent.



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	
1	http://10.10.27.137	GET	/socket.io/?EIO=3&transport=polling&t...	✓		200	344	JSON	io/				10.10.27.137	io
2	http://10.10.27.137	GET	/socket.io/?EIO=3&transport=polling&t...	✓		200	344	JSON	io/				10.10.27.137	io
3	http://10.10.27.137	GET	/rest/user/whoami			304	252						10.10.27.137	
4	http://10.10.27.137	POST	/rest/user/login	✓	✓								10.10.27.137	
5	http://10.10.27.137	GET	/rest/user/whoami										10.10.27.137	
6	http://10.10.27.137	GET	/socket.io/?EIO=3&transport=polling&t...	✓					io/				10.10.27.137	
7	http://10.10.27.137	GET	/socket.io/?EIO=3&transport=polling&t...	✓					io/				10.10.27.137	
8	http://10.10.27.137	GET	/socket.io/?EIO=3&transport=polling&t...	✓					io/				10.10.27.137	
9	http://10.10.27.137	GET	/socket.io/?EIO=3&transport=polling&t...	✓					io/				10.10.27.137	
10	http://10.10.27.137	GET	/socket.io/?EIO=3&transport=polling&t...	✓					io/				10.10.27.137	
11	http://10.10.27.137	GET	/socket.io/?EIO=3&transport=polling&t...	✓					io/				10.10.27.137	
12	http://10.10.27.137	GET	/rest/user/whoami			304	252						10.10.27.137	
13	http://10.10.27.137	POST	/rest/user/login	✓	✓	200	1159	JSON					10.10.27.137	
14	http://10.10.27.137	GET	/rest/user/whoami			200	343	JSON					10.10.27.137	



Outcomes:

CO-3: Comprehend exploitation phase of penetration testing

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

We successfully targeted the login page with burp proxy and bypassed the admin login page.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- www.kali.org