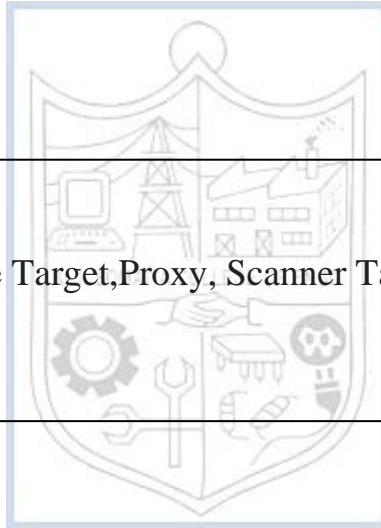


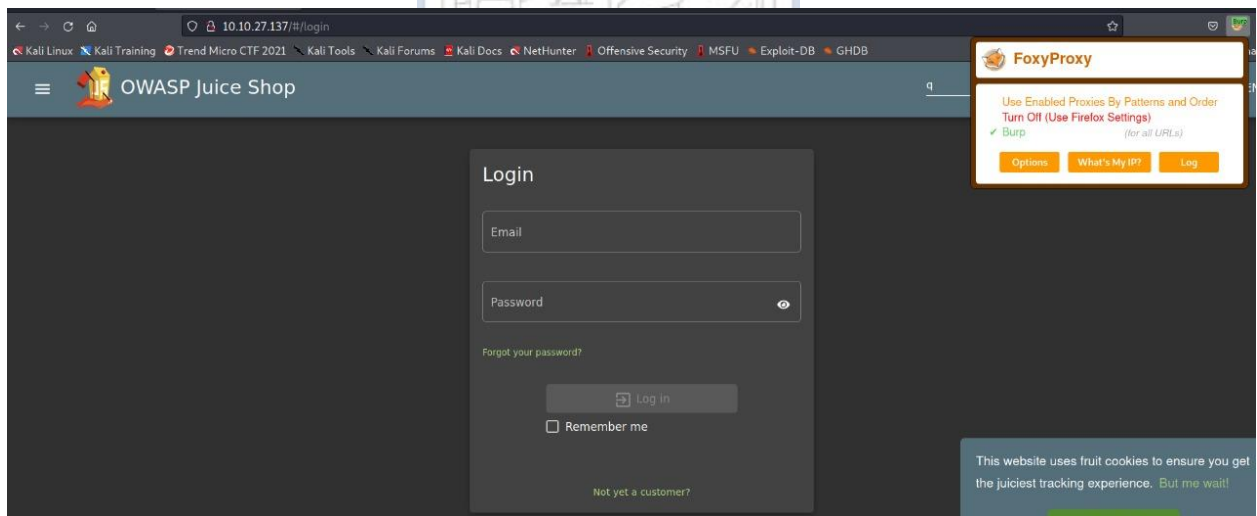
**Experiment No. 10**

Title: BURP - Demonstrate Target, Proxy, Scanner Tab

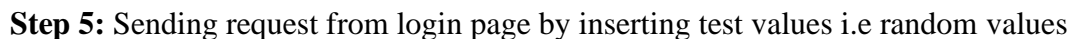
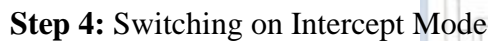


**Roll No.: 16010420075****Experiments No.: 10****Aim:** To demonstrate target, proxy and scanner tab using BURP.**Resources:** Virtual Box**Theory**

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.

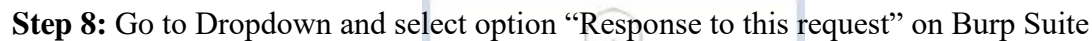
**IMPLEMENTATION AND RESULTS:****Step 1:** Getting Access to Login Page**Step 2:** Turning on burp proxy on browser to route requests to burp network**Step 3:** Checking our target

**(A Constituent College of Somaiya Vidyavihar University)**



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

**(A Constituent College of Somaiya Vidyavihar University)**



The screenshot displays the Burp Suite web application security tool. At the top, there's a navigation bar with tabs: Dashboard, Target, Proxy (selected), Intruder, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn.

Below the navigation bar, the main window shows the intercepted response from `http://10.10.27.137:80/rest/user/login`. The status bar indicates "Intercept is on". Buttons for "Forward", "Drop", "Action", and "Open Browser" are visible.

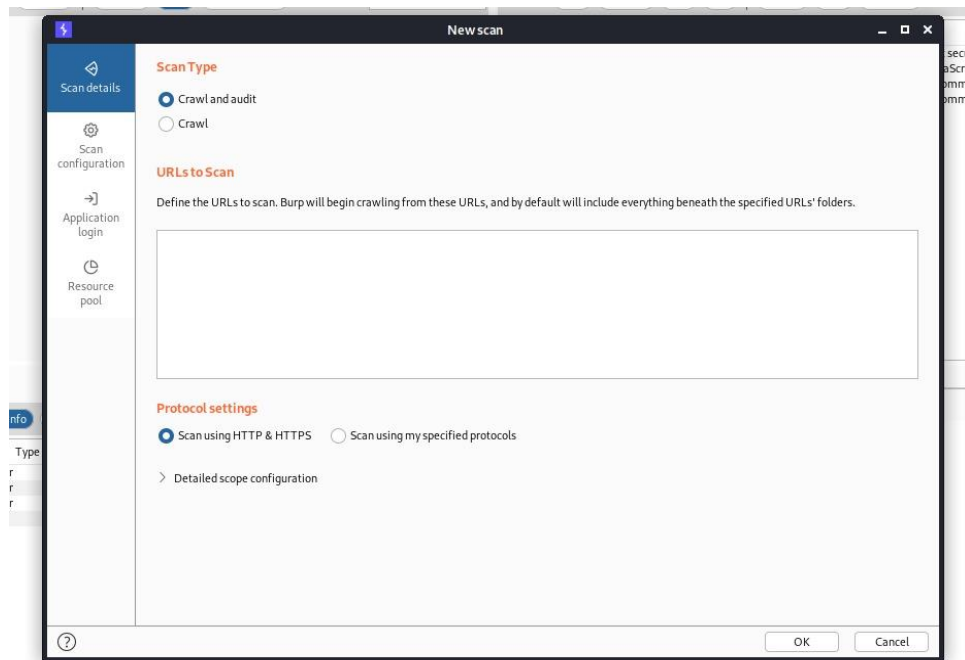
The response details pane shows the following headers:

- HTTP/1.1 200 OK
- Access-Control-Allow-Origin: \*
- X-Content-Type-Options: nosniff
- X-Frame-Options: SAMEORIGIN
- Feature-Policy: payment 'self'
- Content-Type: application/json; charset=utf-8
- Content-Length: 824
- ETag: W/"338-0J6SfSNsBUBRvrmIZwRWl8lpKM"
- Vary: Accept-Encoding
- Date: Sat, 16 Apr 2022 18:16:01 GMT
- Connection: close

The response body is shown as JSON:

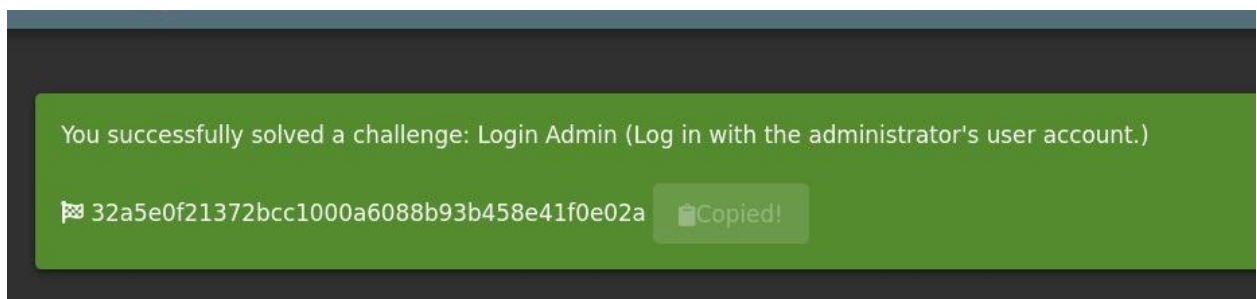
```
{
  "authentication": {
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiaWF0IjE6YyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFPbCI6ImFkbWluQGplawNLNXNoLm9wiicGFzc3dvcmQOIiwMTk5MDIzYTdiYm03MzIlMDUXNmYWNjlkZjE4YyUwMCIsInJvbGUOIjohZGlzbiIsImRva2VrVa2VuIjoiiIiwibGFnZExvZWZlbnRlcjEwIiwiaWwMcA4iIiwicHJvZmlsZSUltYWdlIjoiiYXNzZXRzLSB1YmxpYy9pbWFnZXMvdXBsb2Fkcyc9KZWZhdx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0pjdgLI2SSI6dHJlZSwiY3JlYXRlZEFOIjoiiMjAyMiOwNC0xNiAxODowNDowNS4wNzMyKgAwOjAwIiwidXBkYXRlZEFOIjoiiMjAyMiOwNC0xNiAxODowNDowNS4wNzMyKgAwOjAwIiwidGVzZXRLZEFOIjpudWxsfiSwiaWF0IjoixNjUwMTMyOTYxLCLleHAiOjE2NTAxNTA5NF9.Fgabg4KUZOcnqJmJlkIgOMQOhnPWfUNFTUVWI sR8Upq82_KHMRmHOTSL5IOBKZ6fvSiSM9X2707rHuGv4WAwyb4KMKLdLOPivSlu97WZE-4BSfnsauI807ylpeEvXHNVkzNytREcE680EROUTmZXJl9xe_FqYZDfn-5Y7A",
    "bid": 1,
    "umail": "admin@juice-sh.op"
  }
}
```

**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.

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn													
Intercept HTTP history WebSockets history Options													
Filter: Hiding CSS, image and general binary content													
#	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
2	http://10.10.27.137	GET	/socket.io/?EIO=3&transport=polling&t...	✓		200	344	JSON	io/				10.10.27.137
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



(A Constituent College of Somaiya Vidyavihar University)

**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](http://www.kali.org)



**(A Constituent College of Somaiya Vidyavihar University)**