**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**

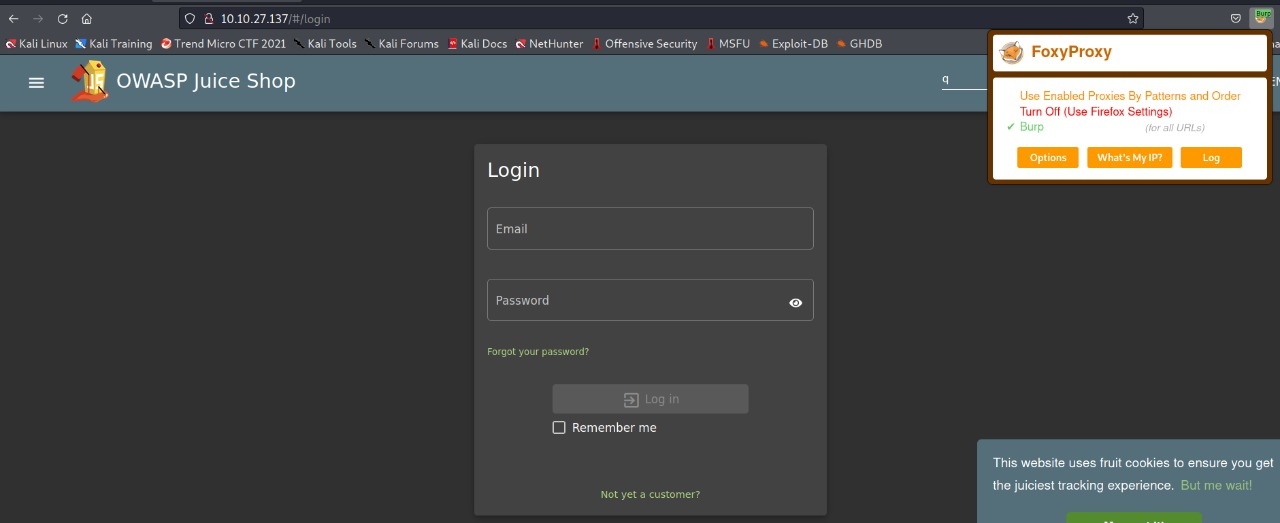
Burp Suite Enterprise Edition is a web-based programme that lets you leverage Burp Scanner's cutting-edge web scanning logic to find dozens of different vulnerabilities. It's made for large-scale automated scanning and integration with software development processes.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

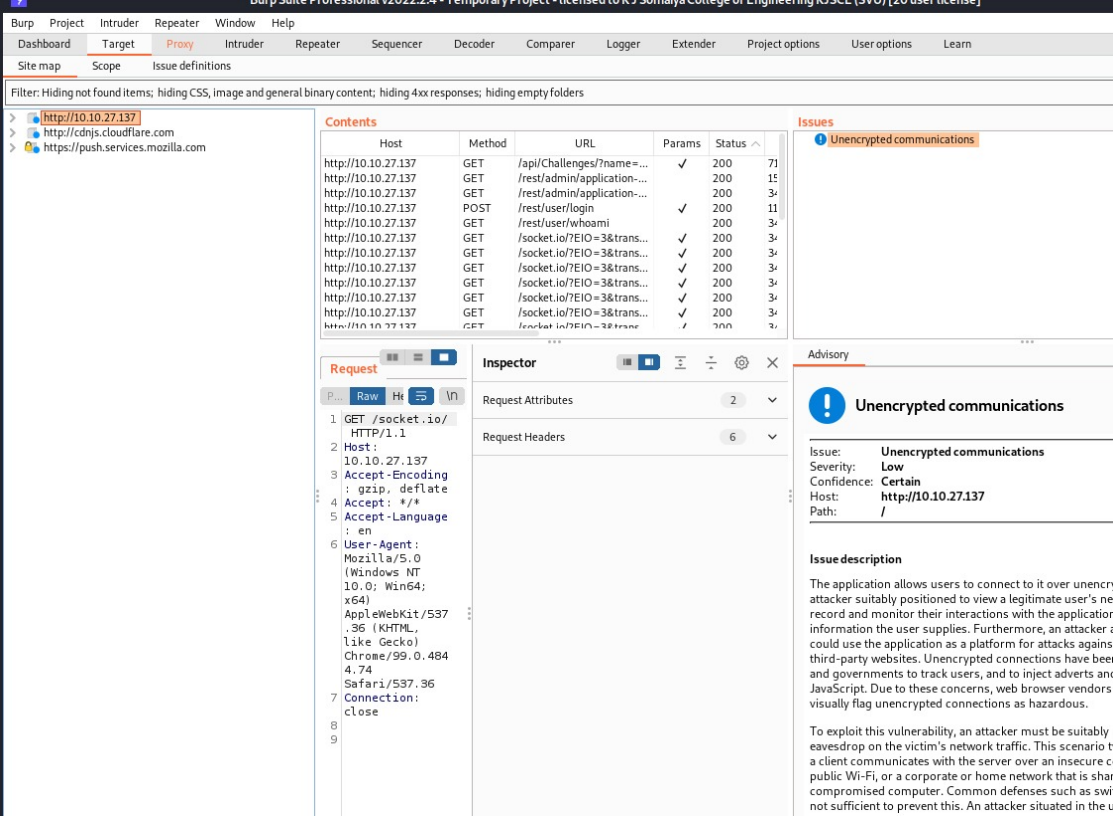
**IMPLEMENTATION AND RESULTS:**

**Step 1:** Getting Access to Login Page

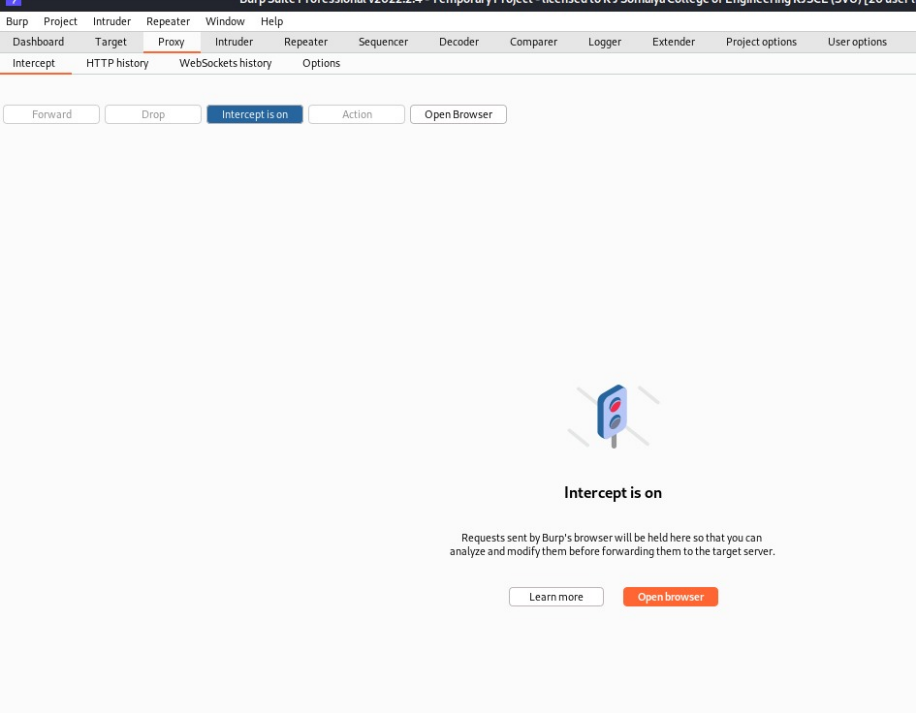
**Step 2:** Turning on burp proxy on browser to route requests to burp network



**Step 3:** Checking our target



**Step 4:** Switching on Intercept Mode



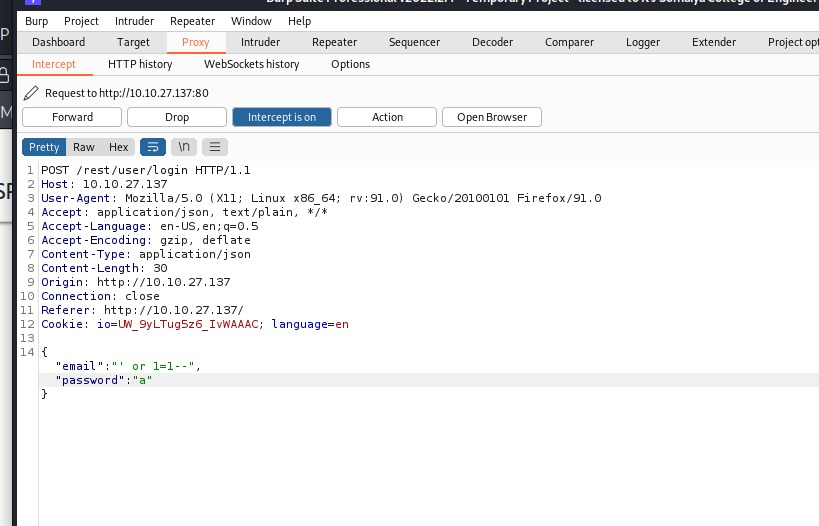
**Step 5:** Sending request from login page by inserting test values i.e random values

**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

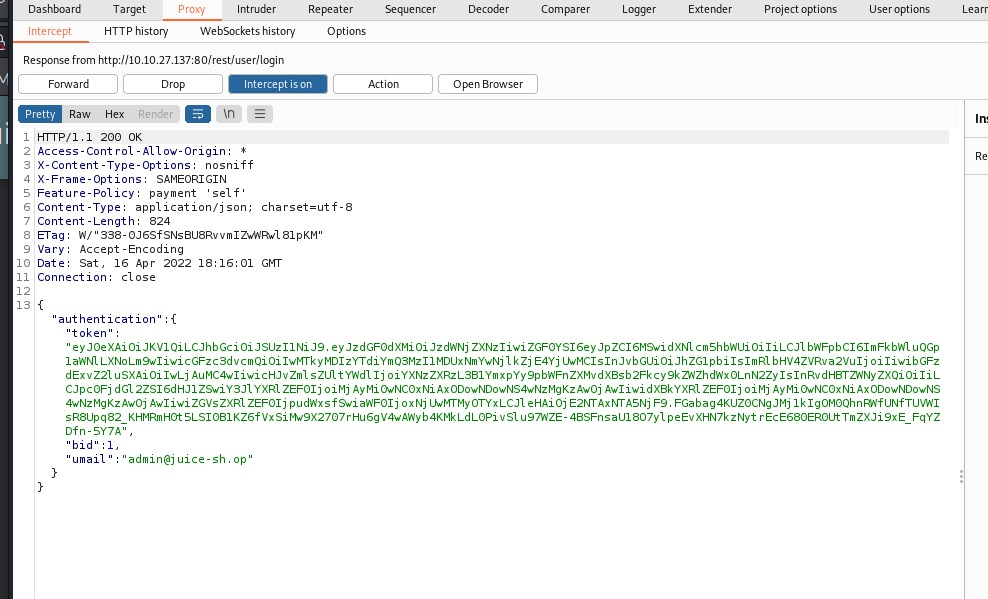
Let password be →test value→”a”



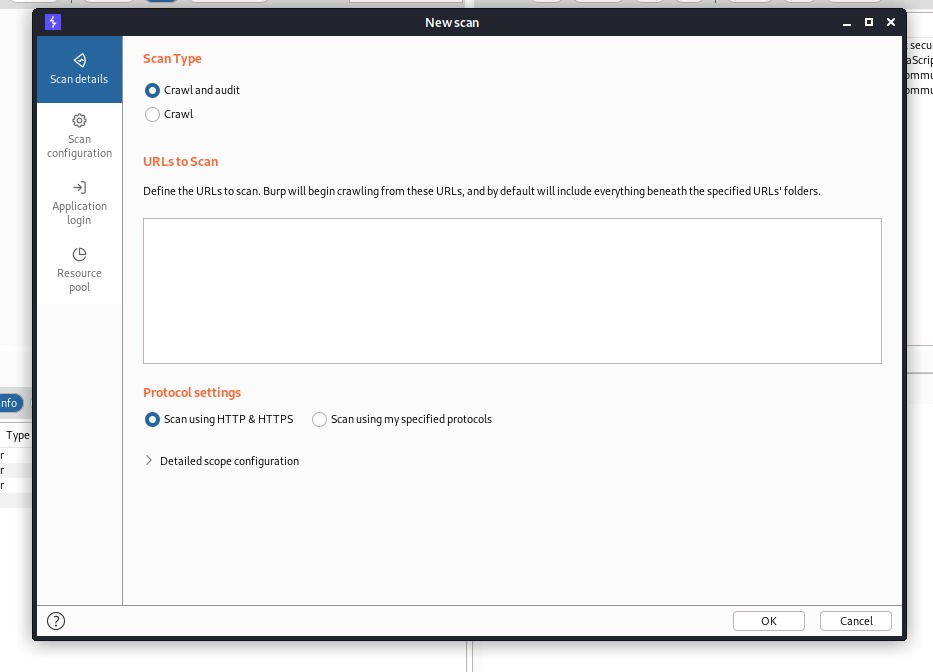
**Step 8:** Go to Dropdown and select option “Response to this request” on Burp Suite

**Step 9:** Click on forward request button until the login is bypassed

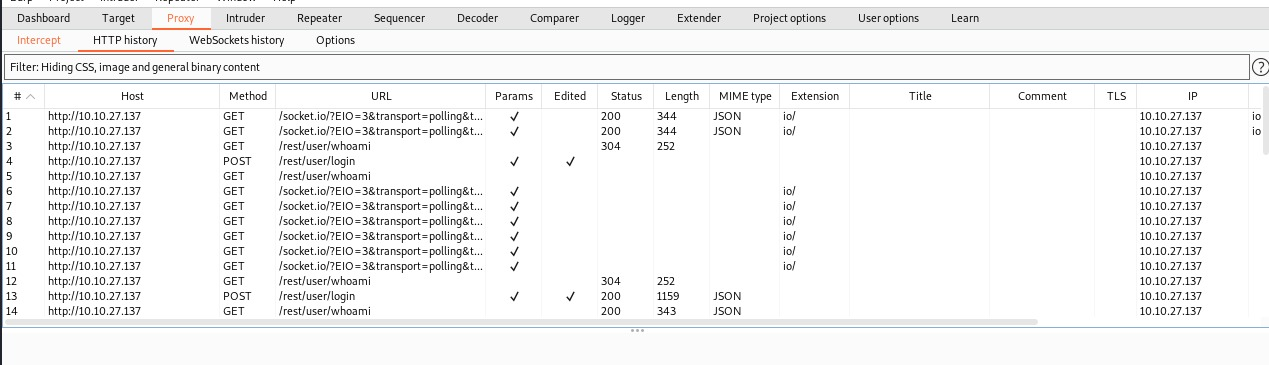
And you get the authentication token

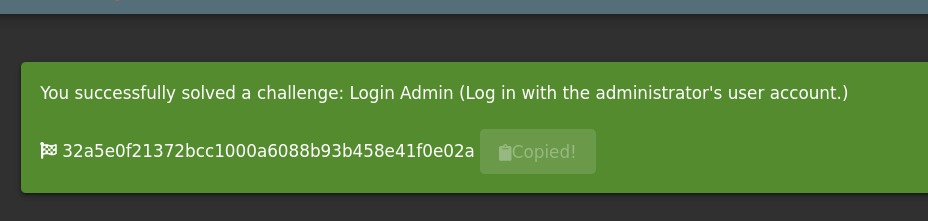


**Step10:** We can initiate scans from burp for further website inspection



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





**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)