Task 2 WEB APPLICATION VULNERABILITY SCANNER

- I am performing web application vulnerability assessment to identify vulnerabilities in a web application To Perform this vulnerability assessment I am using tools like

    1. Burp suite professional
    2. OWASP Broken web applications VM

- I have download Burp suite Professional from fire fox to perform Vulnerability assessment on web application
- I am using OWASP Bricks and BWAPP to perform web application vulnerability Assessment.
- Now I am using OWASP bricks to perform SQL Injection Attacks for authentication bypass on login pages by using SQL injection payloads
- I have used payload
- X') or ('1' ='1
- In the username and password field for authentication bypass of login pages.
- Now I am showing bricks app and bwapp used to perform vulnerability assessment on web application

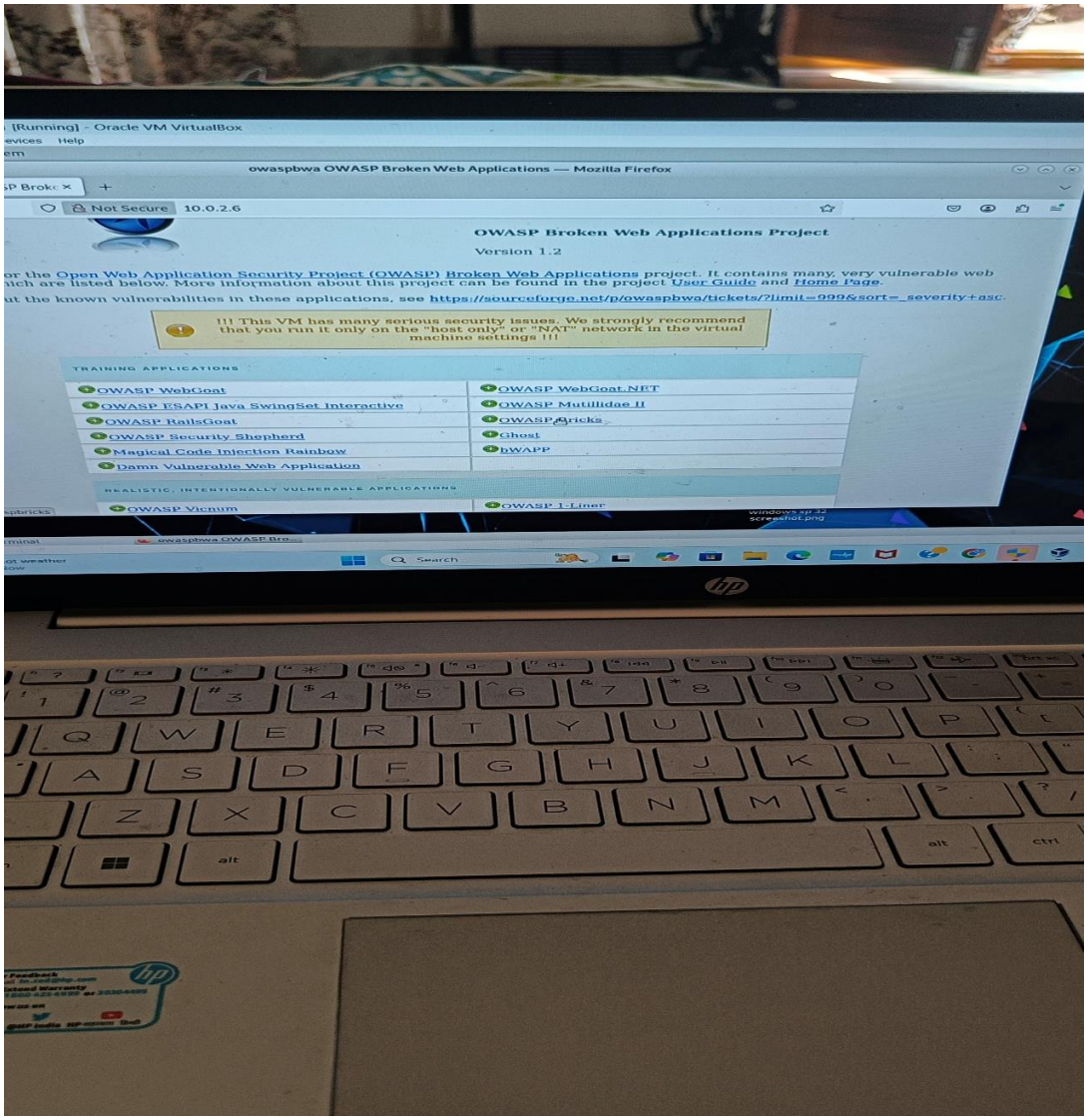
- 

Figure 1.1 shows OWASP Bricks & Bwapp for Vulnerability assessment on a web application

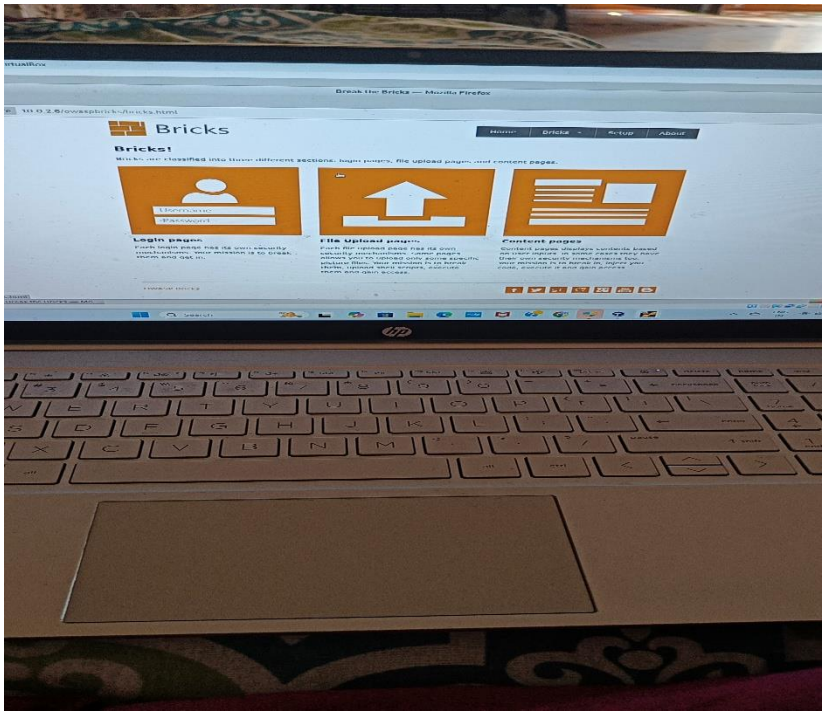


Fig 1.2 show login pages, file upload and content pages used for testing vulnerabilities in a web application

- Now I will attach a screenshot that show the Authentication bypass of a Login page using SQL injection Authentication bypass payloads
- I have used payload of
- X’ or ‘1’=’1 in the username and password field and successfully logged in

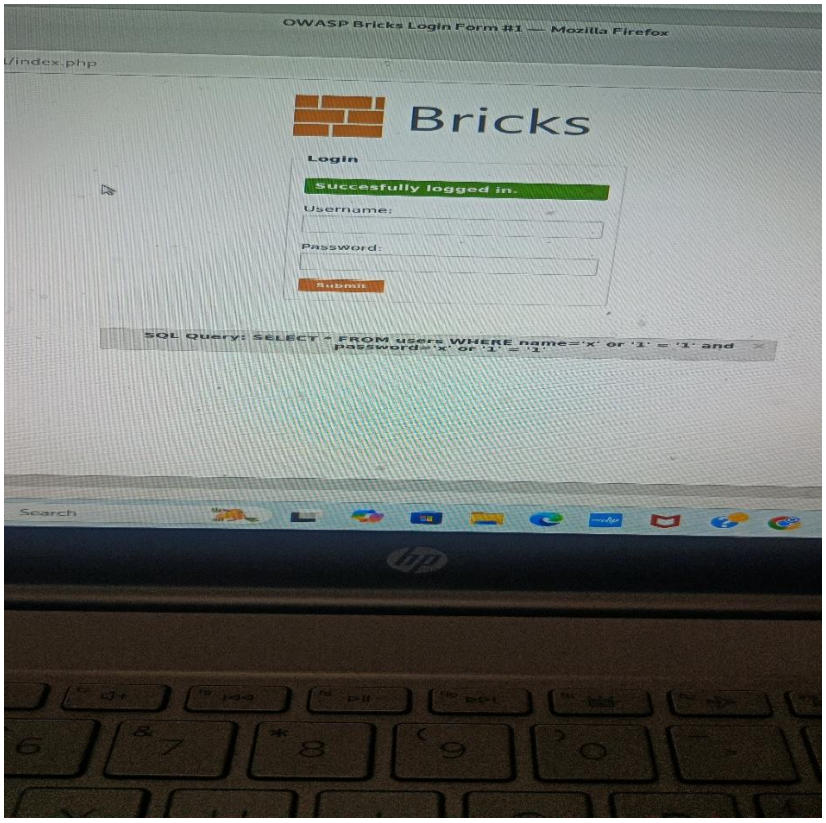


figure 1.3 shows successfully login into a login page using SQL injection payloads

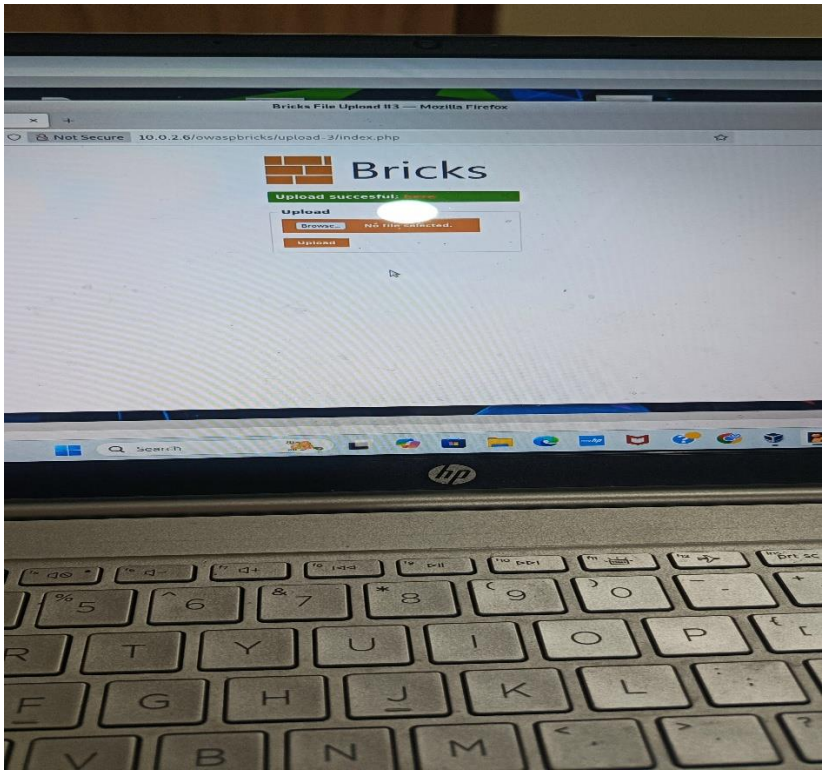


Figure 1.4 shows successfully file upload into a file upload page with the extension jpeg

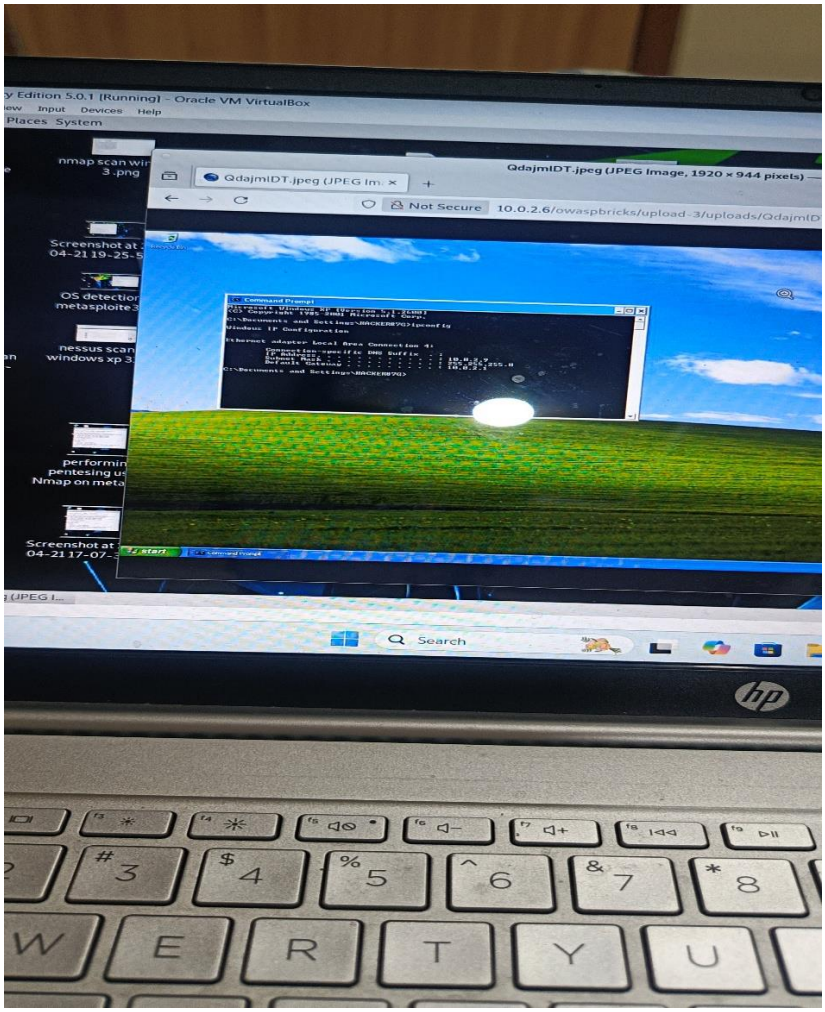


Figure 1.5 redirection to the uploaded image in the file upload page a vulnerability in the application.

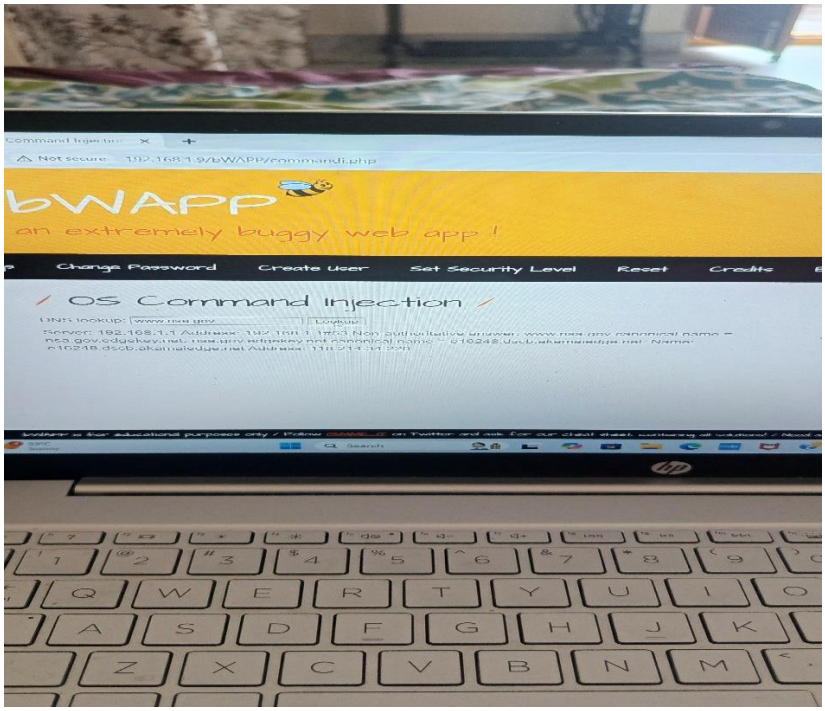


Figure 1.6 shows OS command injection vulnerability in a web application

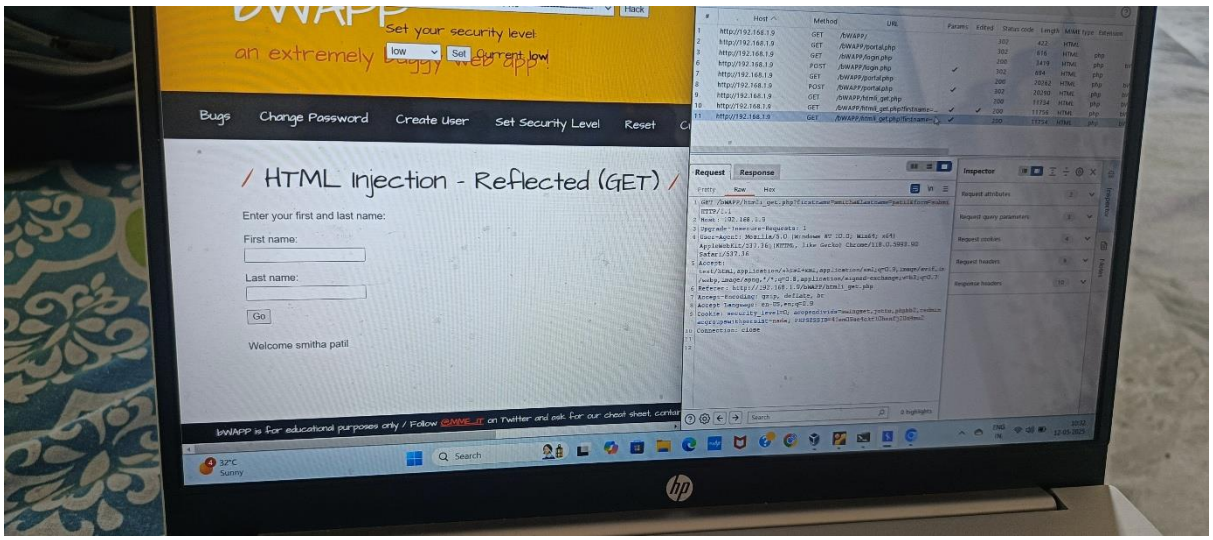


figure 1.7 shows HTML reflected get vulnerability using BWAPP and BURP SUIT Professional.

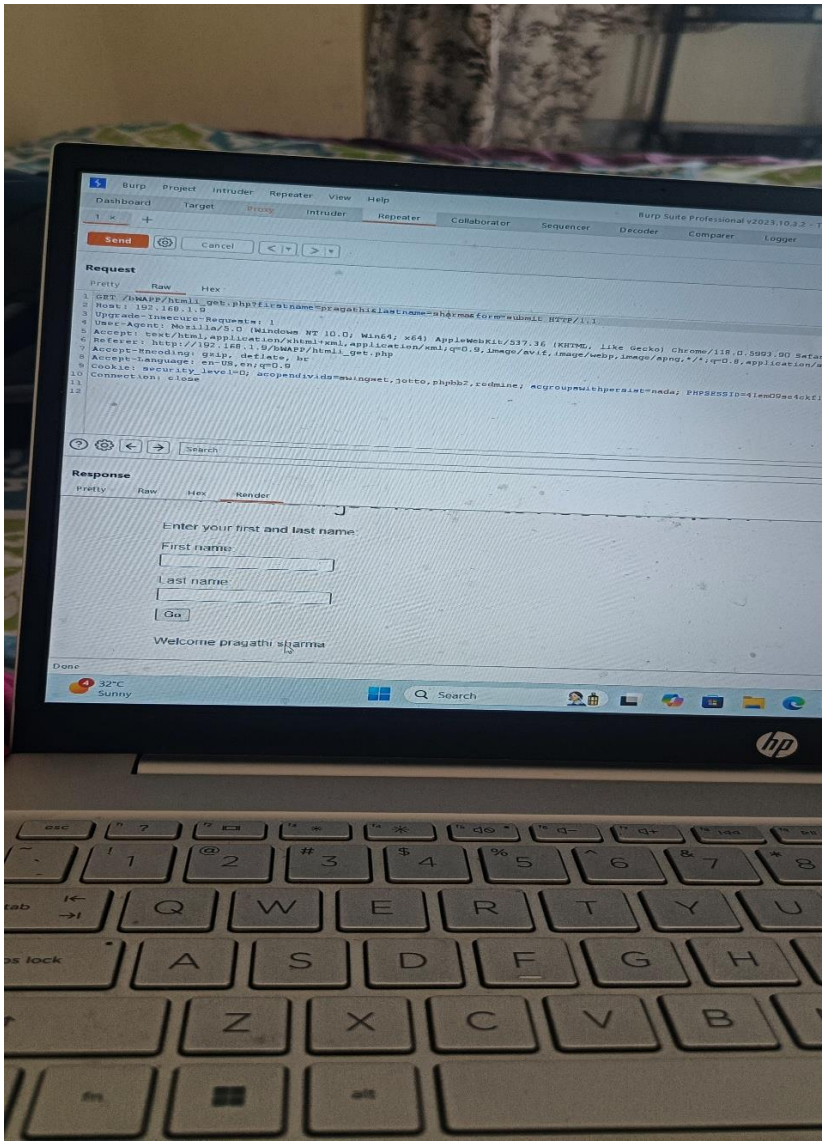


Figure 1.8 shows html reflected get changed username password using repeater in the burp suite professional

- Now I am attaching a screenshot showing stored cross site scripting vulnerability in a web application

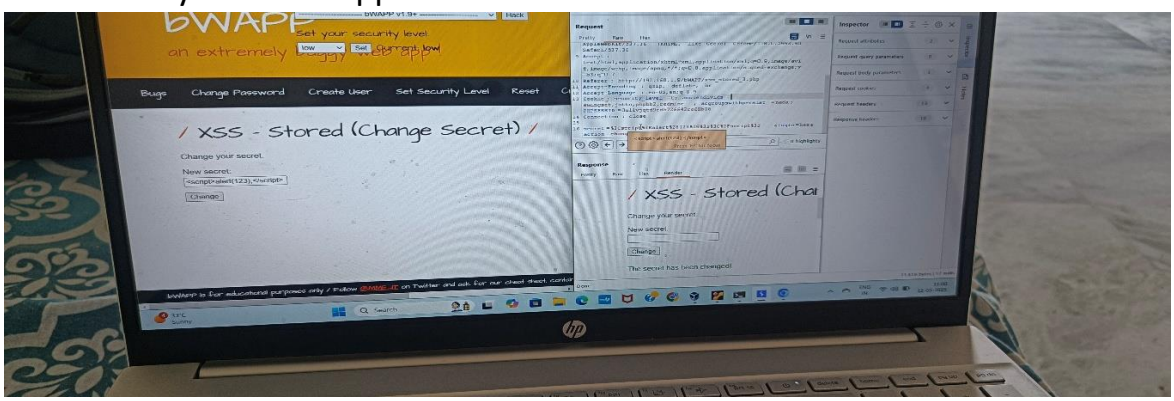


figure 1.9 shows cross site scripting stored change secret vulnerability in a web application

Now I am adding screenshots of authentication bypass of a banking application my manipulating user cookies and login into a user account

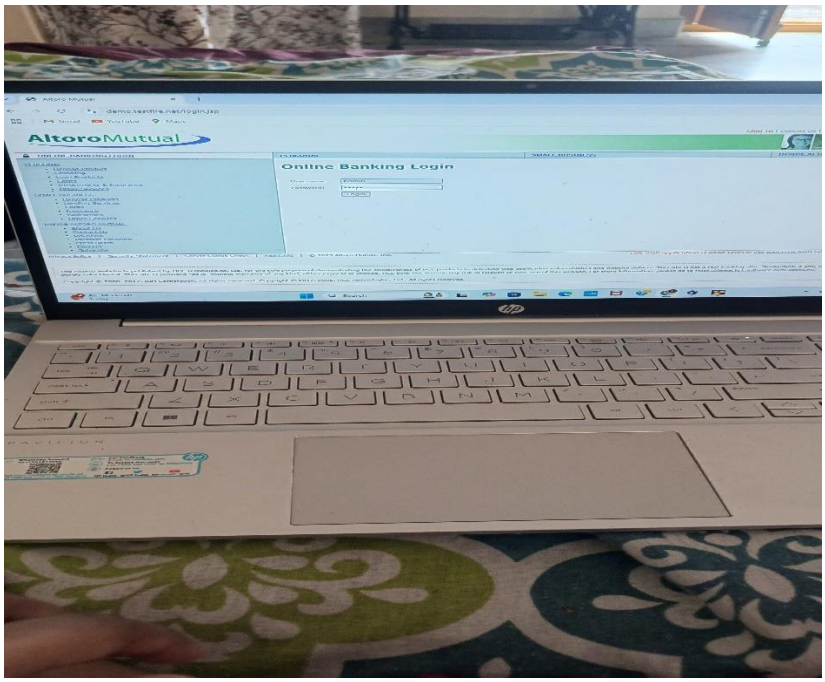


Figure 1.10 shows the login into banking app by using authentication bypass

- Now I am attaching the screenshot of the login into banking app and copying the session id of the admin user bank account

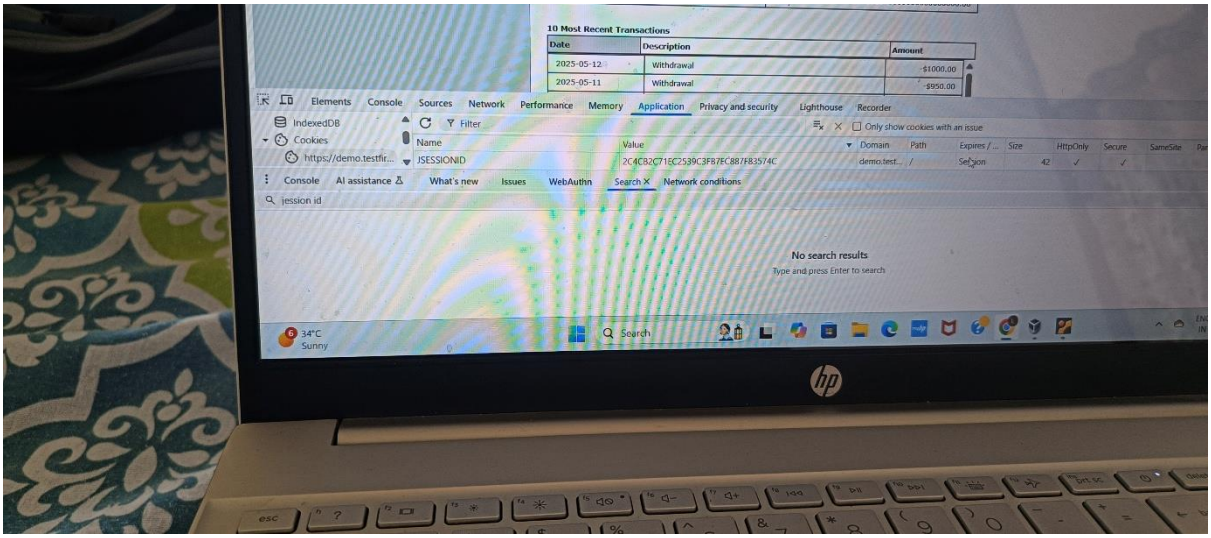


Image 1.11 shows jession id of the banking app

- now I will attach the image of login into banking website with http in other browser and replacing session ID and getting admin access.

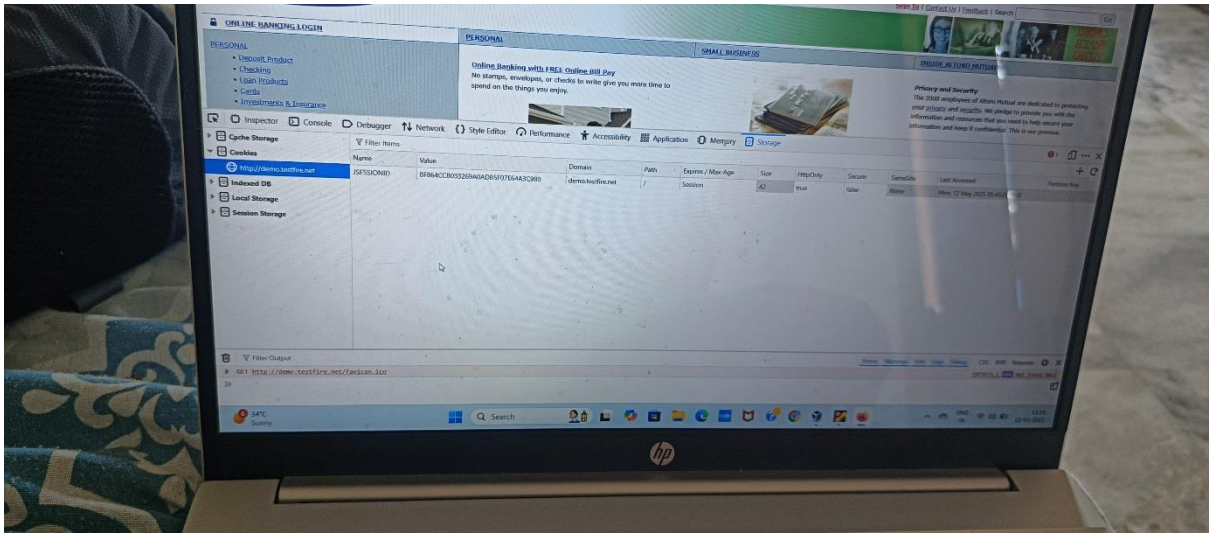


image 1.12 shows Jession ID of banking app and replacing it with https jession value

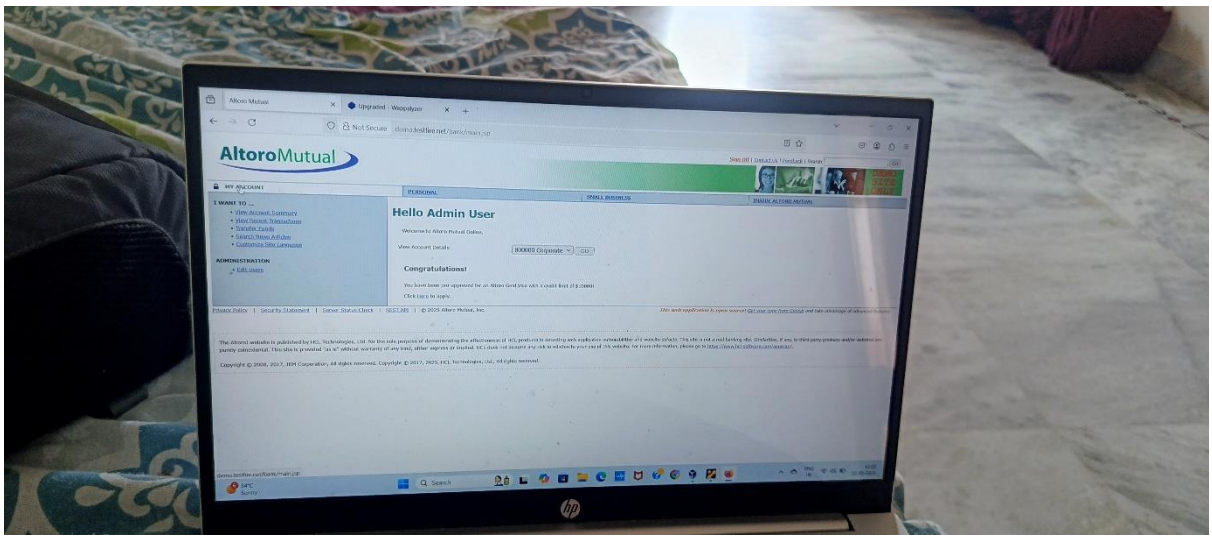


figure 1.13 shows login as admin user by manipulating jession cookie value.