WEB APPLICATION SECURITY TESTING

Conducted By: Future Interns
Author: Hari Rakesh Yengantiwar
Tools Used: Burp Suite, Docker Desktop, Browser(OWASP juice Shop, Altro Mutule, Test php)

Introduction

In today's digital era, web applications play a critical role in business operations, online services, and user interactions. However, with the increase in reliance on web technologies, cyber threats targeting these applications have also grown significantly. Attackers exploit vulnerabilities such as weak authentication, poor input validation, misconfigured security settings, and insecure session handling to gain unauthorized access or compromise sensitive data. Therefore, conducting web application penetration testing has become an essential part of cyber security.

Burp Suite is one of the most popular and powerful tools for performing web application penetration testing. Developed by PortSwigger, it provides a complete testing environment that integrates both manual and automated techniques to evaluate the security of web applications. Acting as an intercepting proxy between the client browser and the server, Burp Suite enables security testers to capture, analyze, and manipulate HTTP/HTTPS traffic in real time.

The suite includes several modules, each serving a unique purpose:

- Proxy: Intercepts and modifies traffic between the browser and the application.

- Repeater: Allows manual testing by modifying and resending specific requests.

- Intruder: Performs automated customized attacks such as brute force or fuzzing.
- Scanner (Pro version): Detects common vulnerabilities such as SQL injection, XSS, and misconfigurations.
- Sequencer: Analyzes randomness in session tokens.
- Decoder & Comparer: Helps encode/decode data and compare different requests or responses.

By combining these components, Burp Suite enables ethical hackers and security professionals to discover vulnerabilities mapped to well-known frameworks such as the OWASP Top 10, which lists the most critical web application security risks.

This project focuses on using Burp Suite to perform penetration testing in a controlled environment, specifically targeting intentionally vulnerable applications such as OWASP Juice Shop and DVWA (Damn Vulnerable Web Application). The aim is to simulate real-world attack scenarios safely, understand how vulnerabilities are exploited, and provide mitigation recommendations.

The outcomes of this project will include:

- Gaining practical experience with Burp Suite's tools and methodology.
- Identifying common security flaws in web applications.
- Documenting findings with evidence and remediation strategies.
- Emphasizing the importance of secure coding practices and proactive vulnerability testing.

Tools Required for the Project

Burp Suite (Community)

- Core penetration testing tool for intercepting, analyzing, and manipulating web traffic.

- Example: Google Chrome or Mozilla Firefox.
- Needs to be configured to route traffic through Burp Suite's proxy (127.0.0.1:8080).
- Burp CA certificate must be installed in the browser for HTTPS interception.
- OWASP Juice Shop (Node.js based vulnerable app).
- Simplifies setup of vulnerable applications.

Operating System / Environment

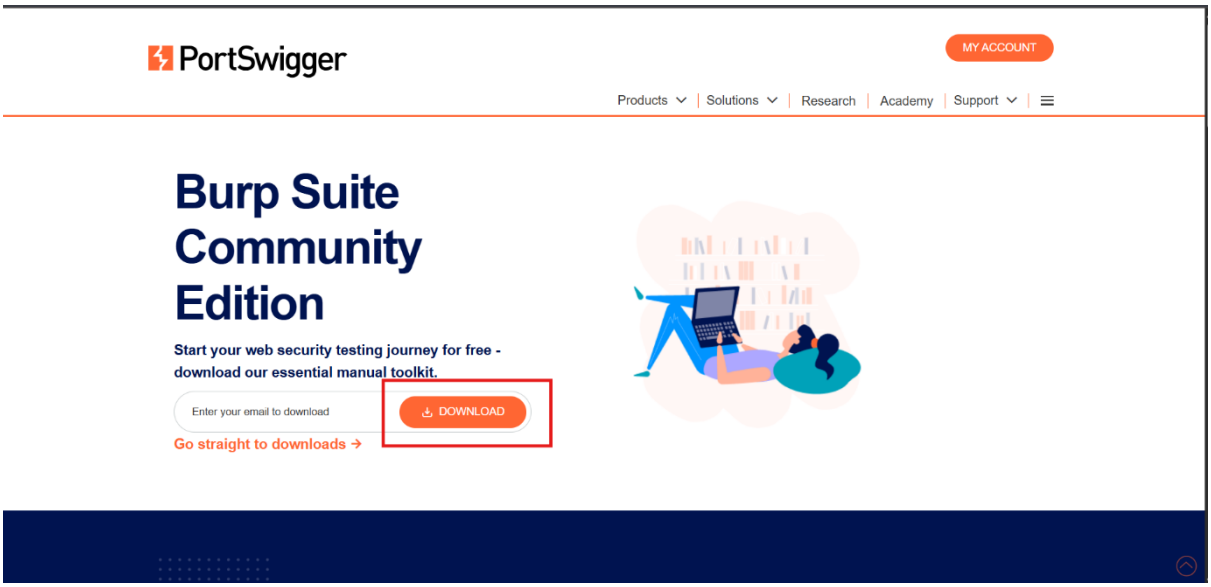
- Windows, Linux, or macOS can be used.

Burp Suite Installation:

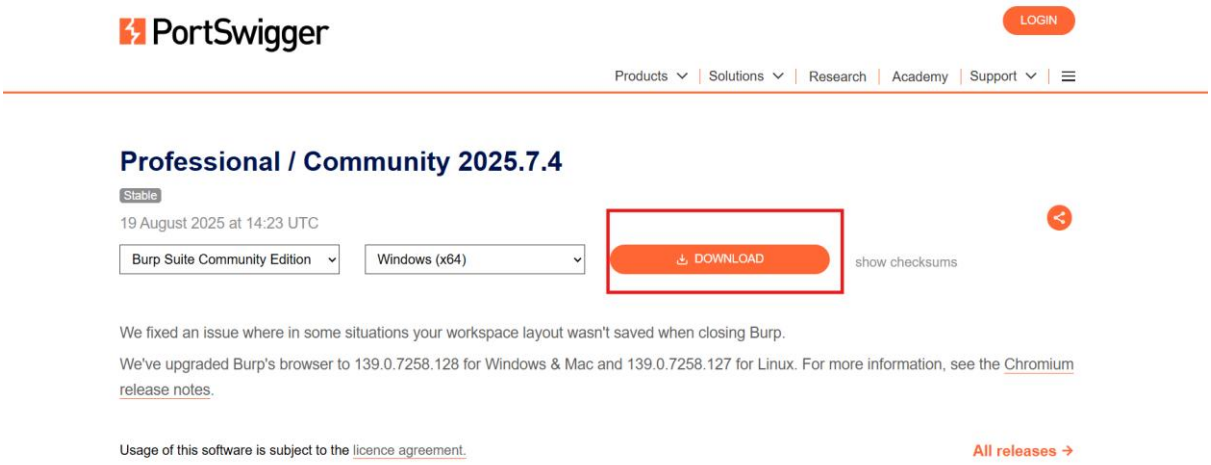
What is Burp Suite?

- Burp Suite is a popular web vulnerability scanner and penetration testing tool used by security professionals, ethical hackers, and bug bounty hunters to test the security of web applications.
- It acts as a proxy between your browser and the target website, allowing you to intercept, inspect, and modify requests and responses. This helps in identifying weaknesses such as SQL injection, XSS, insecure authentication, etc.

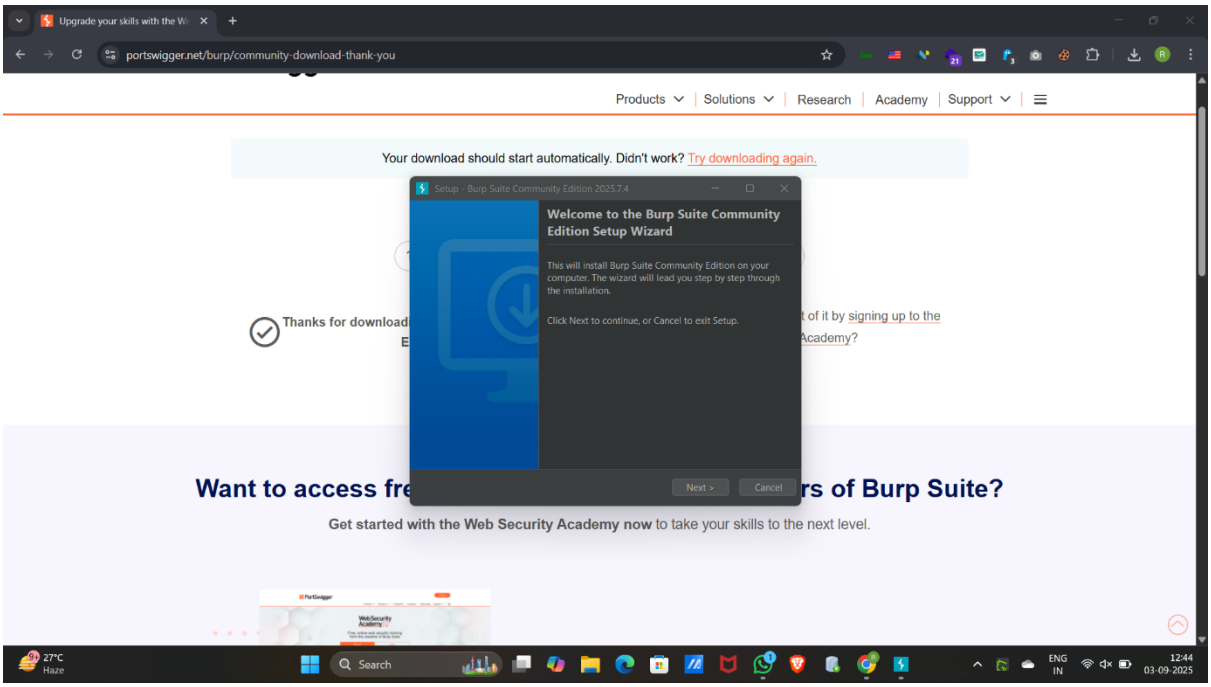
Installation :

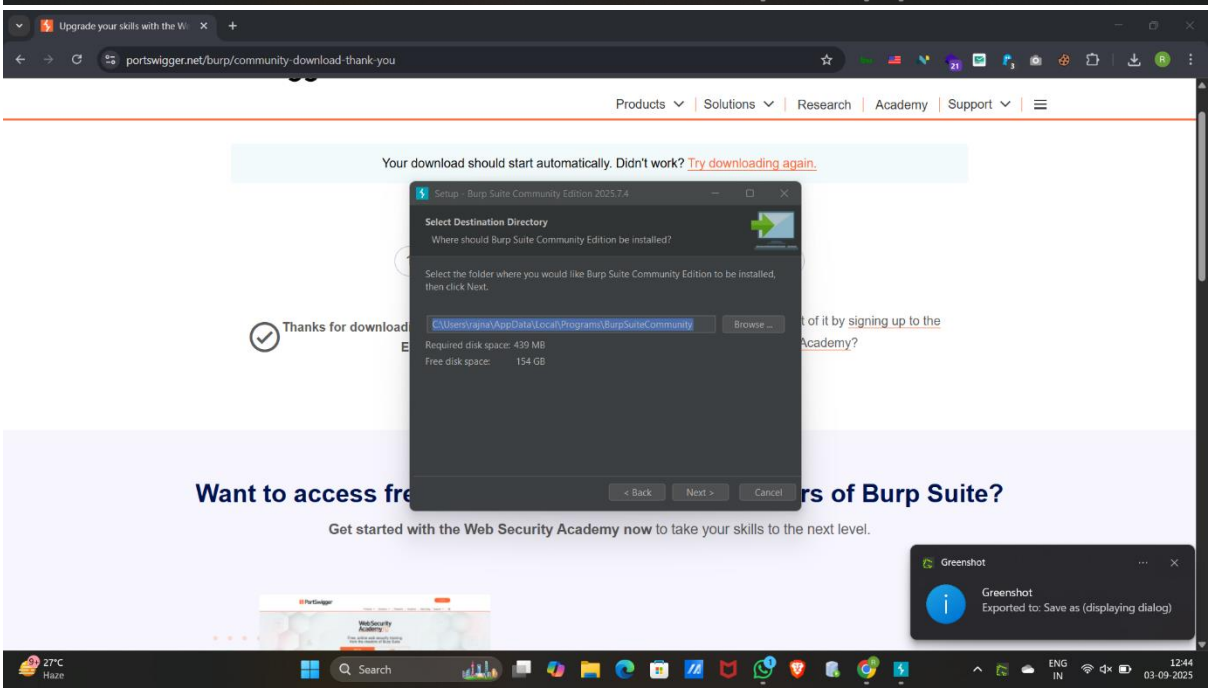


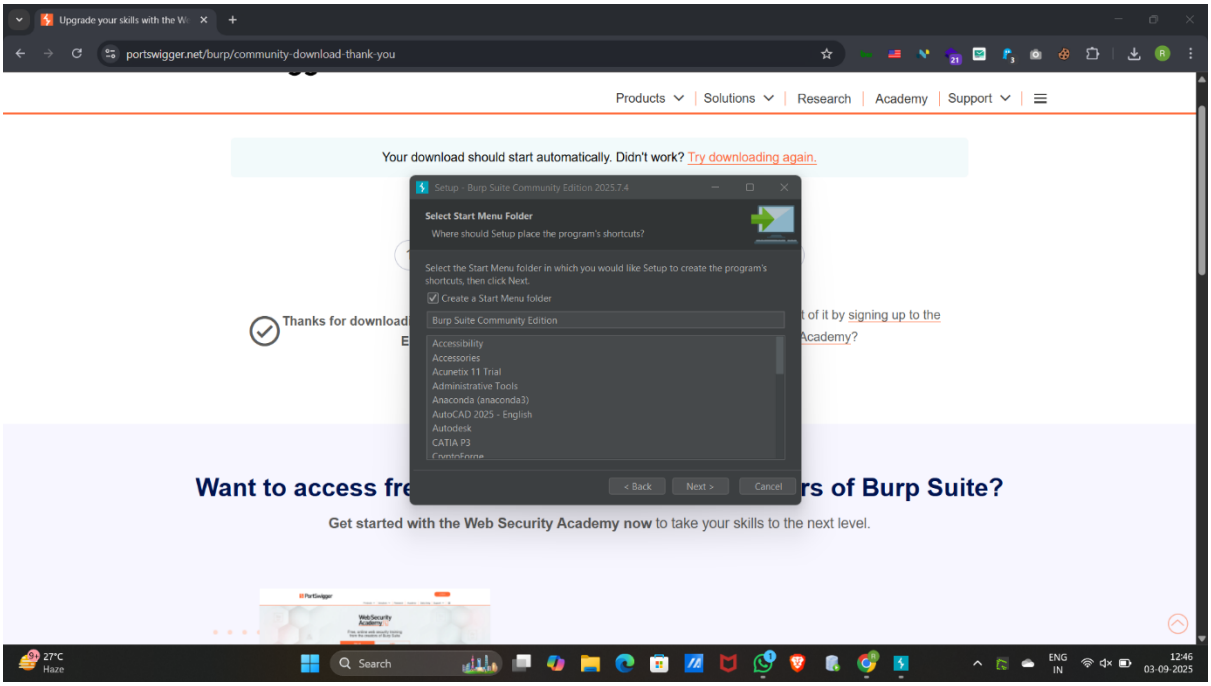
- Open your web browser and go to the official PortSwigger website: https://portswigger.net/burp

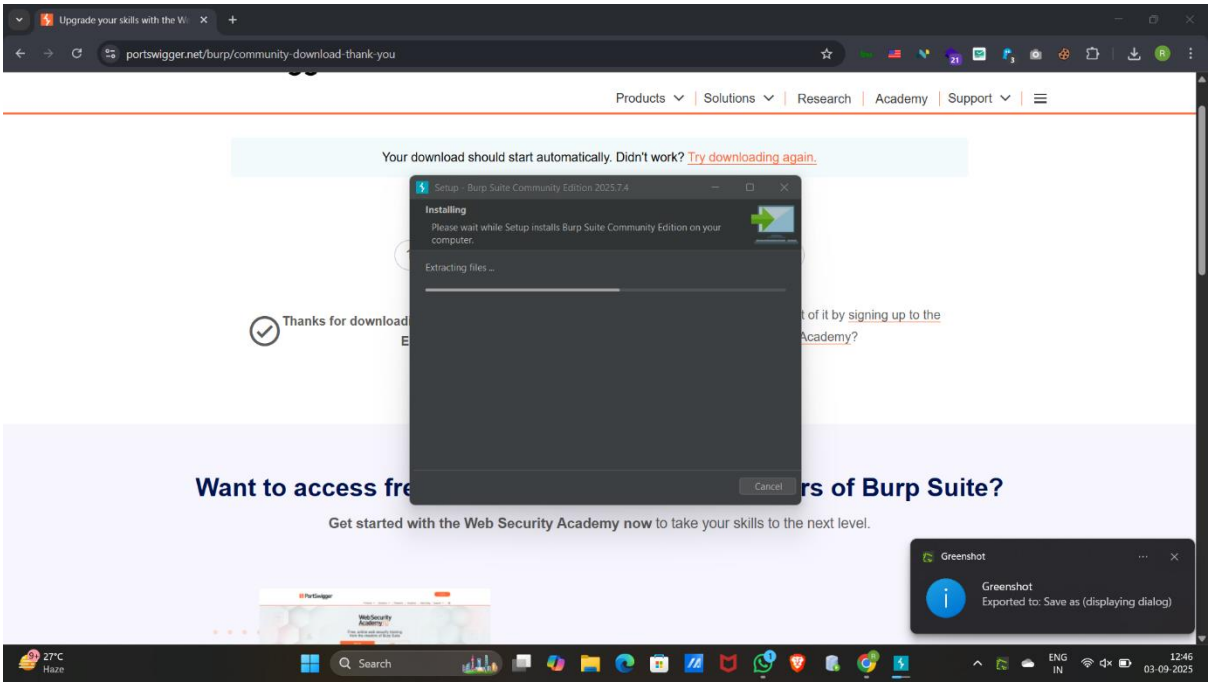


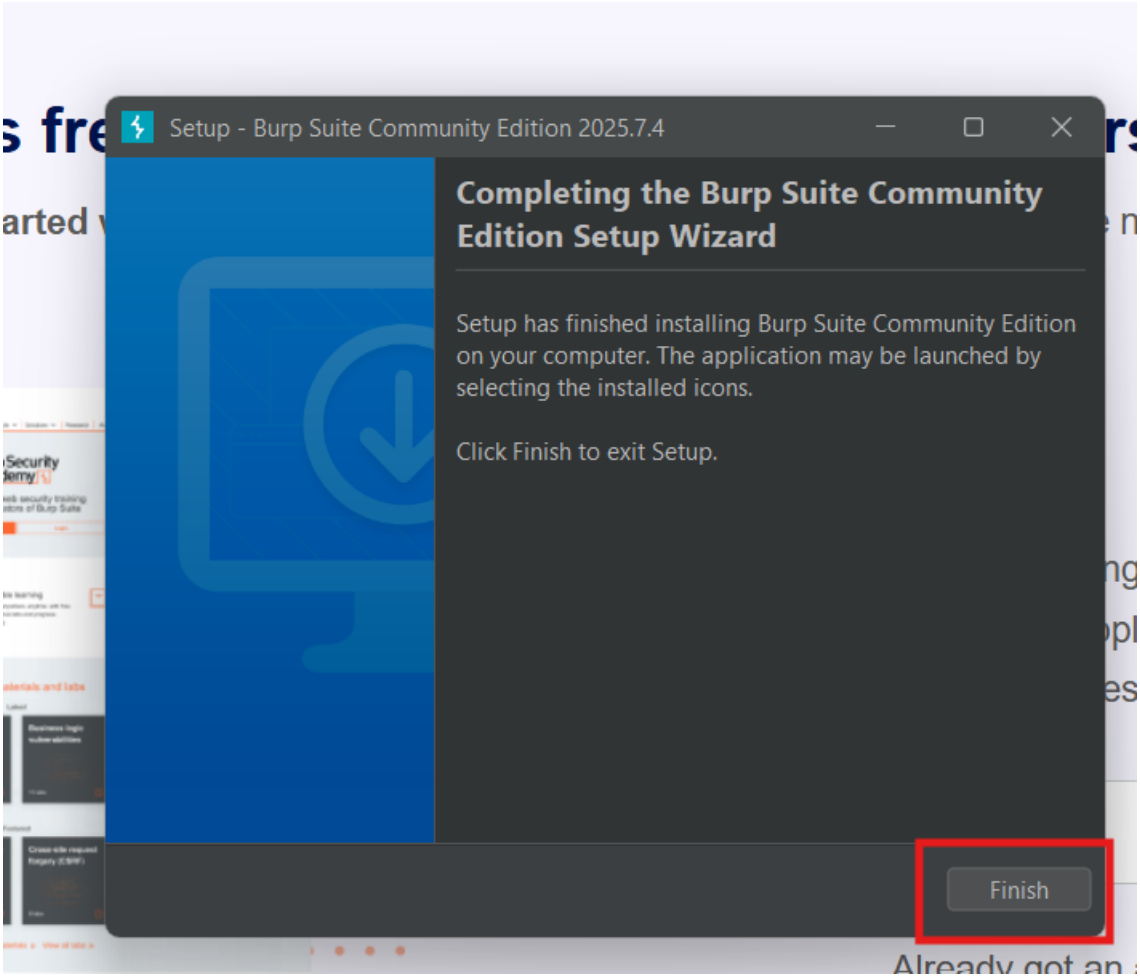
- You will see options for Community Edition (Free).
- Click Download for Windows (.exe installer).
- Wait for the file to download (usually named something like burpsuite_community_windows-x64.exe).


portswigger.net/burp/community-download-thank-you
Products
Solutions
Research
Academy
Support
Your download should start automatically. Didn't work? Try downloading again.
Setup - Burp Suite Community Edition 2025.7.4
Welcome to the Burp Suite Community Edition Setup Wizard
This will install Burp Suite Community Edition on your computer. The wizard will lead you step by step through the installation.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel
Want to access fre
rs of Burp Suite?
Get started with the Web Security Academy now to take your skills to the next level.
Search
ENG
IN
12:44
03-09-2025


portswigger.net/burp/community-download-thank-you
Products
Solutions
Research
Academy
Support
Your download should start automatically. Didn't work? Try downloading again.
Setup - Burp Suite Community Edition 2025.7.4
Select Destination Directory
Where should Burp Suite Community Edition be installed?
Select the folder where you would like Burp Suite Community Edition to be installed, then click Next.
C:\Users\rajna\AppData\Local\Programs\BurpSuiteCommunity
Browse ...
Required disk space: 439 MB
Free disk space: 154 GB
< Back
Next >
Cancel
Want to access fre
rs of Burp Suite?
Get started with the Web Security Academy now to take your skills to the next level.
Greenshot
Greenshot
Exported to: Save as (displaying dialog)
Search
ENG
IN
12:44
03-09-2025

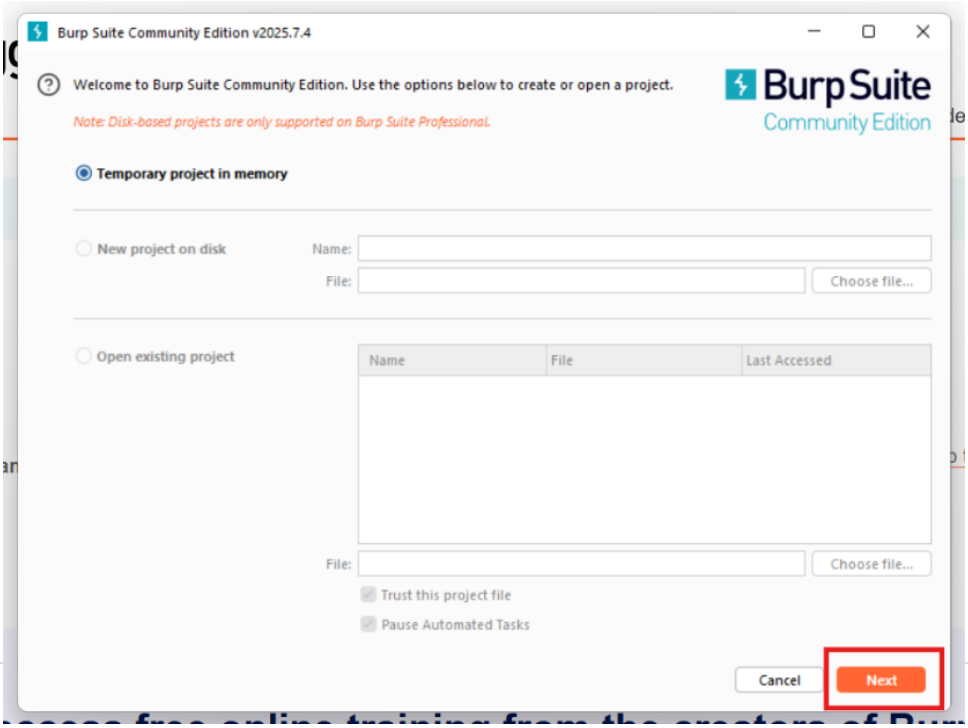

portswigger.net/burp/community-download-thank-you
Products
Solutions
Research
Academy
Support
Your download should start automatically. Didn't work? Try downloading again.
Setup - Burp Suite Community Edition 2025.7.4
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Select the Start Menu folder in which you would like Setup to create the program's shortcuts, then click Next.
Create a Start Menu folder
Burp Suite Community Edition
Accessibility
Accessories
Acunetix 11 Trial
Administrative Tools
Anaconda (anaconda3)
AutoCAD 2025 - English
Autodesk
CATIA P3
< Back
Next >
Cancel
Thanks for download
Want to access fre
rs of Burp Suite?
Get started with the Web Security Academy now to take your skills to the next level.
Search
ENG
IN
12:46
03-09-2025


portswigger.net/burp/community-download-thank-you
Products
Solutions
Research
Academy
Support
Your download should start automatically. Didn't work? Try downloading again.
Setup - Burp Suite Community Edition 2025.7.4
Installing
Please wait while Setup installs Burp Suite Community Edition on your computer.
Extracting files ...
Cancel
Thanks for download
Want to access fre
rs of Burp Suite?
Get started with the Web Security Academy now to take your skills to the next level.
Greenshot
Greenshot
Exported to: Save as (displaying dialog)
Search
ENG
IN
12:46
03-09-2025

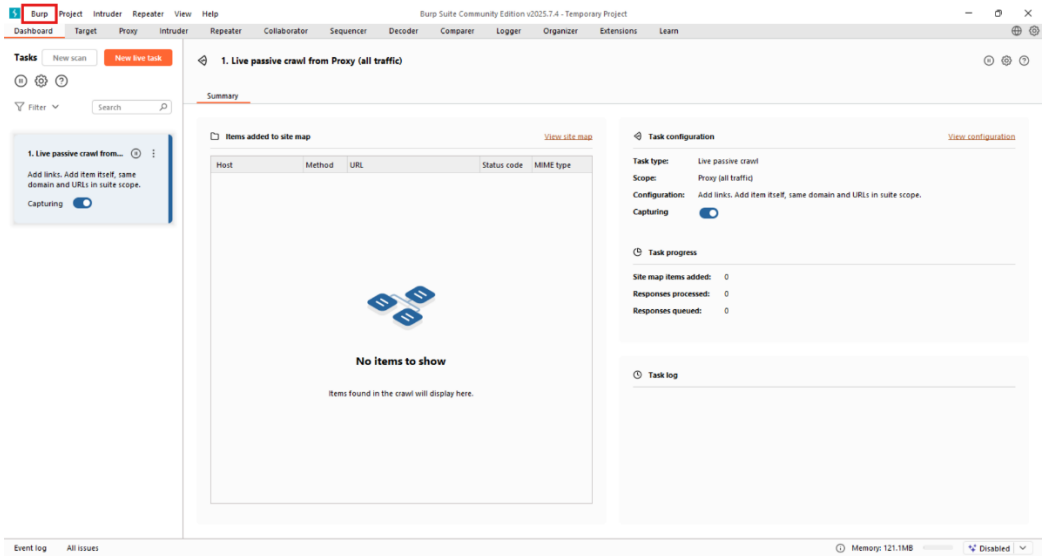


- After processing all installation process, we start burp suite.

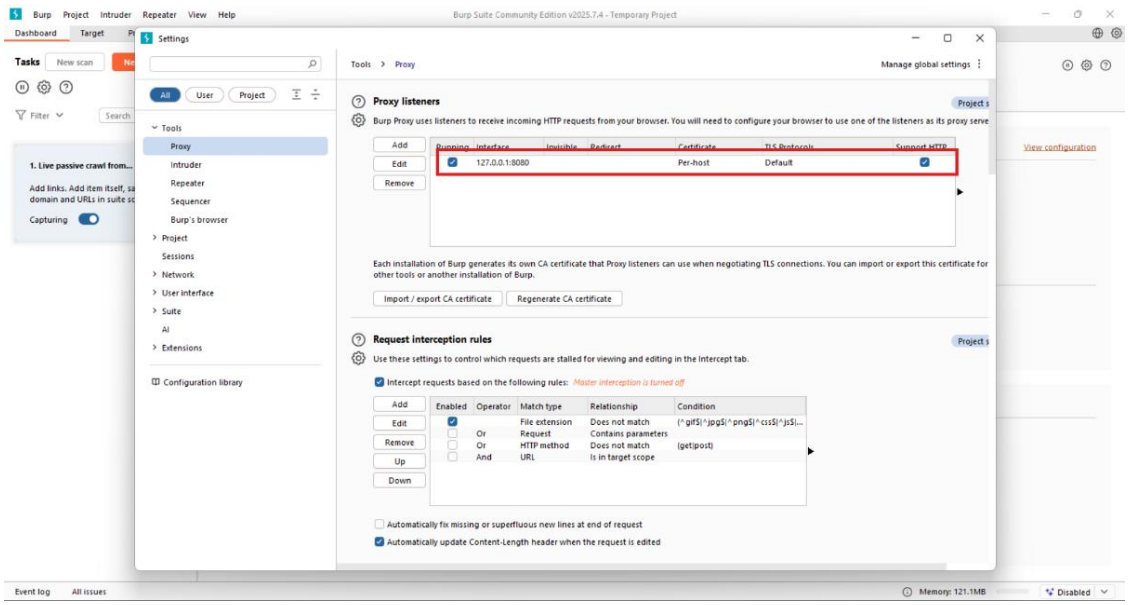
- Let's Start Burp suite.

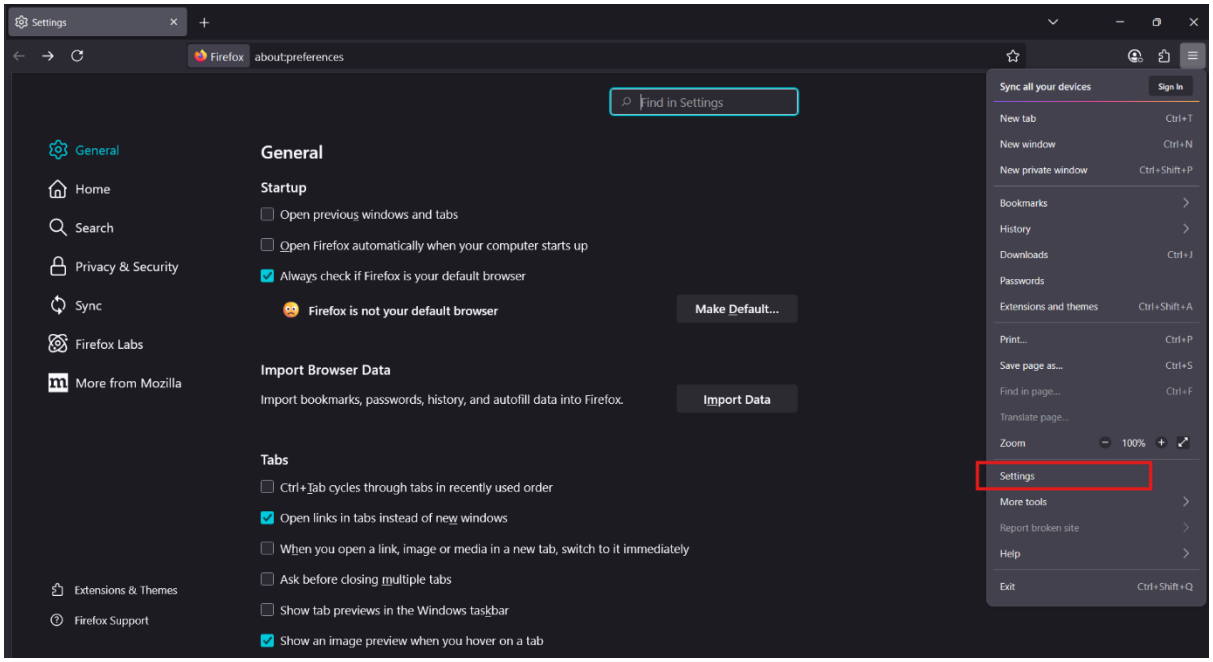


- Click on the burp and enter into a settings.

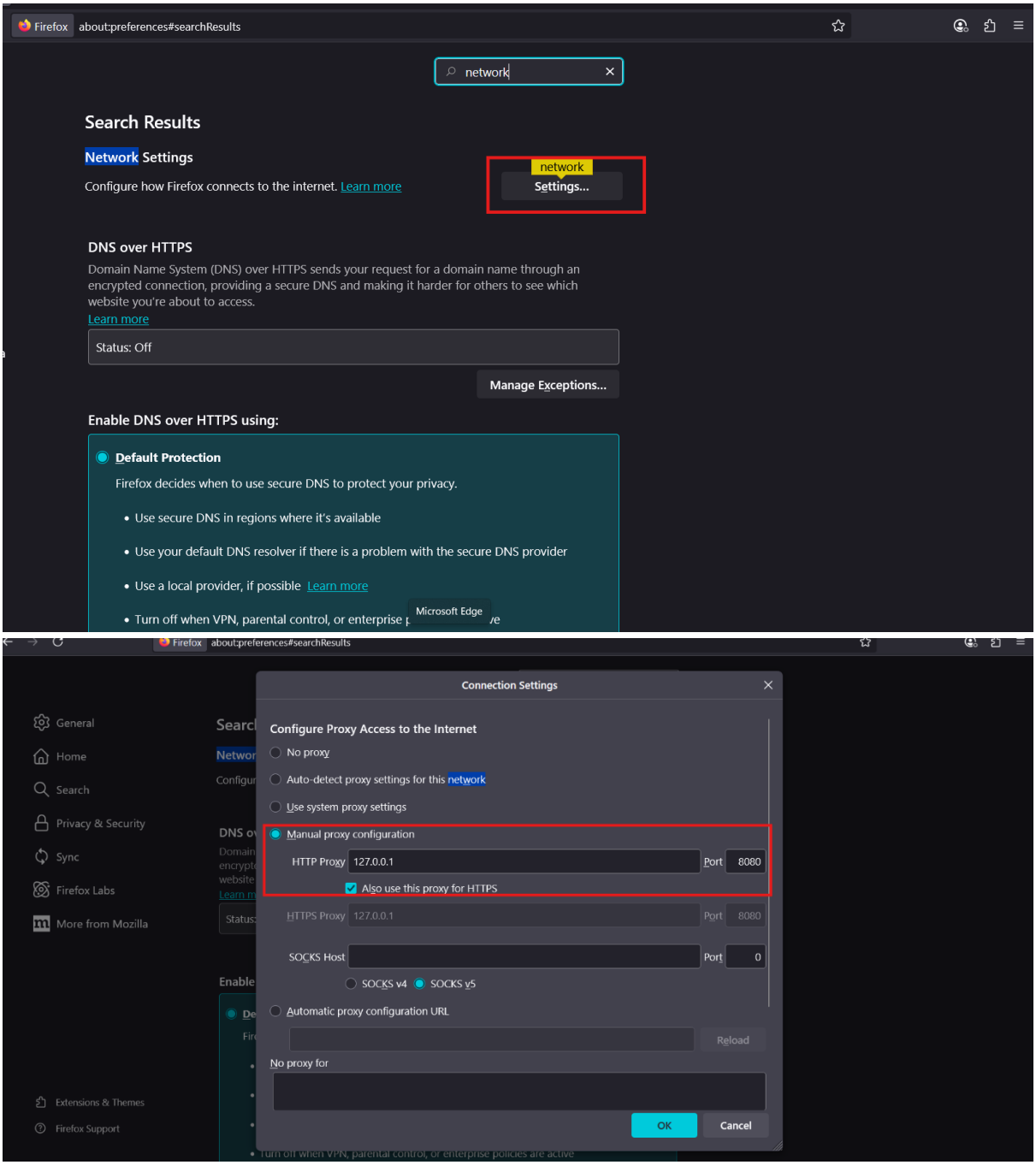


- We have to give that same ip and port as a proxy in the browser.

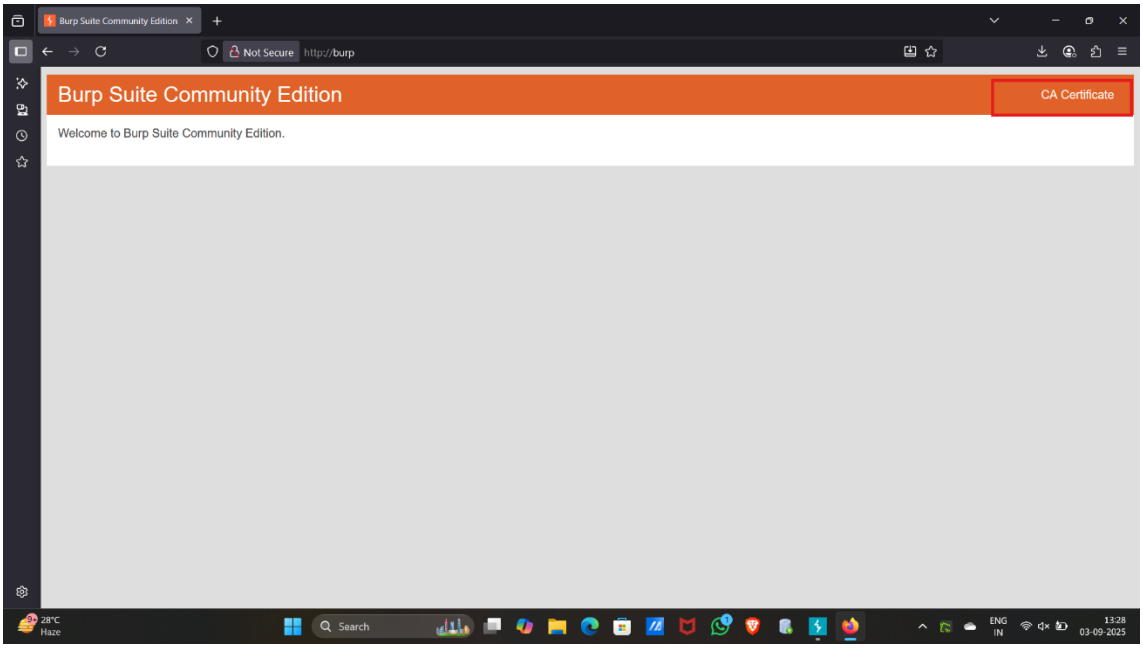


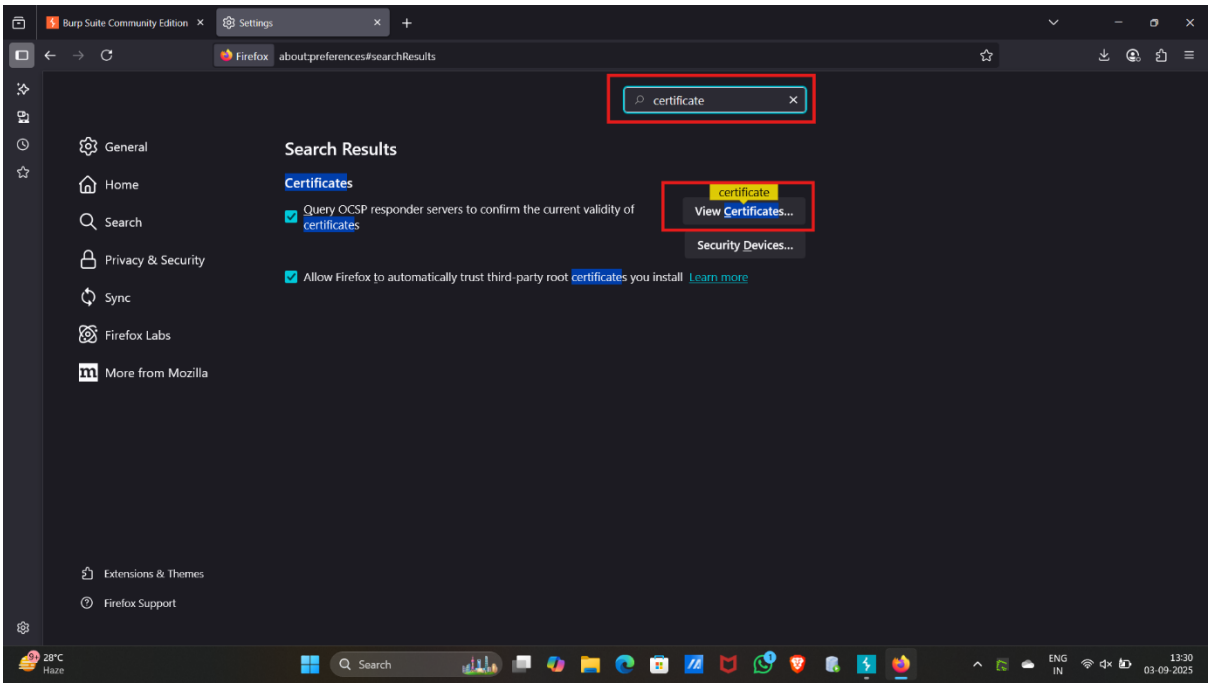


- Open the firefox and go to the settings.
- Search for Network and click network settings.
-

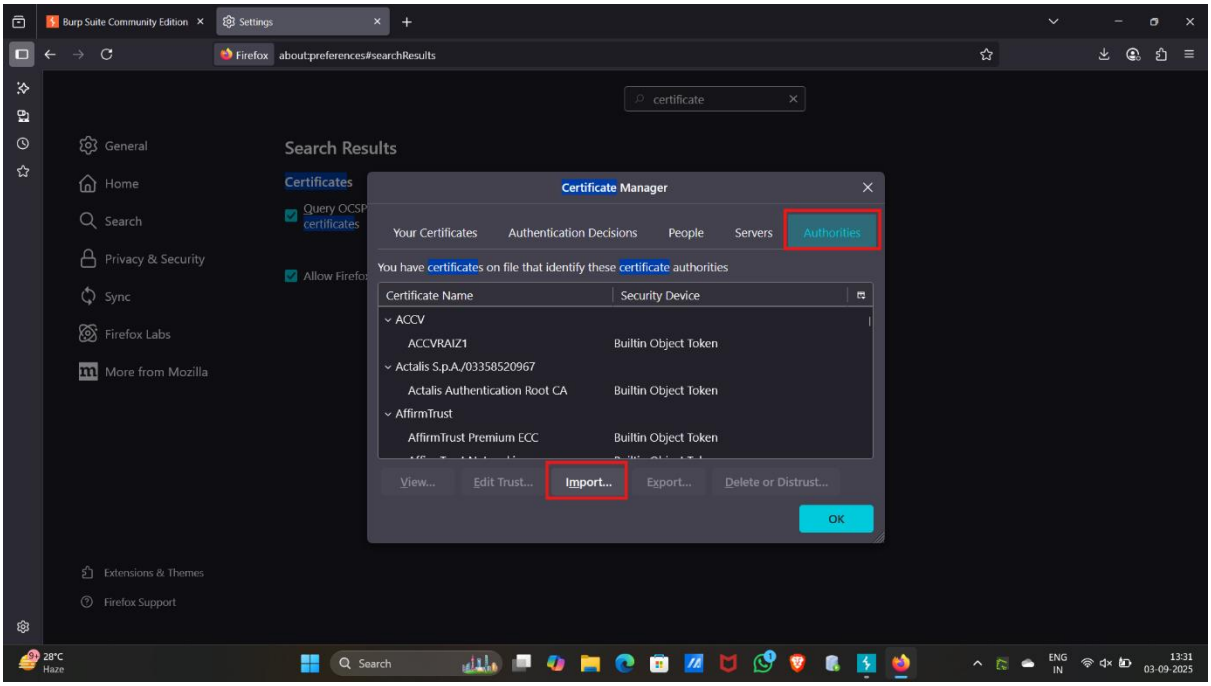


- Click on the Manual Proxy configuration settings give loop ip and port.
- In browser go through this link http://burp
- After going through this link click on CA certificate.

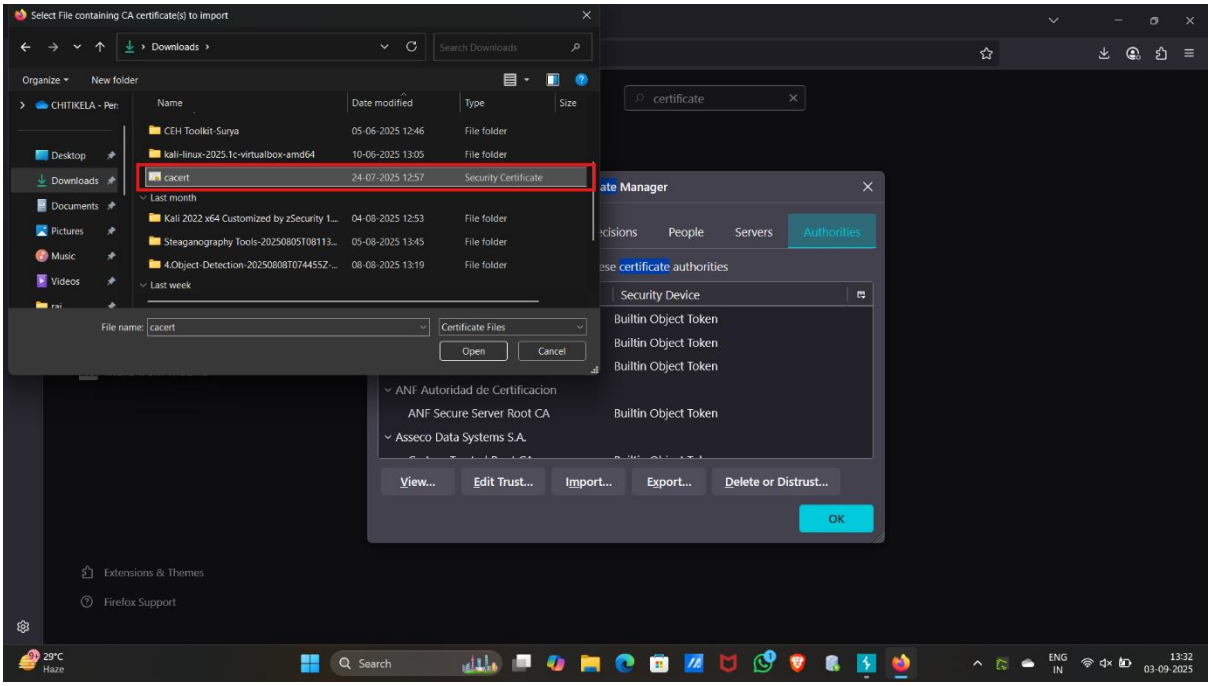




- After downloading the CA certificate go to settings and search certificate then click on view certificates.
- Go through the Authorities and click on import.



- Import the CA certificate that you have been downloaded.



- After importing the CA certificate burp suite ready to perform WAPT framework.

SQL INJECTION :

What is SQL Injection (SQLi)?

SQL Injection is a **web vulnerability** that happens when an application doesn't properly validate user input before sending it to a database.
An attacker can inject **malicious SQL queries** into input fields (like login forms, search bars, or URL parameters) to:

- View sensitive data (users, passwords, credit cards).
- Modify or delete database records.
- Bypass authentication.
- Even take control of the server in severe cases.

Example

A normal query:

SELECT * FROM users WHERE username = 'john' AND password = '1234';

If input isn't sanitized, an attacker can enter:

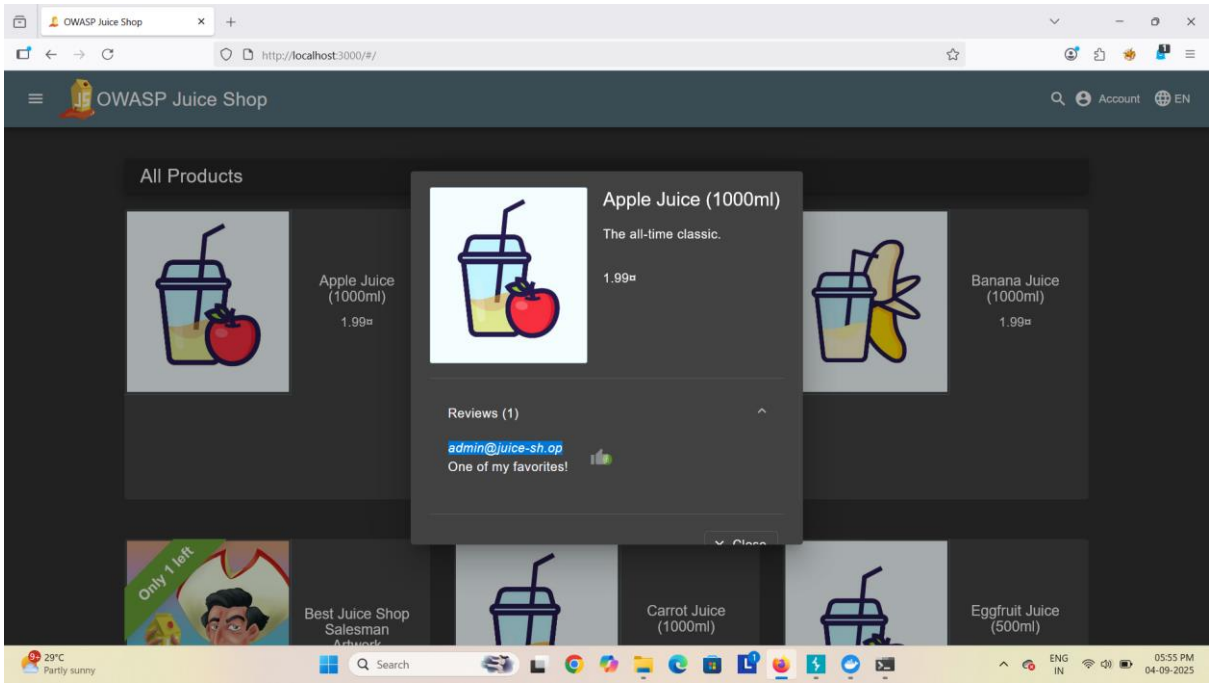
' OR '1'='1--

Resulting query:

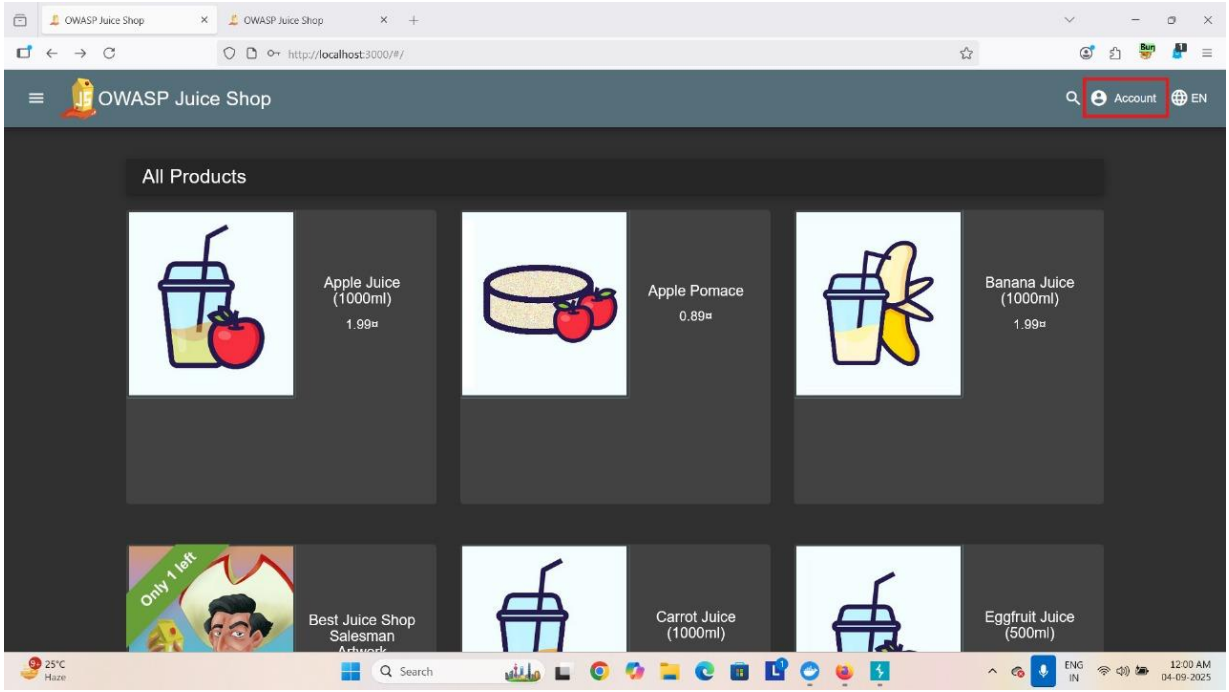
SELECT * FROM users WHERE username = '' OR '1'='1--' AND password = '';

This always returns **true**, letting the attacker **bypass login**.

- Open your web browser and go to OWASP Juice shope website: https://demo.owasp-juice.shop/#/

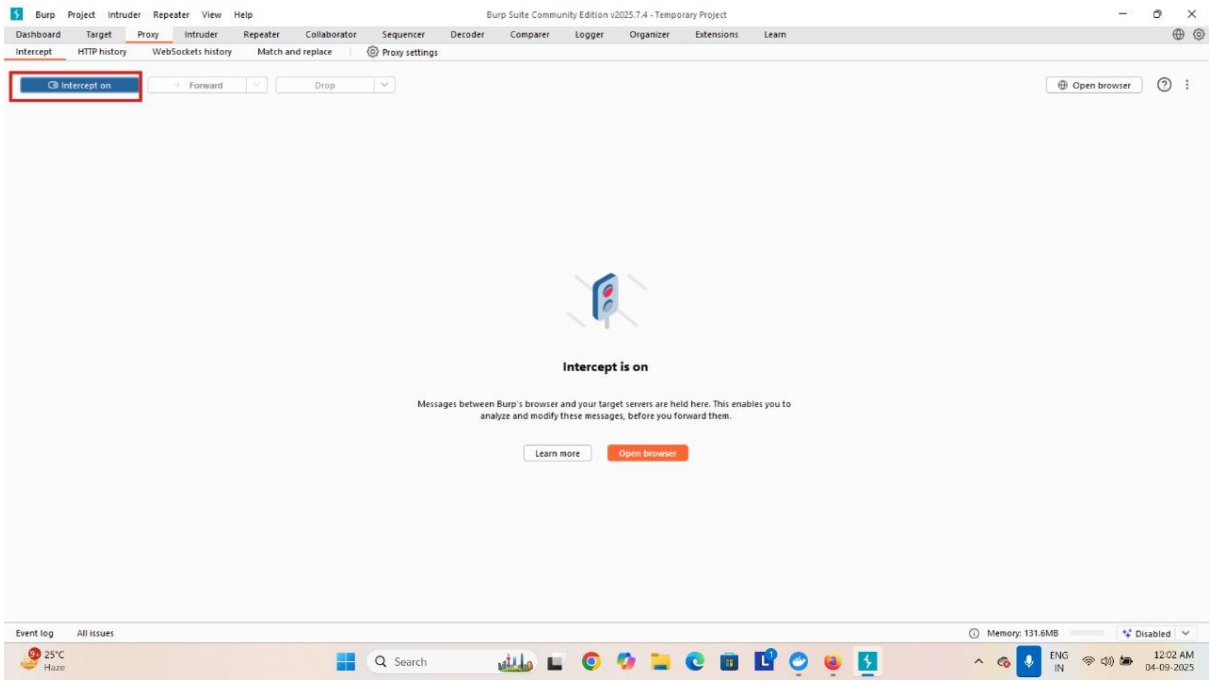


- Click on apple juice and copy “admin@juice-sh.op”

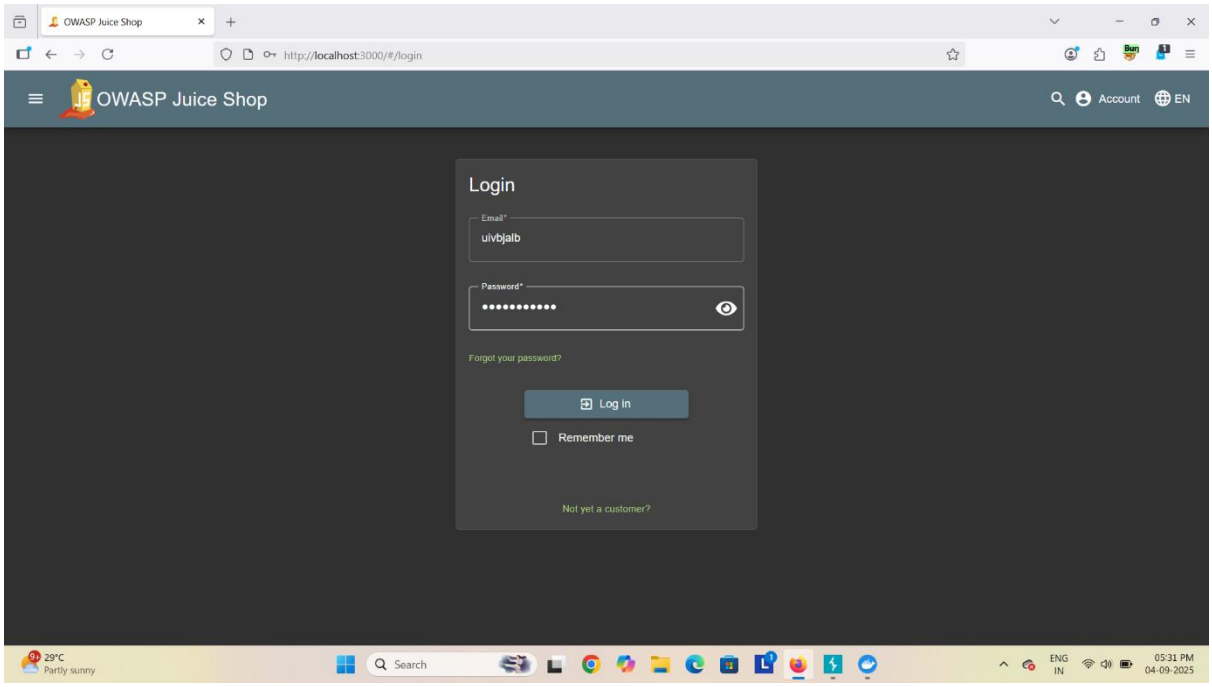


- Click on Account and get into a login page

- In Burp Suite we should enable the “Intercept on”

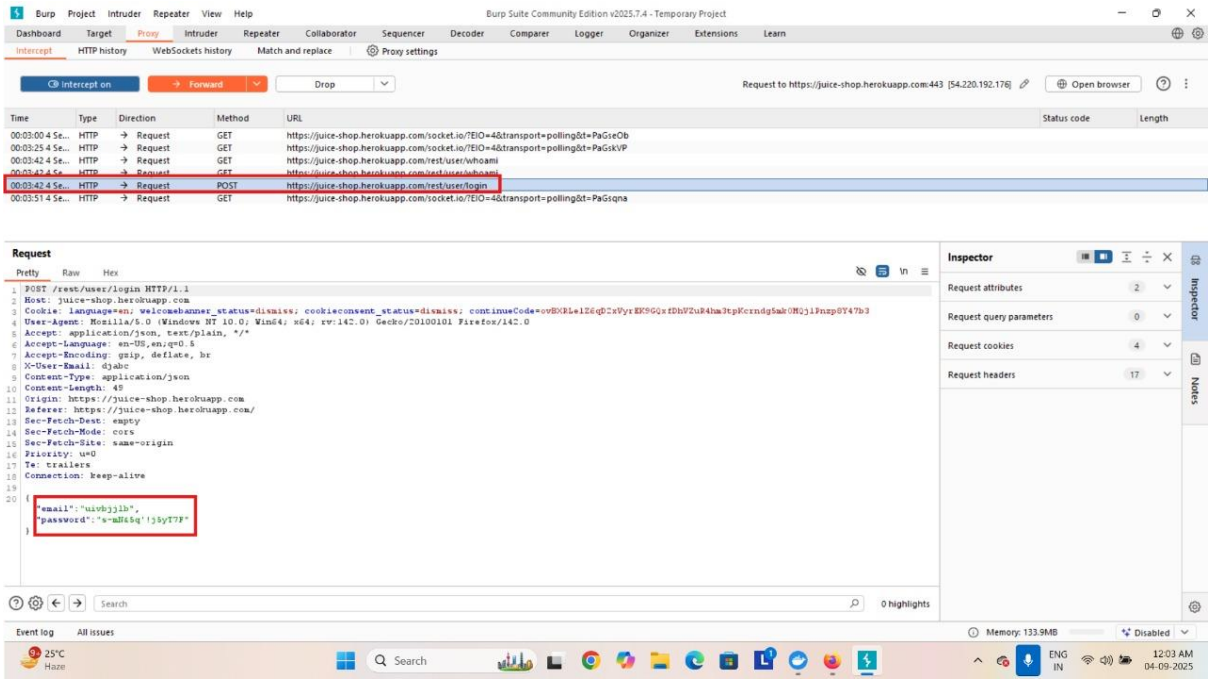


- After that again go to OWASP juice Shope login page

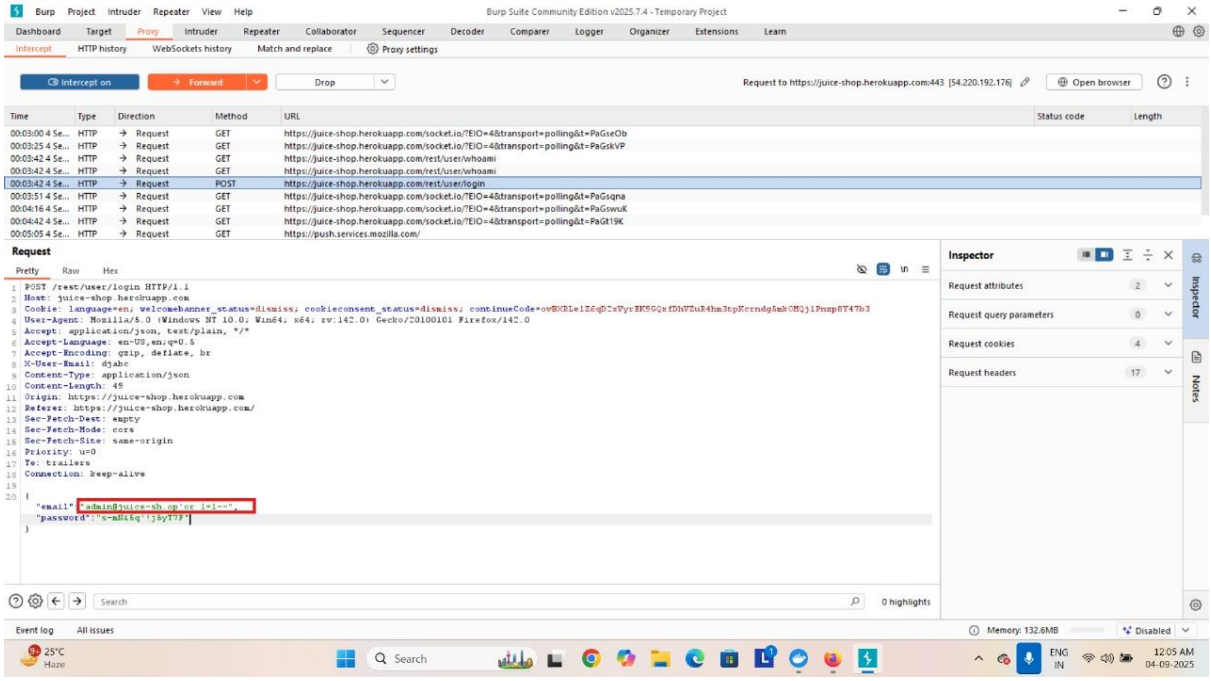


- In OWASP Juice shop login page give any credential and click on login

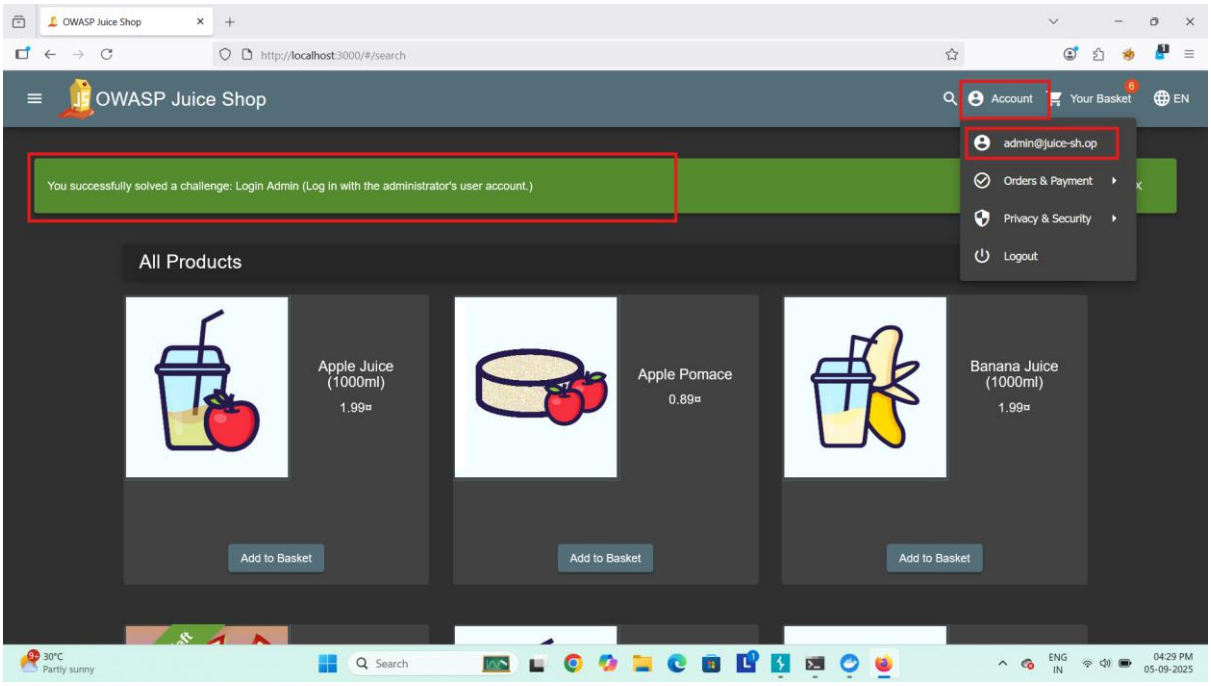
- In Burp suite we received some packets



In that packets find the login packet and click on it then we get to see that credential we have given in login page



- Now we have to edit the email ,from apple juice we had copy "admin@juice-sh.op" ,at the end of the "admin@juice-sh.op" we will give SQL query ' OR 1=1--
- Now we will forward the after editing the email and turn off the intercept

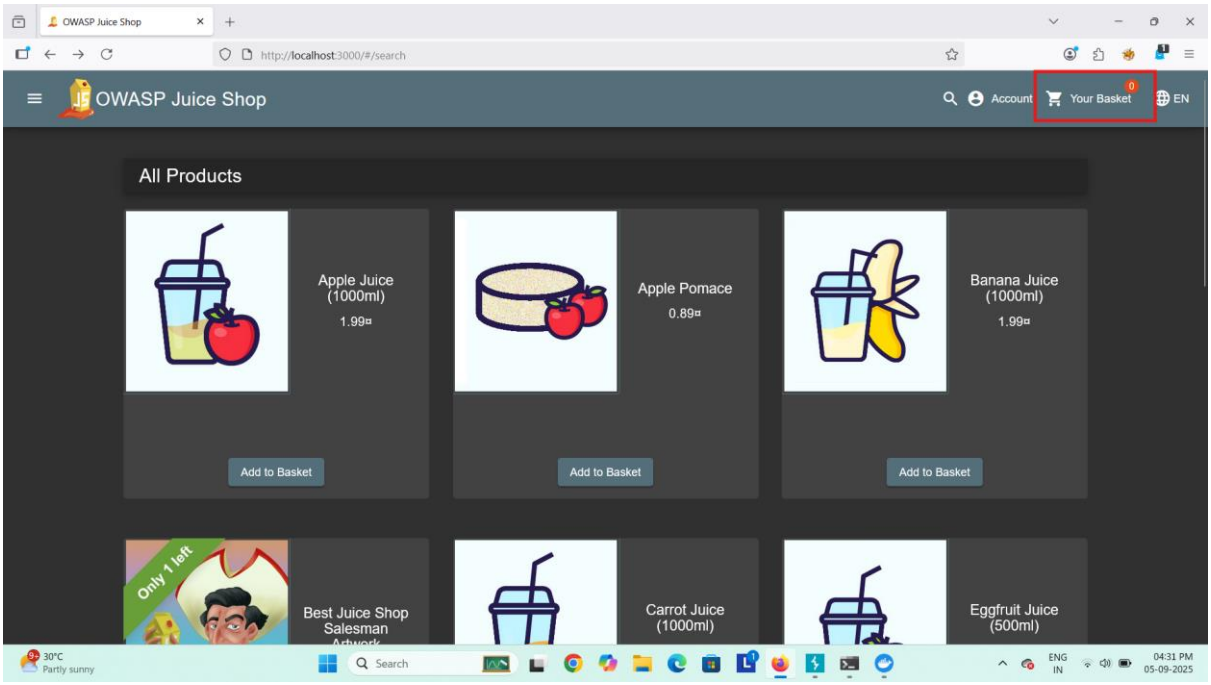


- The forward request confirms that the login was successful.
- Here, we can see that we have successfully login
- So our SQL injection is successfully performed.

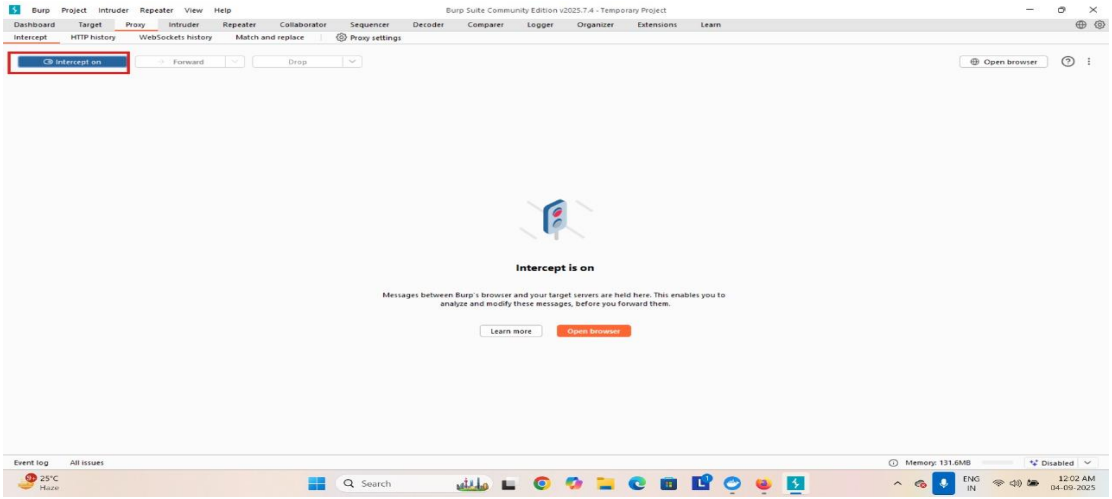
Broken Access Control

Broken Access Control happens when a web application does not properly enforce what users are allowed to do. This means attackers can gain unauthorized access to data or functions.

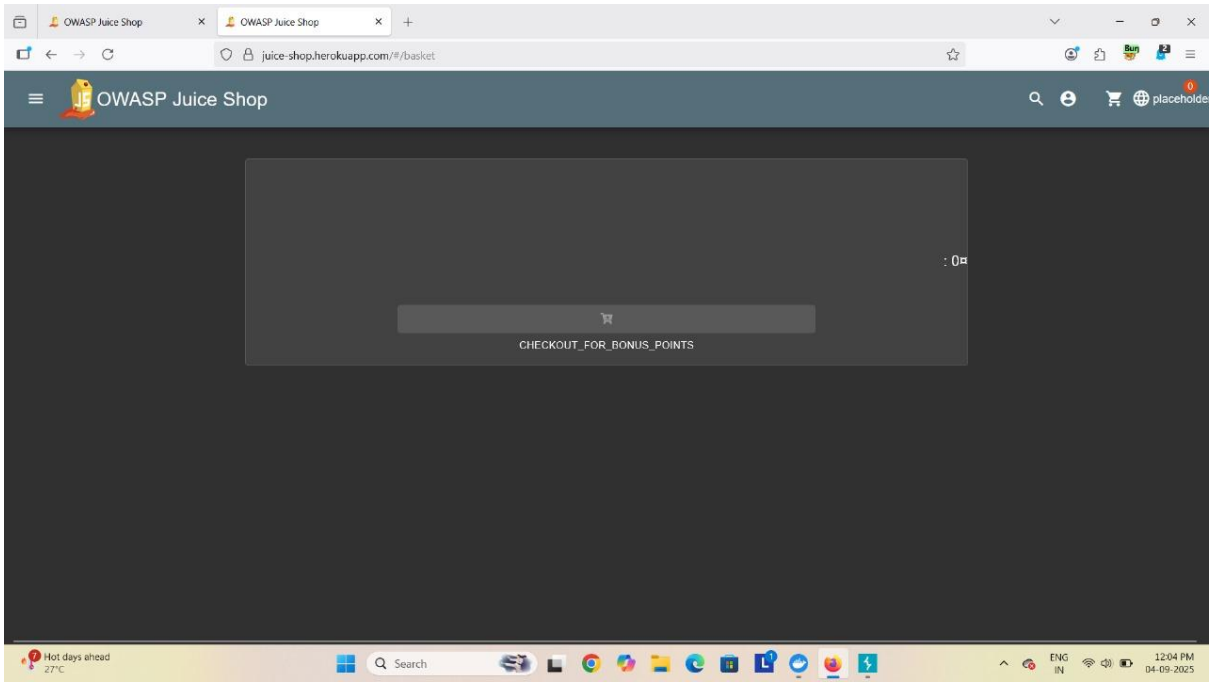
- Viewing other users' sensitive information.
- Modifying or deleting someone else's data.
- Accessing admin-only features without permission.



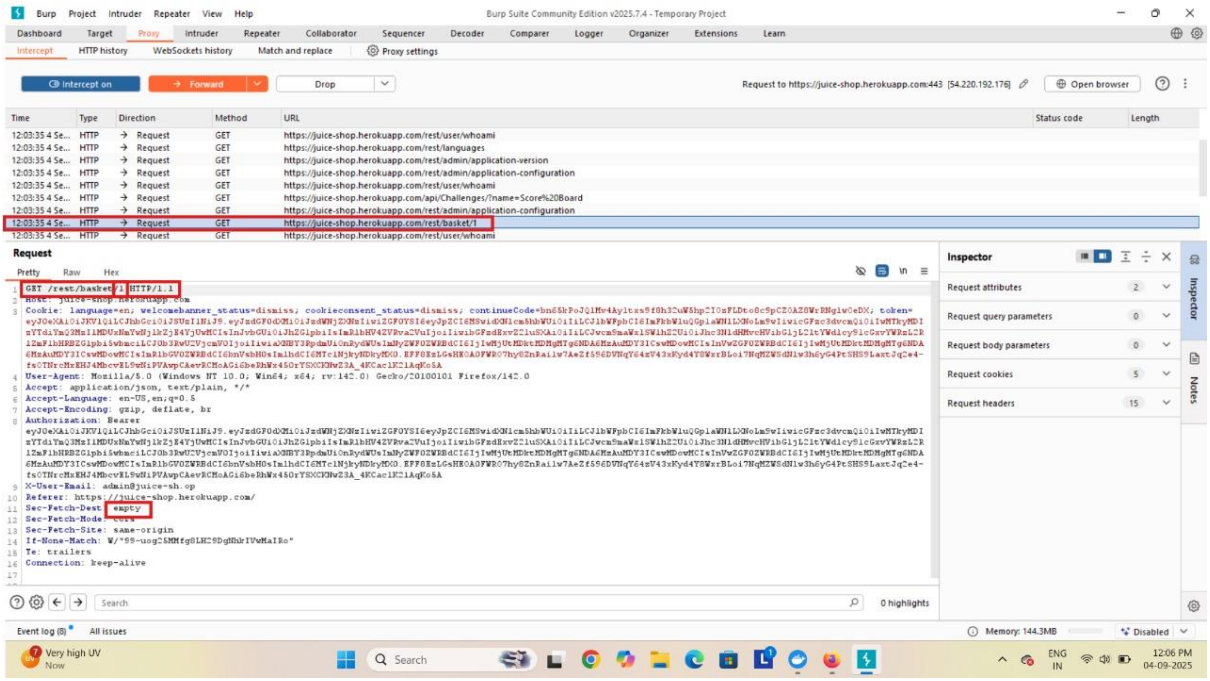
- Open your web browser and go to OWASP Juice shope website: https://demo.owasp-juice.shop/#/
- Click on Your Basket



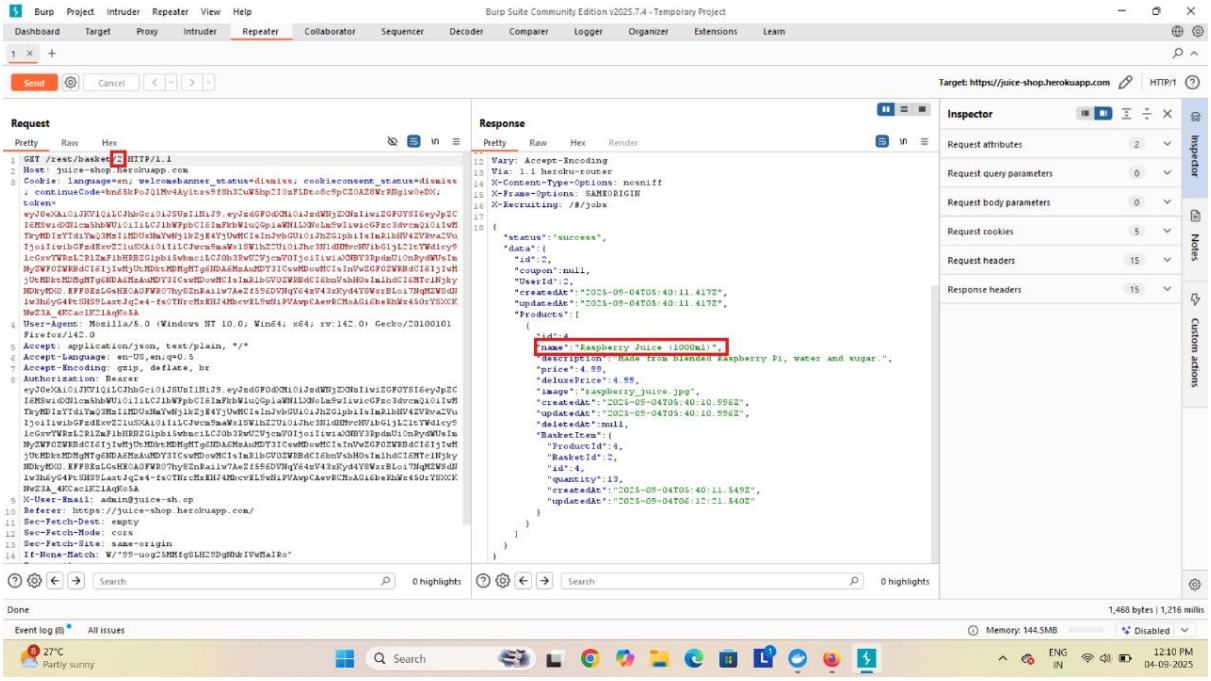
- Turn on the intercept on in Burp Suite



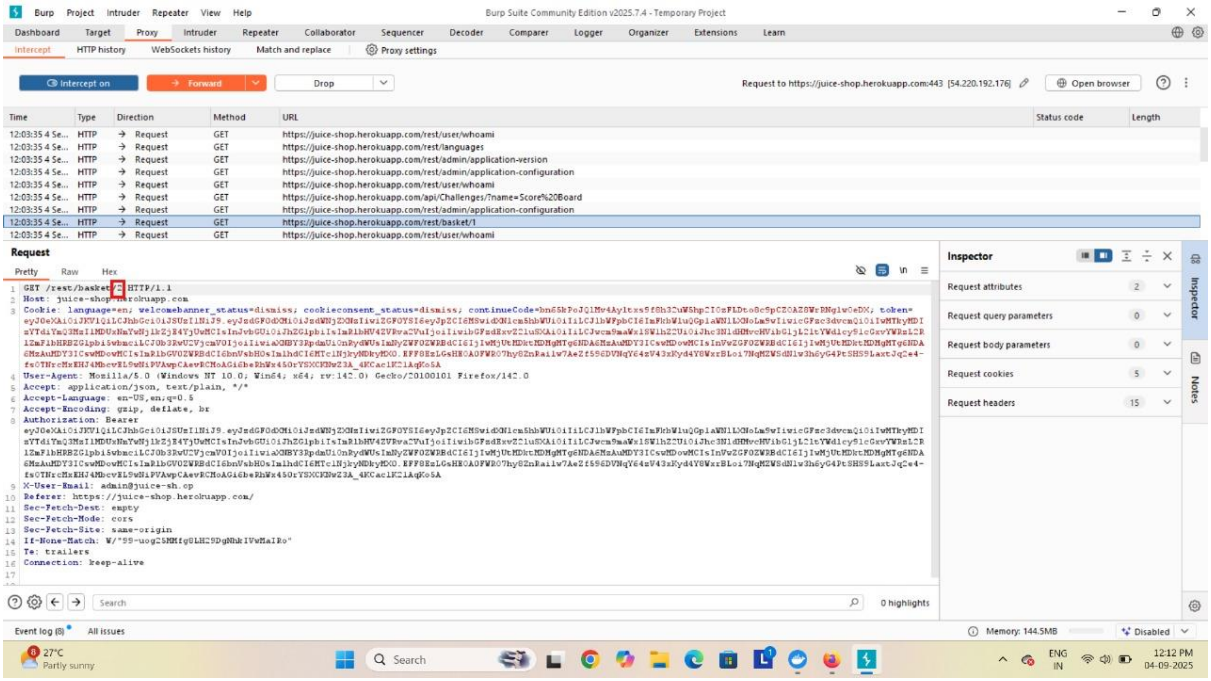
- In our basket there are no item



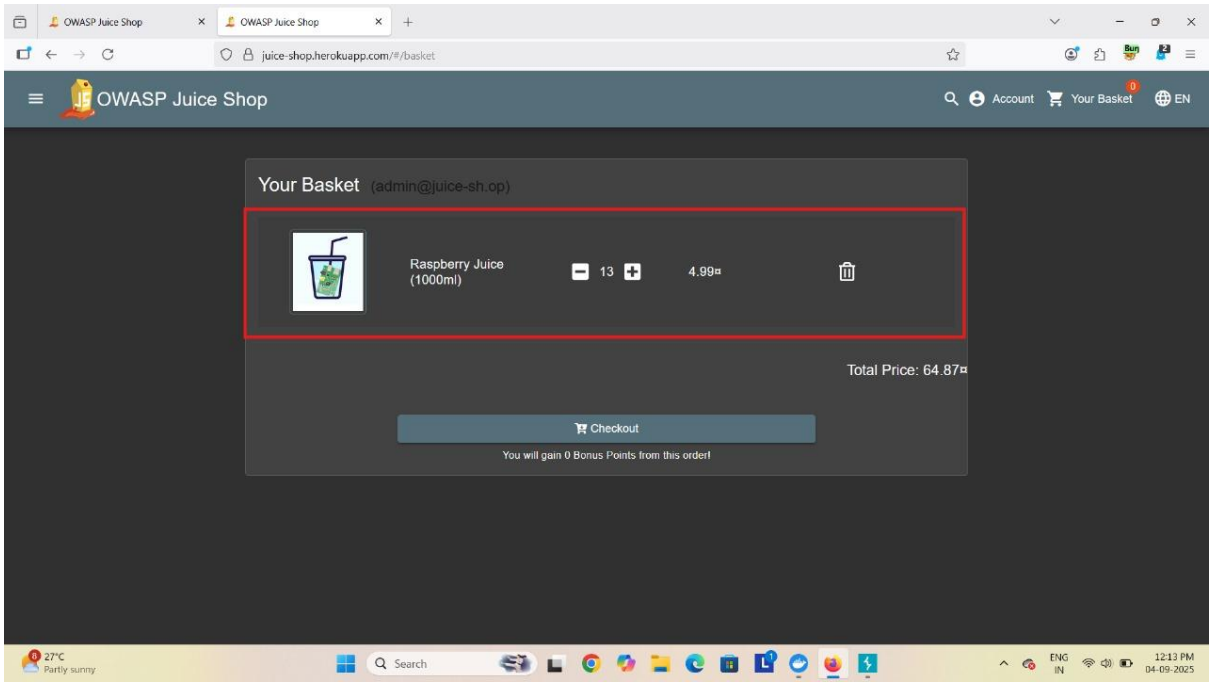
- Now we see that we get some packets .
- In that packets we check for basket packet.
- In basket packet our token no is 1 and our basket is empty
- Now we will send this packet to the repeater



- In repeterwe will change our token as 2 and click on send.
- Now we get to see that in 2 token basket we have one item " Raspberry juice".



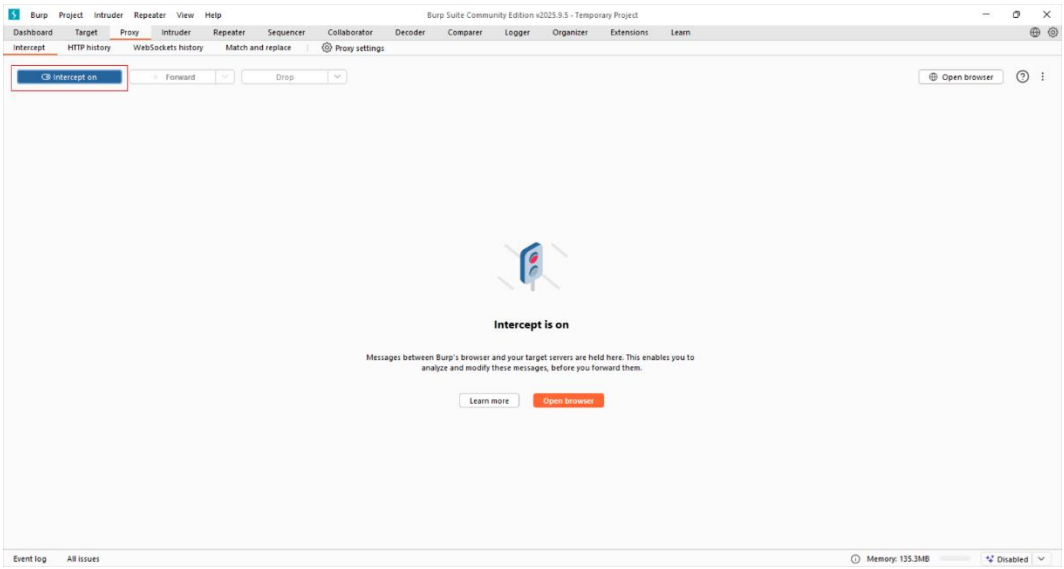
- We come back to the proxy and change a token as 2 and forward that packet .
- Then we turn off our intercept



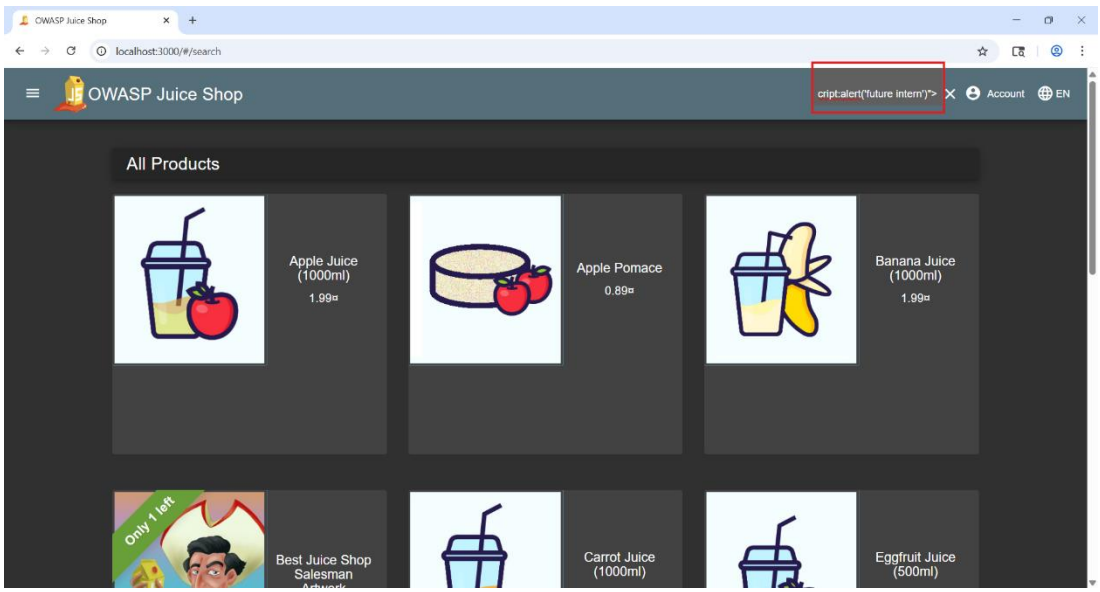
- So in our basket we get to see that 2 token item
- So we have successfully perform broken access control

Cross- Site Scripting (XSS)

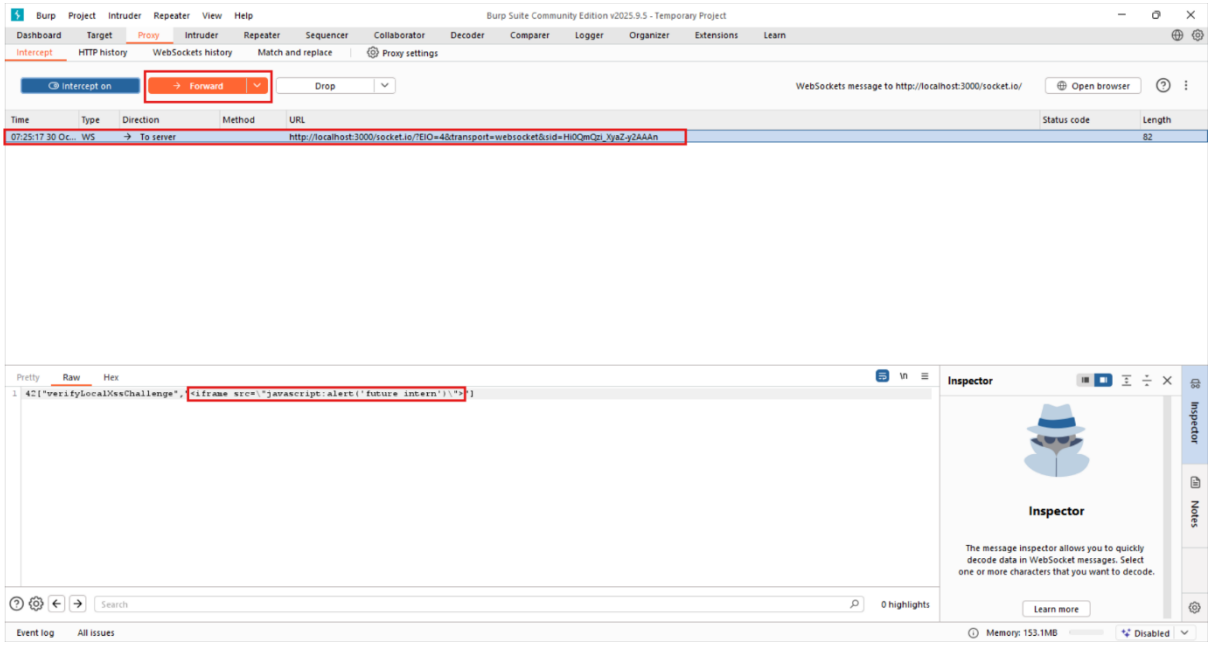
Cross-Site Scripting (XSS) is a type of security vulnerability found in web applications. It allows attackers to inject malicious scripts (usually JavaScript) into web pages that are viewed by other users. When the malicious script runs in a victim's browser, it can steal cookies, session tokens, or other sensitive information, manipulate the DOM, or redirect the user to malicious sites.



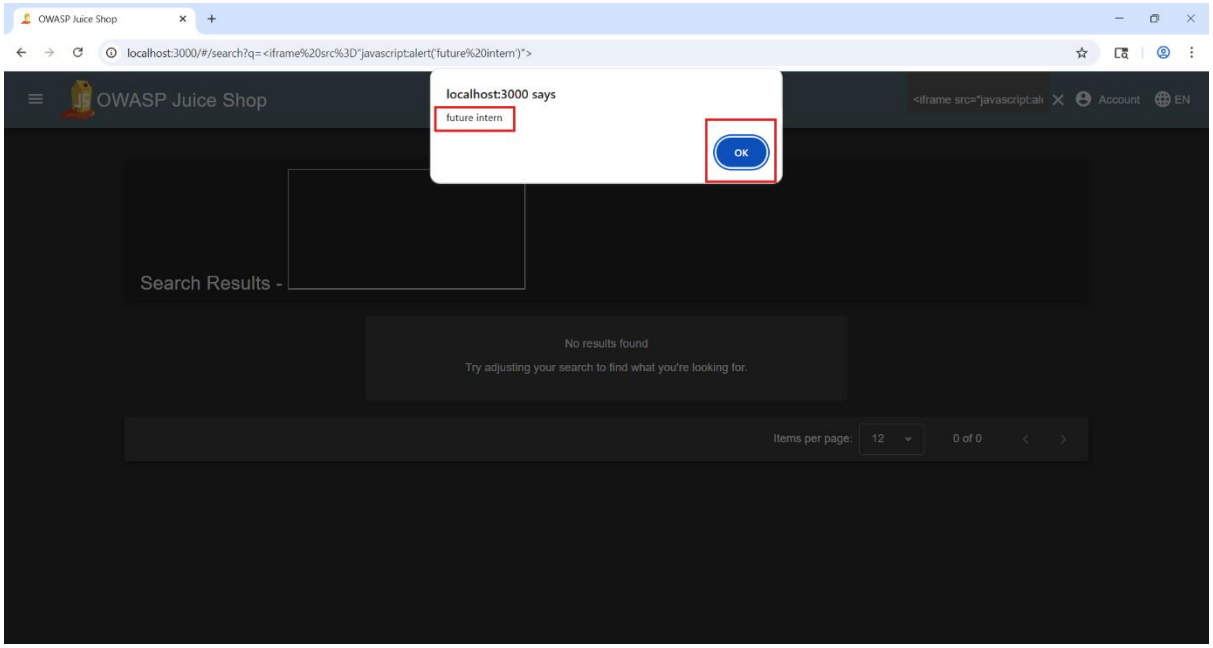
- In burp Suite turn on the intercept



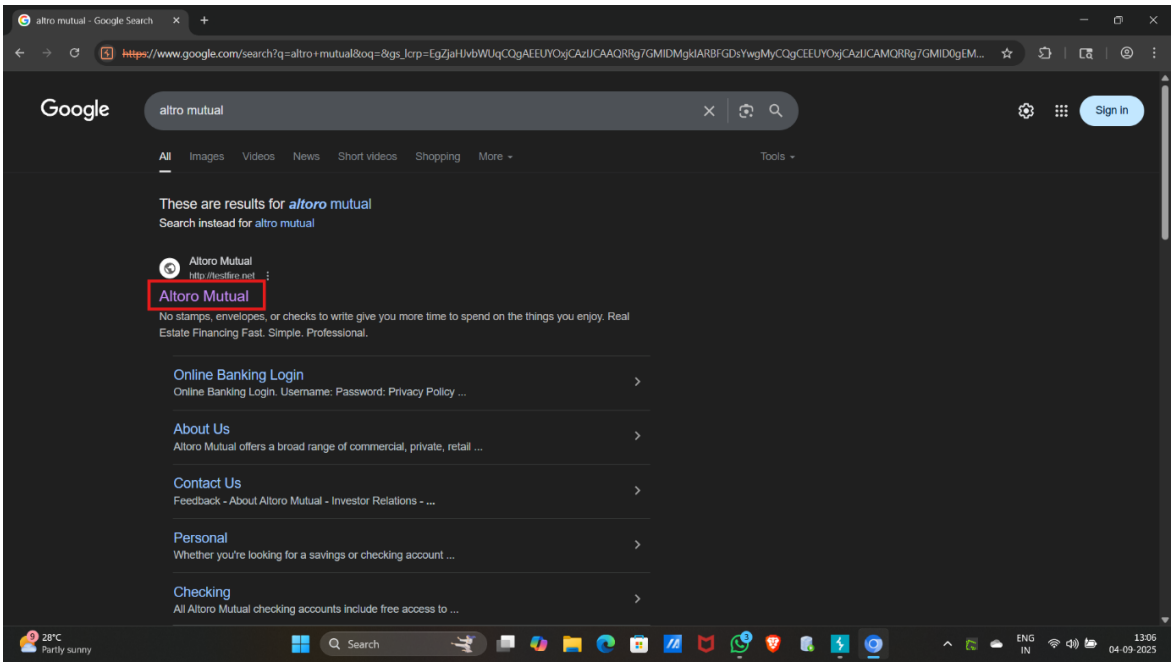
- In search bar write a script <iframe src= “javascript:alert(‘future interns’)”>
- In burp suite we received packets.



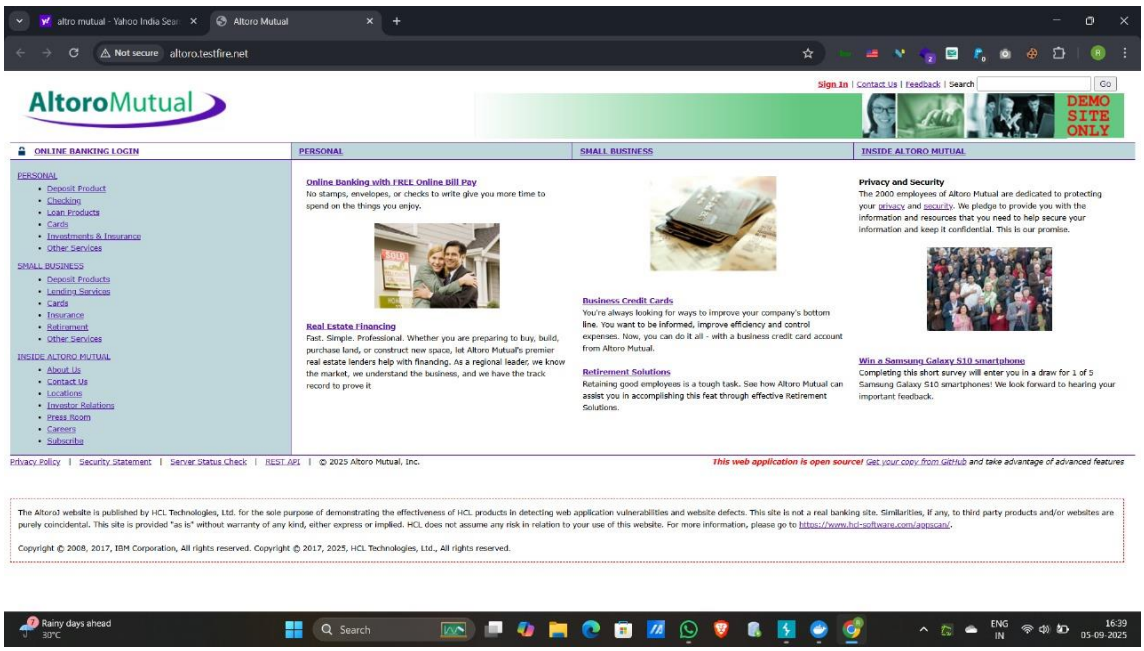
- Find the packet and click on that, now we will see the query.
- Now forward the packet and turnoff intercept.



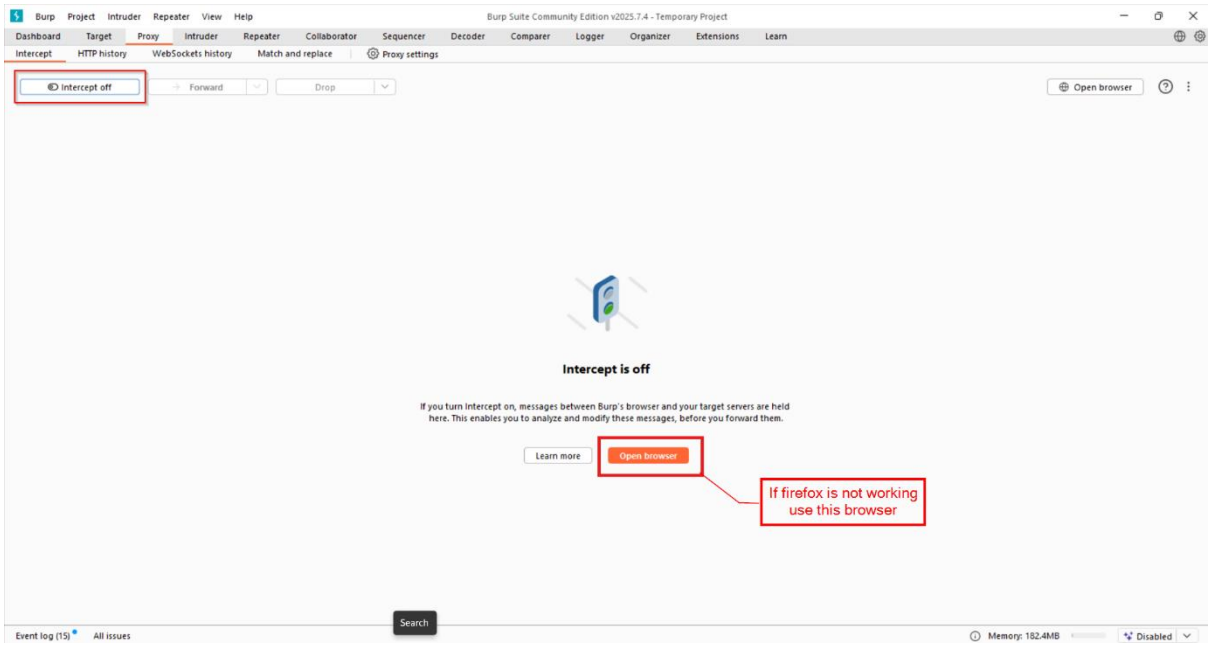
- We can see alert pop up in web application, so it is vulnerable web site.
- We successfully perform cross-site script.



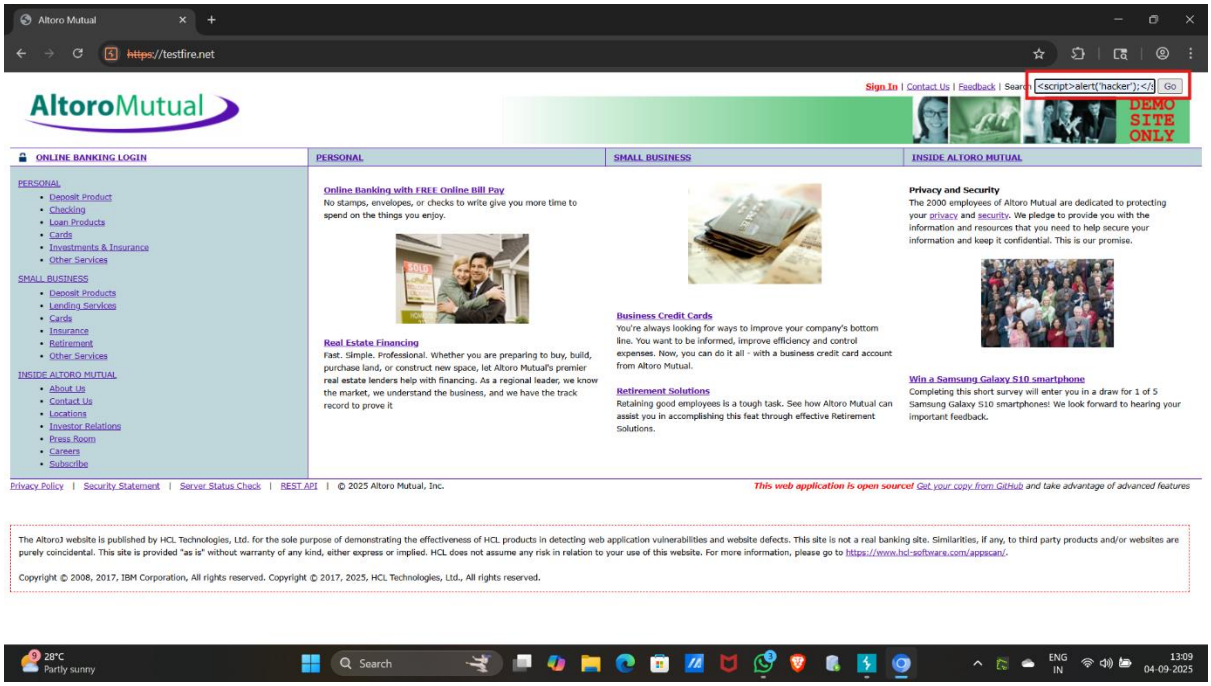
- Open your browser and go to web site http://altoro.testfire.net/



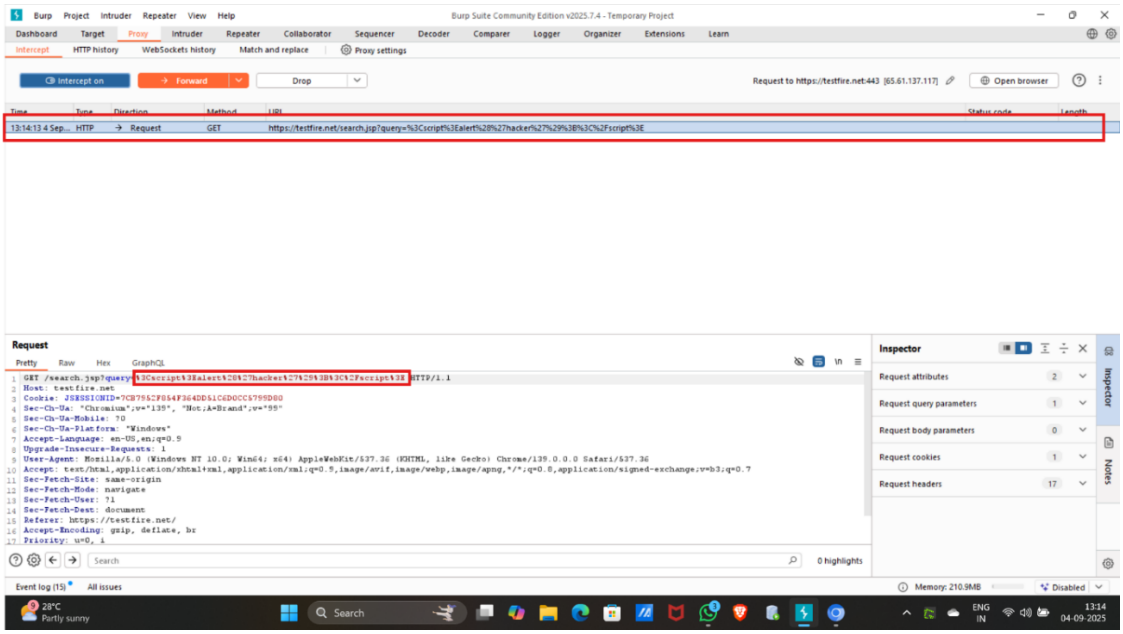
- In burp Suite turn on the intercept



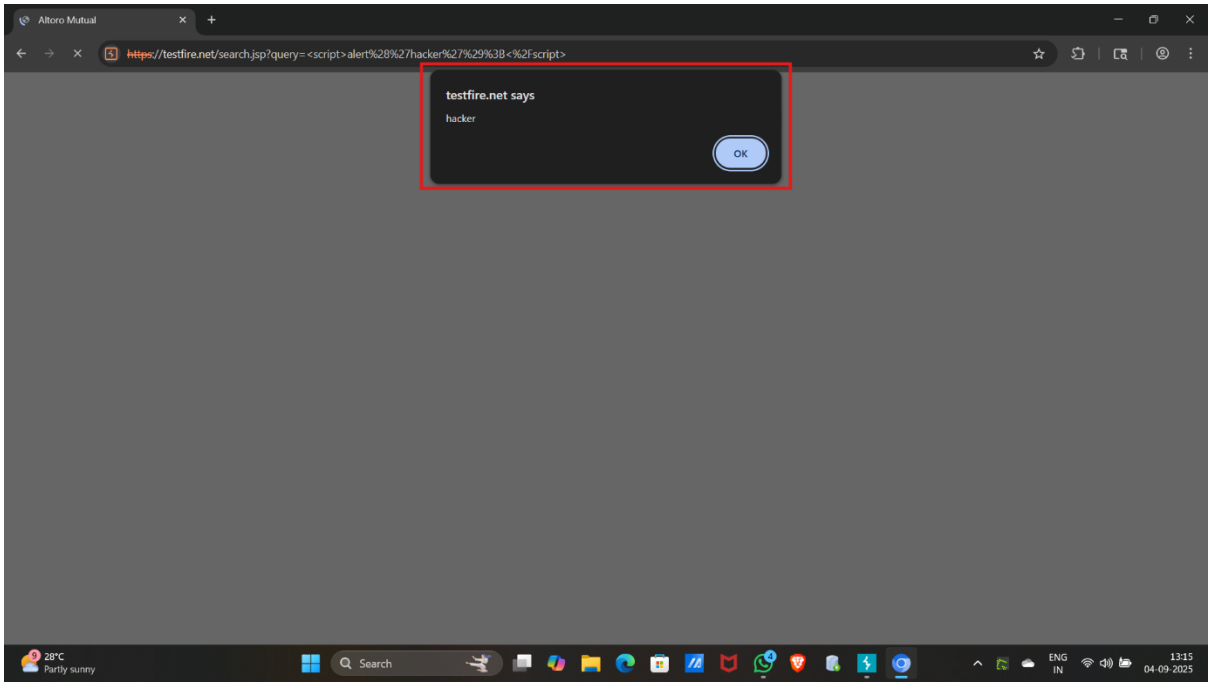
- Atter that again go to Altro mutual home page.



- In search bar write a script “<script>alert(‘hacker’)</script> ”
- In burp suite we received packets.



- Find the packet and click on that, now we will see the query.
- Now forward the packet and turnoff intercept.

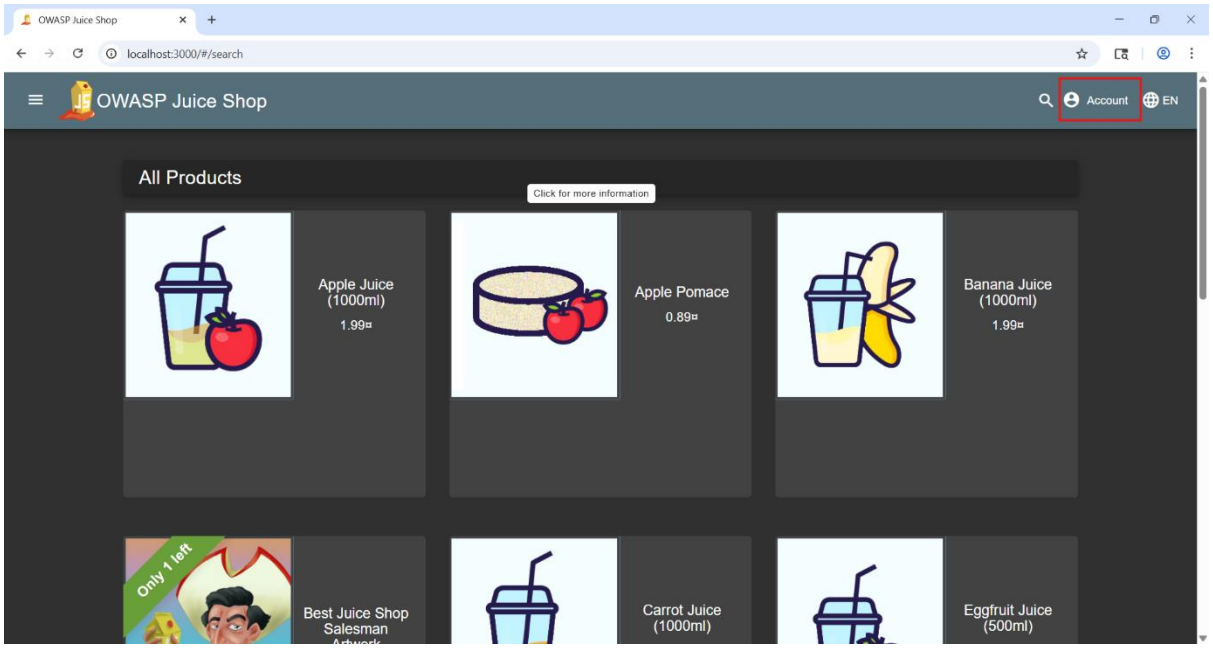


- We can see alert pop up in web application, so it is vulnerable web site.
- We successfully perform cross-site script.

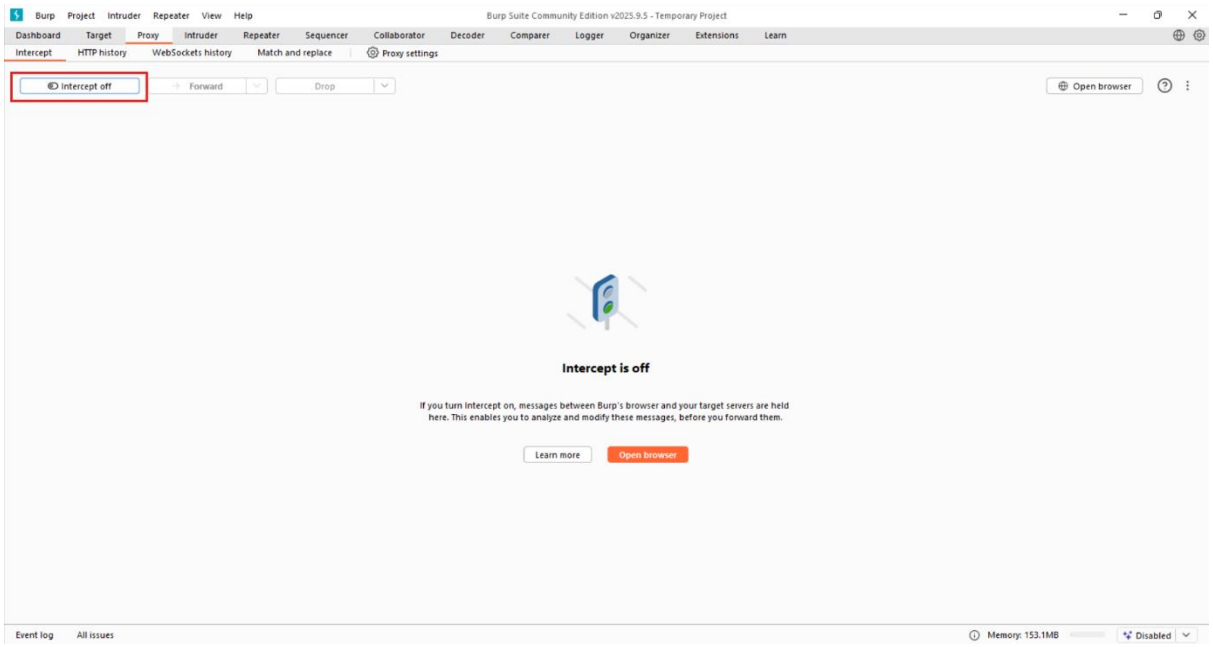
Identification & Authentication Failure

Identification & Authentication Failure is a security vulnerability that occurs when a system does not properly verify the identity of users or services, allowing unauthorized access.

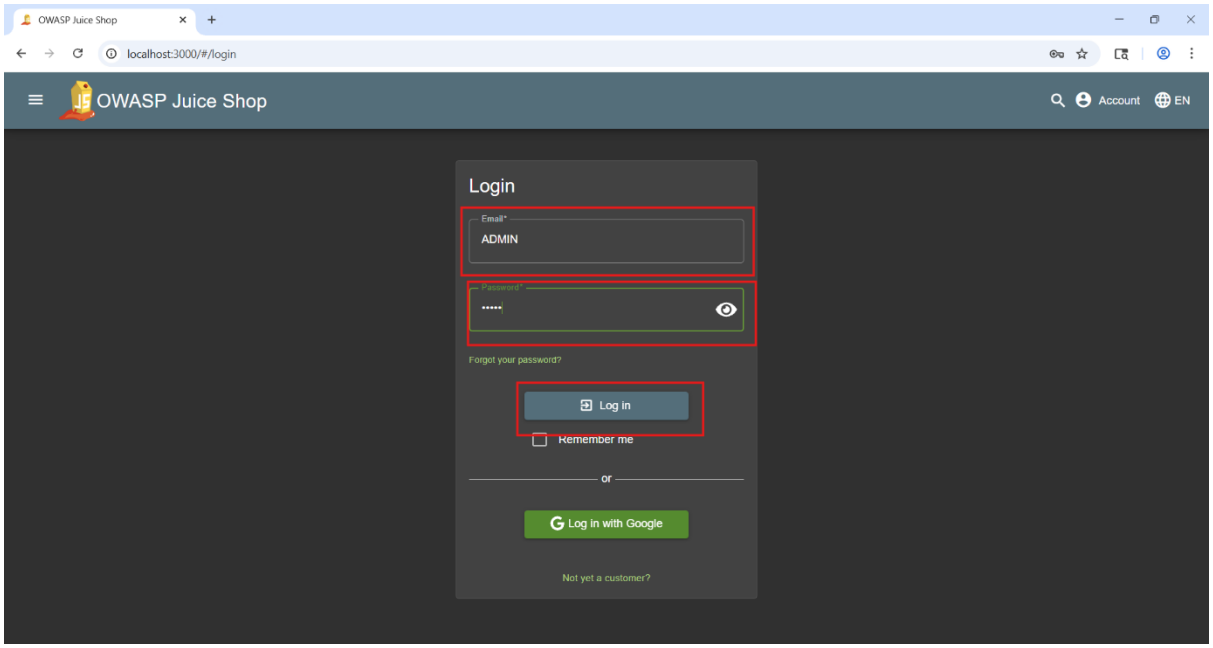
- Identification: Recognizing who the user is (e.g., username or ID).
- Authentication: Verifying that the user is who they claim to be (e.g., via passwords, tokens, biometrics).



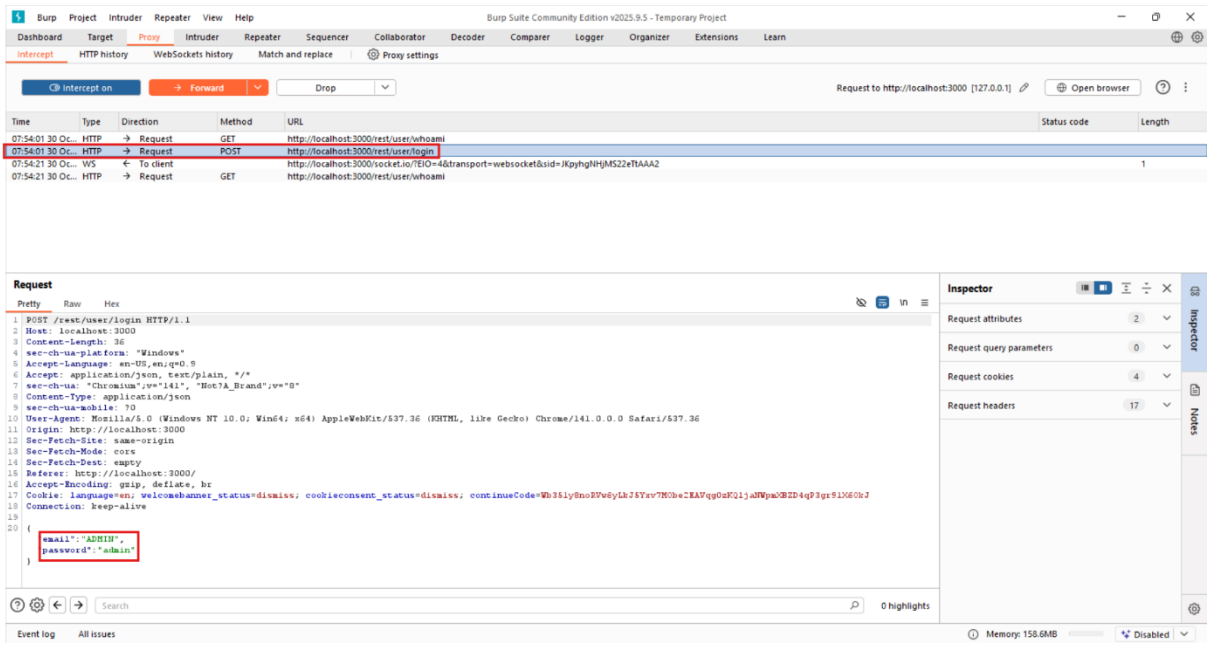
- Open owasp juice shope and click on account



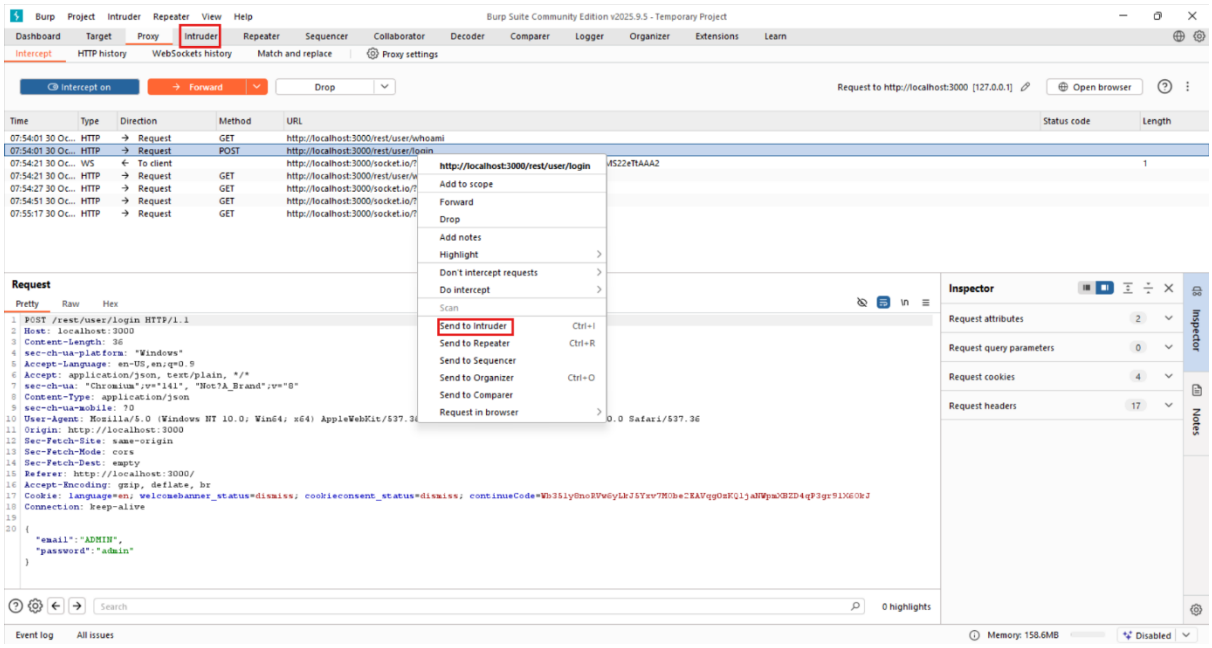
- Turn on the intercept



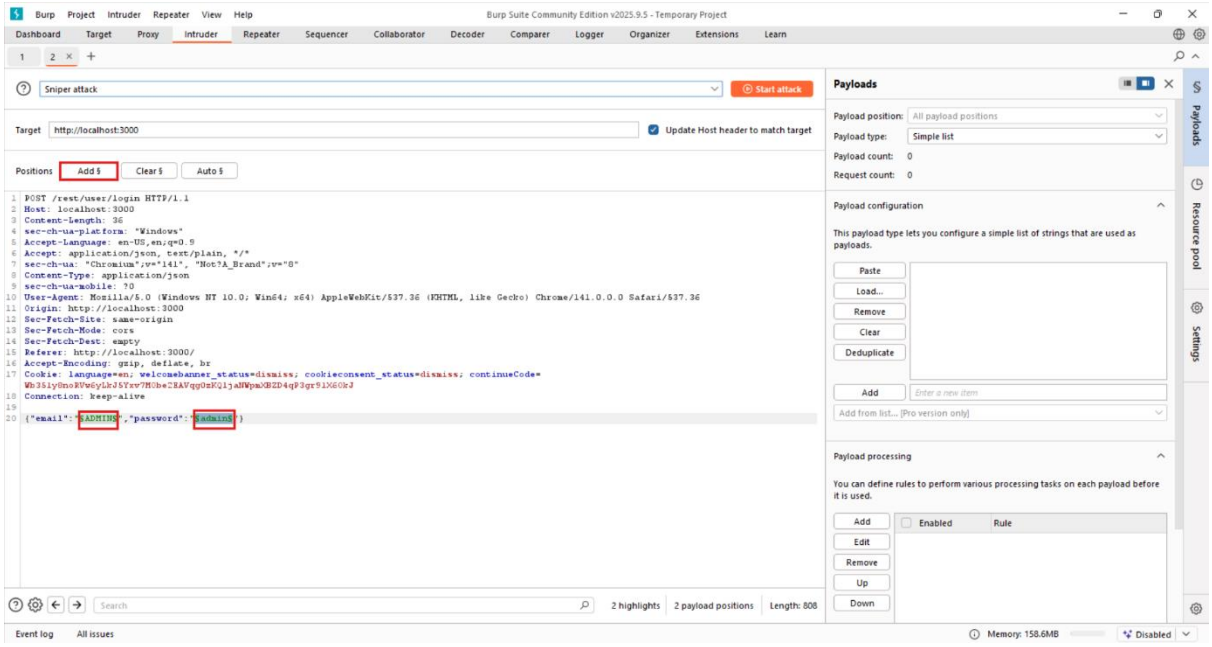
- Give any login credentials here and click on login



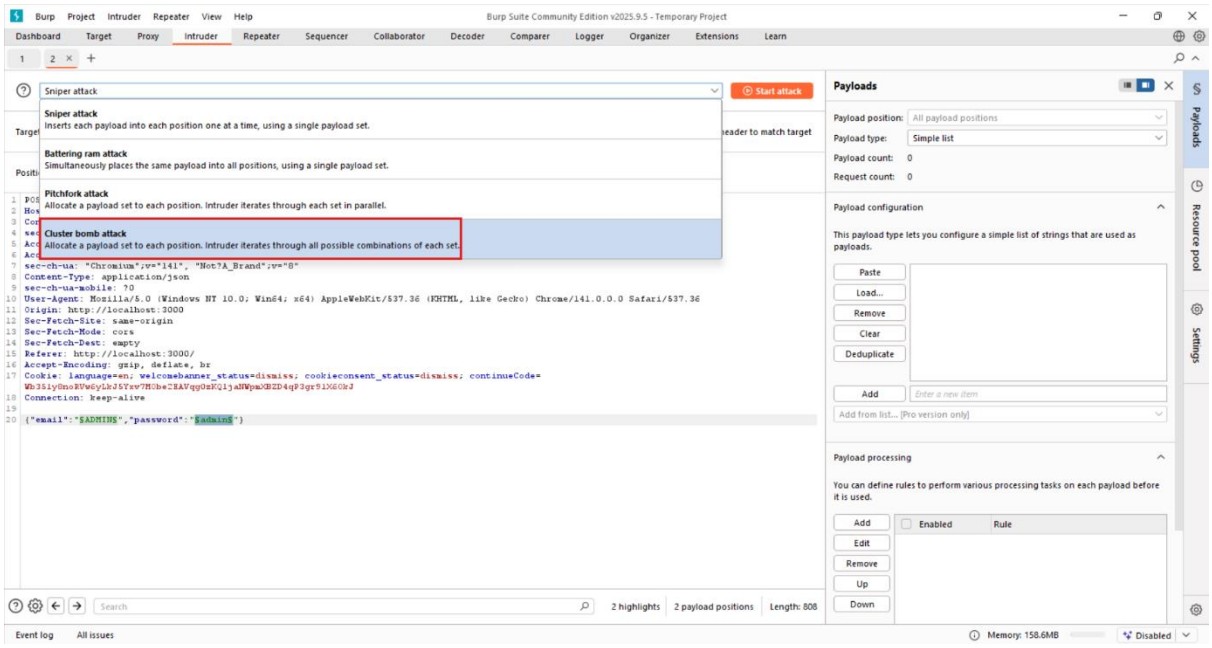
- We received several packets.
- Click on the packet written user/login
- We will get to see our login credential



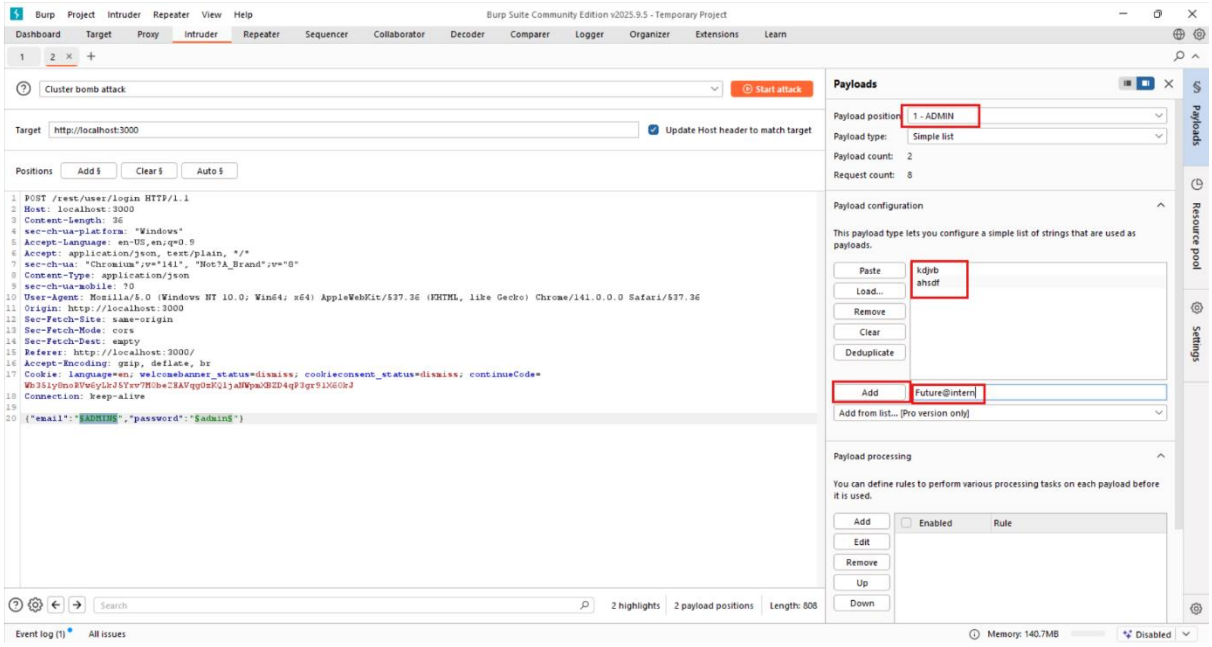
- Those packets send to intruder.



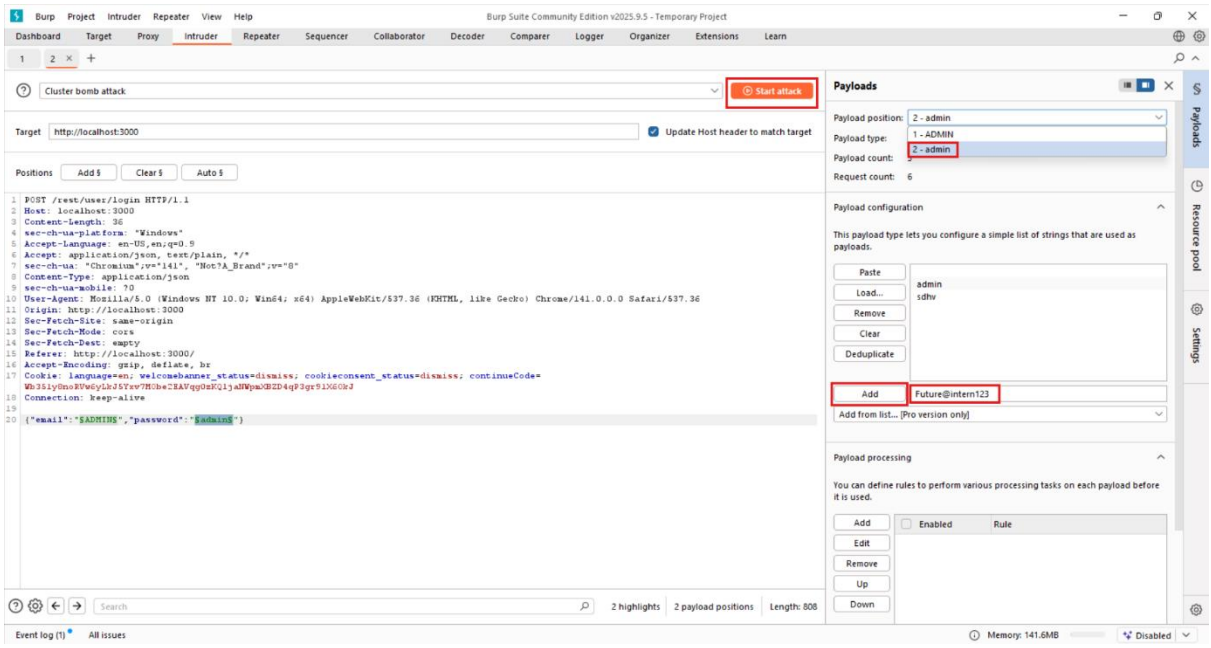
- In intruder, we will add the username and password positions for the payloads.



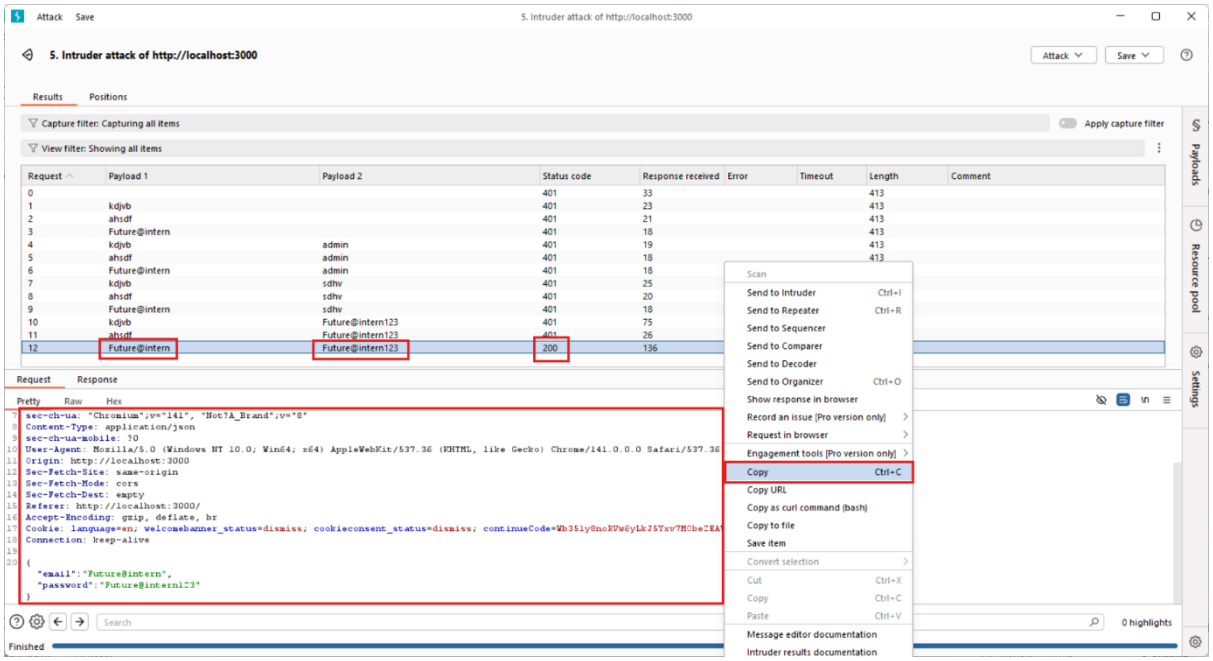
- After that we will select types of attacks, here we select cluster bomb attack.



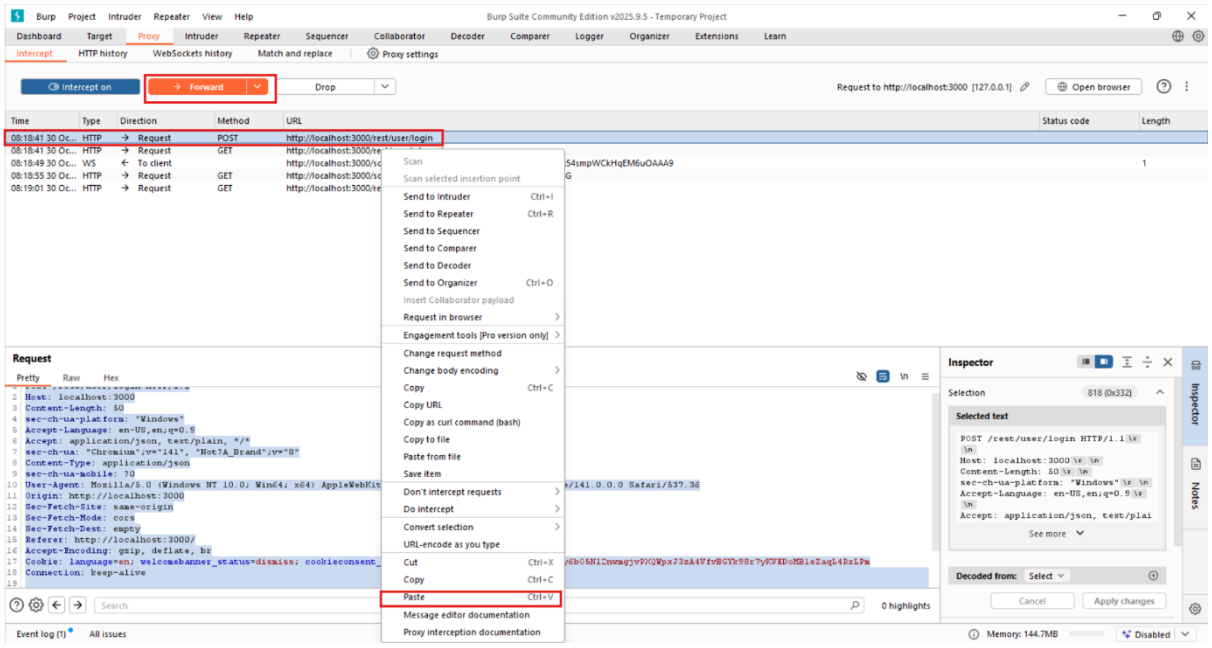
- Then we will give some payloads for username.



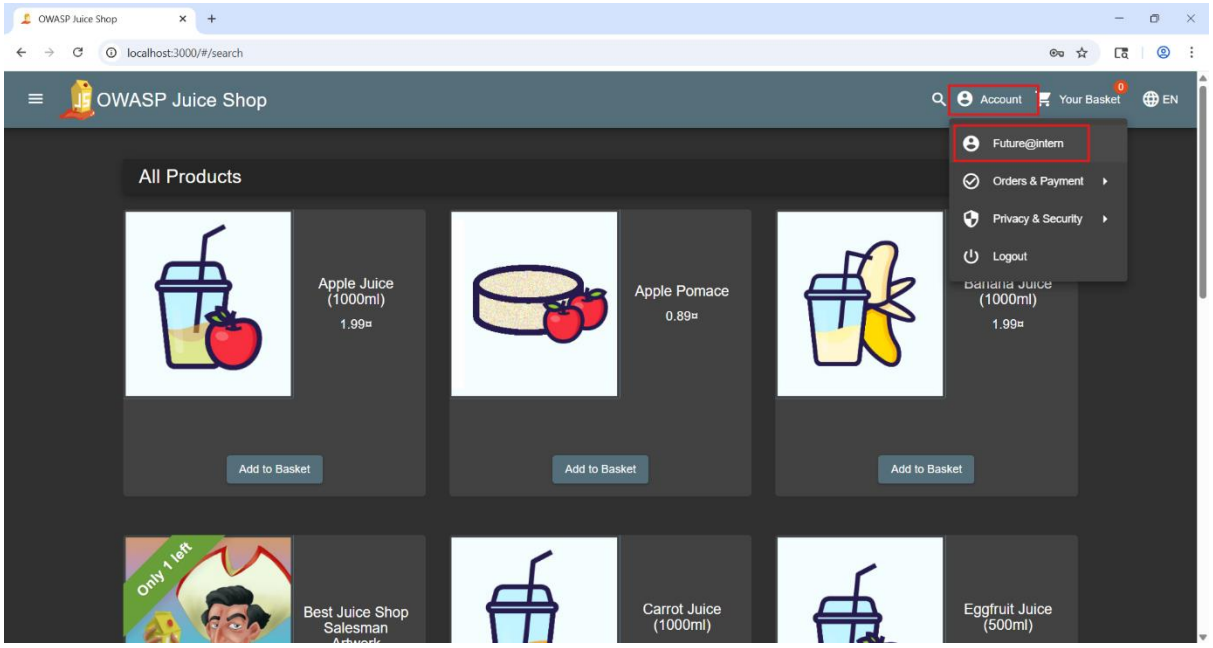
- Then we will give some payloads for password.
- After giving payloads click on start attack.



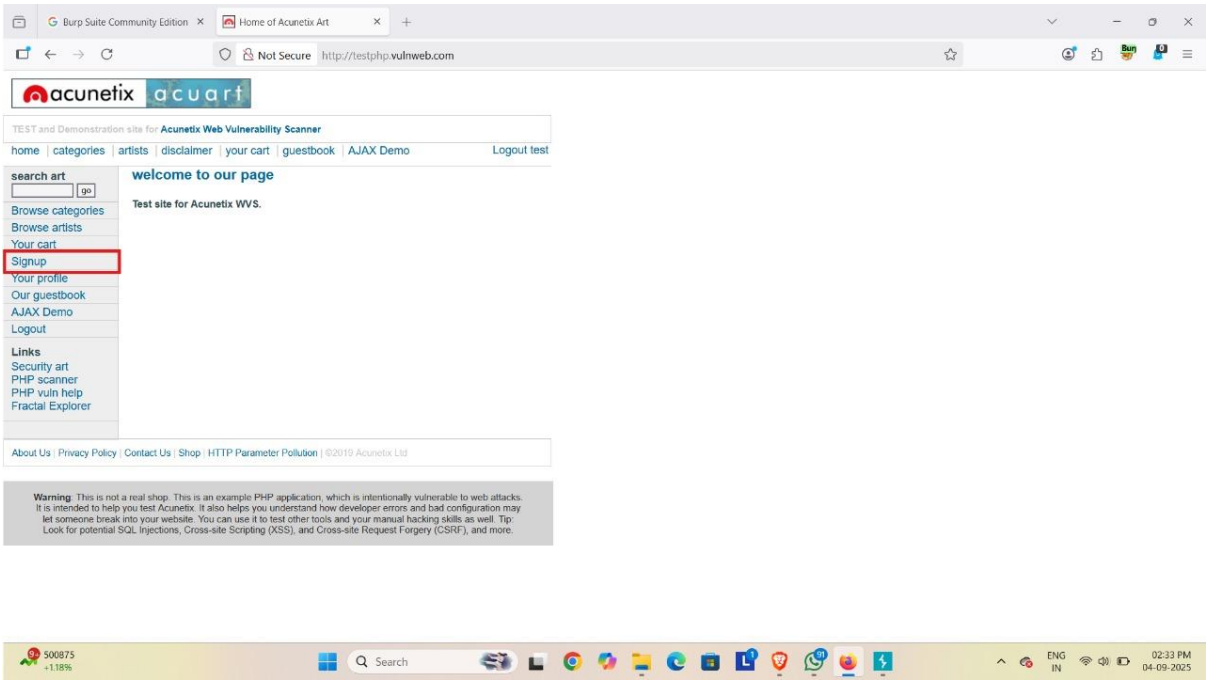
- Here we get status code 200 then it is correct credentials
- We copy the request of the correct credentials



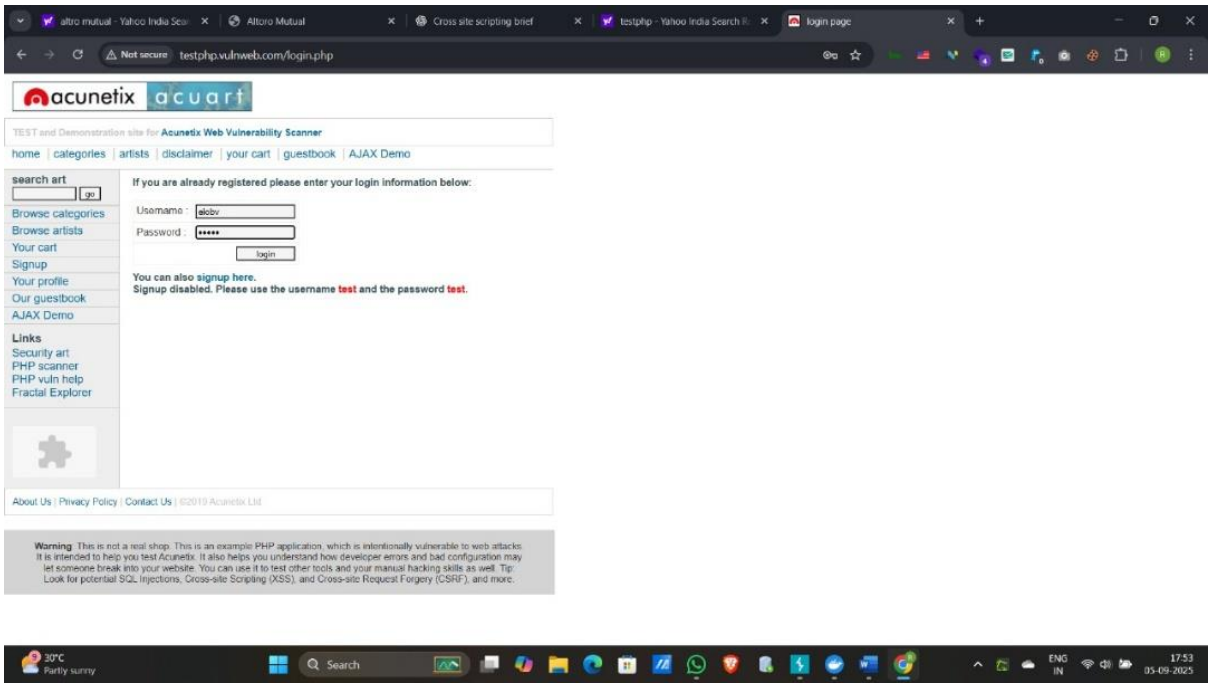
- Go to the proxy and paste request on the packet and forward the packet, after that turnoff the intercept.



- Now, we can see that we have successfully logged into the web application OWASP Juice Shop.

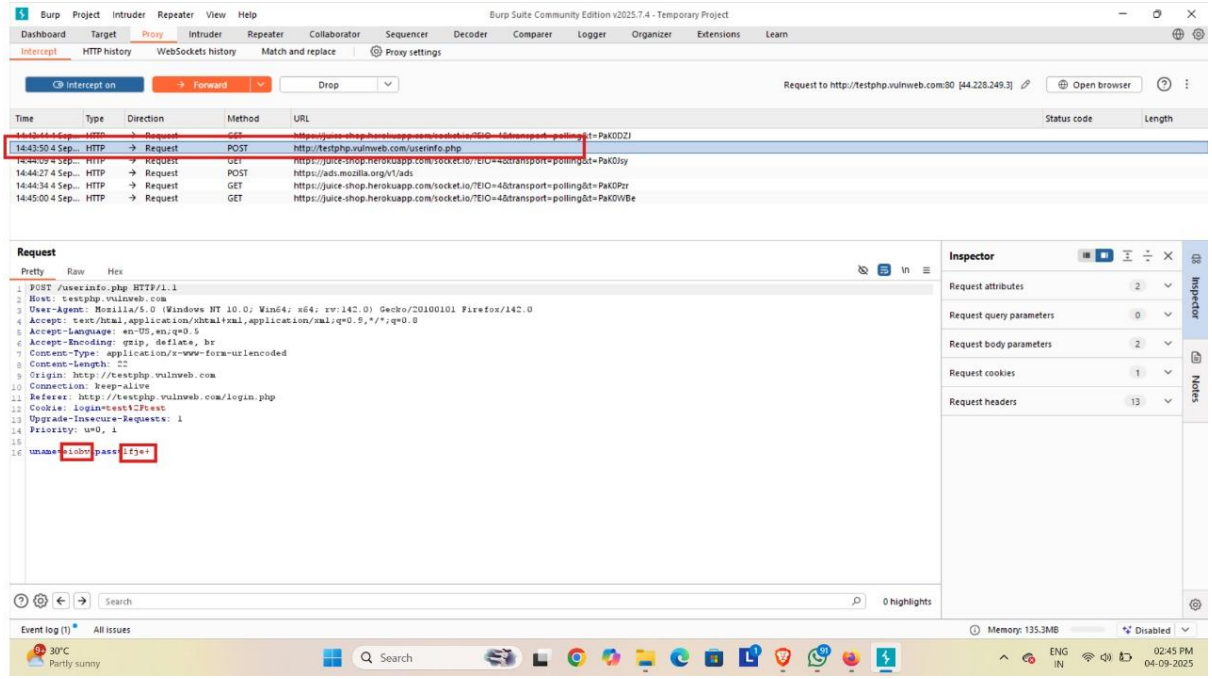


- Open a browser and search http://testphp.vulnweb.com

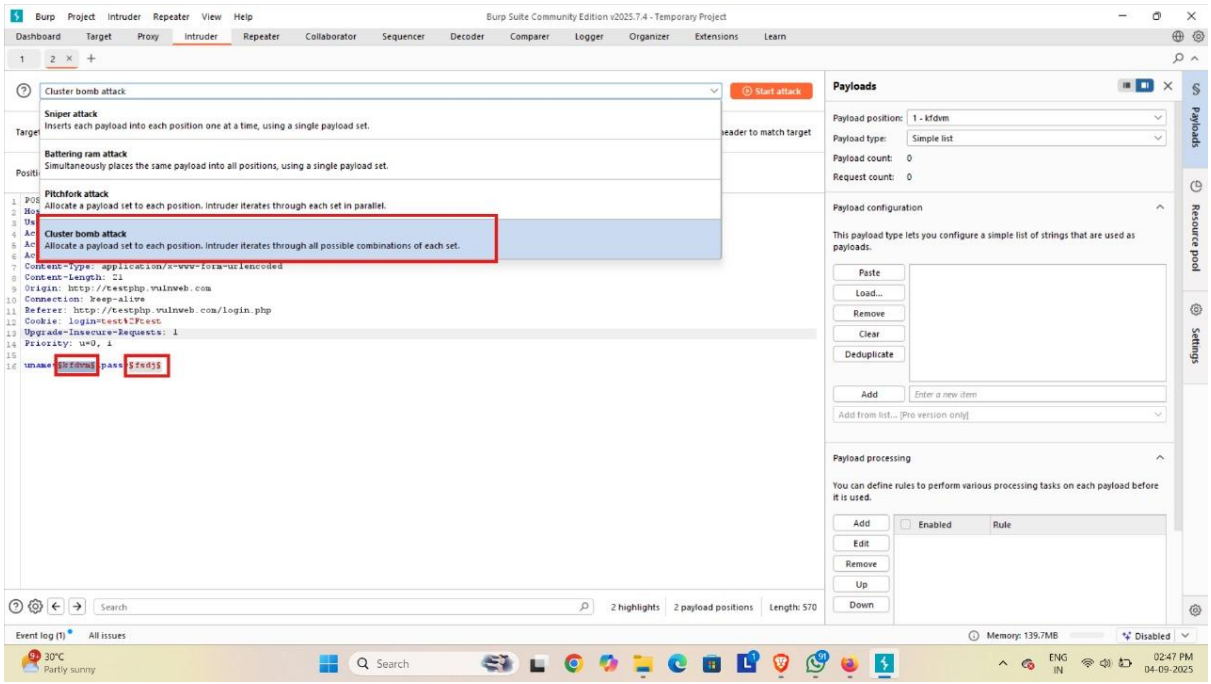


  - Turn on the intercept
  - Give login credentials here and hit enter

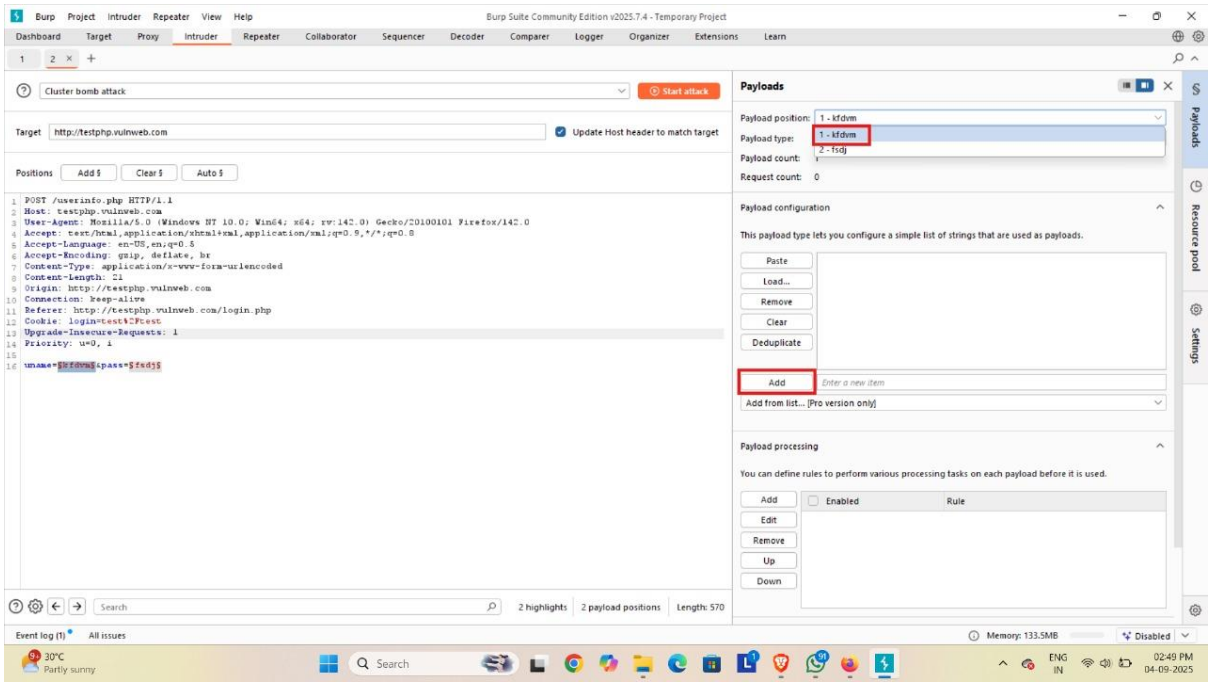
- We received several packets. Find the packet containing the 'testphp' user info and press Enter.



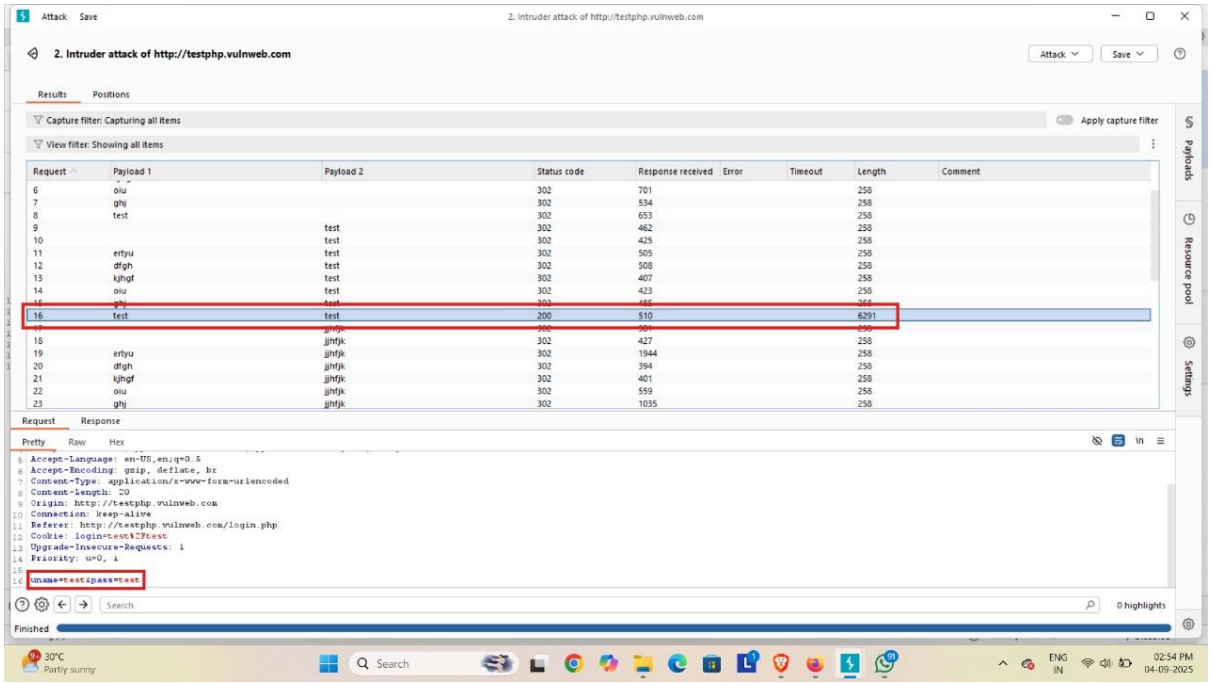
- Those packets send to intruder.
- In intruder, we will add the username and password positions for the payloads.
- After that we will select types of attacks, here we select cluster bomb attack.



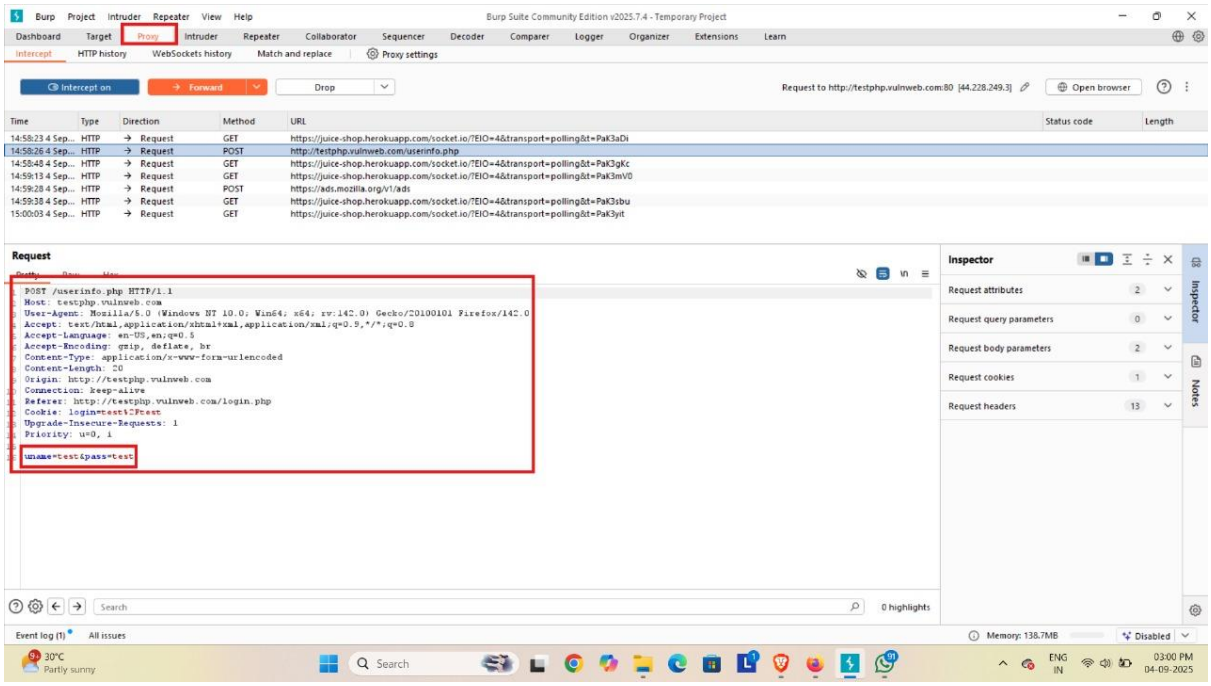
- Then we will give some payloads for username and password.



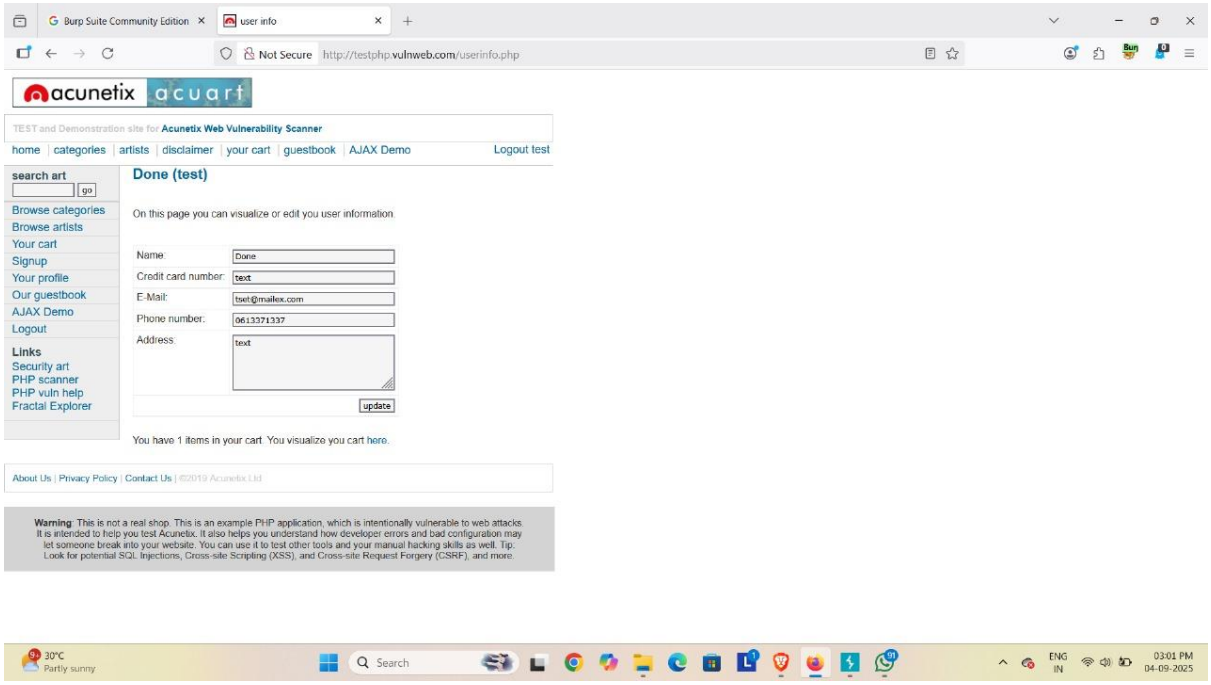
- After giving payloads click on start attack.



- Here we get status code 200 then it is correct credentials
- We copy the request of the correct credentials



- Go to the proxy and paste request on the packet and forward the packet, after that turnoff the intercept.



- Now, we can see that we have successfully logged into the web application

Conclusion

The web application security testing identified critical vulnerabilities like SQL Injection and XSS. Implementing the suggested fixes—such as input validation and parameterized queries—will improve the application's security. Regular security audits and adherence to OWASP best practices are recommended to maintain a strong security posture for Future Interns.