CYS REPORT

## Name: Yara Mohamed (2305259).

## Name: Meran Ramadan (2305193).

## Name: Neama said (2305195)

* 1st Attack Enumeration to Find Admin Path:

1. Enumeration to Find Admin Path

Attack Description

Enumeration is the process of gathering information about a target system to identify hidden or sensitive paths, such as /admin, /dashboard, or /config. An attacker attempts to discover these paths by:

1. Guessing common URL structures manually.

2. Analyzing application responses for clues in HTTP headers, error messages, or directory listings.

3. Using automated tools to brute-force potential paths or directories.

Risk and Impact

Risk:

If sensitive paths like an admin panel or configuration files are exposed, attackers can target these functionalities for further exploitation, such as credential brute-forcing, exploiting vulnerabilities in admin features, or unauthorized access to critical application controls.

Impact:

• Unauthorized access to the administrative area, leading to full control of the application.

• Potential exposure of sensitive information, such as database credentials, API keys, or backup files.

• Increased risk of other attacks, such as privilege escalation or data breaches.

Tools Used

1. DirBuster

2. Gobuster

3. Burp Suite

4. Nikto:

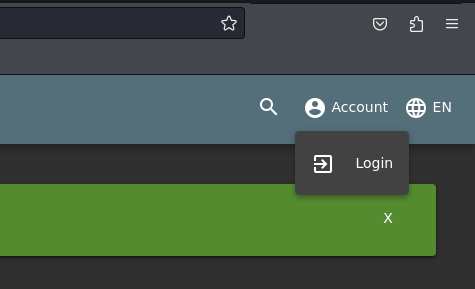
5. Ffuf (Fuzz Faster U Fool):

6. HTTP Response Analysis

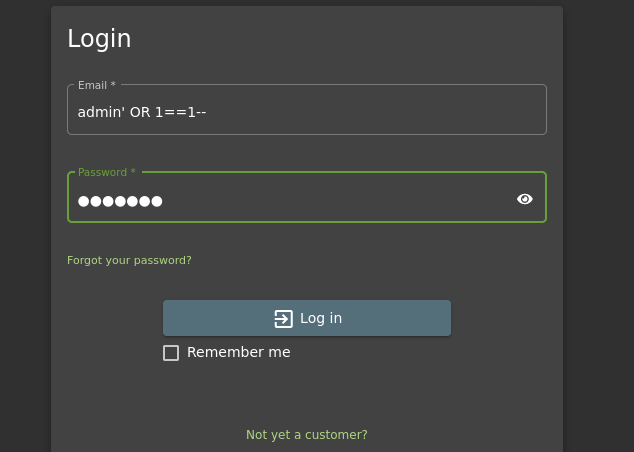
This part of report discusses a security vulnerability where attackers discover hidden paths in an application to access administrative functionalities.

1-First we go to Kali Linux then we enter Firefox to open the website.

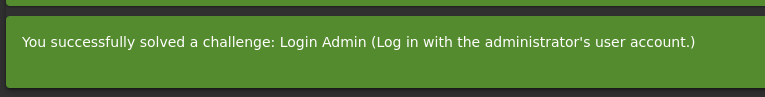
2-When we enter the website we go to the account and login.

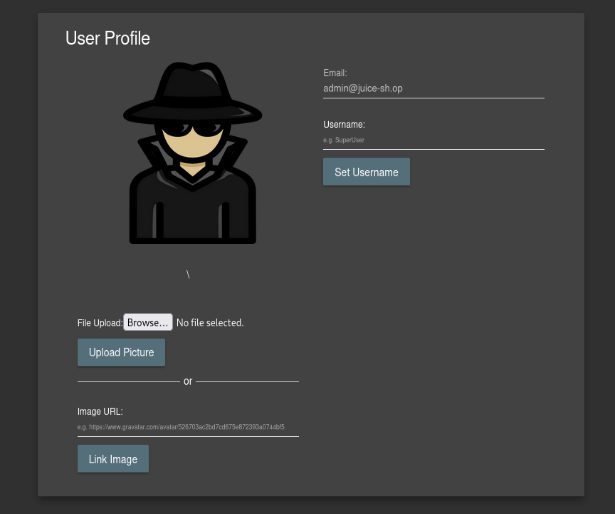
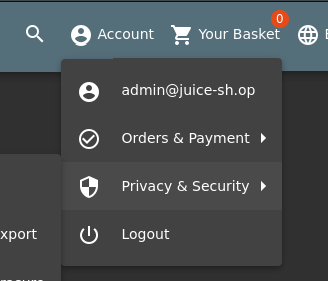


3-we will write in the email the command of the sql injection and any password.



4-When we click on Login, the attack will be done successfully.





# Video Link:

<https://drive.google.com/file/d/1ip3qjYJjuL7vm-QrpAQ0Ia1jH6-zjLPu/view?usp=drive_link>

* 2nd Attack XSS:

Attack Description

Cross-Site Scripting (XSS) is a web vulnerability that occurs when an application reflects untrusted user input directly into the web page without proper sanitization or escaping. In this scenario, the attacker injects a malicious script into the product search bar.

If the application reflects this input directly into the webpage without validation or sanitization, the script will execute in the browser of any user viewing the affected page.

Risk and Impact

1. Steal session cookies, allowing account takeover.

2. Redirect users to phishing or malicious websites.

3. Log keystrokes to steal sensitive user inputs like passwords.

4. Perform actions on behalf of a logged-in user (e.g., unauthorized transactions).

• Impact:

• Compromise of user accounts or sensitive data.

• Decreased trust in the application due to security risks.

• Potential exploitation of browser vulnerabilities or delivery of malware.

Tools Used

1. Burp Suite:

2. OWASP ZAP:

3. BeEF (Browser Exploitation Framework):

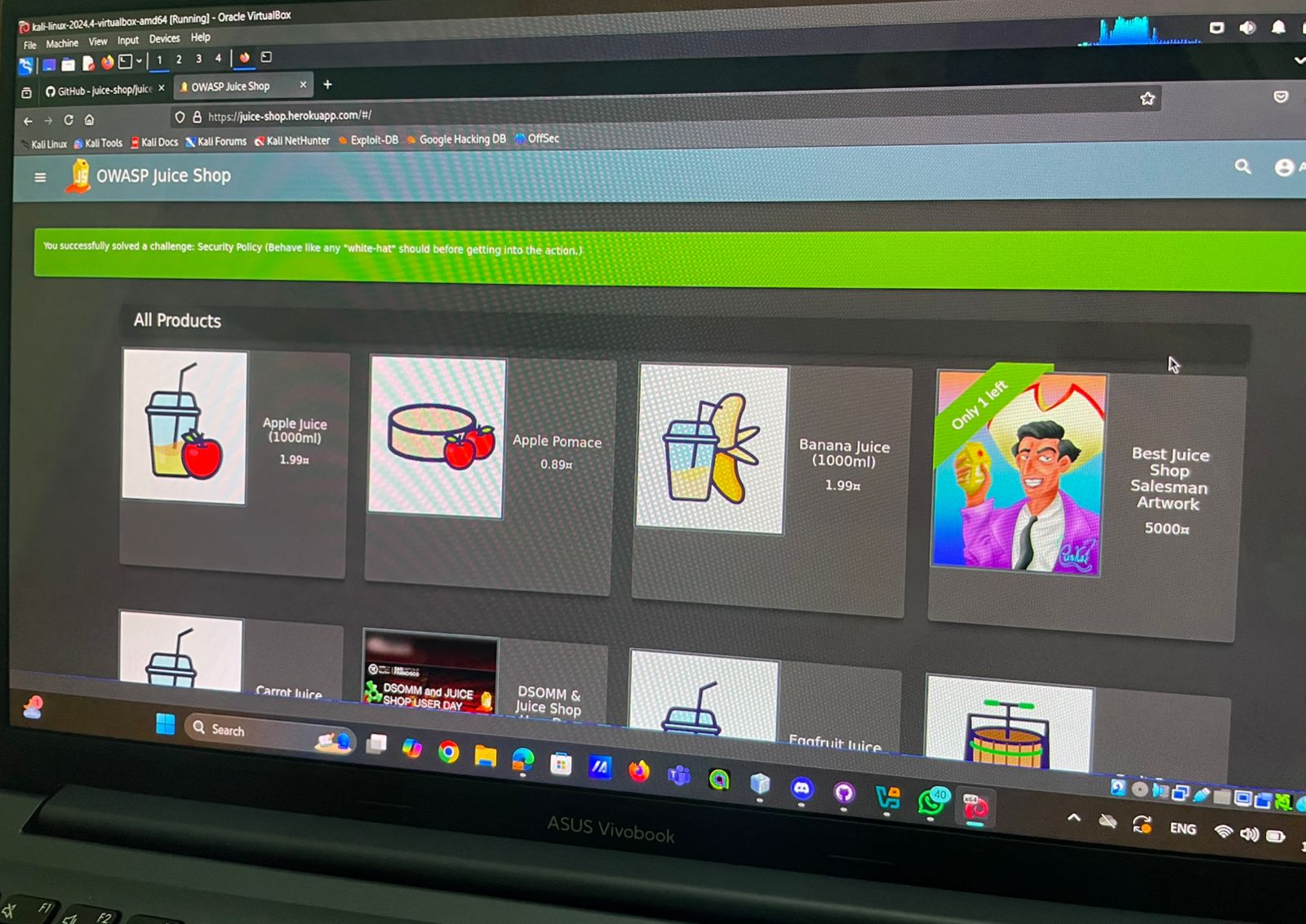
4. Postman:

5. Fuzzing Tools (e.g., XSStrike):

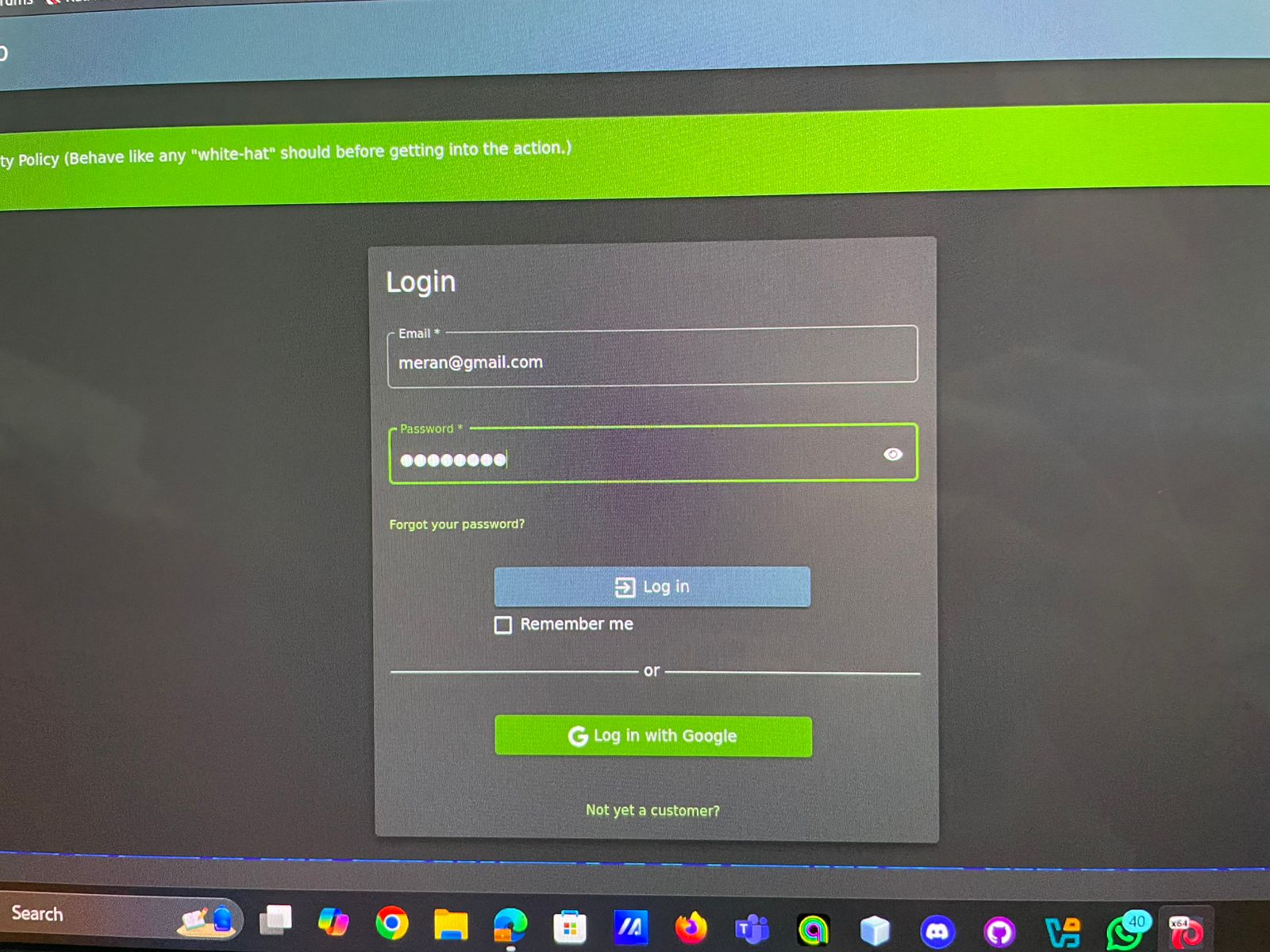
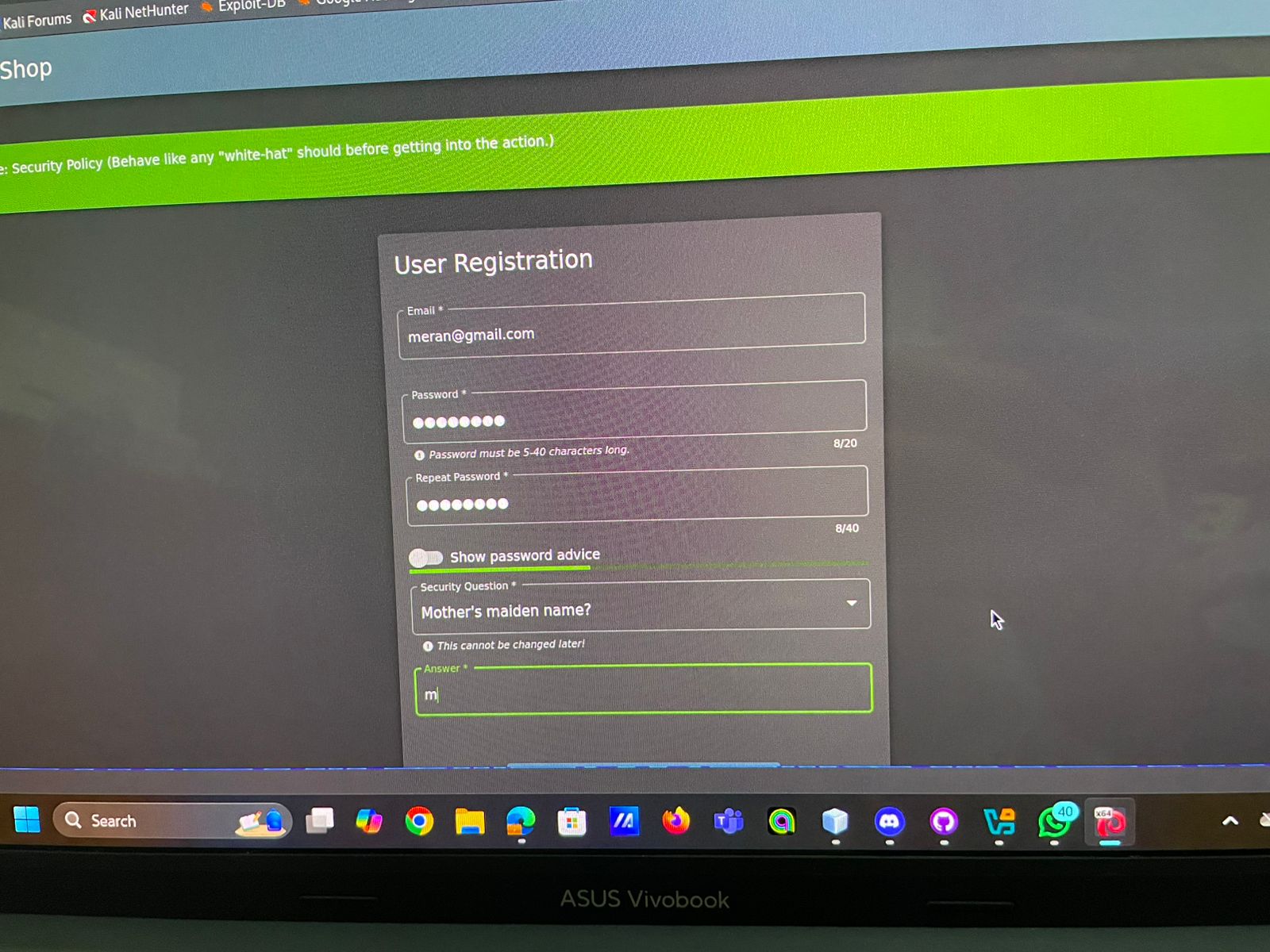
6. Manual Inspection:

The vulnerability arises due to improper handling of user input, which is reflected back to users without sanitization or encoding.

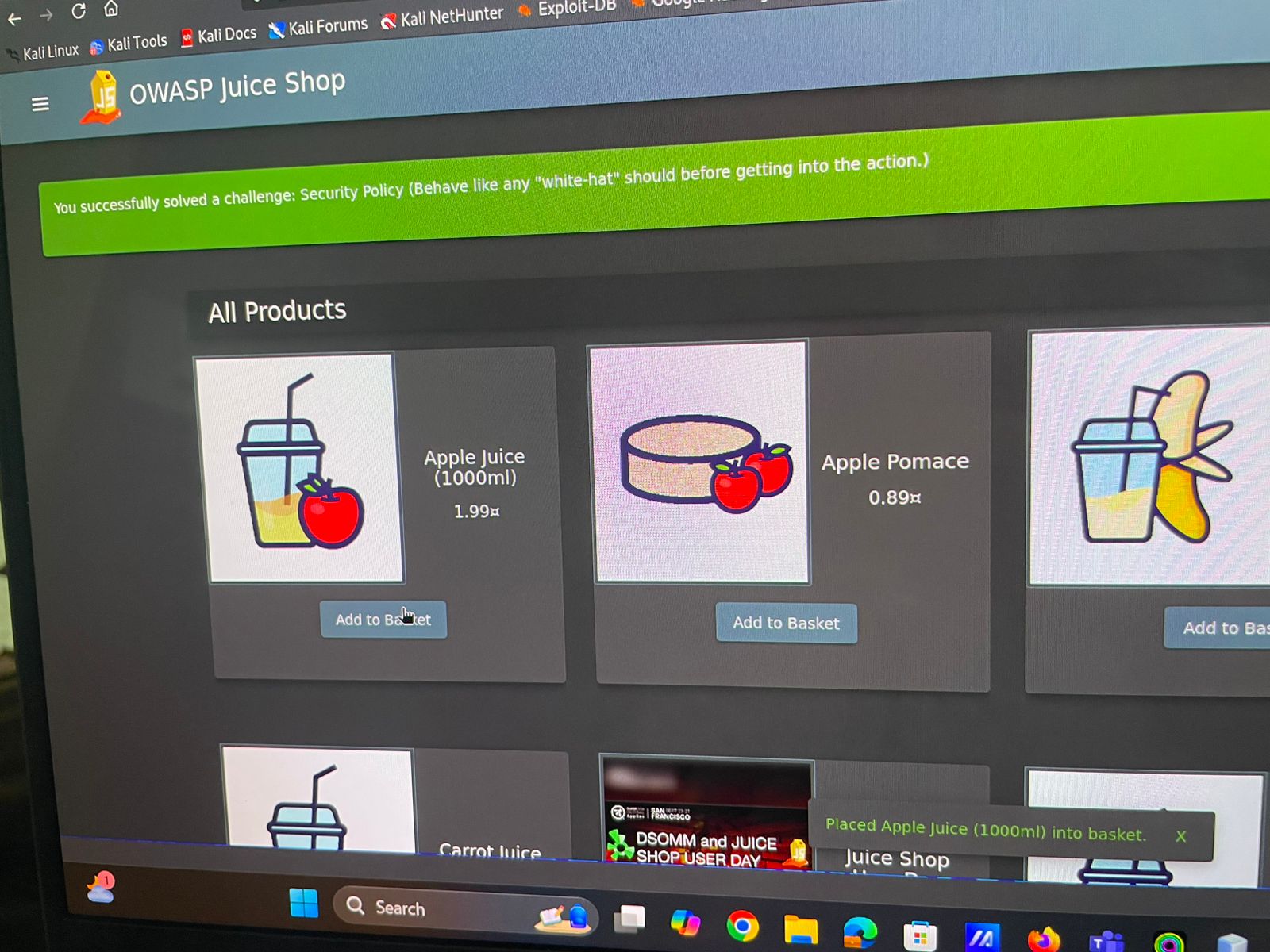
1-First open owasp juice shop on firefox in linux.

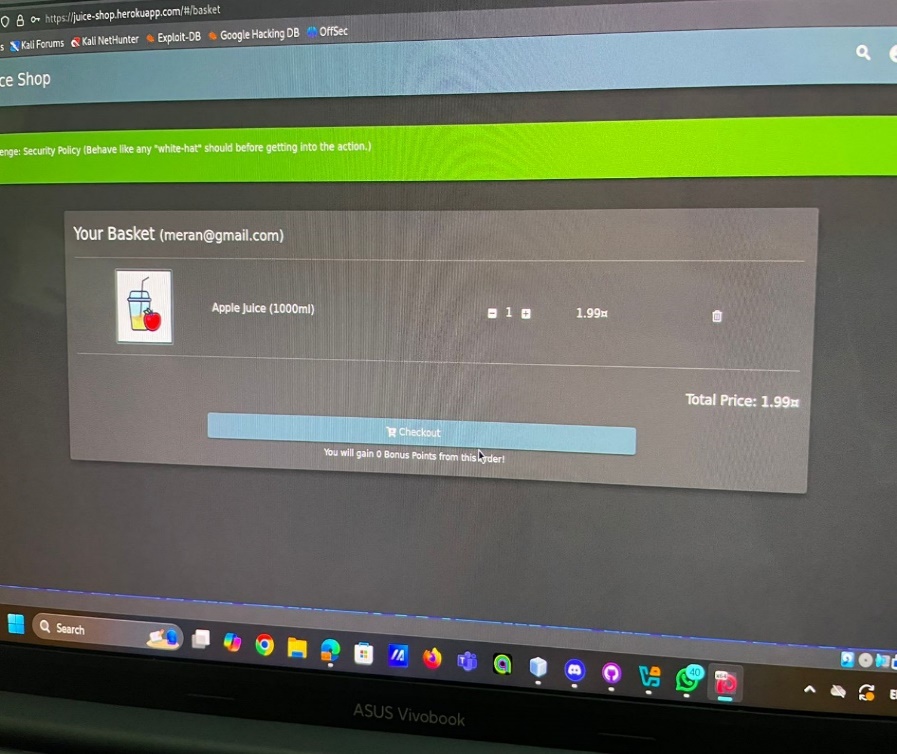


2-Sign in Then Login.

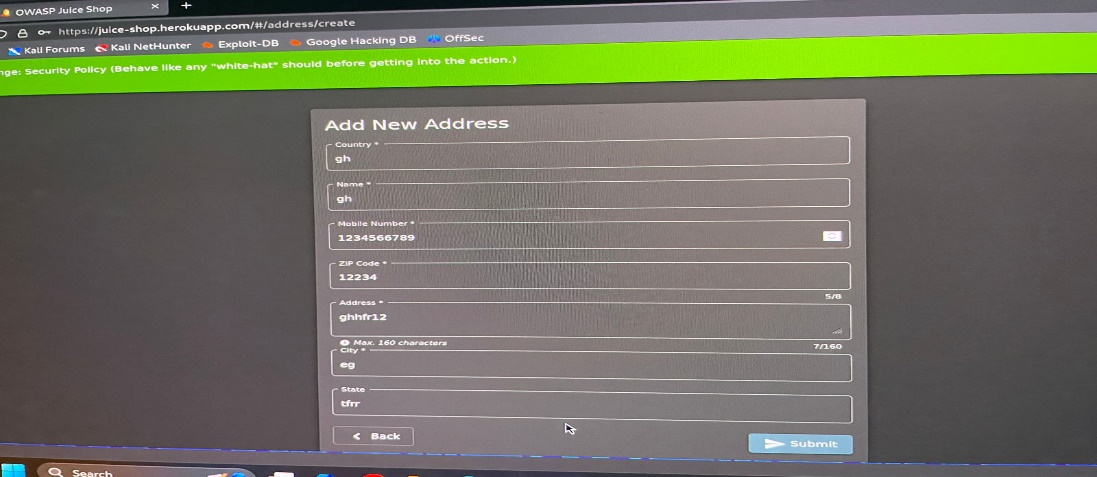


3-Choose any product and add it to basket and check out.

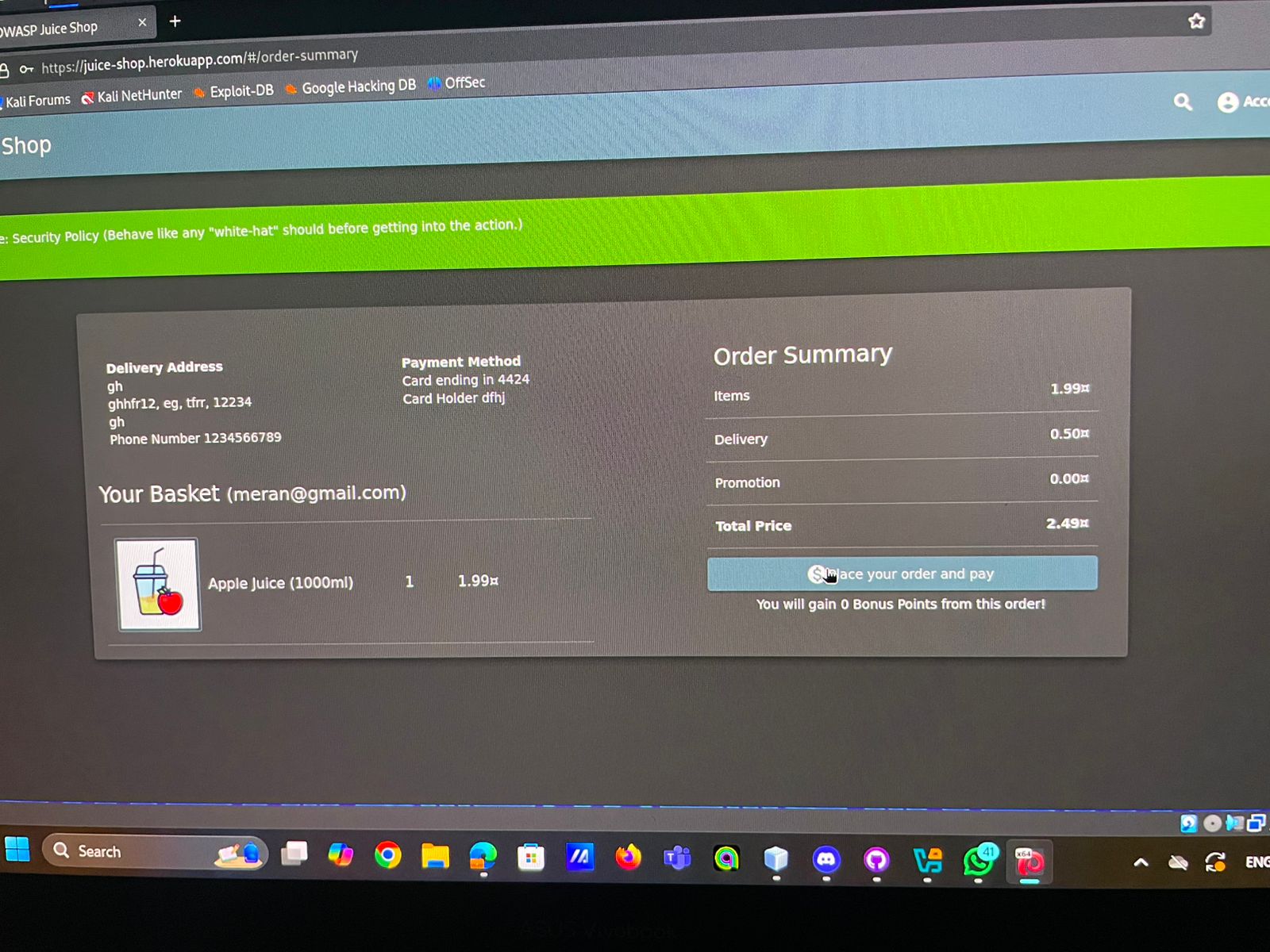
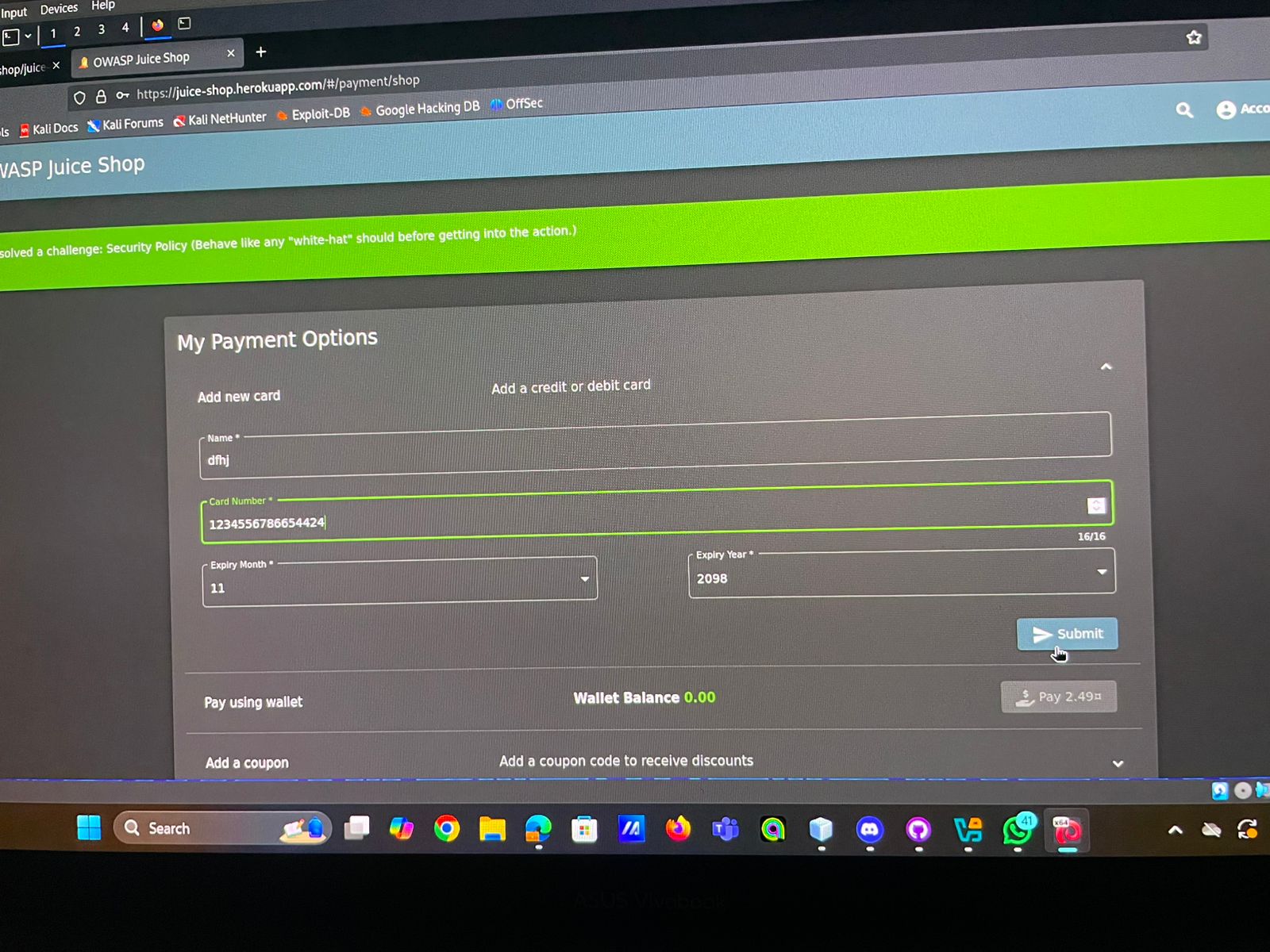




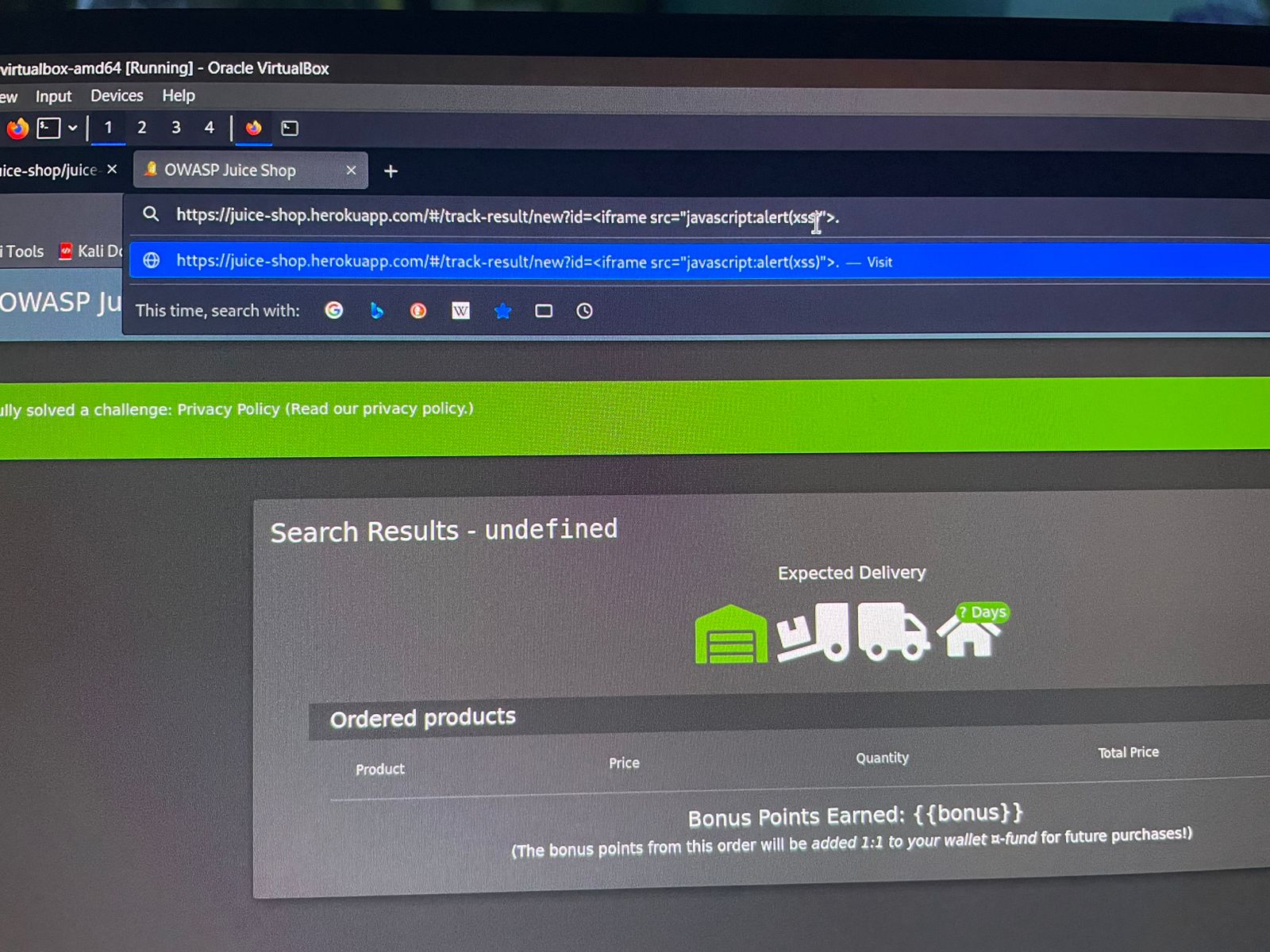
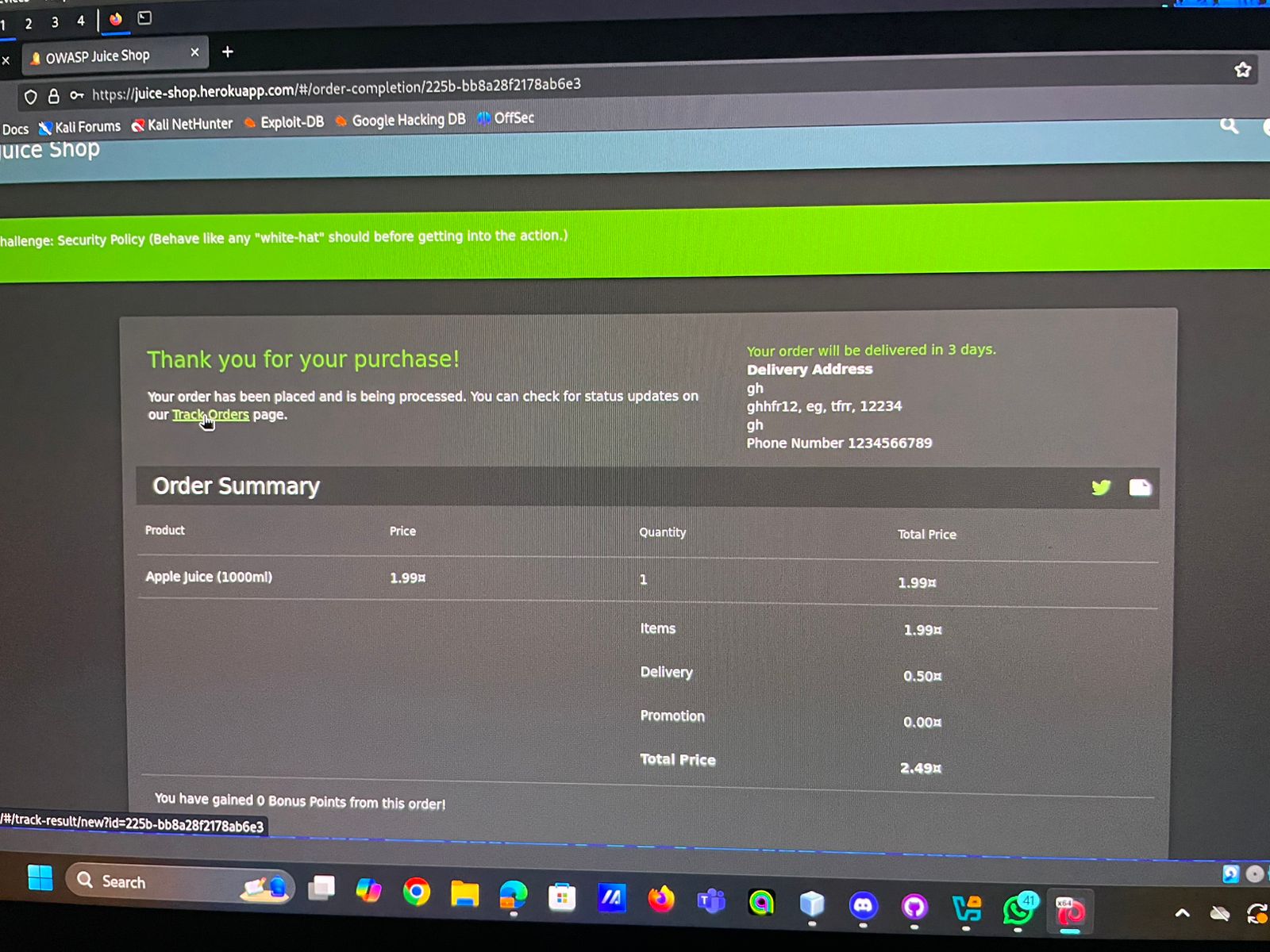
4-Add new address.

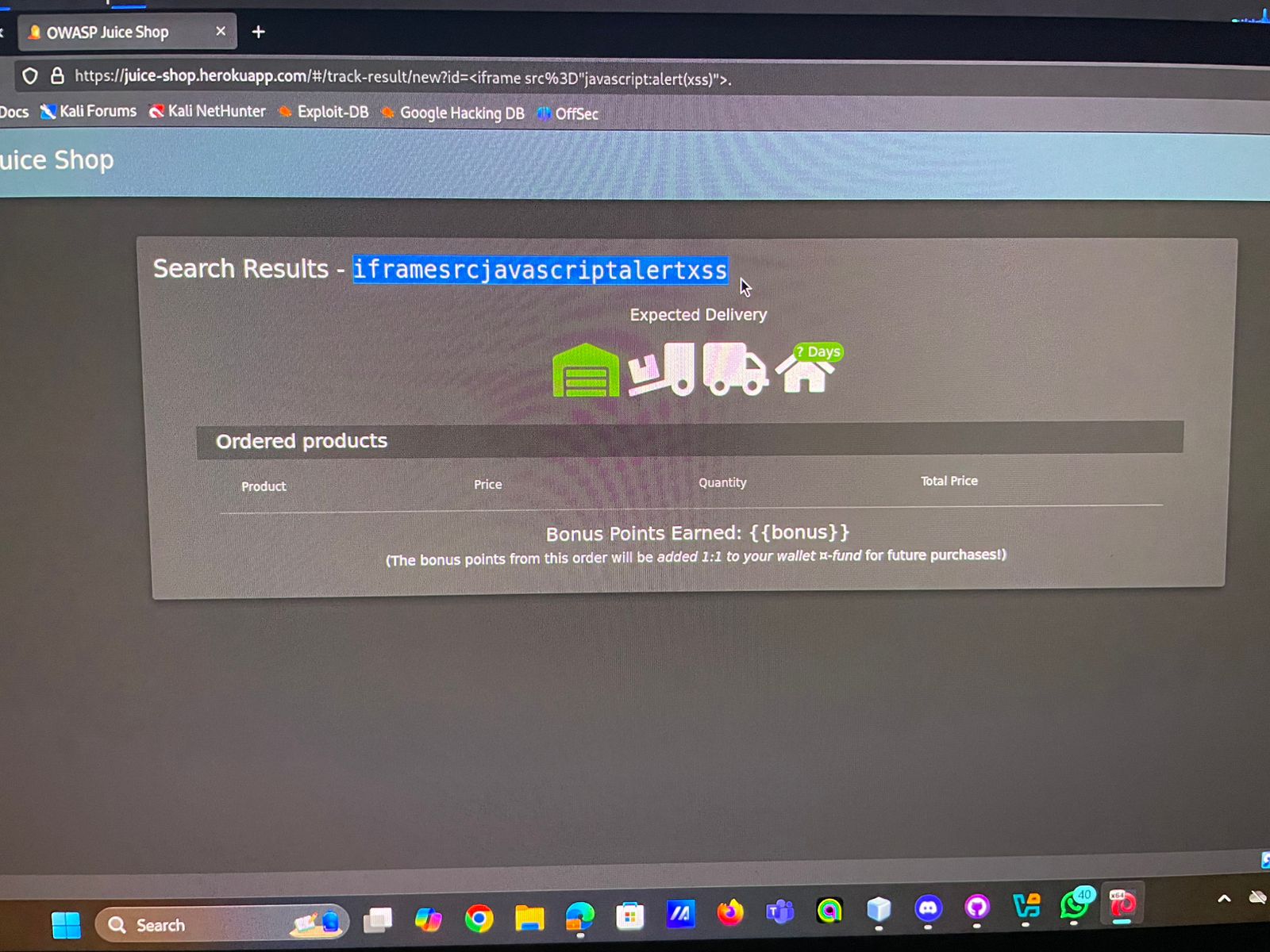


5-Payment details and place my order.



6-press on track orders then write javascript code after id= in the path.



7-click refresh and the attack will be done.

# Video Link:

<https://drive.google.com/file/d/1GLYVSck1IBDuv_gsgNmsB23weyiGgTde/view?usp=drive_link>

* 3rd Attack Brute Force on Admin Credentials.

Attack Description

Brute-forcing is a method of systematically trying all possible password combinations to gain unauthorized access.

In this scenario, the attacker has discovered the admin login page and obtained a valid email (e.g., admin@juice-sh.op). The attacker uses an automated tool to guess the password. The absence of security mechanisms such as rate limiting, CAPTCHA, or account lockouts allows unlimited attempts, making brute-forcing successful.

Risk

1. Unauthorized access to administrative functionalities.
2. Exposure of sensitive data (e.g., user information, transaction details).
3. Manipulation or deletion of critical application data.
4. Potential for installing backdoors or malware in the system.

Impact

1. Full compromise of the application and its data.
2. Financial, reputational, or legal damage due to data breaches.

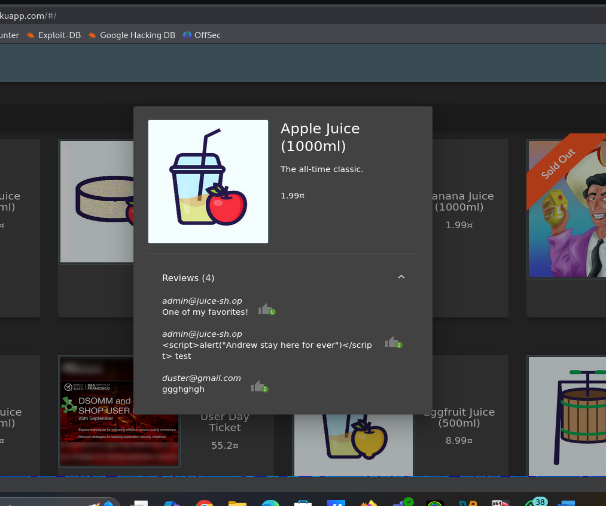
Tools Used

1. Hydra
2. Burp Suite Intruder
3. Medusa
4. OWASP ZAP
5. Crunch
6. Custom Scripts

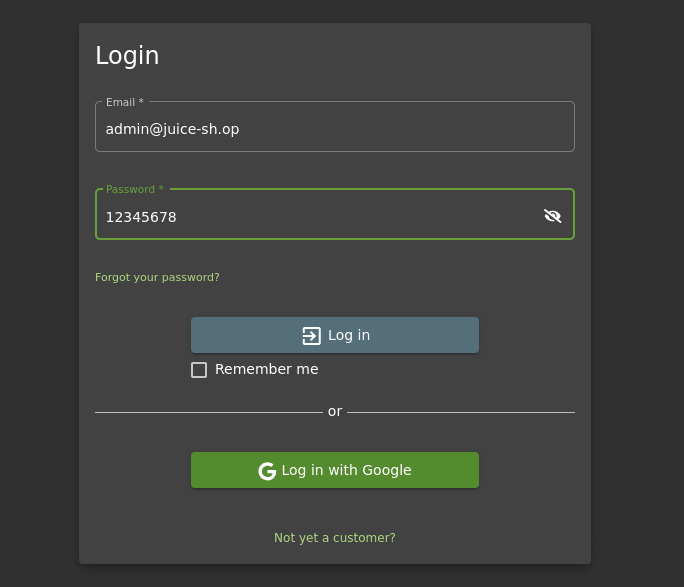
This part of report highlights the risks and methods involved in brute-force attacks targeting admin credentials and proposes preventive measures.

1. First open the website and choose the email you want to hack for example we will use

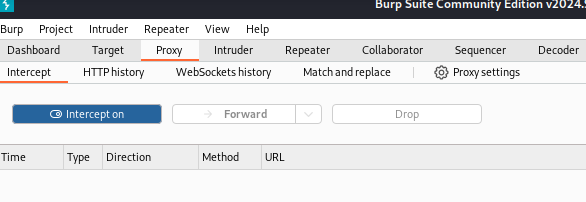
[admin@juice-sh.op](mailto:admin@juice-sh.op).



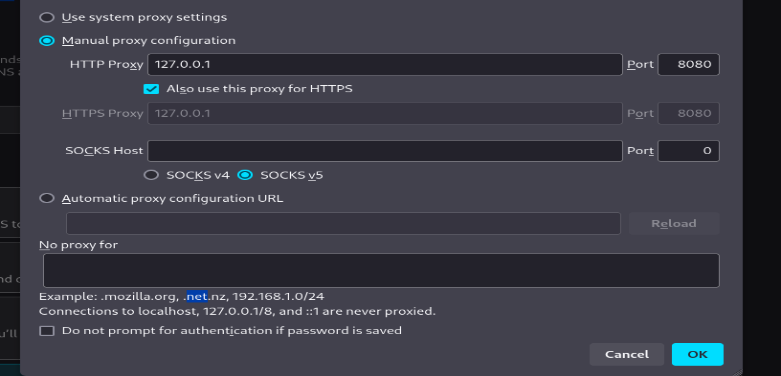
1. And then login with any password



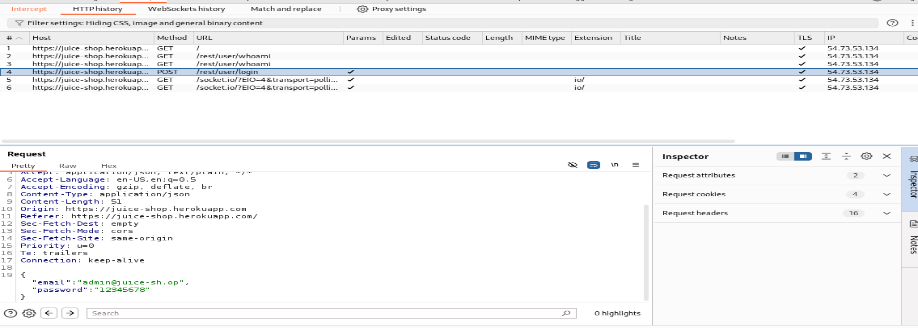
1. And then go to brup suite and go to proxy and press intercept on



1. And then go to settings in website and search network and press manual proxy and write HTTP Proxy and Port and press ok

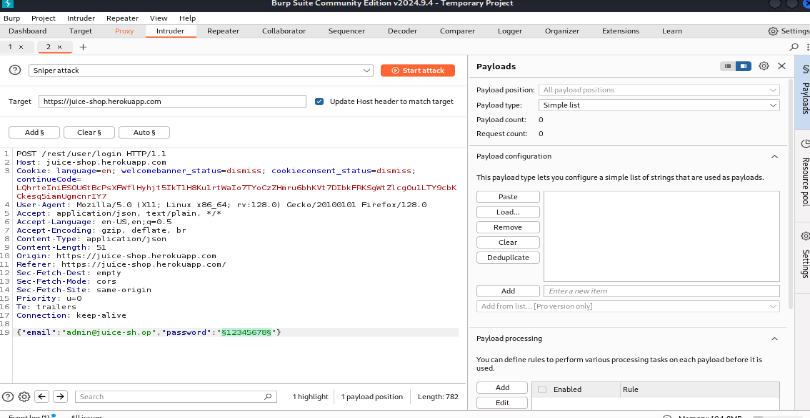


1. And login again with wrong password and go to brup suite and go to HTTP history and press on login



1. And then right click and sent to repeater and press send and go again to HTTP history

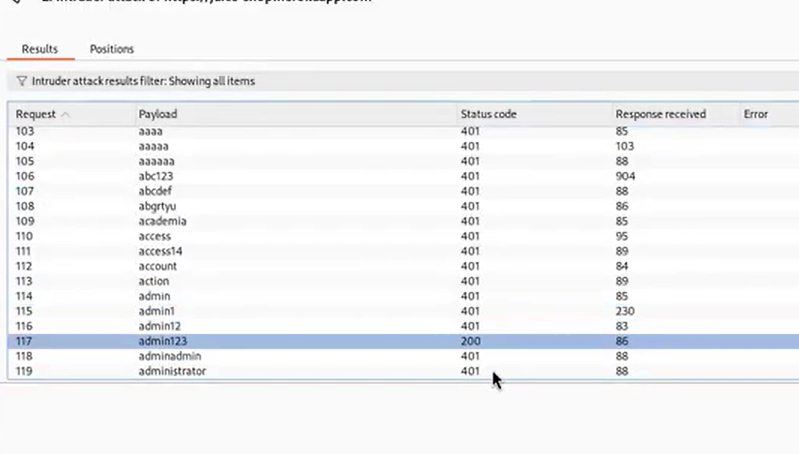
And right click and sent to intruder and select the wrong password and press add$



1. And go to git hub and copy all the passwords in best1050 file

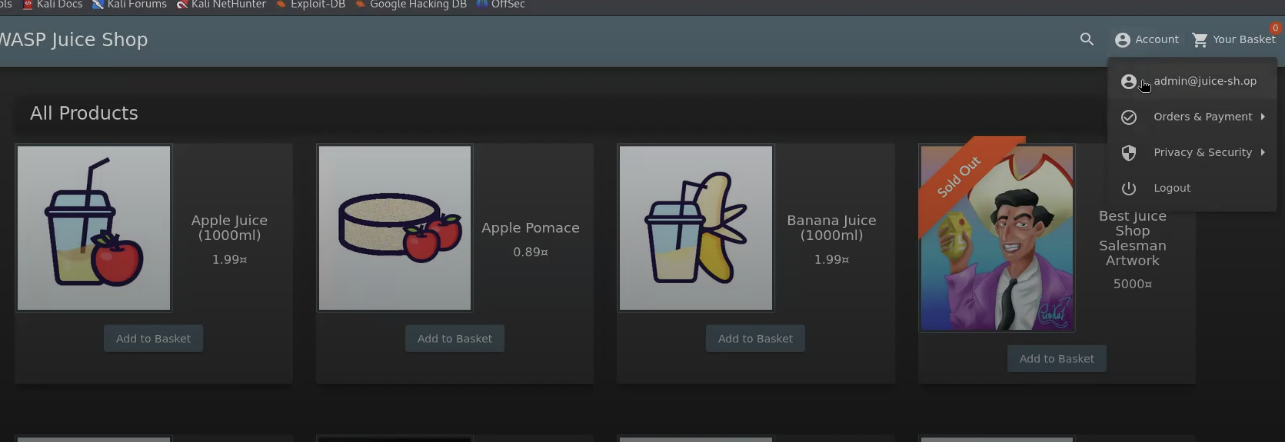
And paste in Payloads and press start attack

And in the results the password whose status code is different from 401 this is the right password press on it and send it to repeater and know it.



1. Go to settings in the website and change the configure proxy access to the internet

to be Auto-detect proxy settings for this network and try to login again with the right password



# Video Link:

Video1:

<https://drive.google.com/file/d/1hSmZVswuwXeohFe0FVy04SnRACouBt1_/view?usp=drive_link>

video2:

<https://drive.google.com/file/d/1hSmZVswuwXeohFe0FVy04SnRACouBt1_/view?usp=drive_link>