## Name : John mina elthaalb ID: 2305524

**1st Attack: 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:** Exposure of sensitive paths may allow attackers to exploit vulnerabilities, perform credential brute-forcing, or gain unauthorized access.
- **Impact:**
    - Unauthorized access to administrative controls.
    - Exposure of sensitive information such as database credentials or API keys.
    - Increased risk of privilege escalation or data breaches.

**Tools Used:**

1. DirBuster
2. Gobuster
3. Burp Suite
4. Nikto
5. Ffuf
6. HTTP Response Analysis

**Attack Steps:**

1. Open Kali Linux and launch Firefox.
2. Access the website and navigate to the login page.
3. Use SQL injection commands in the email field with any password.
4. Click on Login to execute the attack.

**Video Link:**

**https://drive.google.com/file/d/1uG2bf4pBoeFfSIs9BojS91wBKv02teM6/view?usp=drive_link**

**2nd Attack Description:** SQL Injection (SQLi) is a vulnerability that occurs when user input is improperly handled, allowing attackers to manipulate SQL queries executed on the database. Attackers can exploit this vulnerability to bypass authentication, retrieve, modify, or delete data.

**Risk and Impact:**

- **Risk:** Unauthorized access to database information.
- **Impact:**
  - Data leakage, including sensitive user information.
  - Unauthorized modifications or deletions in the database.
  - Full database compromise.

**Tools Used:**

1. SQLMap
2. Burp Suite
3. SQLi Dumper
4. Manual SQL Query Testing

**Attack Steps:**

1. Open the target website.
2. Identify input fields vulnerable to SQL Injection (e.g., login forms, search boxes).
3. Inject SQL payloads such as `' OR 1=1 --`.
4. Analyze database responses to refine injection techniques.
5. Extract data or gain administrative access.

**Video Link:**

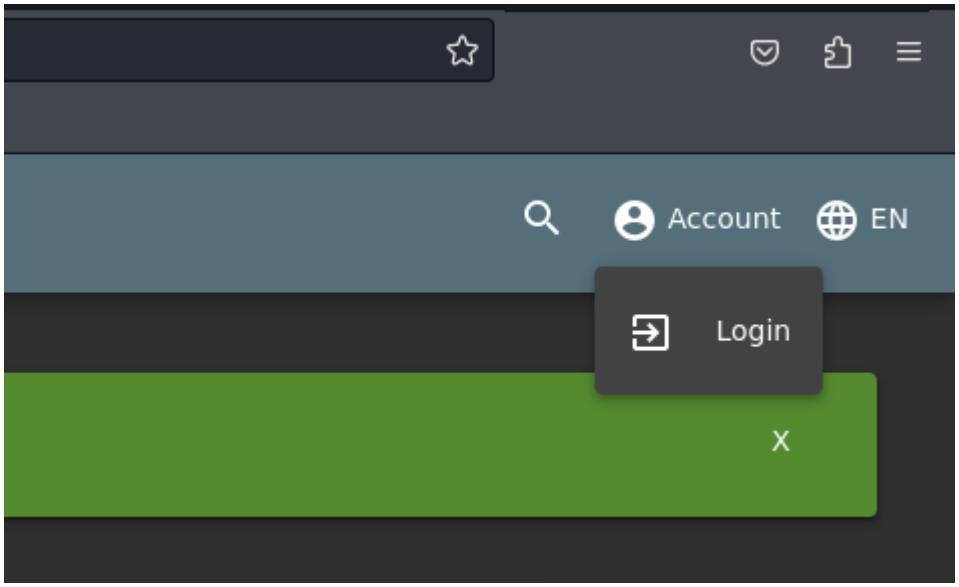
**https://drive.google.com/file/d/1ER3taOQqCY28KbcyrLzcWJiKJWl4caJe/view?usp=drive_link**

---

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

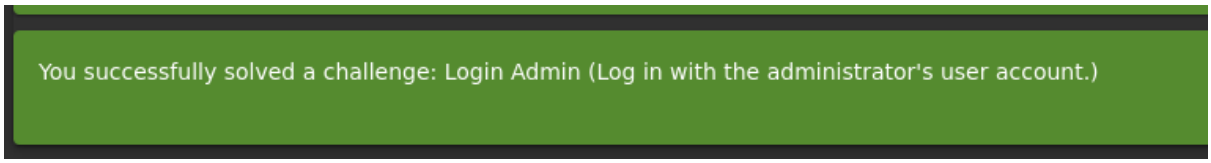
1-First we go to Kali Linux then we enter Firefox to open the website.

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.




**3rd Attack: XSS (Cross-Site Scripting)**

**Attack Description:** Cross-Site Scripting (XSS) occurs when an application reflects untrusted user input into the web page without proper sanitization. Attackers inject malicious scripts, which execute in users' browsers.

**Risk and Impact:**

1. Steal session cookies.
2. Redirect users to phishing websites.
3. Log keystrokes.
4. Perform unauthorized actions.

**Impact:**

- Account or data compromise.
- Decreased trust in the application.
- Potential malware delivery.

**Tools Used:**

1. Burp Suite
2. OWASP ZAP
3. BeEF
4. Postman
5. XSStrike
6. Manual Inspection

**Attack Steps:**

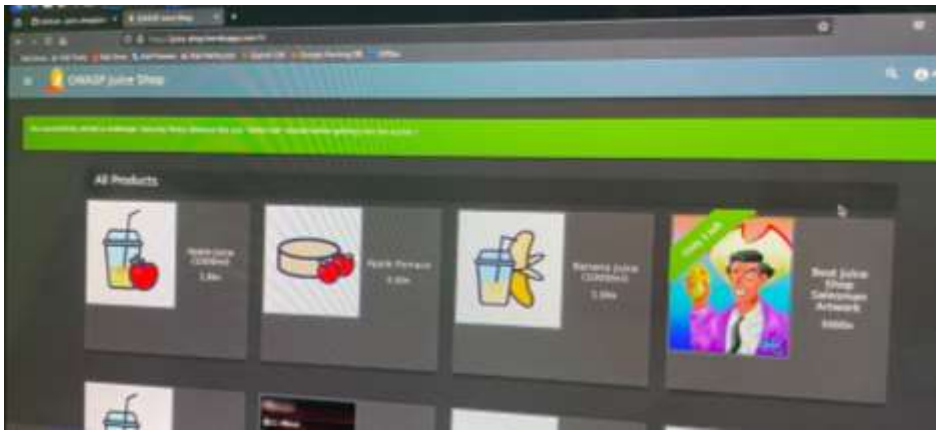
1. Open OWASP Juice Shop on Firefox.
2. Sign in and select a product.
3. Add it to the basket and proceed to checkout.
4. Add a new address and payment details.
5. Write JavaScript code in the order tracking path and refresh.

**Video Link:**
https://drive.google.com/file/d/1A3a2FhbjAWyeW6OhtVAtaTVw64UVAXXh/view?usp=drive_link

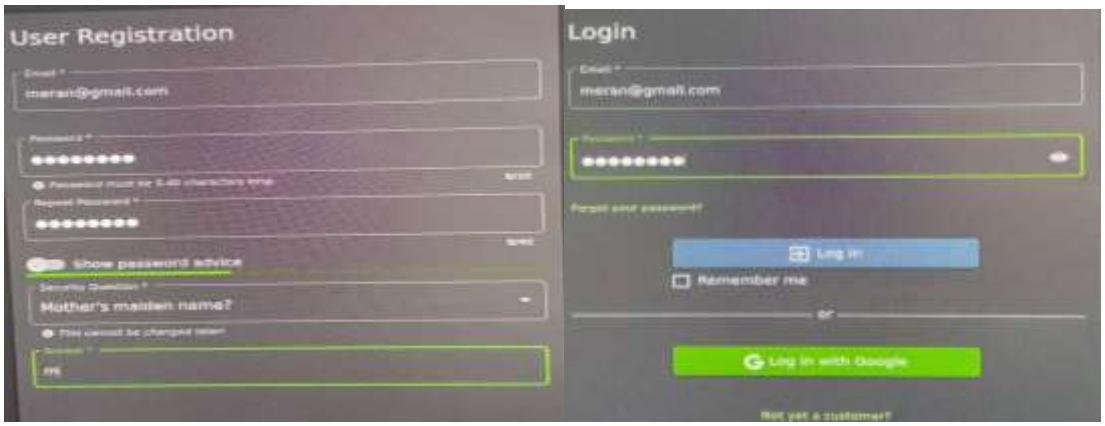
---

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

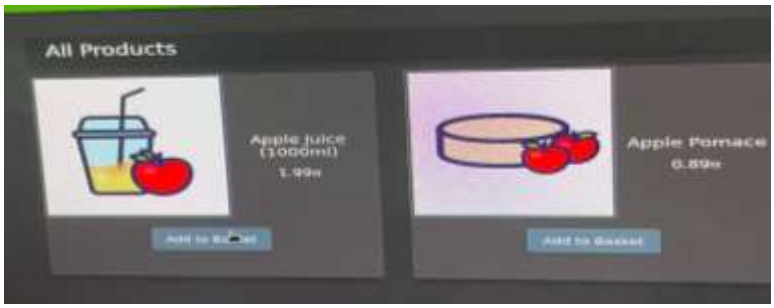
1-First open owasp juice shop on firefox in linux.




2-Sign in Then Login.

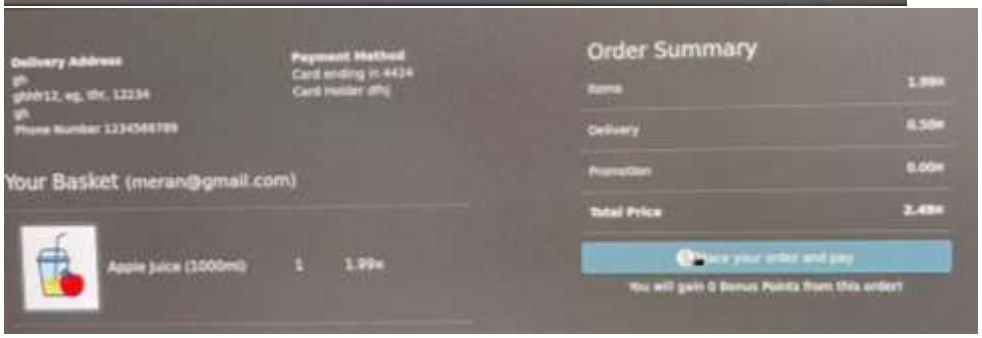



3-Choose any product and add it to basket and check out.

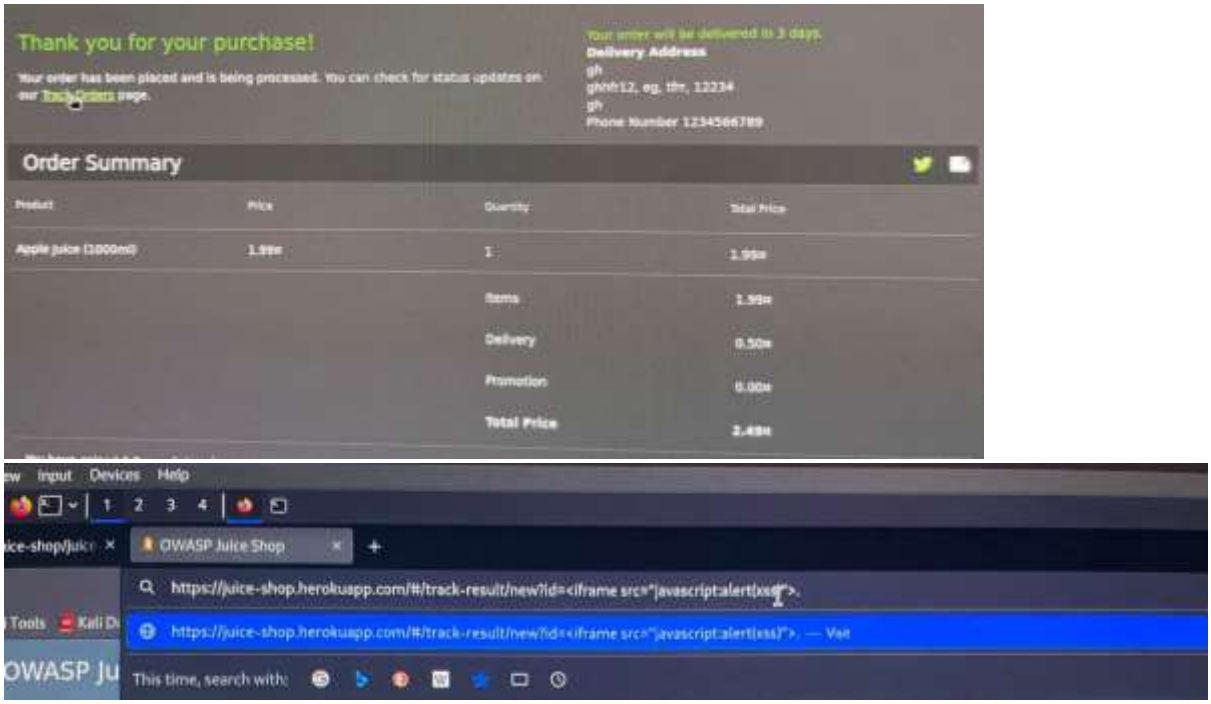



4-Add new address.


5-Payment details and place my order.

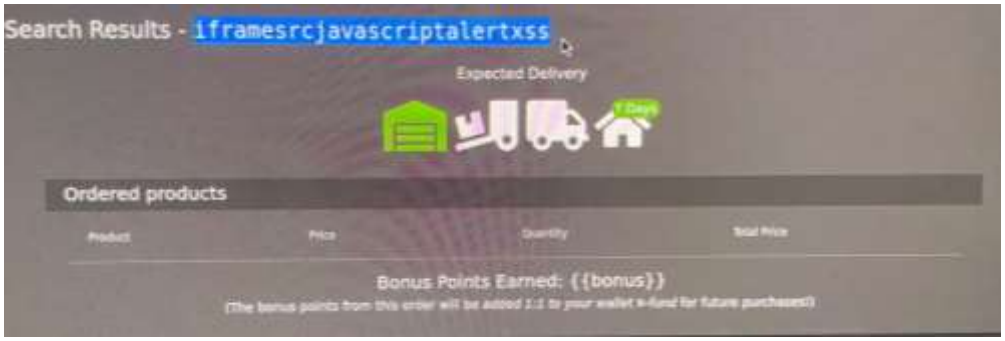

6-press on track orders then write javascript code after id= in the path.







7-click refresh and the attack will be done.



**4th Attack: Brute Force on Admin Credentials**

**Attack Description:** Brute-forcing systematically tries password combinations to gain unauthorized access. Without rate limiting or CAPTCHA, attackers can repeatedly attempt logins.

**Risk and Impact:**

1. Unauthorized access to admin functions.
2. Exposure of user data.
3. Data manipulation or deletion.
4. Potential installation of backdoors.

**Impact:**

- Full application compromise.
- Financial, reputational, or legal damage.

**Tools Used:**

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

**Attack Steps:**

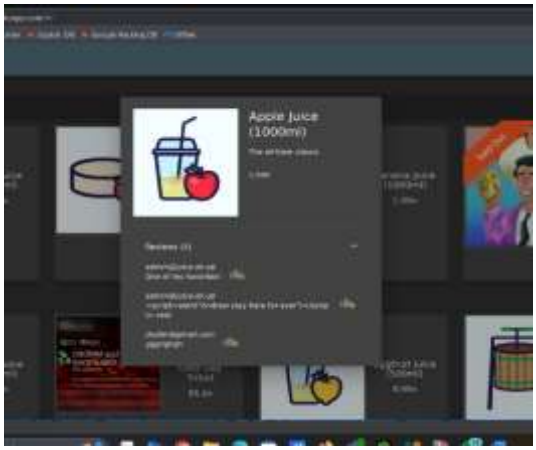
1. Open the website and use an example admin email.
2. Intercept login requests with Burp Suite.
3. Configure proxy settings.
4. Send the request to Burp Suite Repeater and Intruder.
5. Use a password list from GitHub.
6. Identify the valid password.
7. Reconfigure proxy settings and log in.

**Video Links:**
**https://drive.google.com/file/d/1C82rHmqTWgiAjKQo00VScABsQTdqHMtq/view?usp=drive_link**

---

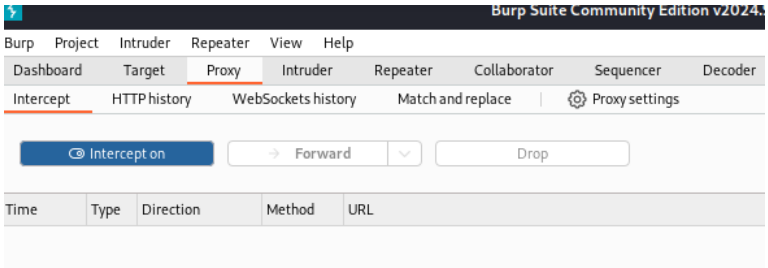
This part of report highlights the risks and methods involved in brute-force attacks targeting admin credentials and proposes preventive measures.

1- First open the website and choose the email you want to hack for example we will use admin@juice-sh.op.




2- And then login with any password


3- And then go to brup suite and go to proxy and press intercept on



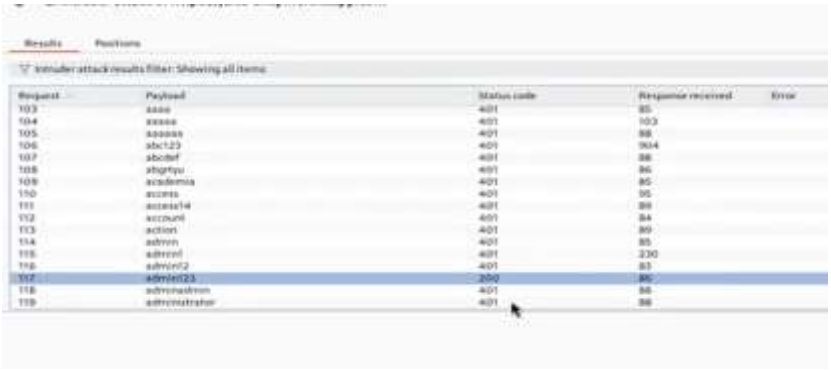

4- And then go to settings in website and search network and press manual proxy and write HTTP Proxy and Port and press ok

5- And login again with wrong password and go to brup suite and go to HTTP history and press on login

6- 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$

7- 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.



8- 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