**Web Penetration Testing Report**

*Video link :* https://drive.google.com/file/d/1Qc\_X1a5MjkbotmWT19thlGT5Gpiik\_xT/view?usp=sharing

**Executive Summary**

* **Purpose of the Test**:  
  The purpose of this test is to evaluate the security of websites and applications, identify vulnerabilities, and analyze their potential impact.
* **Key Findings**:  
  Several vulnerabilities were identified, including critical ones that could pose significant threats to data and system integrity.
* **High-Level Impact**:
  + **SQL Injection**: Potential for sensitive data exposure or manipulation.
  + **Enumeration**: Enumeration to Find Admin Path.
  + **XSS (Cross-Site Scripting)**: Risk of stealing user information or executing malicious scripts.
  + **Brute Force on Admin Credentials**: Risk of unauthorized access to the admin panel through credential guessing.
* **Summary of Recommendations**:
  + Update and secure application code to mitigate discovered vulnerabilities.
  + Strengthen security configurations for servers and applications.
  + Implement account lockout and two-factor authentication (2FA) to prevent brute force attacks.

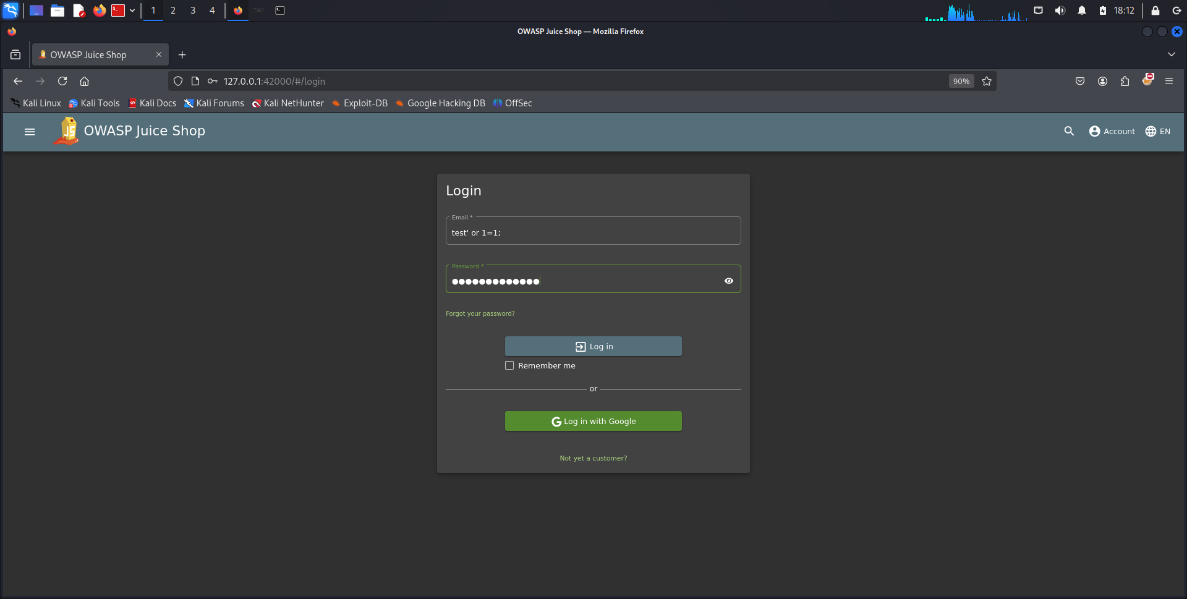
**Scope and Methodology**

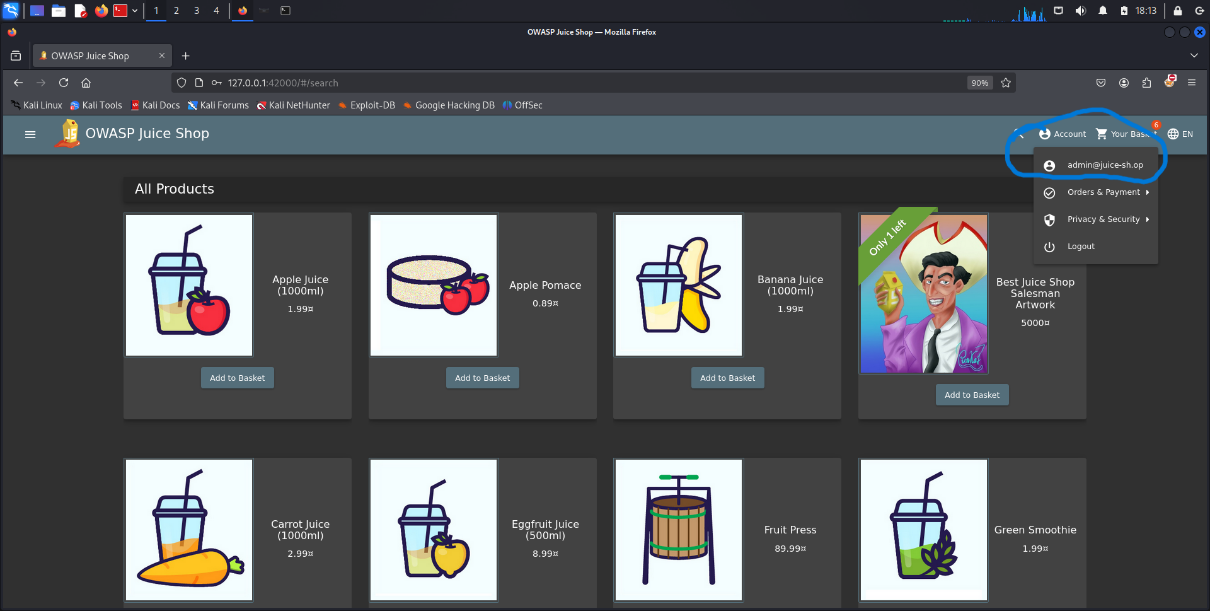
* **Scope**:  
  The test covered the following websites, and applications:
  + Juice shop

**Approach**:  
The following penetration testing approaches were used:

* + **Grey-box testing**: Limited knowledge of the system.
* **Tools Used**:
  + Burp Suite
  + ffuf
  + Dirb

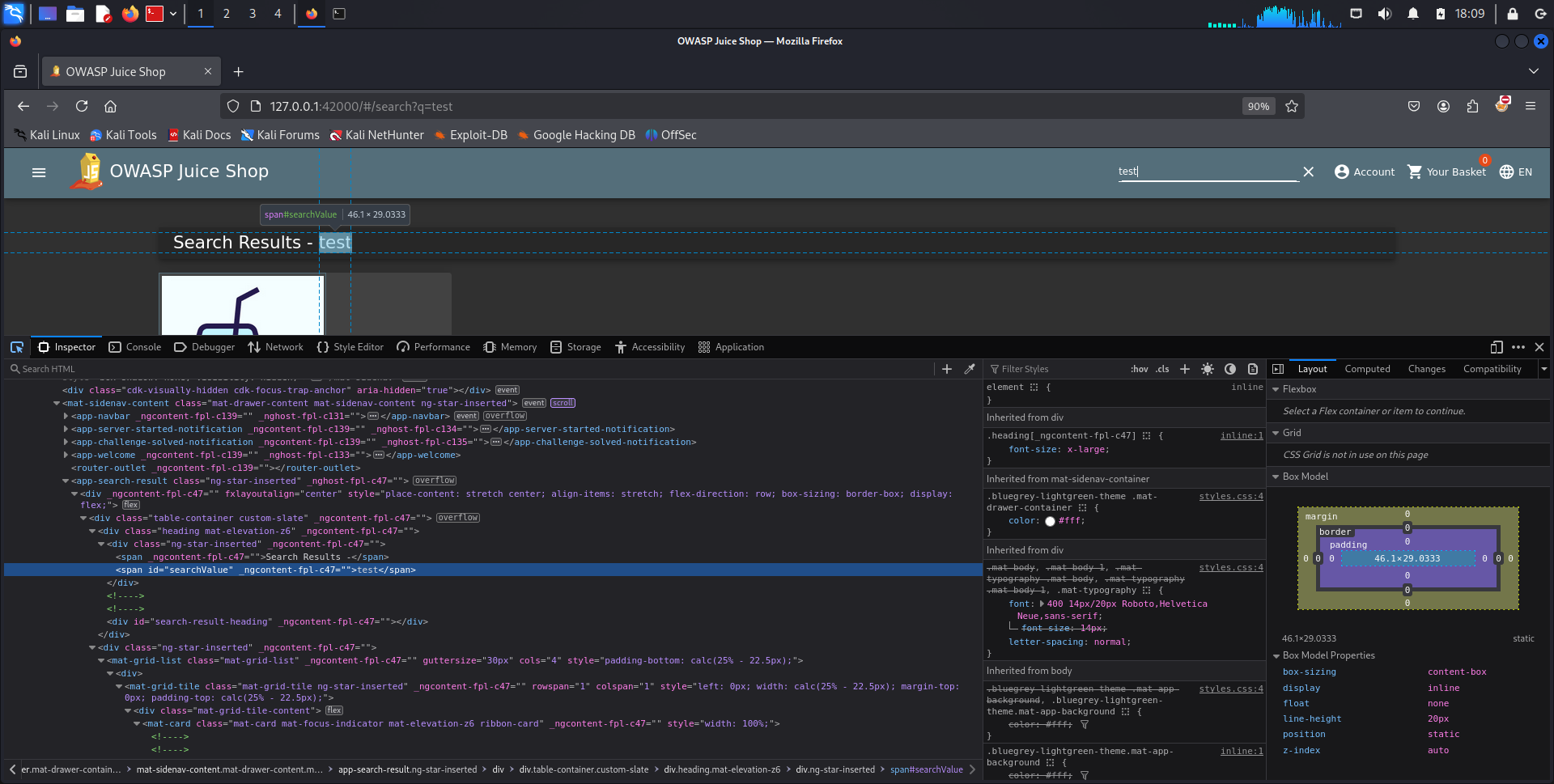
**Vulnerability Findings**

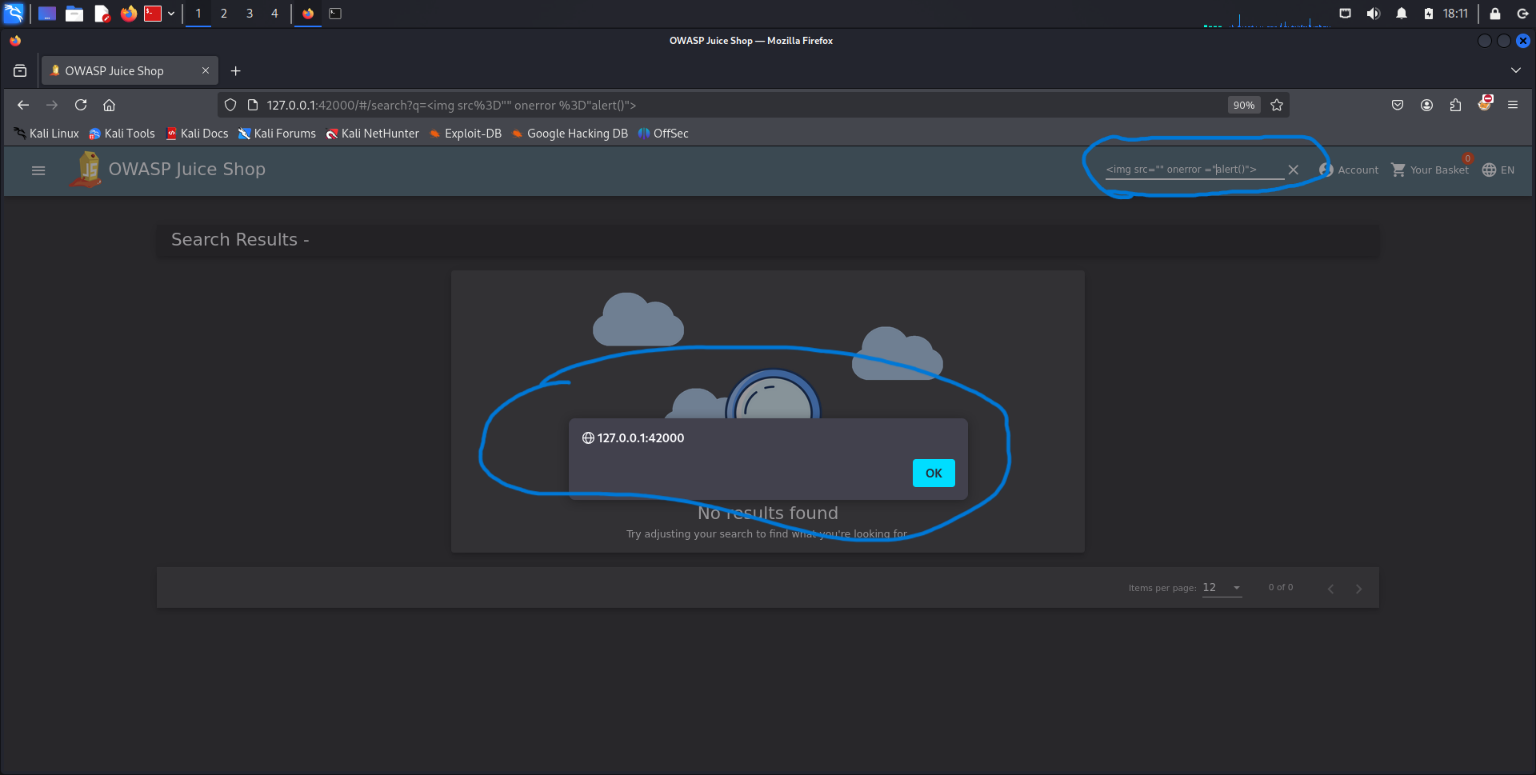
* **Critical Vulnerabilities**:
  1. **SQL Injection**
     + **Description**: A vulnerability that allows malicious SQL queries to be executed on the database.
     + **Risk and Potential Impact**:
       - Unauthorized access to sensitive data or database manipulation.
     + **Evidence**:
       - **Screenshot :**



* + - **Remediation Steps**:
      * Use parameterized queries (Prepared Statements).
      * Audit and fix vulnerable code.
  1. **Cross-Site Scripting (XSS)**
* **Description**: A vulnerability that allows injecting malicious JavaScript into web pages.
* **Risk and Potential Impact**:
  + Theft of user credentials or execution of malicious actions.
* **Evidence**:
  + **Logs**: write <iframe src=" https://alexu.mans.edu.eg/static/index.html "></iframe> in search bar OR <img src ="" onerror="alert()">
* **Remediation Steps**:
  + Properly validate and sanitize user inputs.
  + Implement a Content Security Policy (CSP).

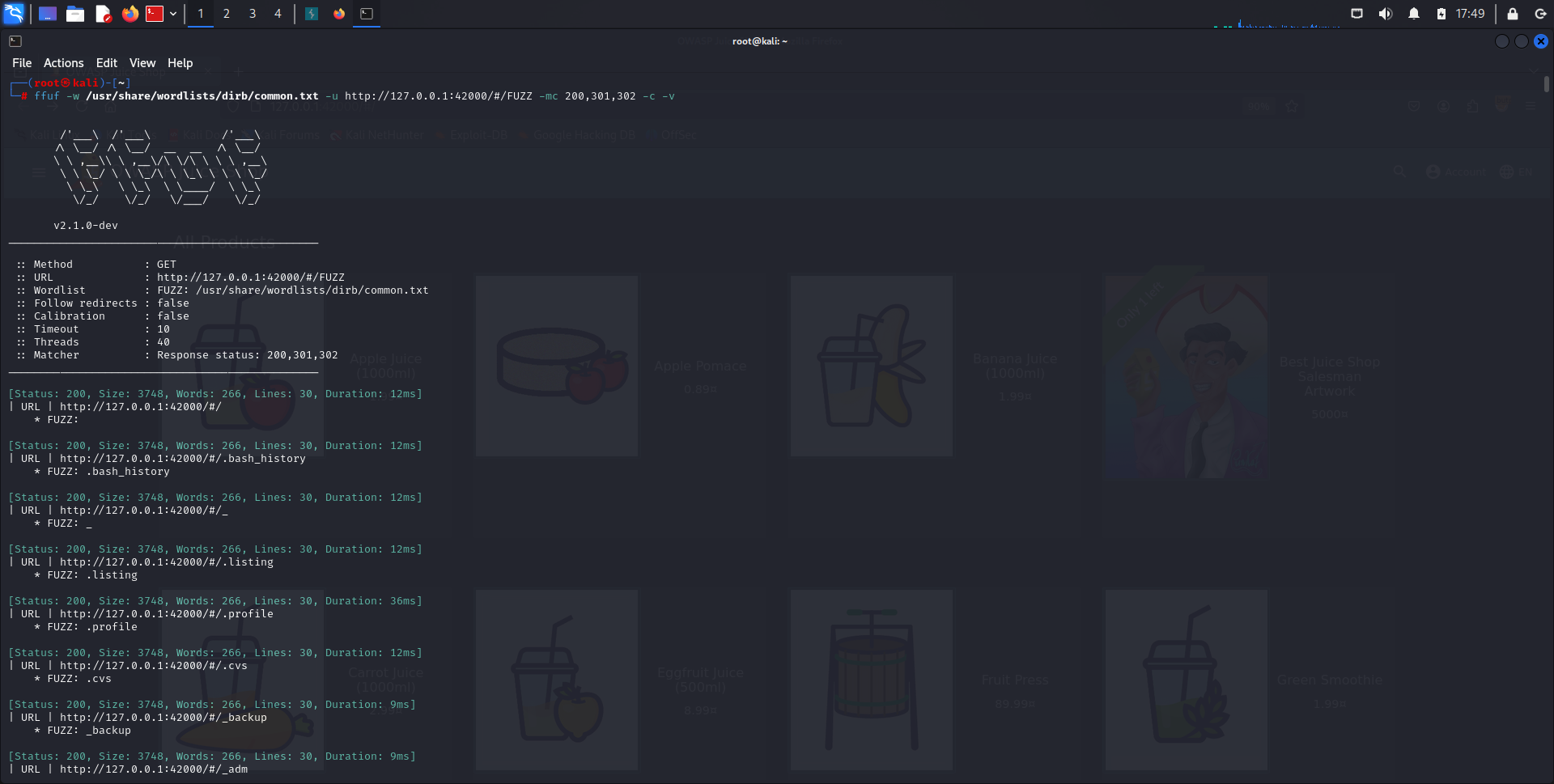
**Screenshot :**

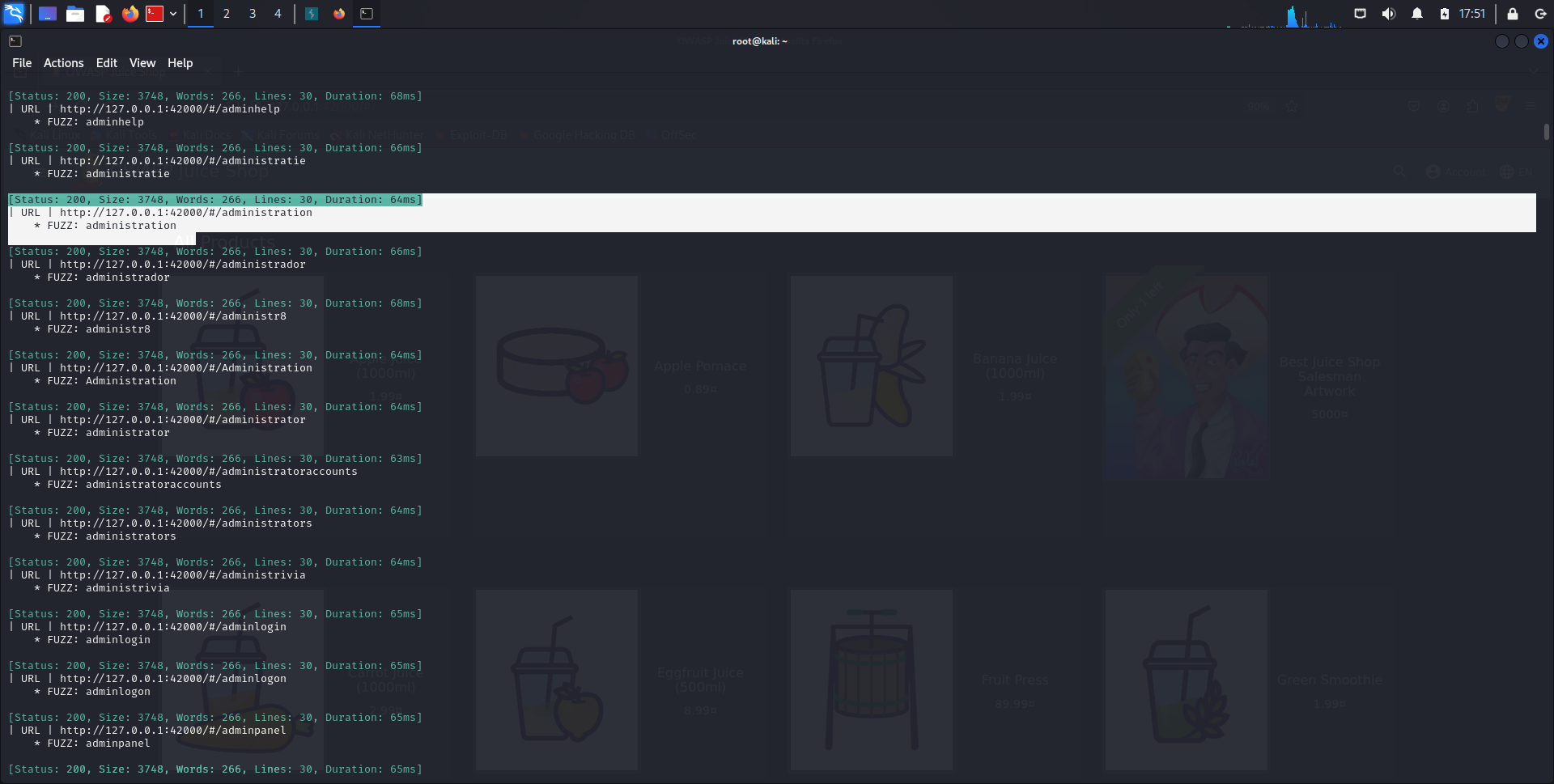


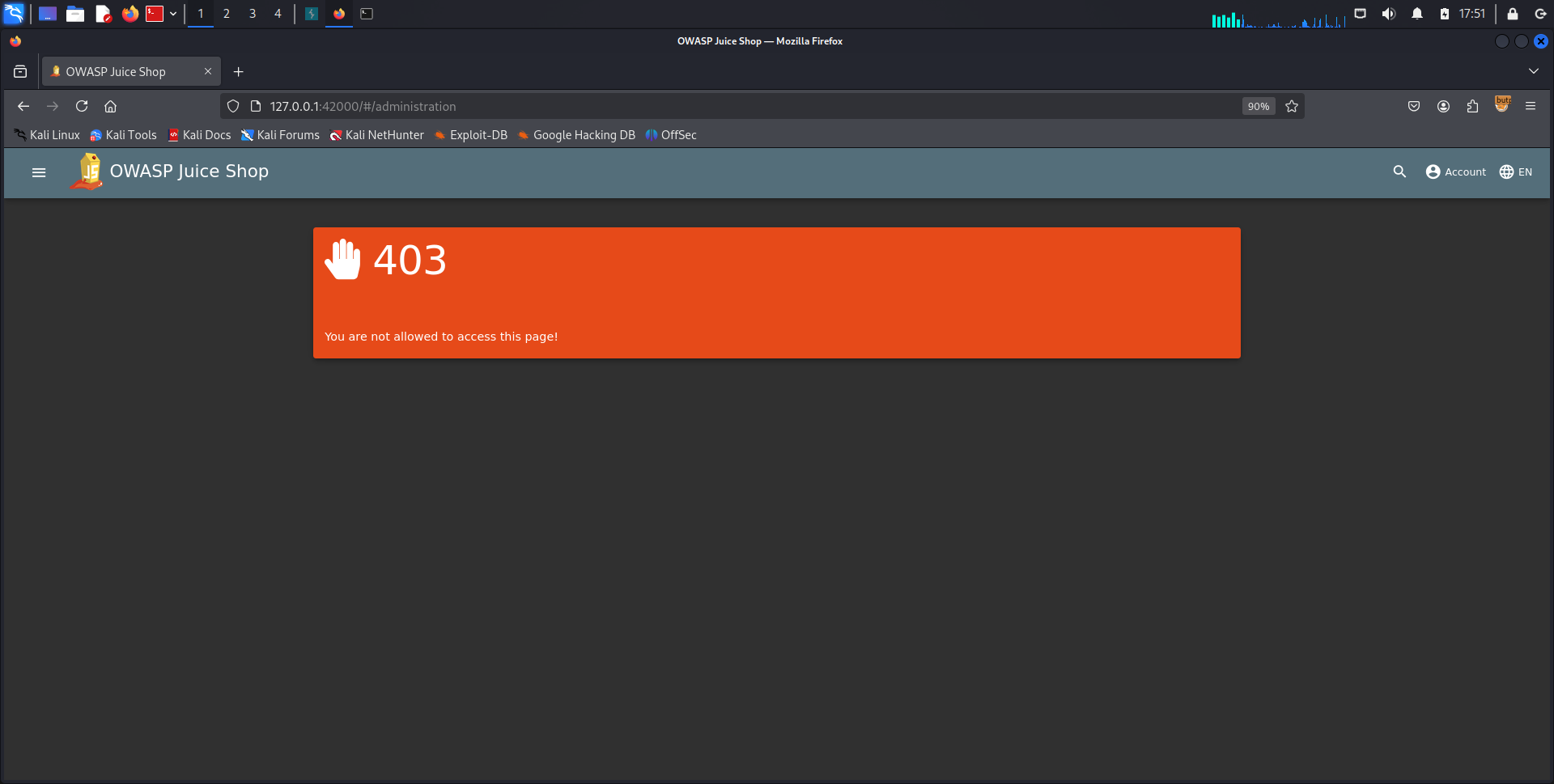


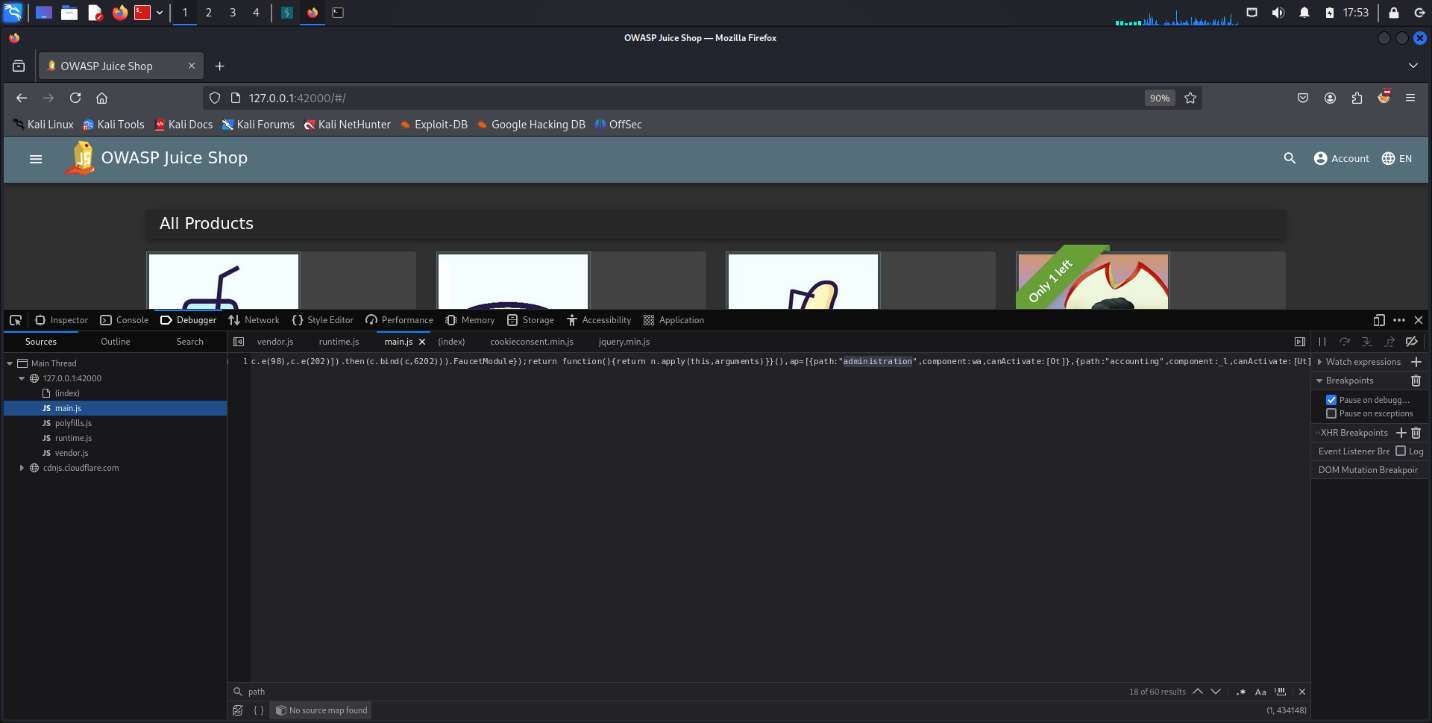
**3. Enumeration to Find Admin Path**

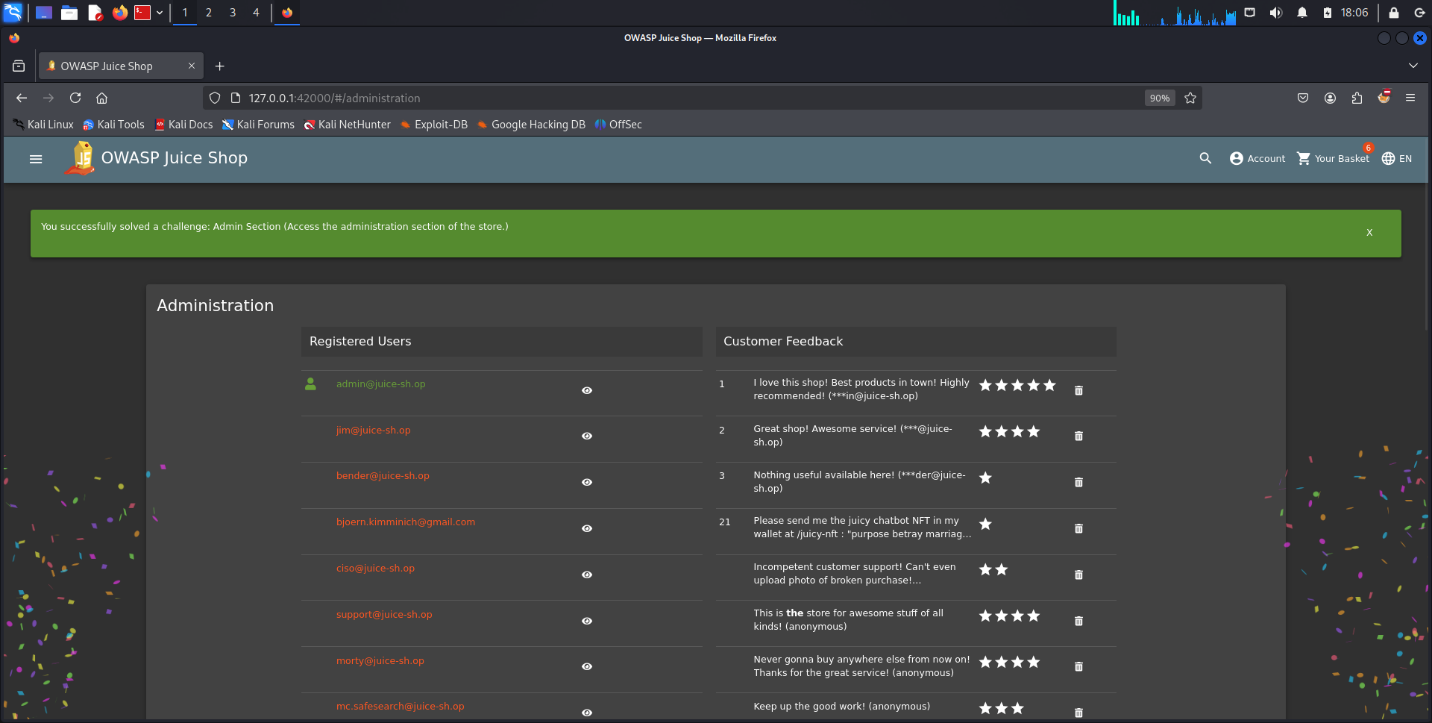
* + - **Description**: An attacker can enumerate URLs or directories to discover hidden admin paths This can be exploited to gain unauthorized access or prepare for brute force attacks.
    - **Risk and Potential Impact**:
      * Unauthorized access to the admin portal.
      * Increased likelihood of targeted attacks, such as credential stuffing or brute forcing.
    - **Evidence**:
      * **Screenshot**:



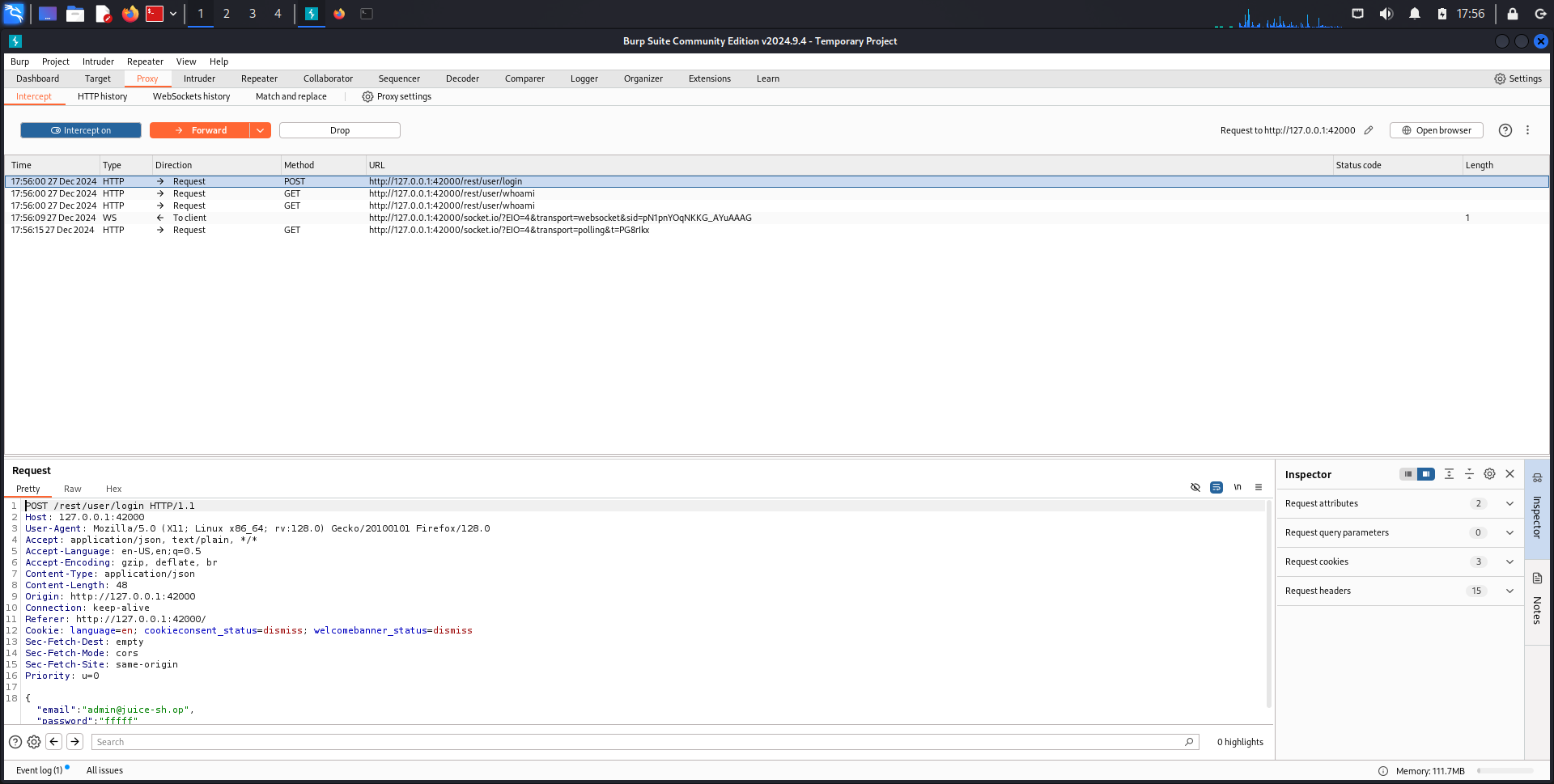


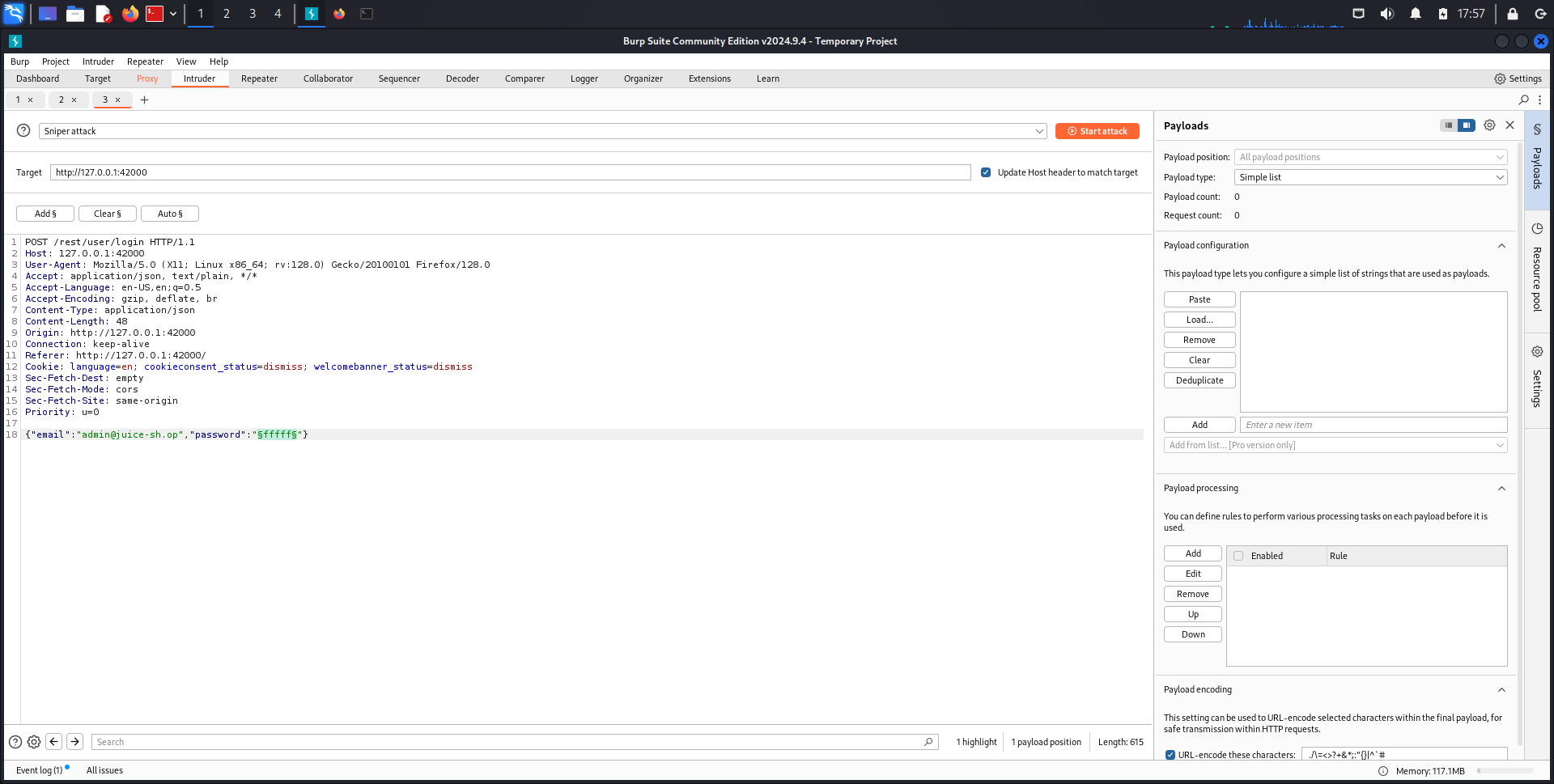


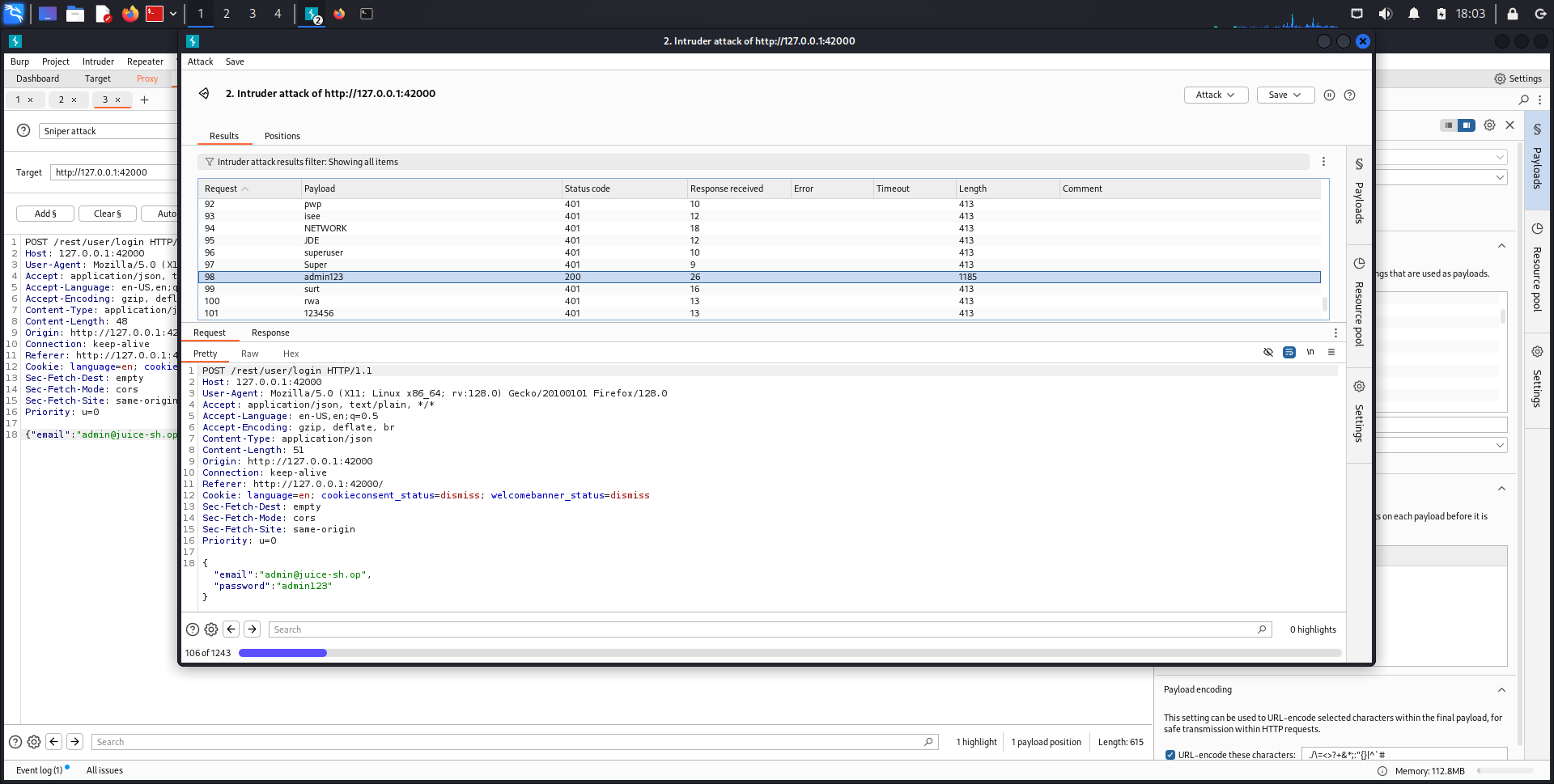


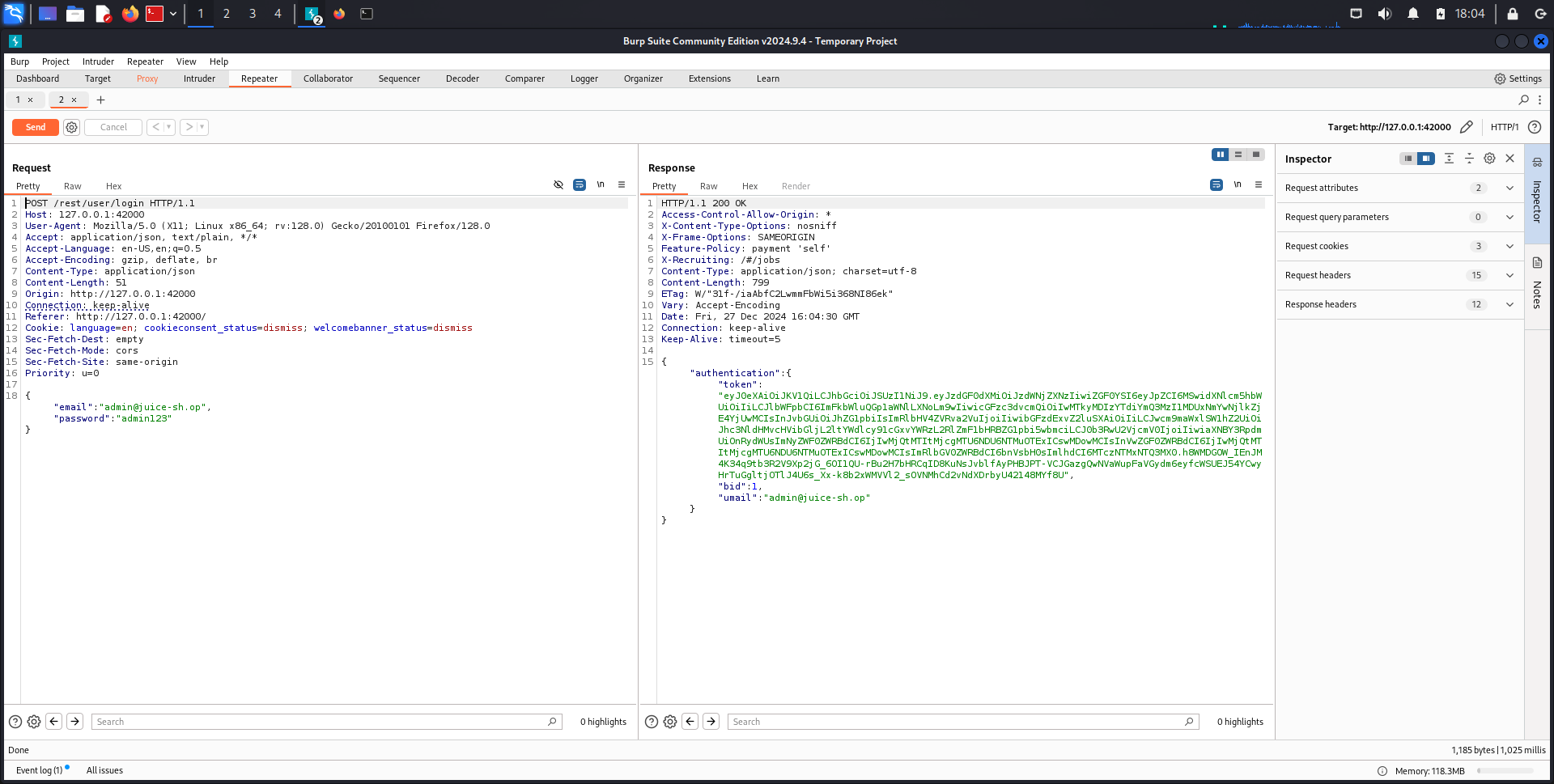


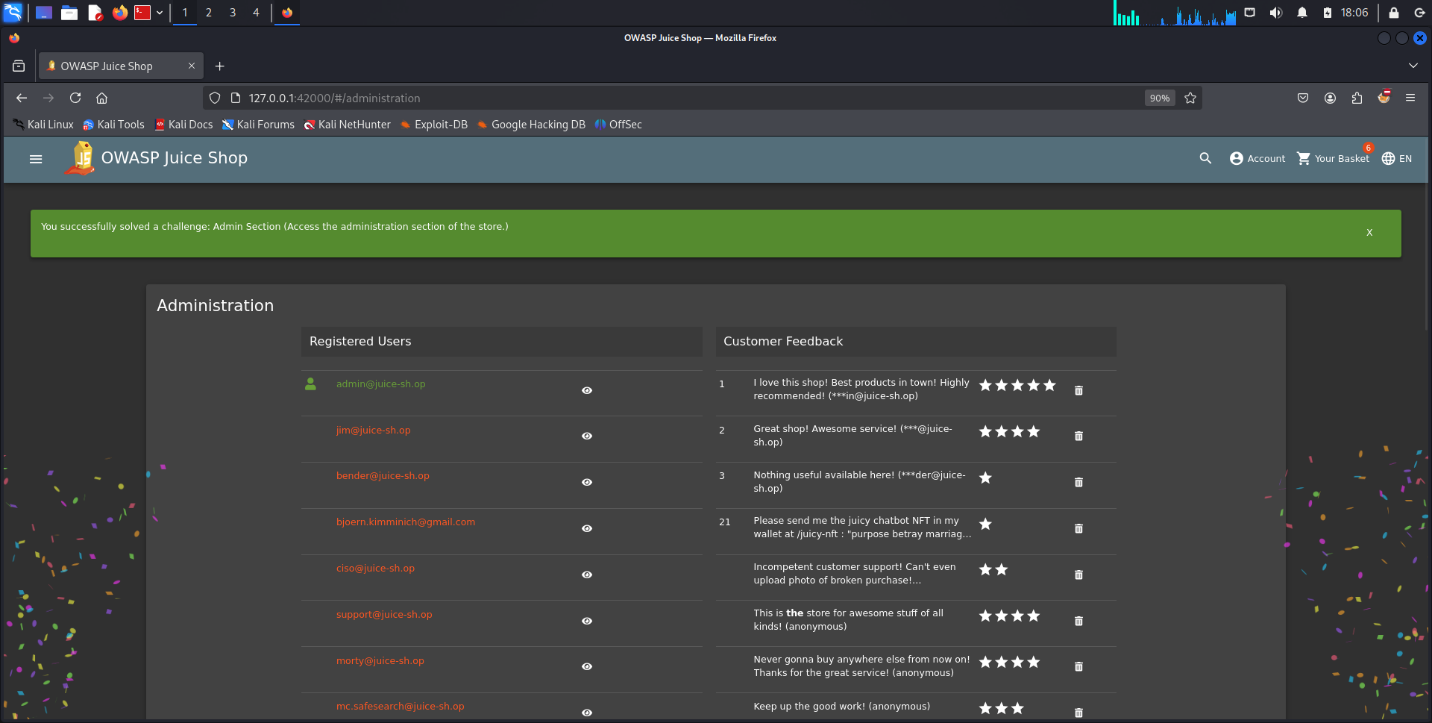
* + - **Remediation Steps**:
      * Implement obscurity by renaming admin paths to non-standard names.
      * Use proper authentication and access controls for sensitive directories.
    1. **Brute Force on Admin Credentials**
* **Description**: An attack method that involves attempting multiple username and password combinations to gain access to admin accounts.
* **Risk and Potential Impact**:
  + Unauthorized access to the admin panel, allowing the attacker full control over the system.
* **Evidence**:
  + **Screenshot**:

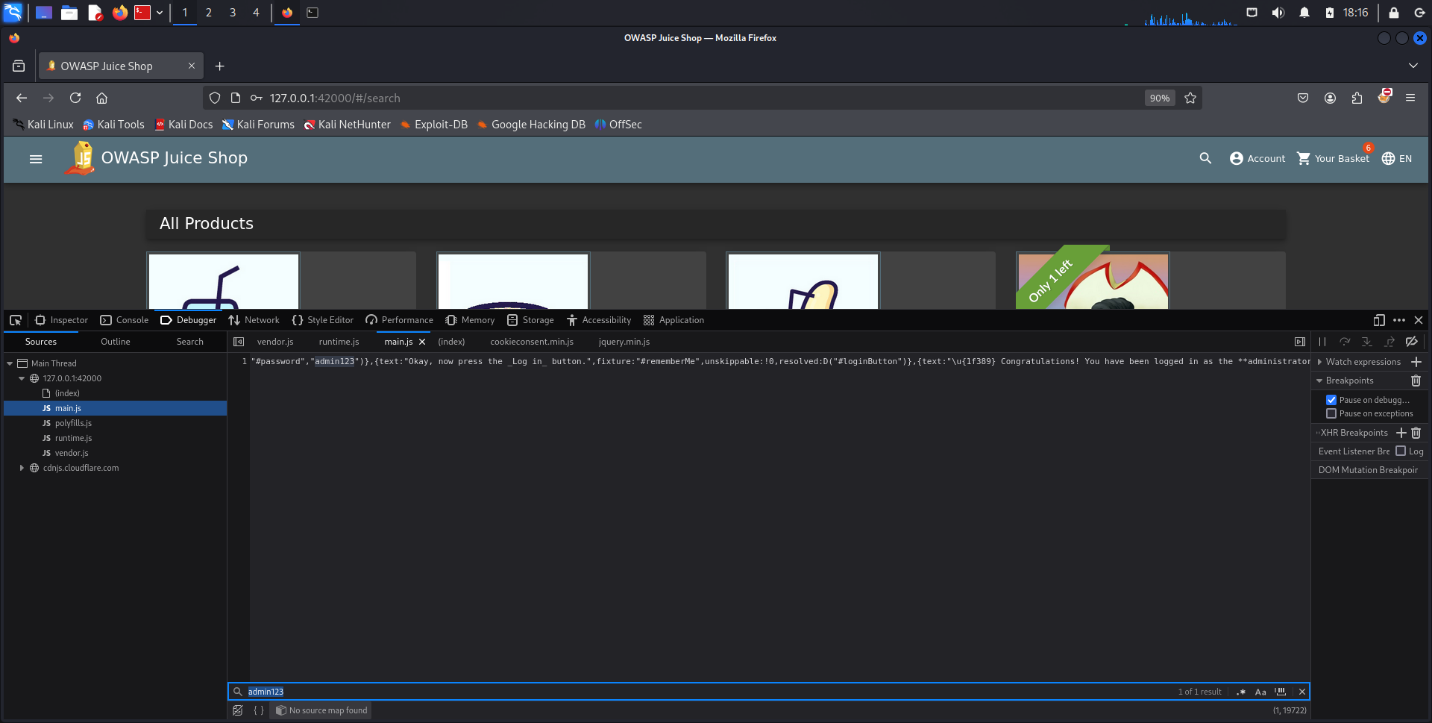












* **Remediation Steps**:
  + Implement account lockout after a defined number of failed login attempts.
  + Enable two-factor authentication (2FA).
  + Enforce strong password policies.
  + Regularly monitor logs to identify unusual activity

يوسف محمد السيد متولي 2305074

عمر حسان يعقوب 2305043

فارس ايهاب الزوكه 2305044