# **Final project (report)**

# 

**Team leader : Omar Abdelaal Saad**

**ID: 2305165**

**Member 2 : Mustafa Aly Mustafa   
ID : 2305616   
Member 3 : Mohammed Osama Mohammed   
ID : 2305180**

**Executive Summary   
  
Purpose of the Test**:  
  
We identify the vulnerabilities in Juice Shop and analyze how attackers can exploit them.  
 **High-level impact and critical vulnerabilities.**

1. Presence of an XSS vulnerability.
2. Lack of rate-limiting led to multiple brute-force attacks, resulting in system compromise.
3. Hidden administrative paths can be discovered through random URL enumeration.

**Summary of Recommendations:**

1. Implement login attempt rate-limiting.
2. Restrict access to administrative paths.

**Scope and Methodology  
  
Tools Used:**

* **Burp Suite**
* **OWASP ZAP**
* **Hydra**
* **Kali Linux**

**Vulnerability Findings  
  
1. Critical Vulnerability:** **XSS in Product Search**

**a. Description:**   
The vulnerability is exploited by injecting a malicious JavaScript payload (<iframe src=javascript:alert('xss')>) into the search bar. The application reflects this input back without any sanitization or validation, causing the script to execute in the user's browser.

**b. Risk & Impact:**   
This flaw allows an attacker to:

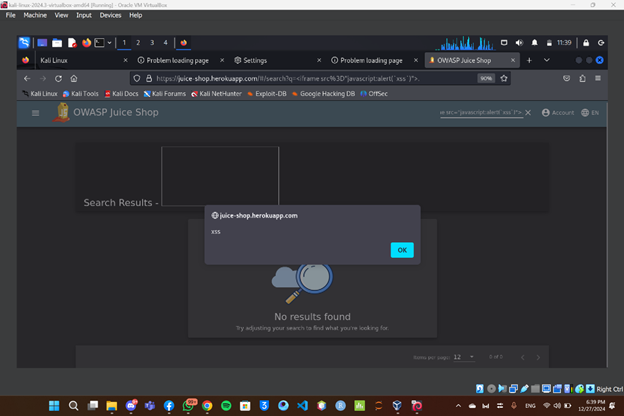
Execute arbitrary JavaScript in the victim’s browser.

Steal session cookies or other sensitive data.

Redirect users to malicious websites.

**c. Remediation:**   
Use Security Tools: Regularly test your app with tools like Burp Suite or OWASP ZAP to catch issues early.

**d. Evidence:**



**2. Critical Vulnerability:** **SQL Injection in Login Page**

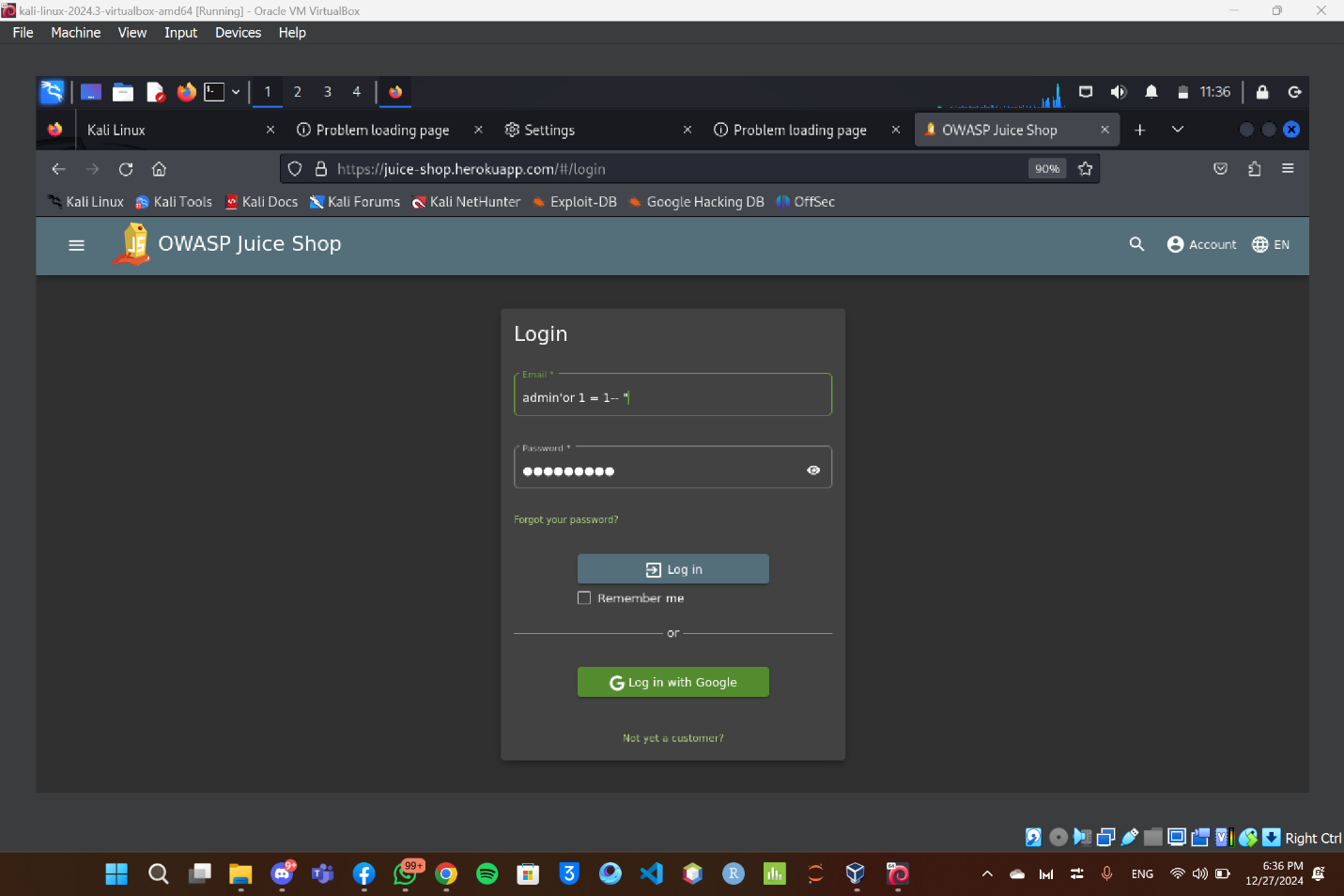
**a. Description:**   
The login page is vulnerable to SQL Injection, allowing attackers to bypass authentication. By entering malicious SQL code  
such as: admin' OR 1=1 --

the attacker forces the database to accept the condition as always true, granting unauthorized access to the admin account.

**b. Risk & Impact:**   
1. Authentication Bypass: Attackers can gain admin-level access without valid credentials.  
2. Data Breach: Sensitive user data and application integrity are at risk

**c. Remediation:**

Monitor logs for suspicious activity to detect and respond to attacks.

**c. Evidence:**

**3. Critical Vulnerability:** **Brute Force on Login Page**

**a. Description:**   
The login page lacks adequate protection mechanisms, such as rate-limiting or account lockouts. This allows attackers to use automated tools (like Burp Suite) to try various username-password combinations until a valid one is found.

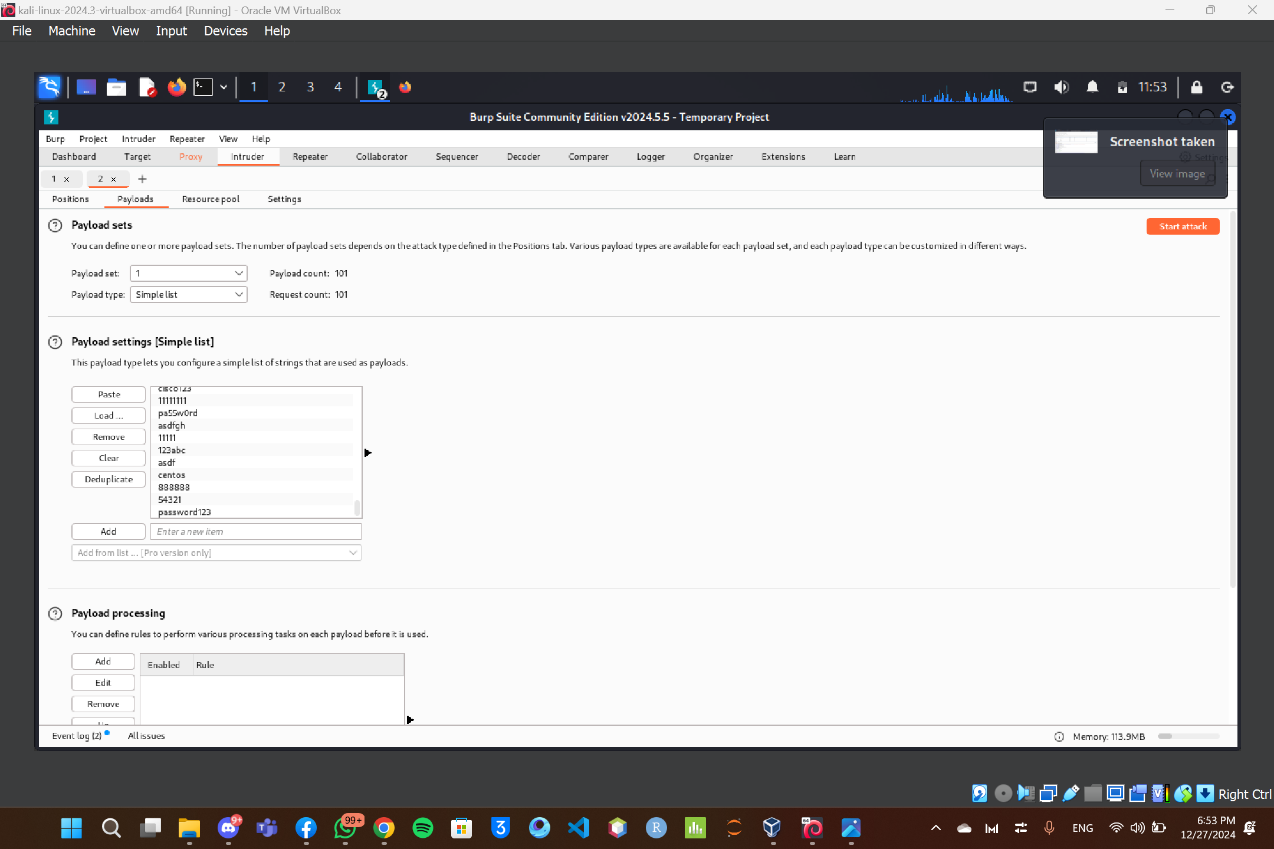
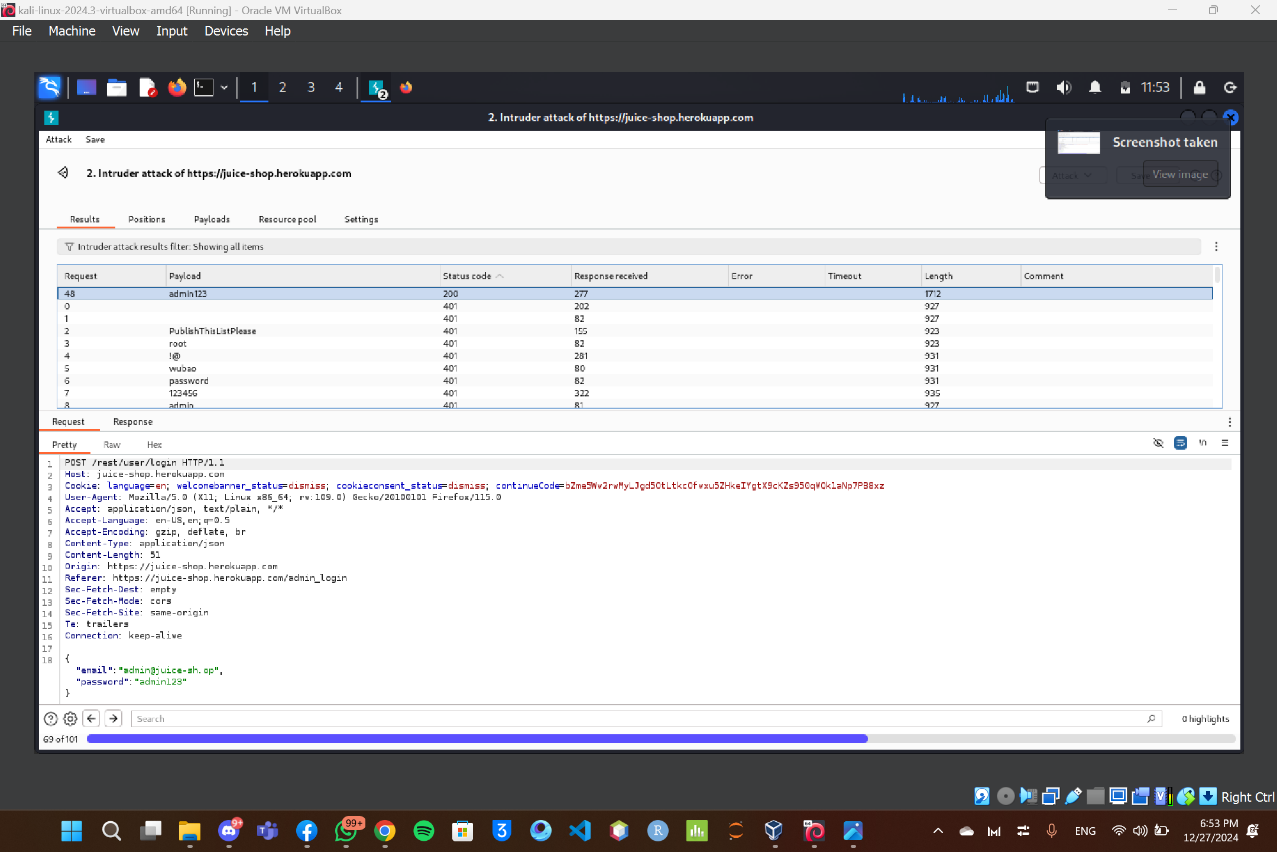
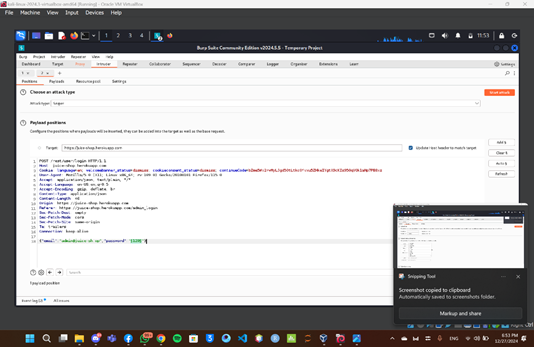
**b. Risk & Impact:**   
1. Credential Compromise: Attackers can gain unauthorized access to accounts, including admin accounts.

2. System Abuse: A successful brute-force attack could lead to data theft, privilege escalation, and compromised user trust.

**c. Remediation:**

1. Logging and Monitoring: Detect and respond to brute-force attempts by monitoring login activity.

2. Multi-Factor Authentication (MFA): Add an extra layer of security to reduce reliance on password strength alone

**d. Evidence:**

**Exploitation and attacks**We used:

* **Hydra** to perform brute-force attacks.
* **Gobuster** to identify hidden paths.
* **Burp Suite** to test for XSS vulnerabilities.

The owner's account was successfully accessed through brute-force attacks, allowing us to gain full control over the website.

**Conclusion**

The OWASP Juice Shop website contains numerous critical vulnerabilities that pose significant risks to both the site and its registered users if exploited.

**This link contains the team's videos.**

https://drive.google.com/drive/folders/1sHfWJy4JoQOWGzKsmwAhHLHfQDMaQyCj?usp=drive\_link