Cyber security project

Name : Abdelrahman nagy elbehery

Id : 2305**160**

Name : farah Mohamed mansour

Id : 2305**174**

Name : afnan sobhy eldewer

Id : 2305**131**

### Tools Used: • Burp Suite • OWASP ZAP • Kali Linux Test Objective:

The aim of this penetration testing was to discover and exploit vulnerabilities within the OWASP Juice Shop application.

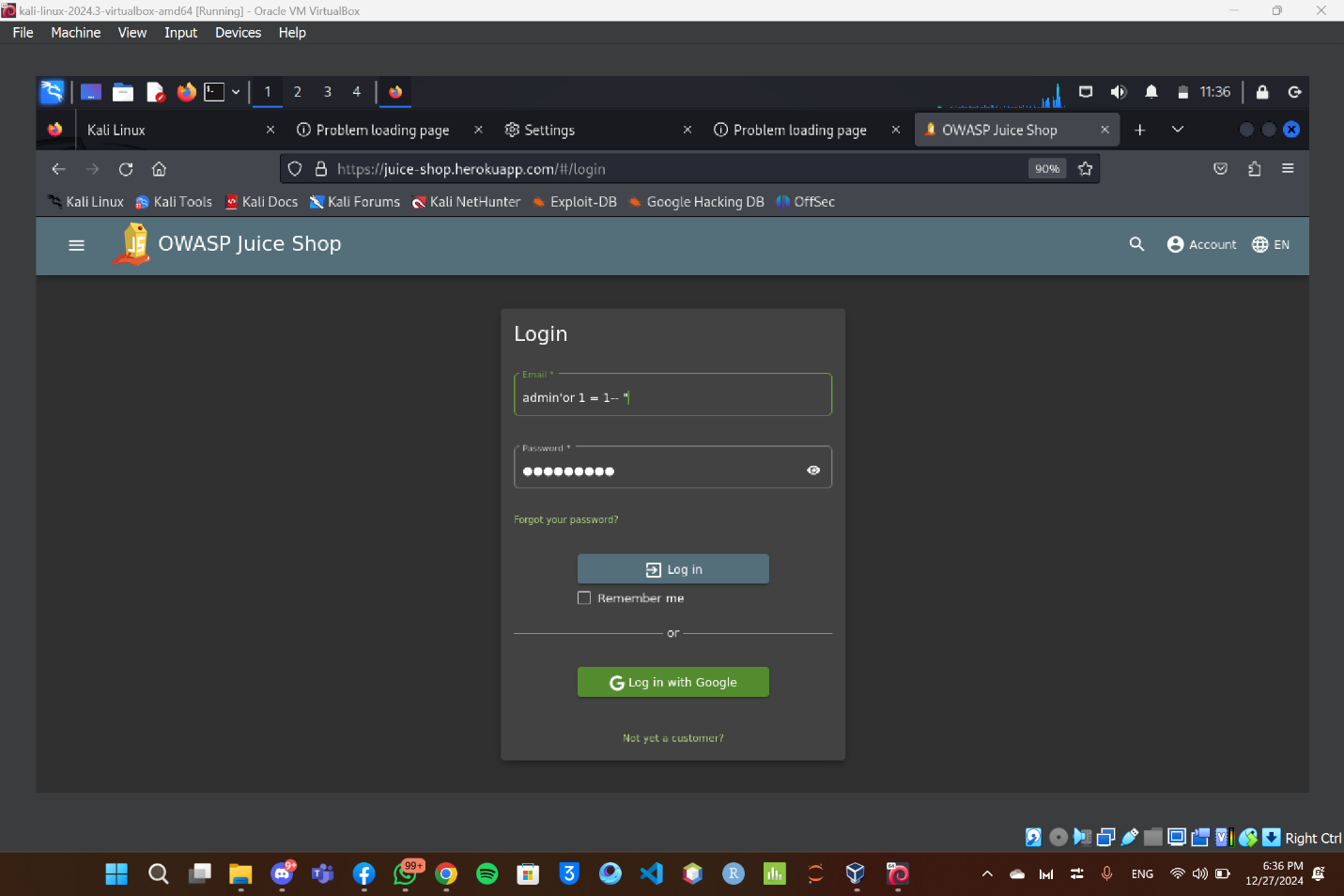
**Key Findings:**

* Several high-risk vulnerabilities were found, including **SQL Injection**, **Cross-Site Scripting (XSS)**, and **weak authentication mechanisms**.
* Exploiting these flaws demonstrated severe security risks, such as **unauthorized access**, **potential data leakage**, and **session hijacking**.

**Recommendations:**

It is crucial to address and fix these vulnerabilities immediately to safeguard the application from any potential threats.

**Sql enjection**



### SQL injection is a type of attack where malicious SQL code is inserted into an input field or request to manipulate a database. potentially gaining unauthorized access to data, modifying or deleting information, or performing other harmful actions.

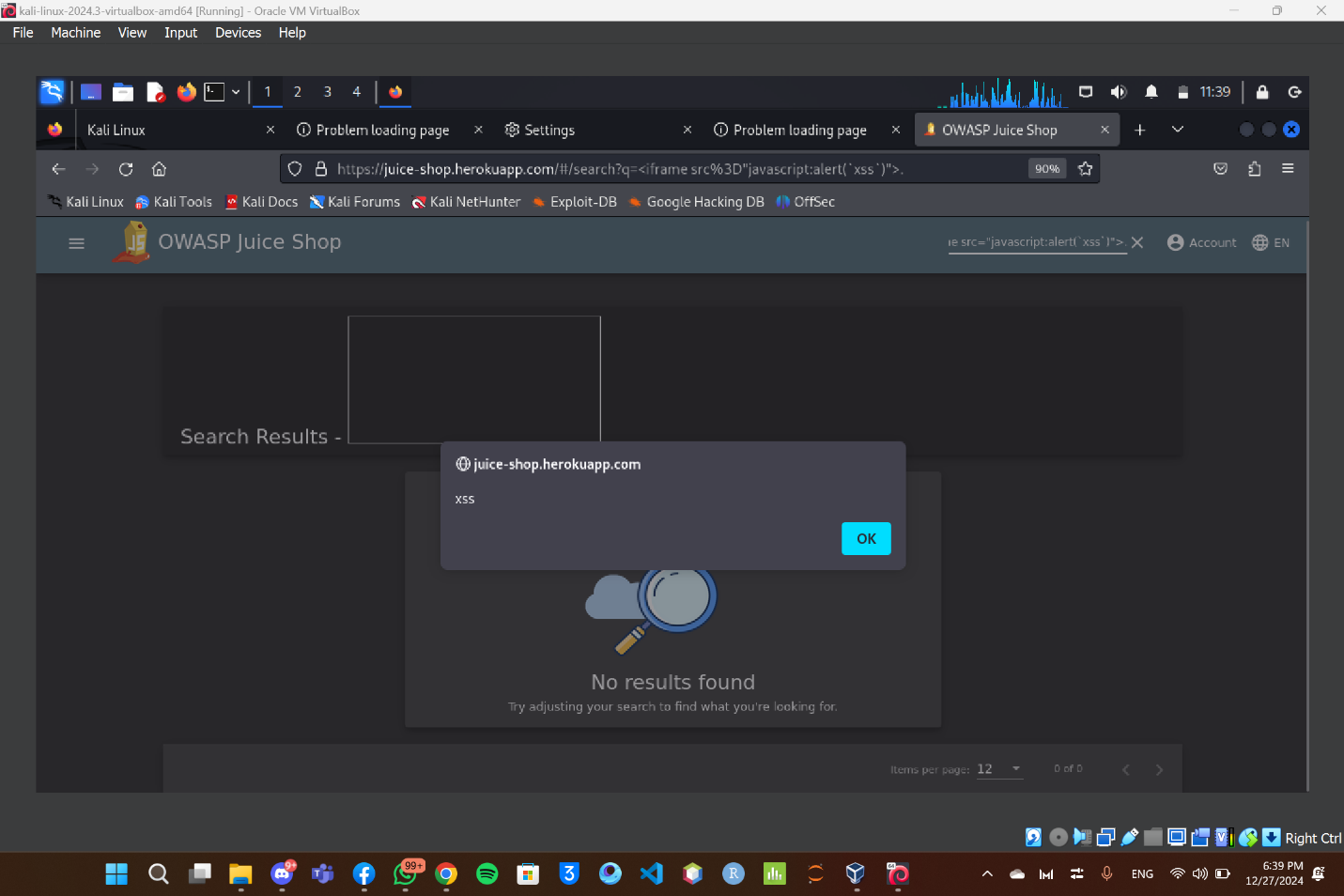
### Impact:

1. **Bypass Authentication**: Attackers can access the admin panel without valid credentials, potentially gaining full control over the system.
2. **Data Exposure**: Sensitive information such as user data, passwords, and other critical details could be accessed, leading to a potential data breach.

### ****Remediation****:

* **Use Parameterized Queries**: Replace dynamic SQL queries with parameterized statements or prepared queries to prevent SQL Injection attacks.

**Xss**



An **XSS attack** is a type of cyberattack in which an attacker exploits a web application’s vulnerability to inject malicious scripts into a webpage. These scripts then execute in the browser of other users who access the compromised page, potentially causing harmful effects.

### ****Impact****:

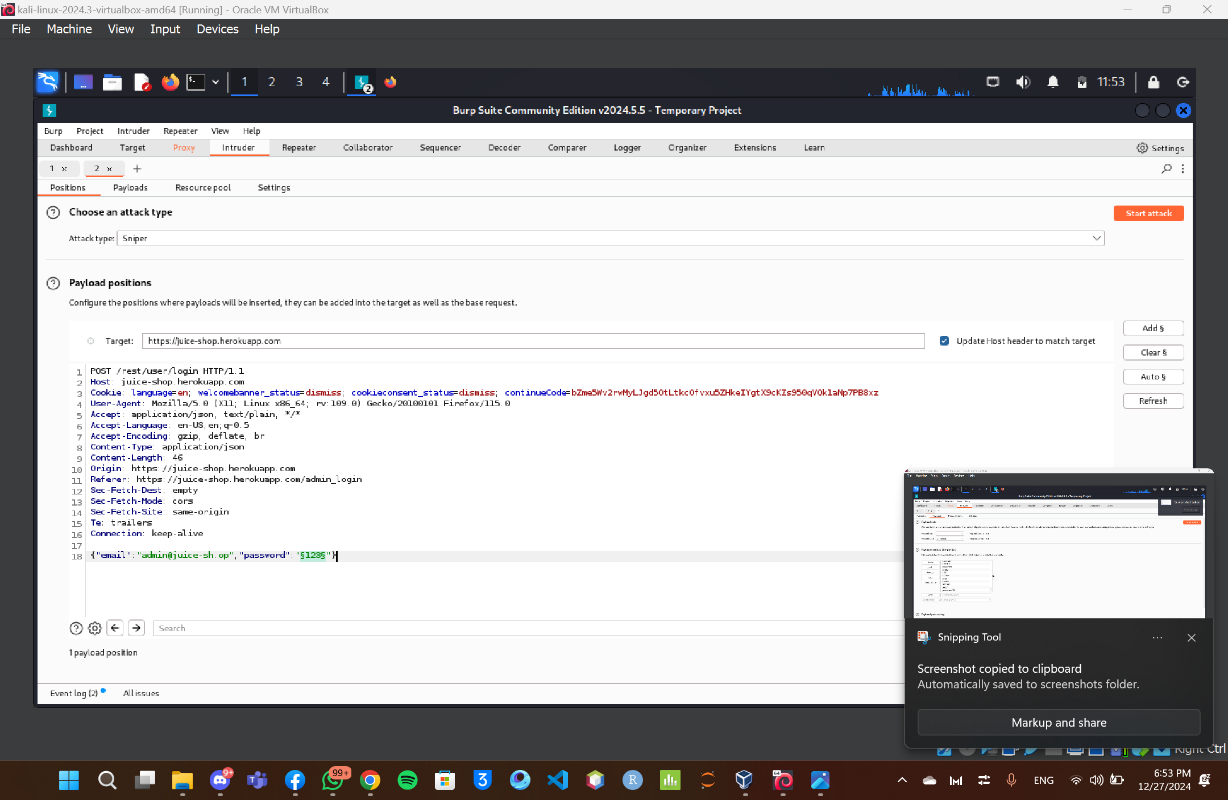
This vulnerability enables an attacker to:

* Inject and execute malicious JavaScript in the target user's browser.
* Steal sensitive information, such as session cookies or personal data.
* Redirect users to harmful websites, potentially leading to phishing attacks or malware infections.

### ****Remediation****:

* **Implement Security Best Practices**: Regularly scan your application using security tools like Burp Suite or OWASP ZAP to identify and resolve potential vulnerabilities early.

**Brute force**



A **brute force attack** is a type of cybersecurity attack where an attacker systematically tries all possible combinations or inputs (such as passwords, encryption keys, or other credentials) until the correct one is found. The goal is to gain unauthorized access to systems, accounts, or data by exhaustively testing all potential solutions.

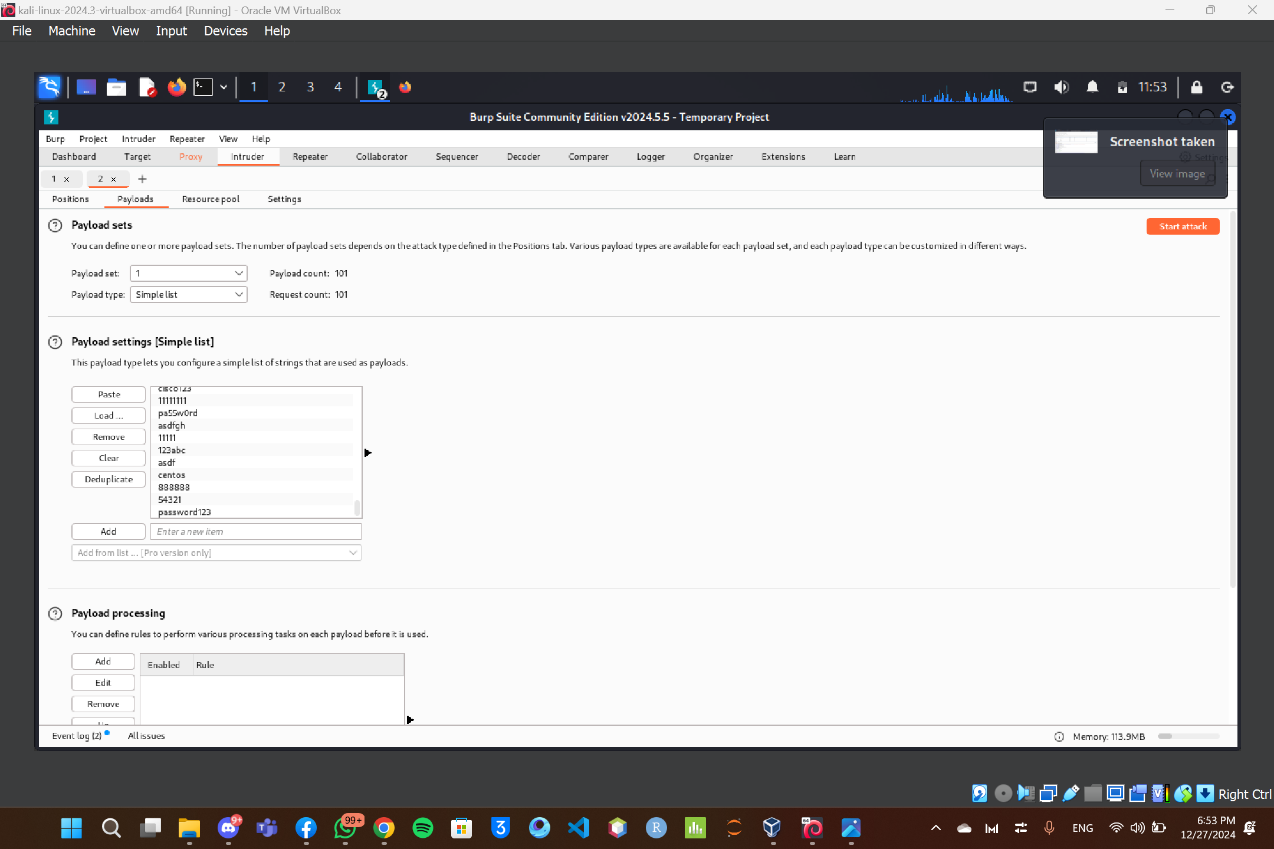
### ****Impact****:

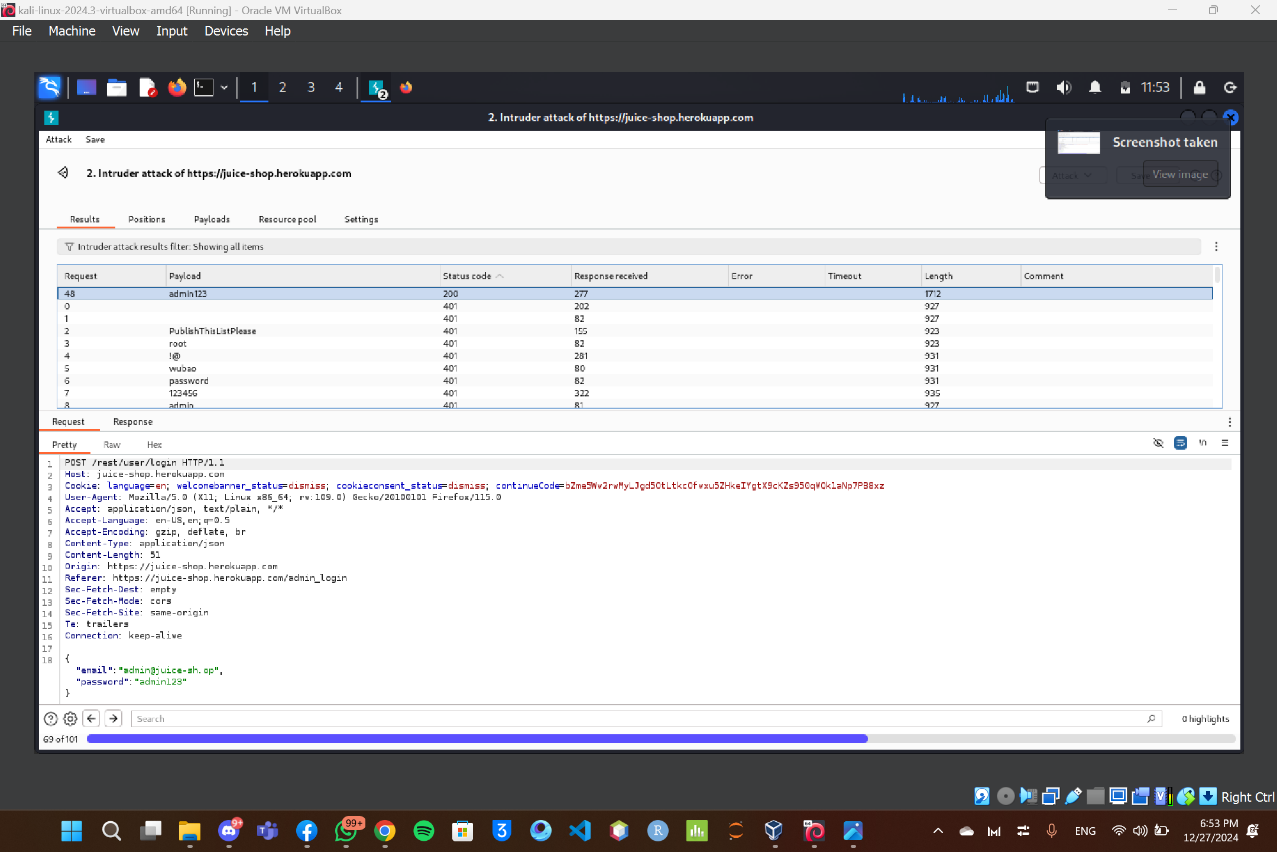
**Unauthorized Access**: Attackers could successfully compromise user credentials, gaining access to accounts, including those with administrative privileges.

**Exploitation of System**: If a brute-force attack succeeds, it could lead to data breaches, elevation of privileges, and a breakdown of user confidence in the system’s security.

### ****Remediation****:

**Implement Monitoring and Alerts**: Continuously monitor login attempts and set up alerts to identify and respond to brute-force attacks quickly.





Enumeration

