cyber security

farah negm ahmed (2305562)
ganna eslam hamed (2305523)
kenzy yasser helmy (2305297)

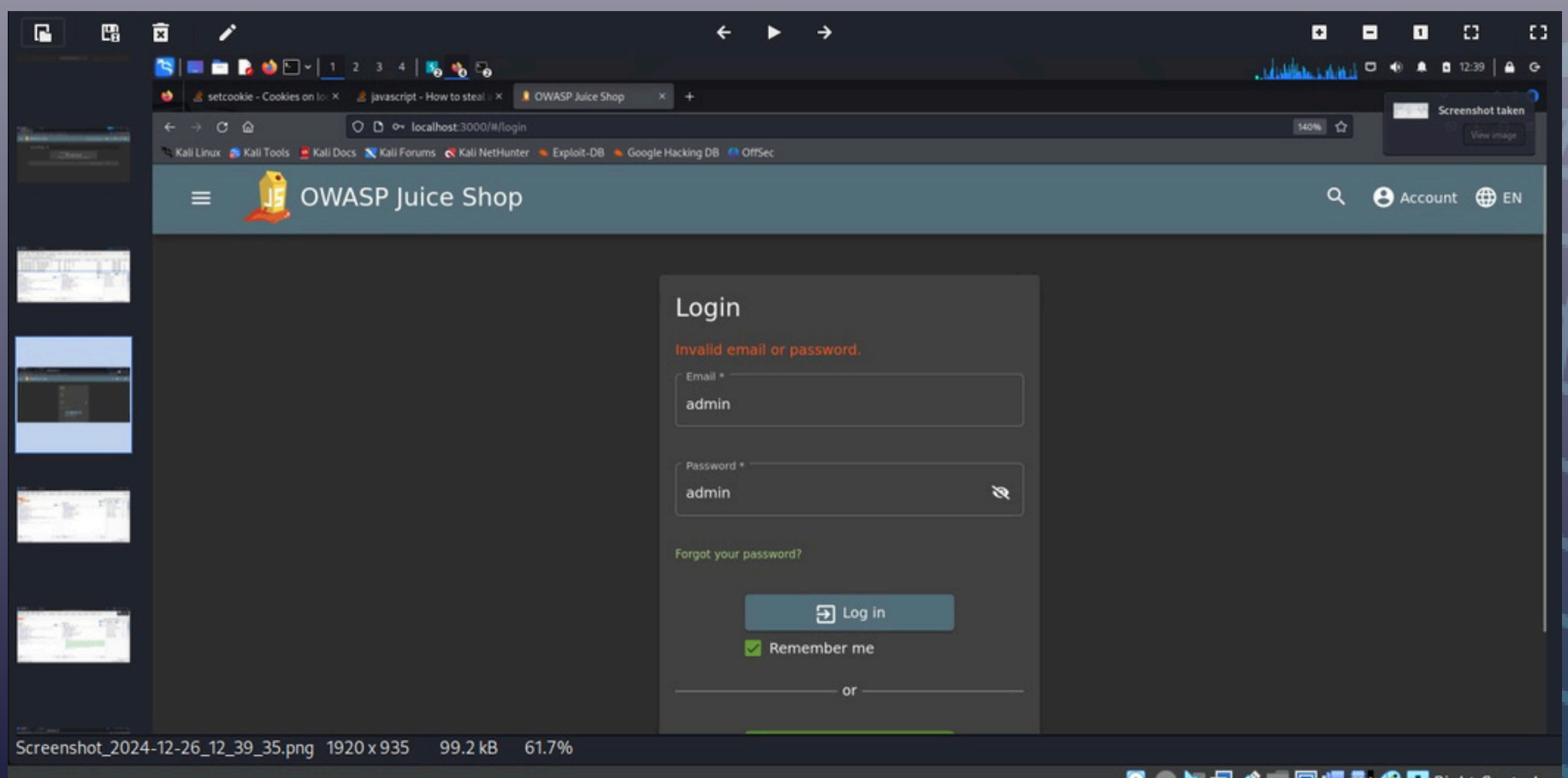
Scope and Methodology

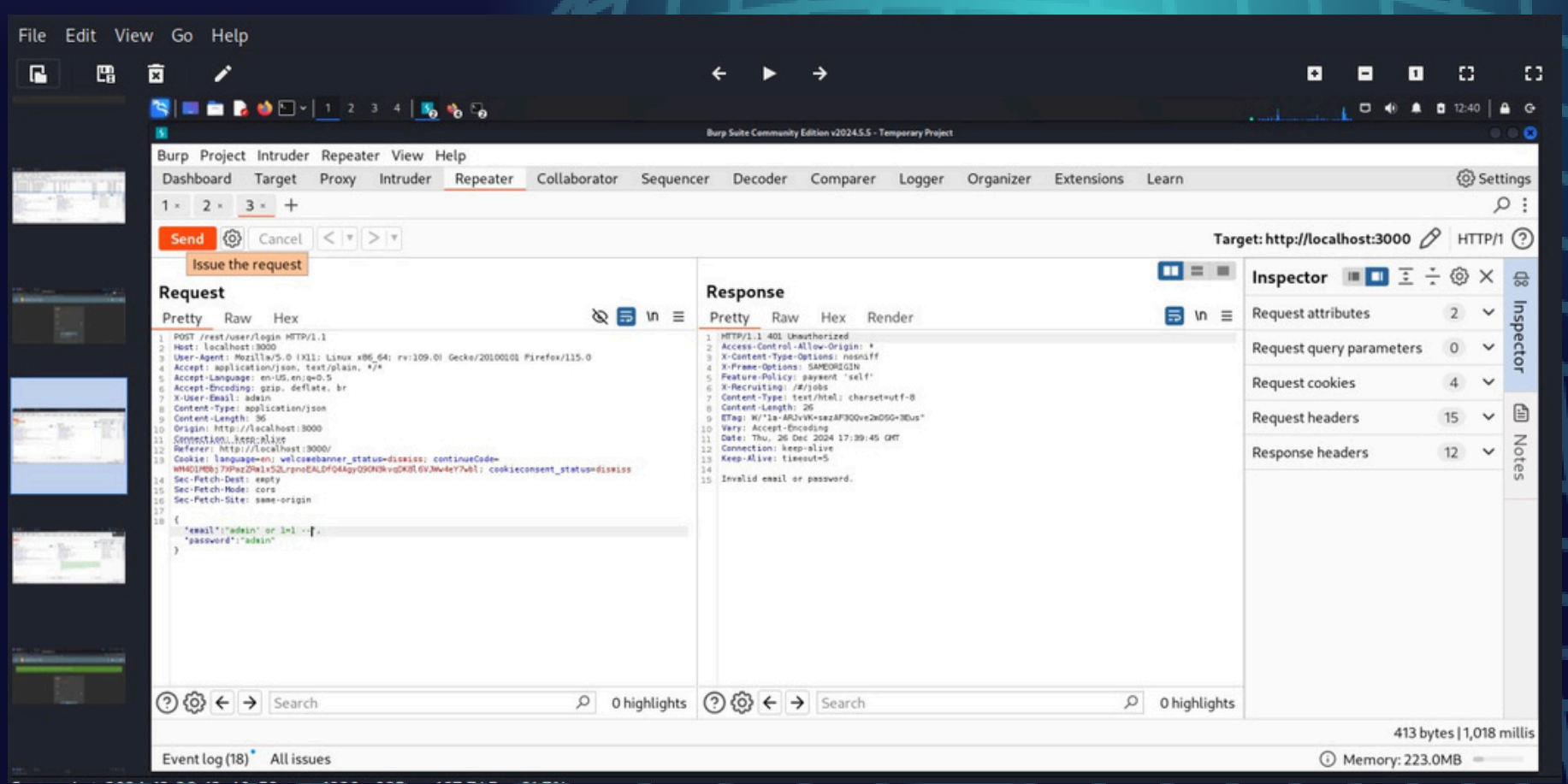
Scope:

Websites and APIs tested: OWASP Juice Shop application.

Methodology:
Black-box testing was performed, simulating real-world attack scenarios without access to source code.

Tools Used:
Burp Suite: For traffic analysis and vulnerability detection.
Hydra: For brute force attacks.
Dirb: To discover hidden directorie





Critical Vulnerabilities - SQL Injection

Description:

A SQL Injection vulnerability was discovered on the login page, allowing attackers to bypass authentication using payloads like admin' OR 1=1 --.

Risk:

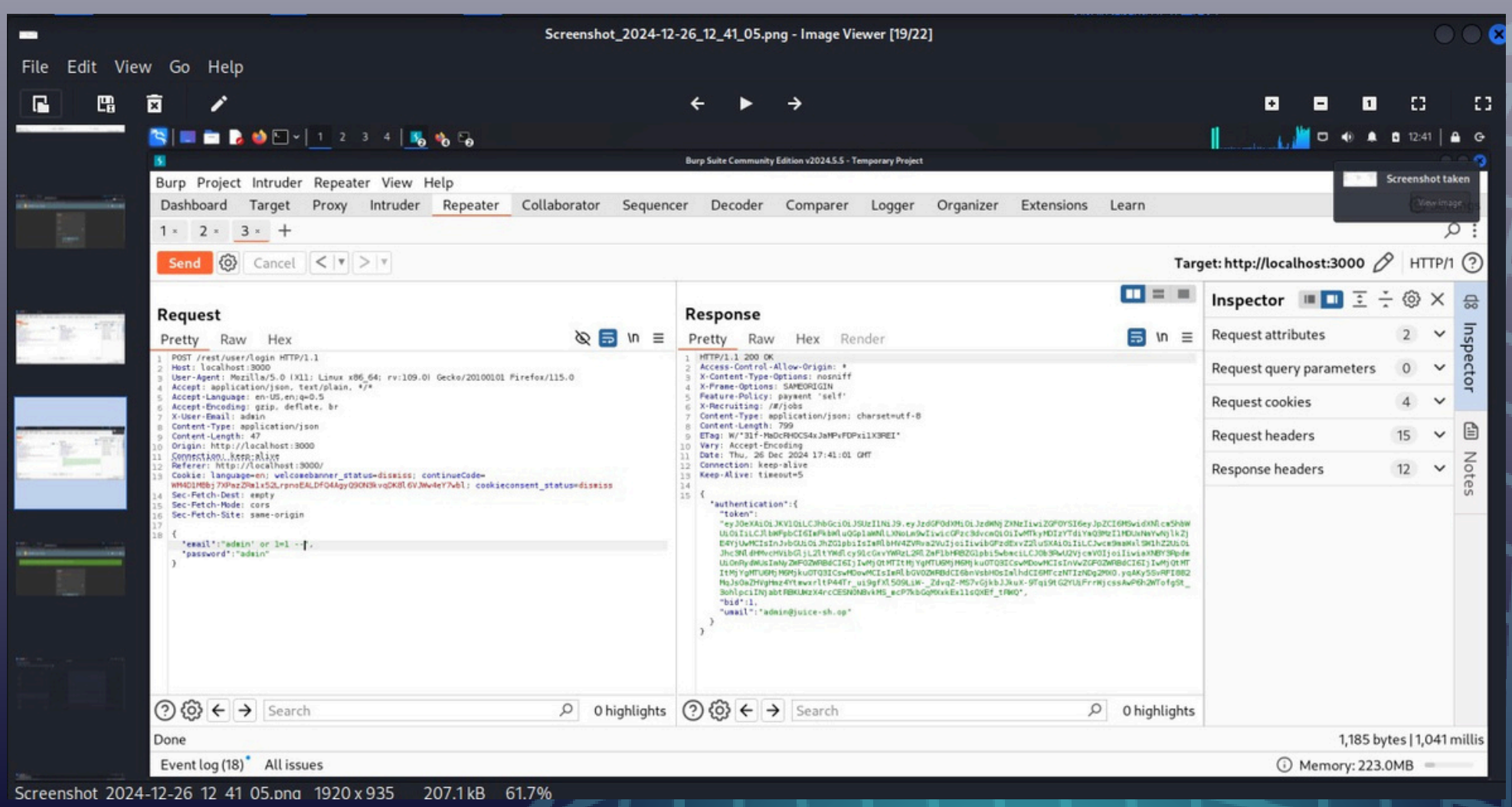
Exploiting this flaw grants unauthorized access to sensitive user accounts.

Evidence:

A successful login attempt with an admin account was achieved using a crafted SQL payload.

Recommendations:

- Use parameterized queries (prepared statements) to prevent SQL Injection.
- Validate and sanitize user inputs on the server side.
- Validate and sanitize user inputs on the server side.



The screenshot shows that you successfully completed the “Login Admin” challenge in the OWASP Juice Shop platform, which involves logging in using the administrator account.

The enumeration process successfully revealed hidden administrative paths, which could be leveraged by attackers to gain unauthorized access..

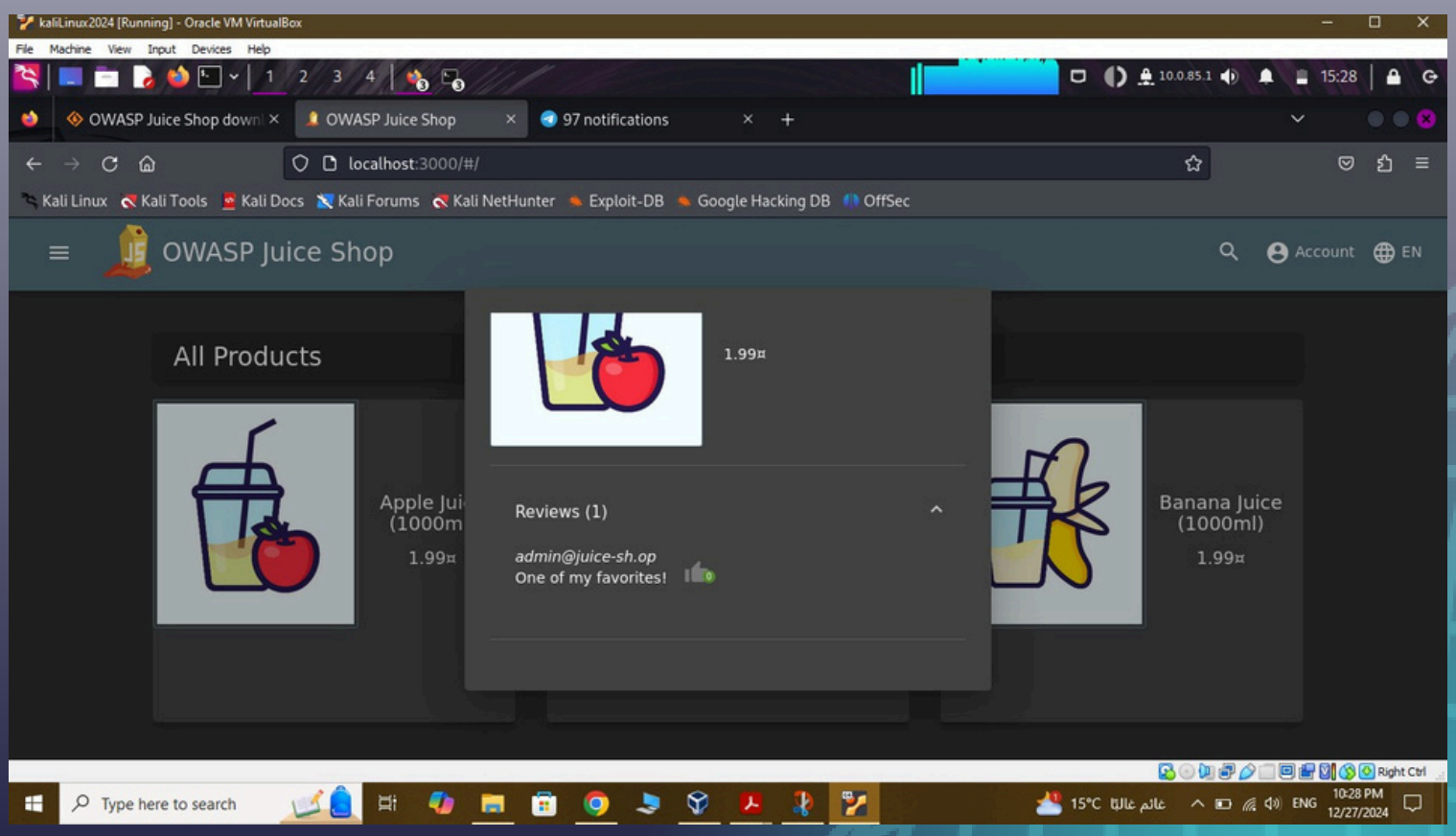
dirb: This is the command to run the directory buster tool.

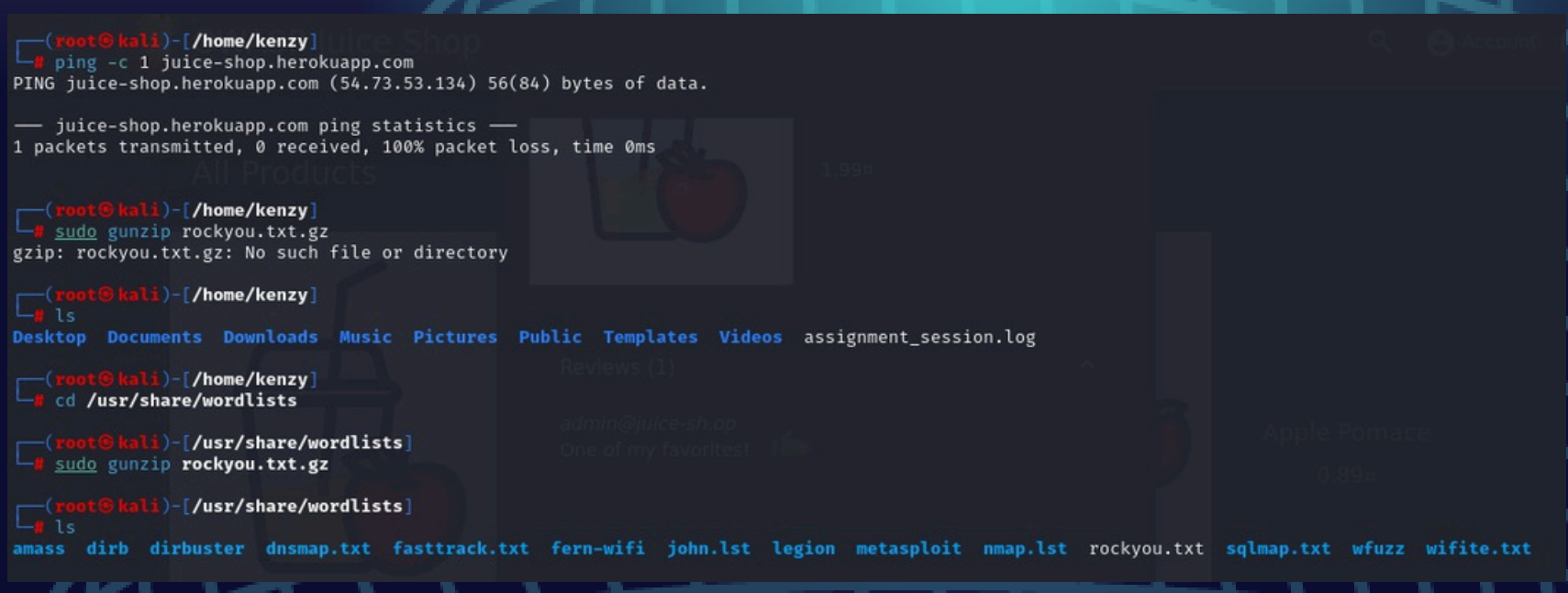
https://juice-shop.herokuapp.com: This is the target website being scanned.

/usr/share/wordlists/dirb/common.txt: This specifies the wordlist dirb uses. common.txt is a standard wordlist containing common directory and file names often used in web applications.

-v: This option enables verbose output, showing more details about the requests and responses.

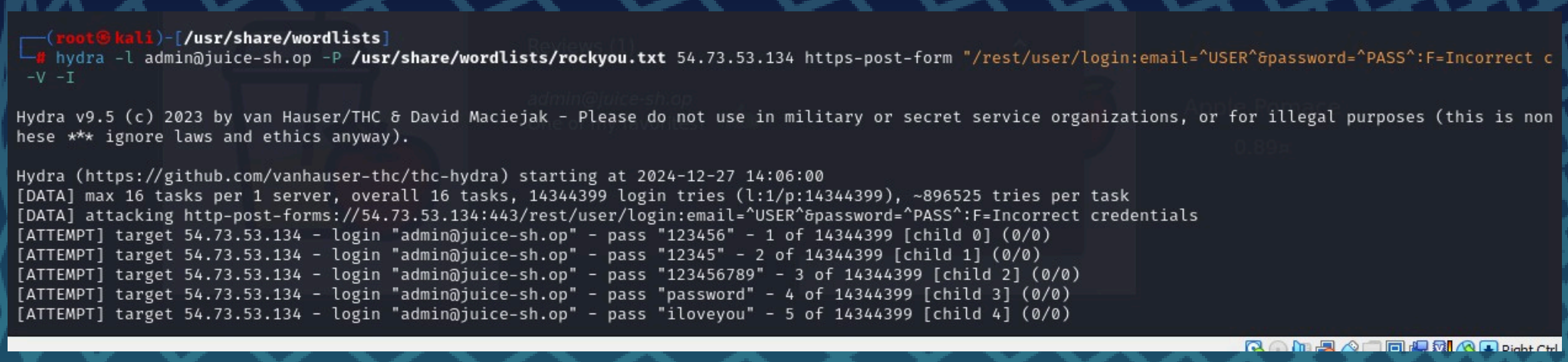
| grep admin: This pipes the output of dirb to the grep command. grep admin filters the output, displaying only lines containing the word "admin." This helps to quickly identify potential administrative interfaces.
Interpreting the Output:

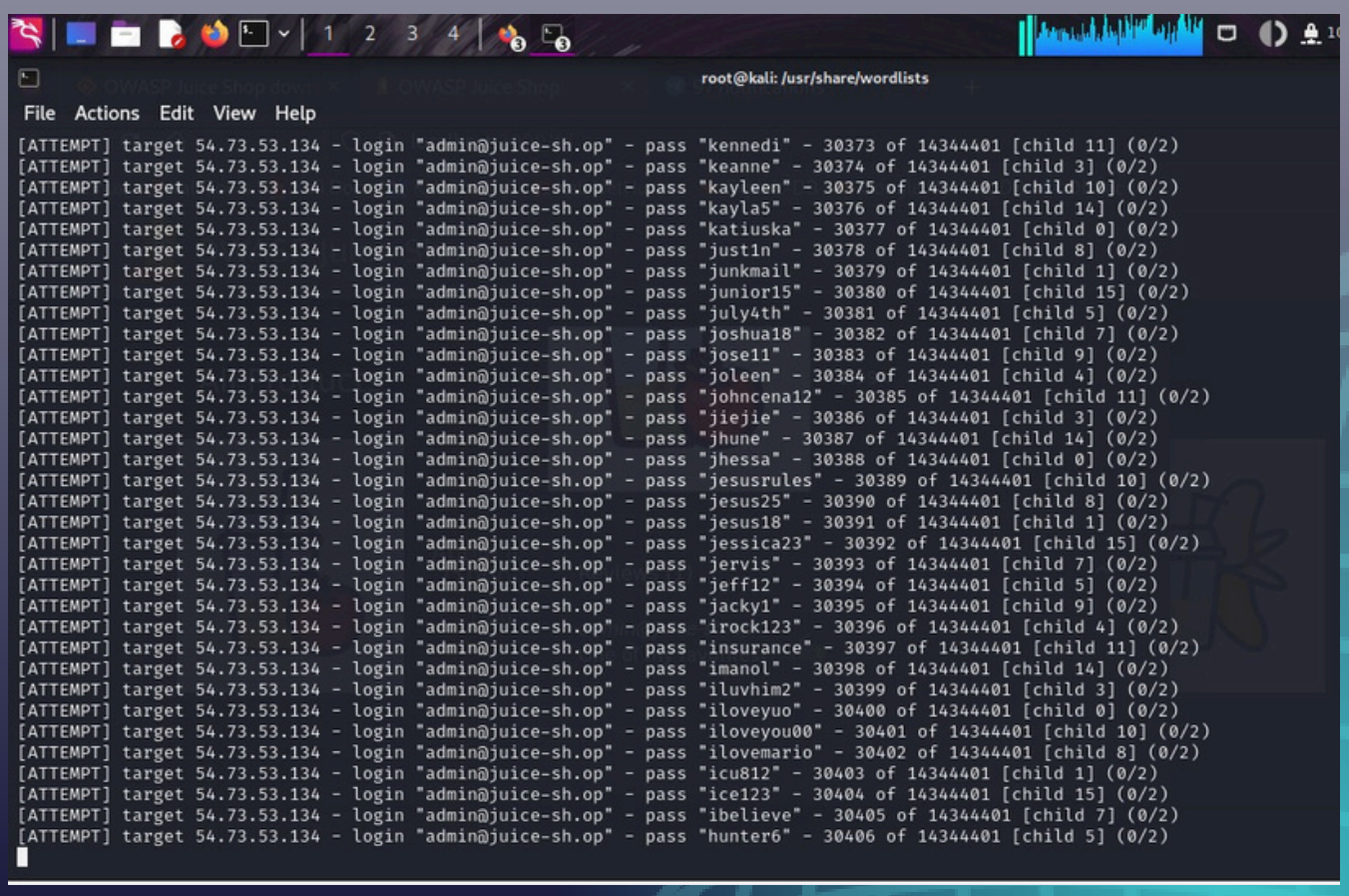




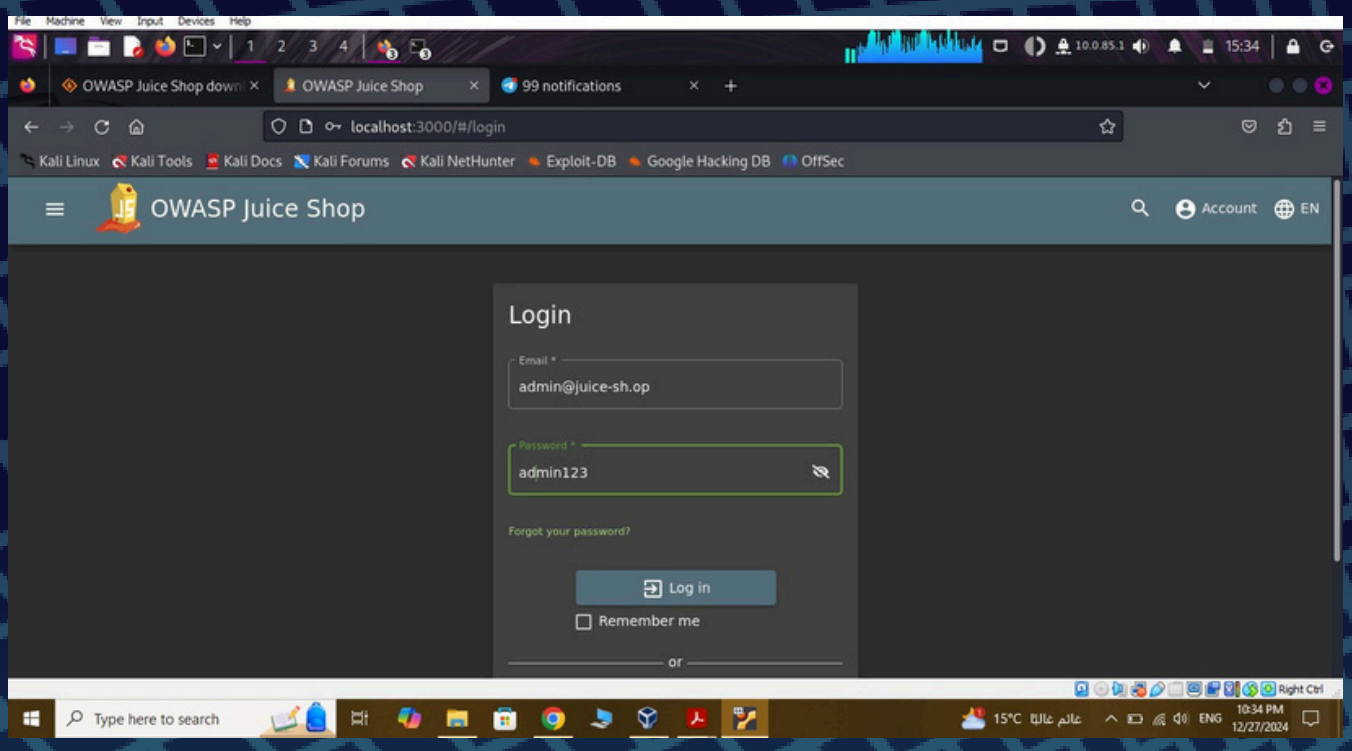
Brute Force Attack Description:

A brute force attack was performed against the admin login page using the email we found in the reviews using Hydra and the rockyou.txt wordlist after un zipping it and knowing the ip using ping in the previous commands.



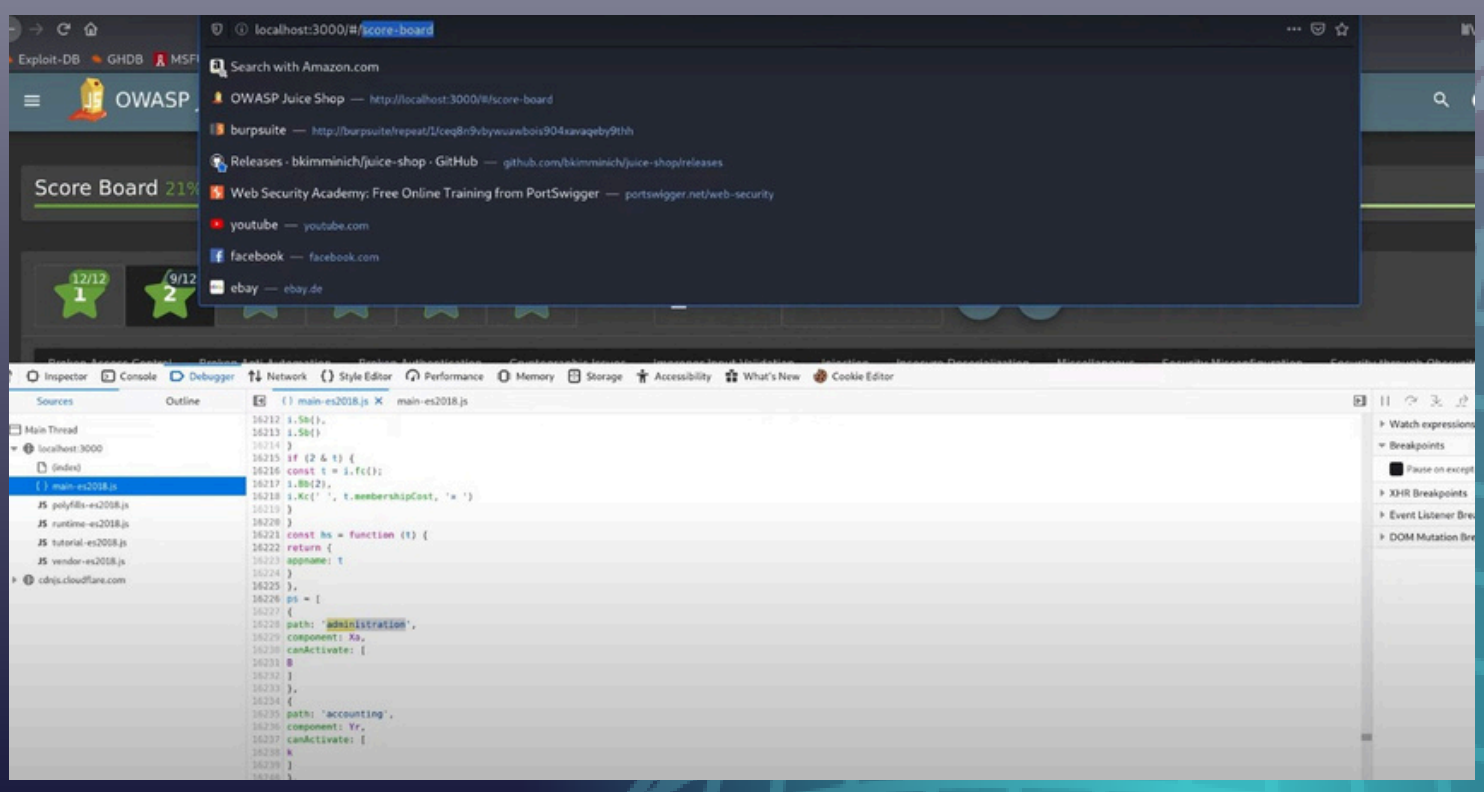


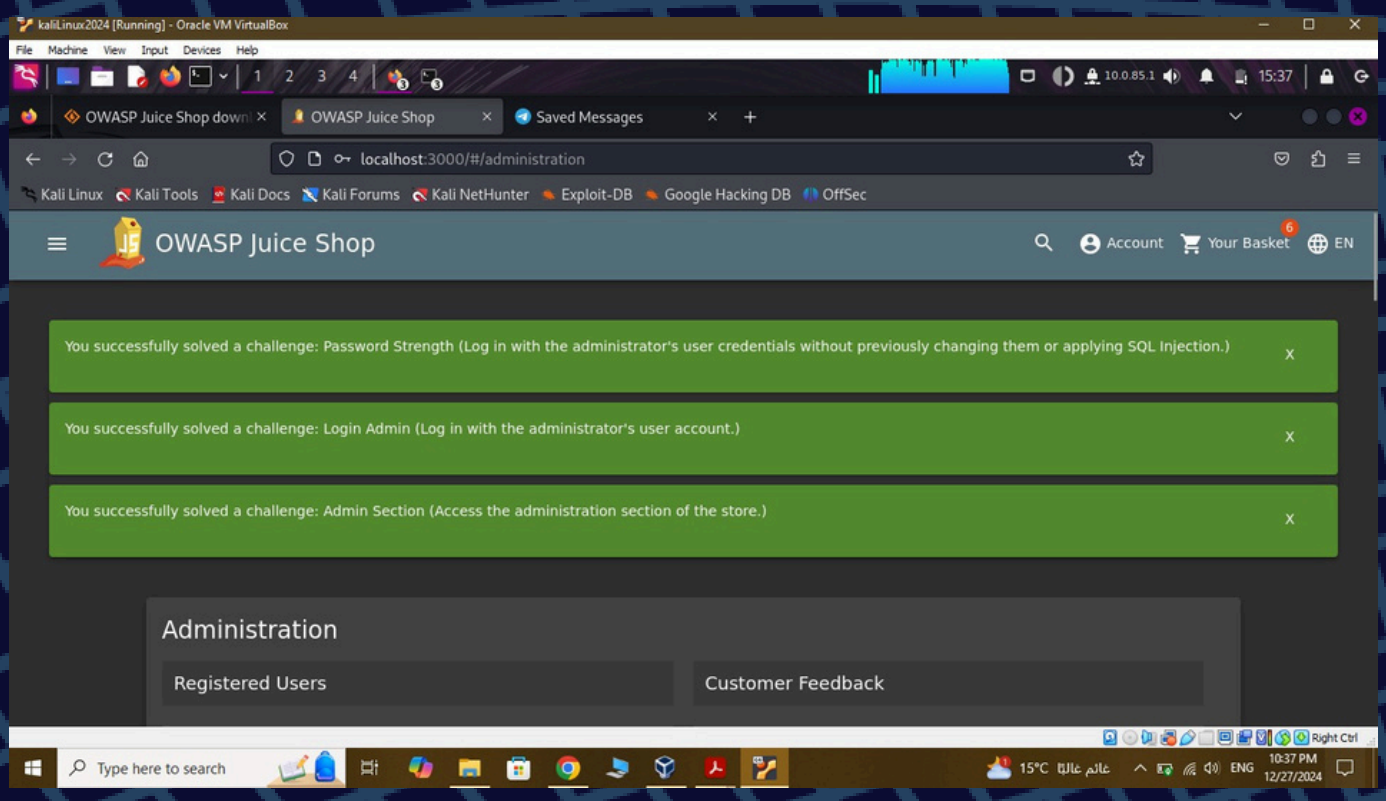
- the Hydra password cracking tool in action, performing a brute-force attack against the admin@juice-sh.op user on the server 54.73.53.134. It's using rockyou.txt to try various passwords.
- The output shows the progress of the attack, with each line representing a password attempt, including the password being tried and the attempt number out of the total attempts.
- the output is admin123



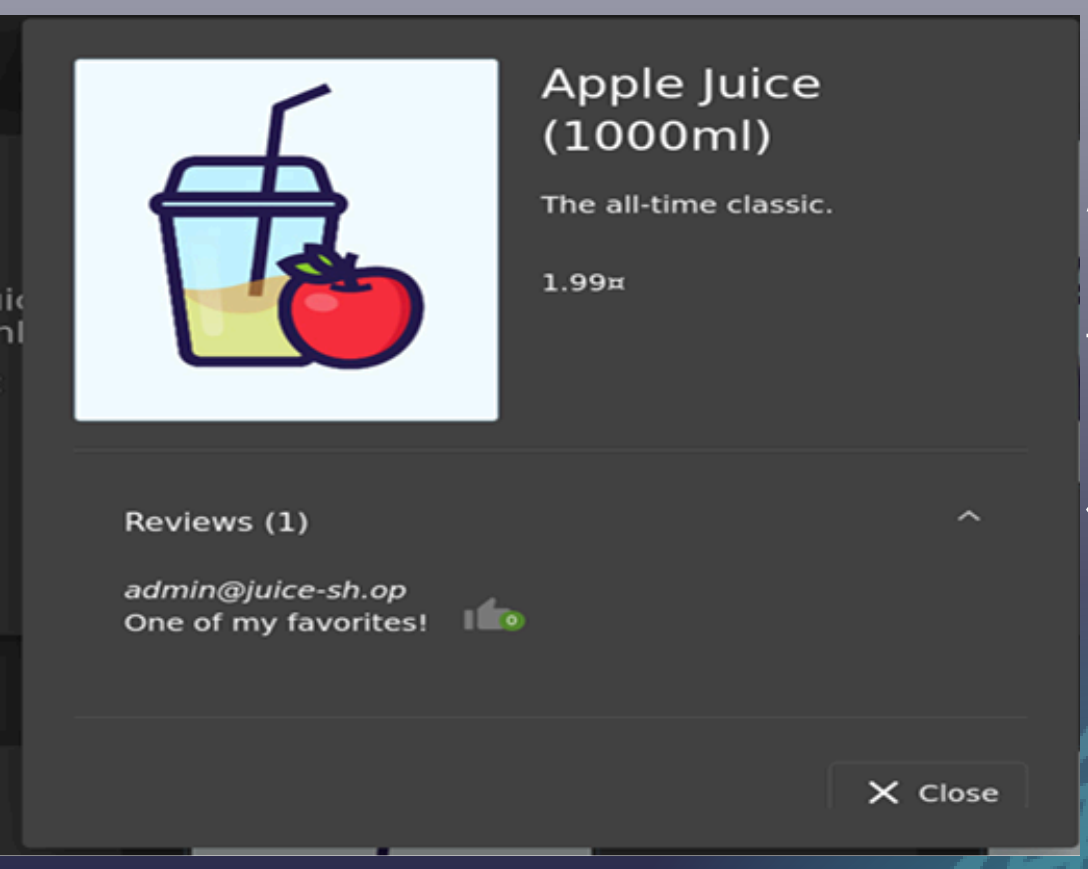
The screenshot shows the login page of the OWASP Juice Shop application.we have entered the email address admin@juice-sh.op and the password admin123. and logged in perfectly.

we used the java script code of the main page to know the admin path

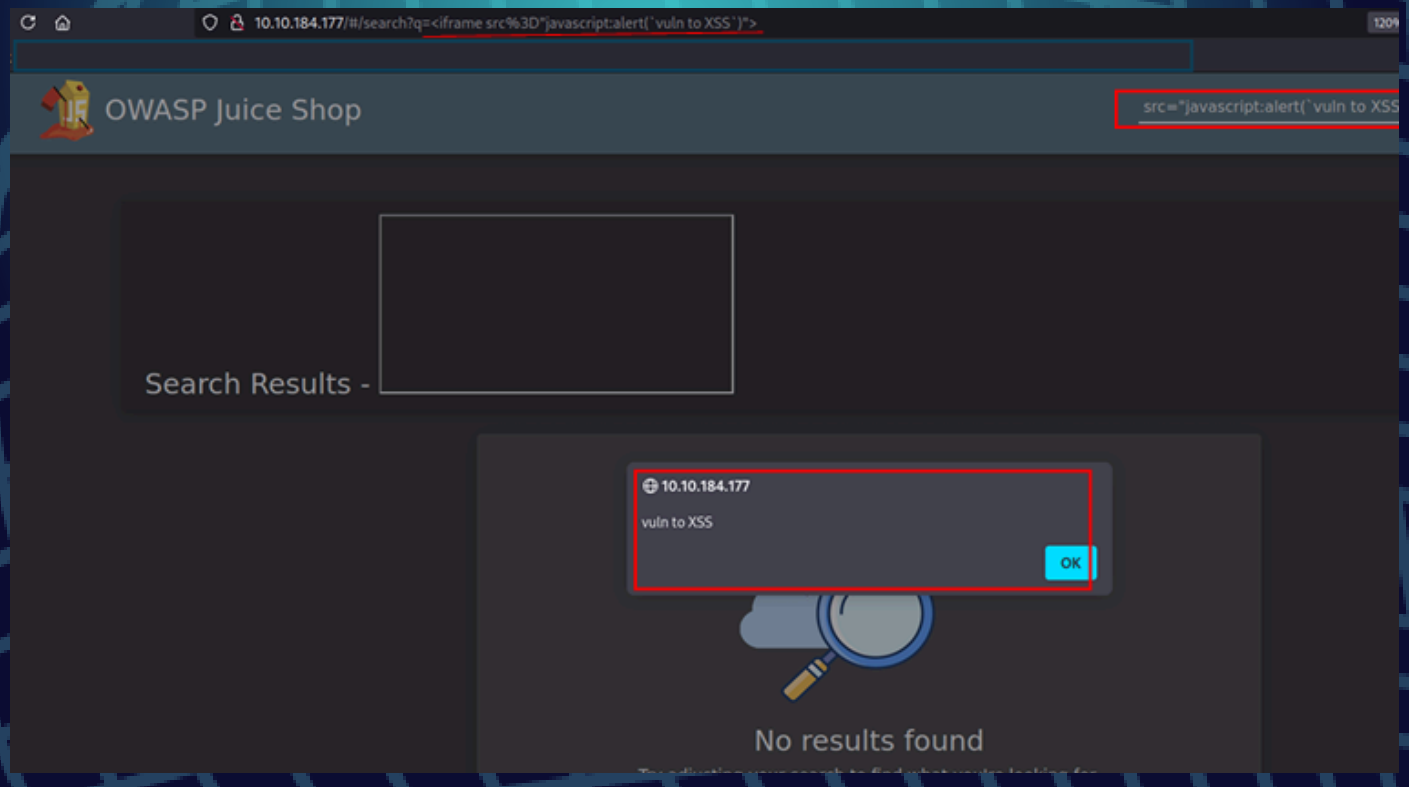




that a user has successfully gained administrative access to the OWASP Juice Shop. They have accessed the administration section, which provides management options. This demonstrates successful exploitation of likely weak default credentials.



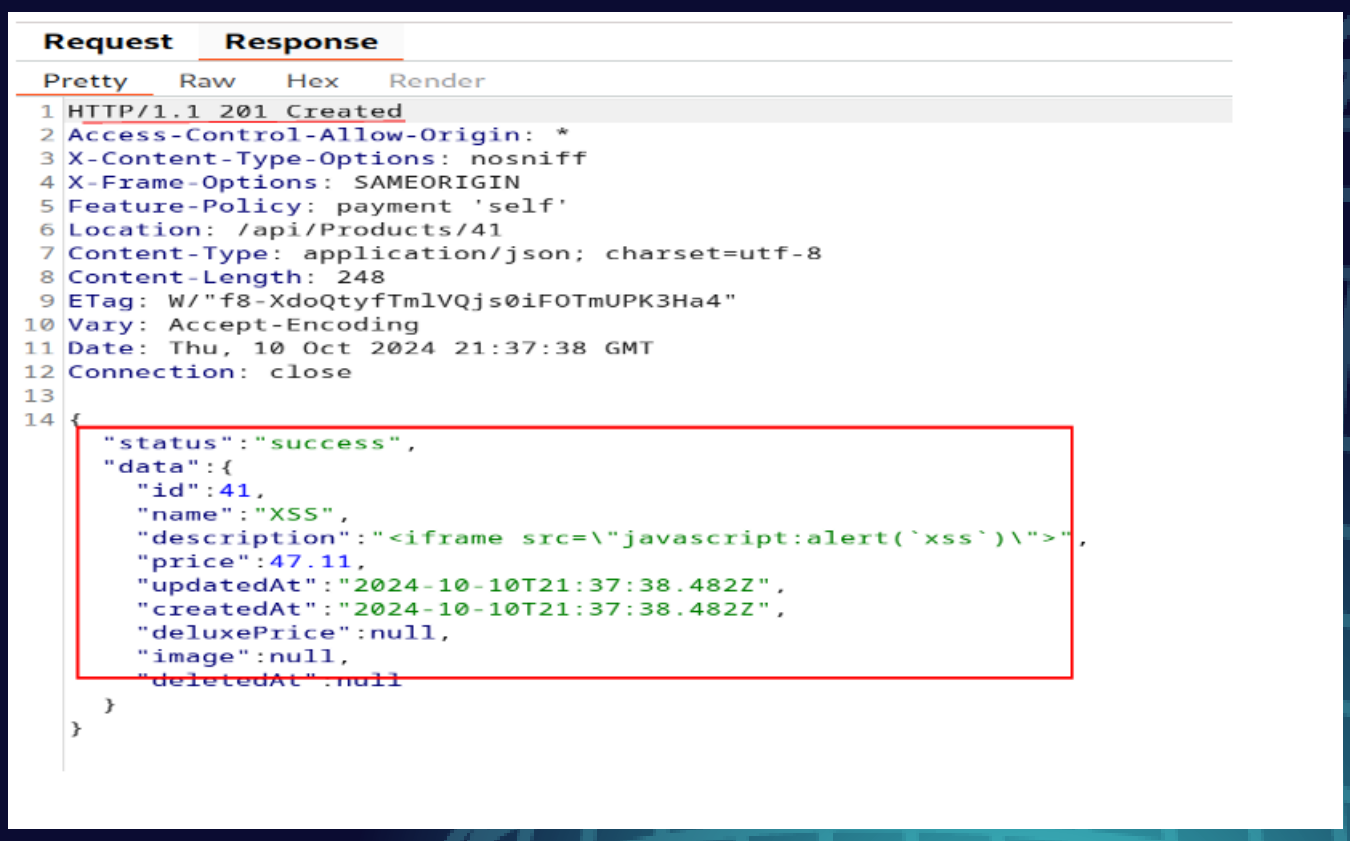
A. DOM-Based XSS 1. Inject Malicious Code: • In the search field, enter the following payload: • html • Payload • This payload attempts to execute a JavaScript alert when processed by the browser.



Cross-Site Scripting (XSS) is a type of web security vulnerability that allows attackers to inject malicious scripts into web applications. This vulnerability arises when user-supplied data is not properly sanitized or validated by the web application before being included in the response sent back to the user's browser.

Steps to reproduce:

- Use the search bar in the OWASP site
- Entered the Java payload: <iframe src=javascript:alert('xss')">
- An XSS prompt window shows up along with search results which is a vulnerability



Impact:

- Reflected Cross-Site Scripting (XSS) can lead to data theft where attackers can exploit XSS vulnerabilities to steal sensitive information from users.
- Attackers can hijack the user's account when they get access to login credentials, session cookies, personal data, credit card numbers, or other confidential information.
- Attackers can use XSS to create convincing phishing pages that appear legitimate to users.
- XSS attacks can lead to a denial of service situation, where the malicious script overwhelms the server or client-side resources, causing the application to become unresponsive or crash.