Project intro to cyber security

Names of team:

Ariam Elsharkawy 2305128

Zainab Elsayed 2305112

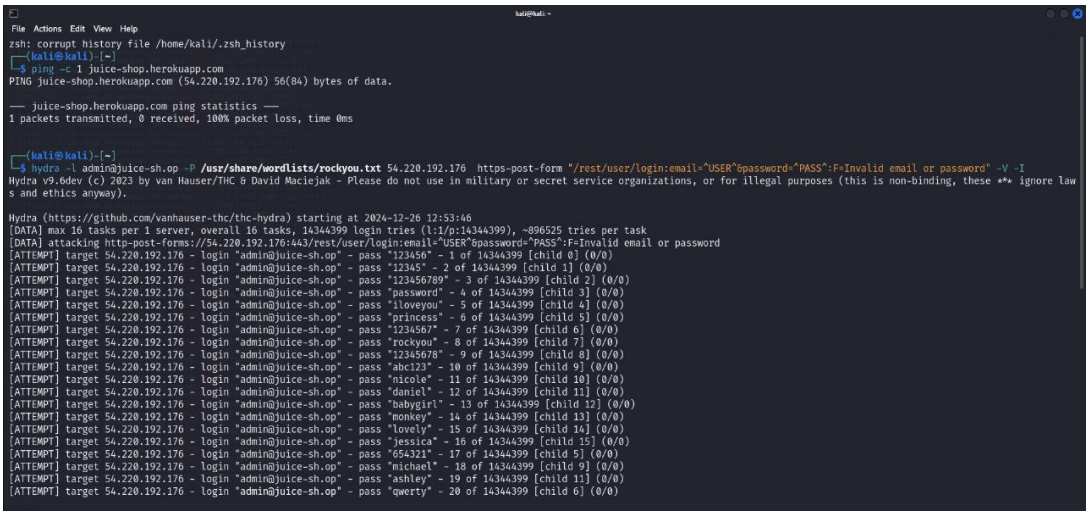
Menna tamer 2305192

1. Enumeration to Find Admin Path:

The paths by using dirb:

Dirb: For discovering hidden files and directories.

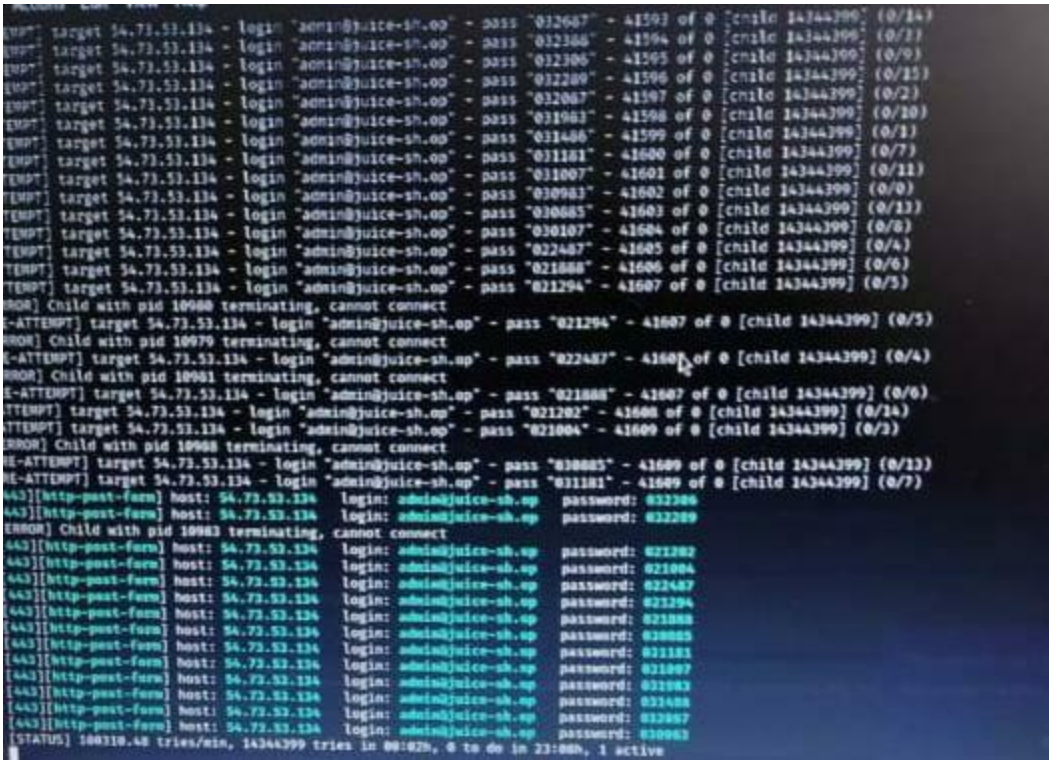
2. Brute Force on Admin Credentials:



ping -c 1 juice-shop.herokuapp.com: Result: Indicates the server is not responding (100% packet loss) and check the ip of website.

Hydra: iterates through the wordlist to find the correct password.

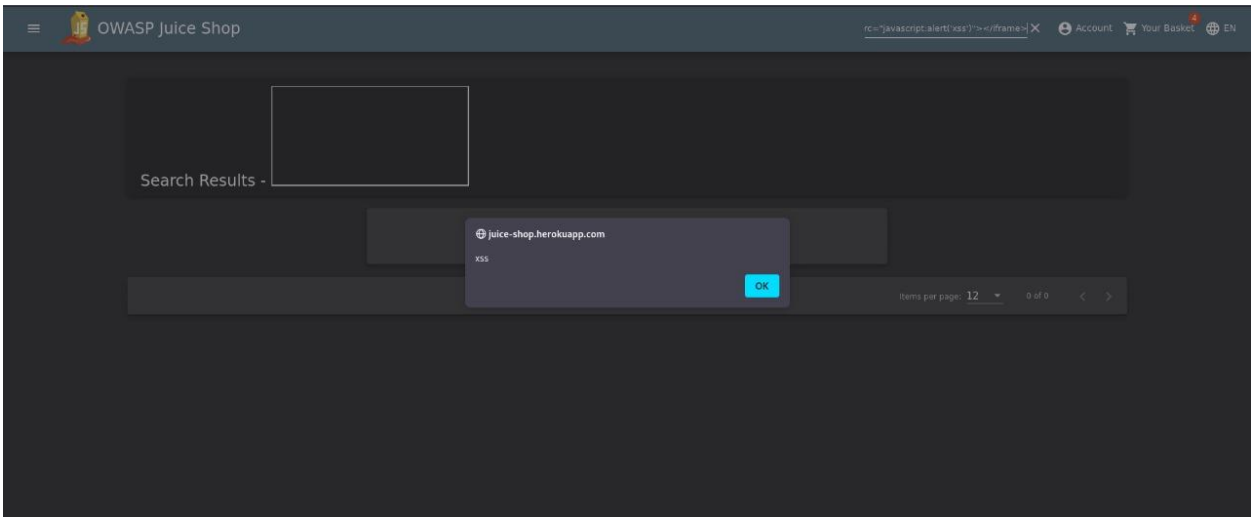
the outcomes:



3. Cross-Site Scripting (XSS) in Product Search:

Code:<iframe src="javascript:alert('xss')"></iframe>:

Exploiting an input processing weakness to run malicious code inside the user's browser and detect if there is xss vulnerability or not.



There is xss vulnerability.

Cookies by decrybtion:

python3 -m http.server 8000 :Serves files from the current directory over HTTP for testing or debugging.:

echo "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9" | base64 -d:

Purpose: Decodes a Base64-encoded string.

Input: The encoded string is part of a JWT (JSON Web Token) header.

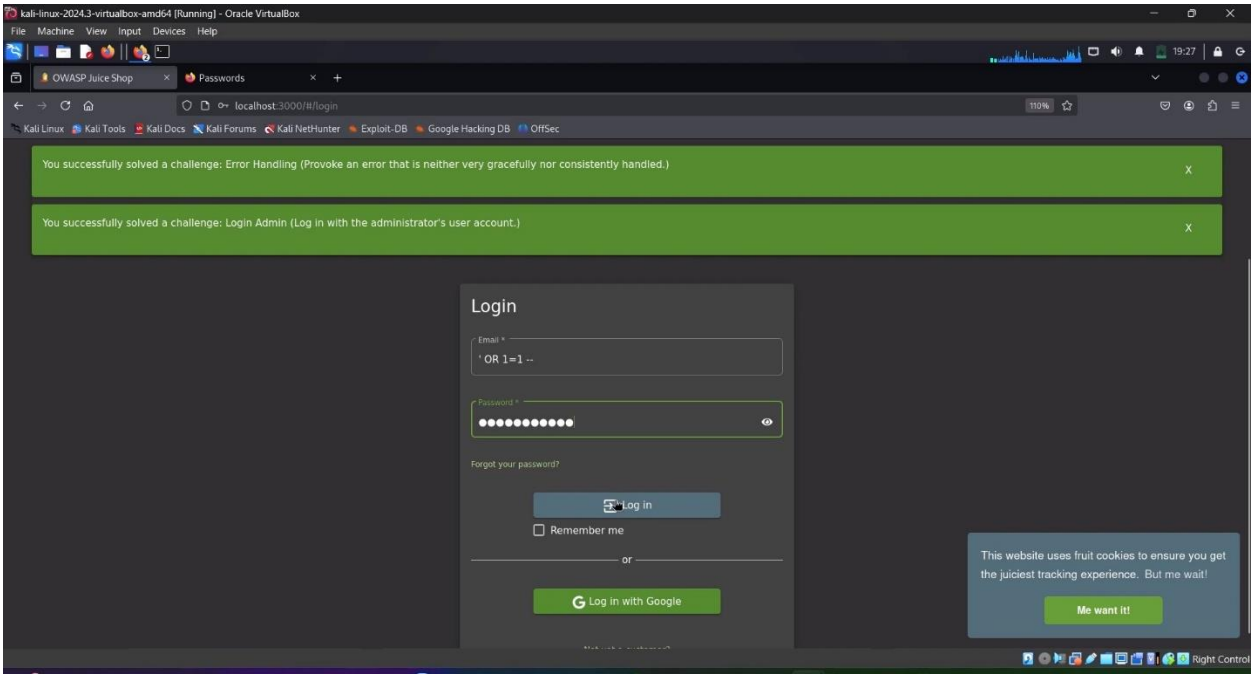
Output: The decoded JWT header, which contains information like the algorithm (alg) and token type (typ).

echo "eyJzdWI6IjoxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ==" | base64 -d:

Purpose: Decodes another Base64-encoded string, which represents the payload of a JWT.

Output: The decoded JWT payload, showing user-specific data (e.g., id, username, email, etc.).

4- sql injection:



OR 1=1 -- is commonly used in SQL Injection attacks, a type attack targeting databases by injecting malicious code into SQL queries.