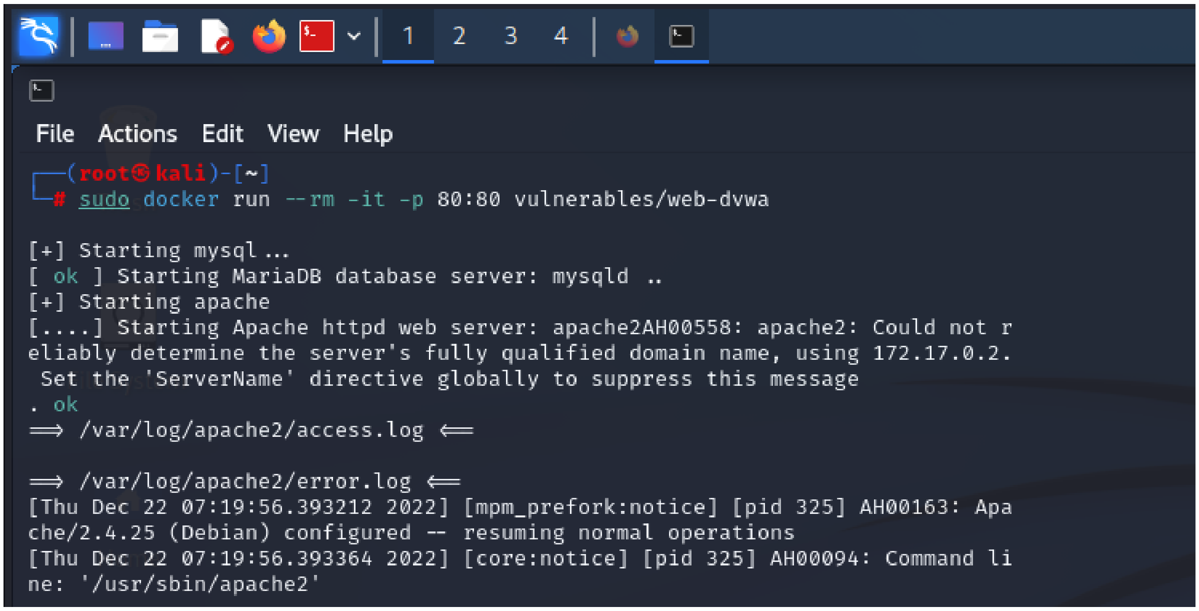
Brute Force

DVWA

Procedure:

Step 1: Run Docker in root terminal

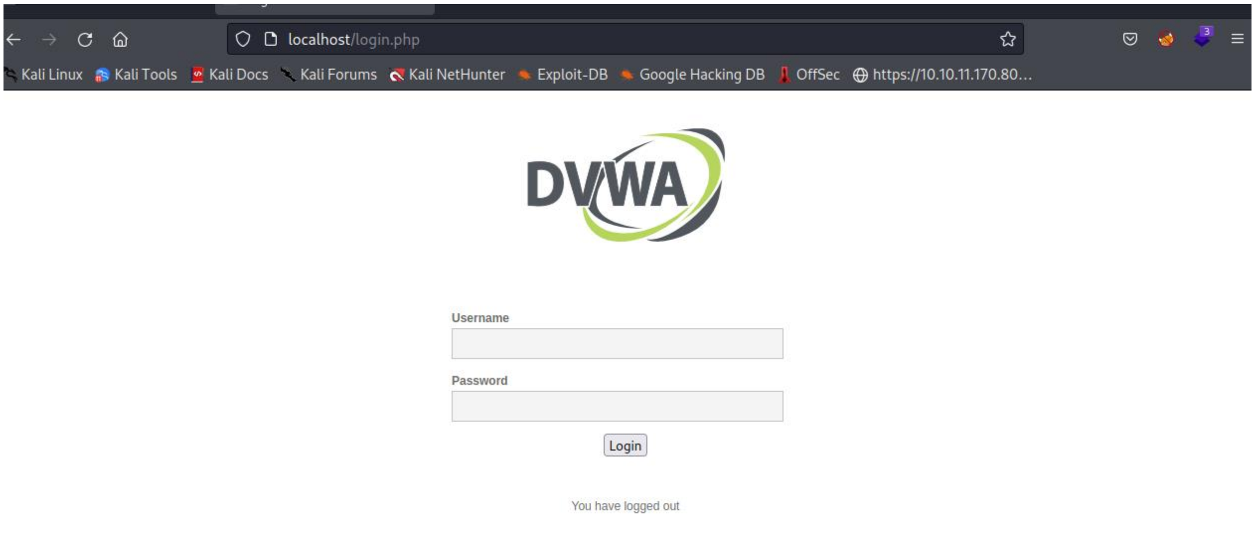


```
┌──(root㉿kali)-[~]
└─# sudo docker run --rm -it -p 80:80 vulnerables/web-dvwa

[+] Starting mysql...
[ ok ] Starting MariaDB database server: mysqld ..
[+] Starting apache
[....] Starting Apache httpd web server: apache2AH00558: apache2: Could not r
eliably determine the server's fully qualified domain name, using 172.17.0.2.
 Set the 'ServerName' directive globally to suppress this message
. ok
==> /var/log/apache2/access.log <==

==> /var/log/apache2/error.log <==
[Thu Dec 22 07:19:56.393212 2022] [mpm_prefork:notice] [pid 325] AH00163: Apa
che/2.4.25 (Debian) configured -- resuming normal operations
[Thu Dec 22 07:19:56.393364 2022] [core:notice] [pid 325] AH00094: Command li
ne: '/usr/sbin/apache2'
```

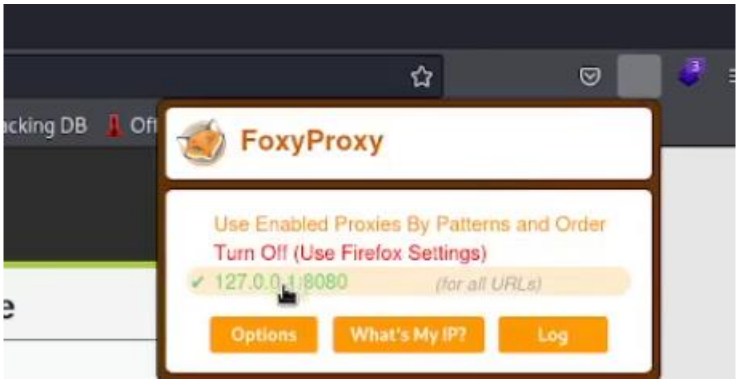
Step 2: connect with localhost on browser and login with username: admin & password: password



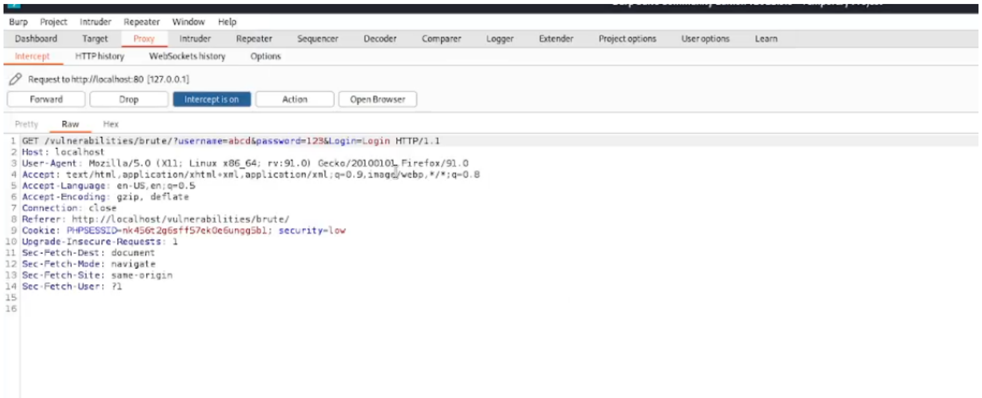
You have logged out

Step 3: select Brute Force and Start find the username and password by using Burp Suite

Step 4: Turn on Foxy proxy


FoxyProxy
Use Enabled Proxies By Patterns and Order
Turn Off (Use Firefox Settings)
✓ 127.0.0.1:8080 (for all URLs)
Options
What's My IP?
Log

Step 5: open Burp Suite tool then go to proxy turn on intercept mode and capture the request.

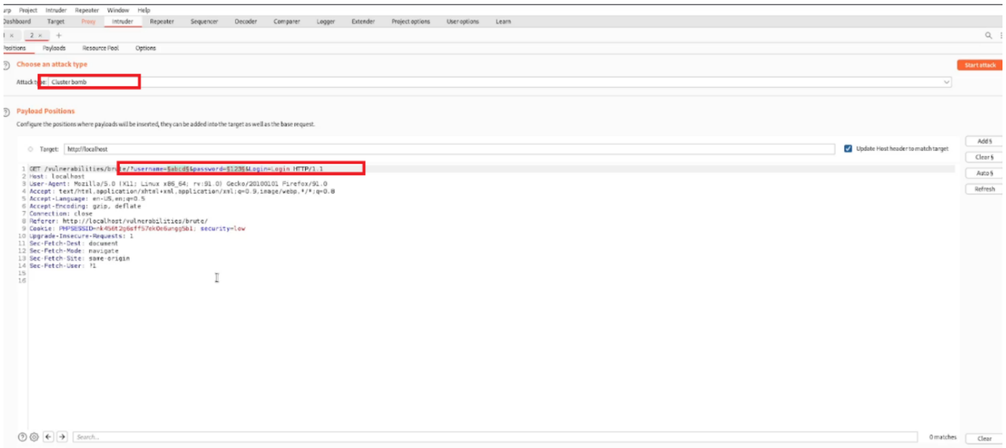


Request to http://localhost:80 [127.0.0.1]

```
GET /vulnerabilities/brute/?username=abcd&password=123&Login=Login HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost/vulnerabilities/brute/
Cookie: PHPSESSID=nk456t2g6sff57ek0e6ungg5bl; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Step 6: click Action to send the to send the request to the intruder

Step 7: select user name & password and change attack type into cluster bomb



Choose an attack type

Attack type: Cluster bomb

Payload Positions

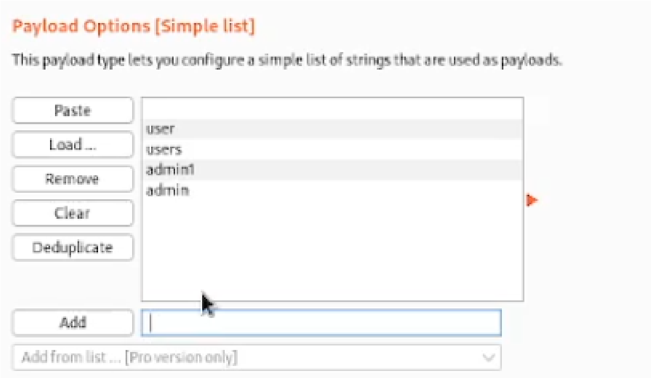
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost

☑ Update Host header to match target

```
GET /vulnerabilities/brute/?username=§abcd§&password=§123§&Login=Login HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost/vulnerabilities/brute/
Cookie: PHPSESSID=nk456t2g6sff57ek0e6ungg5bl; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

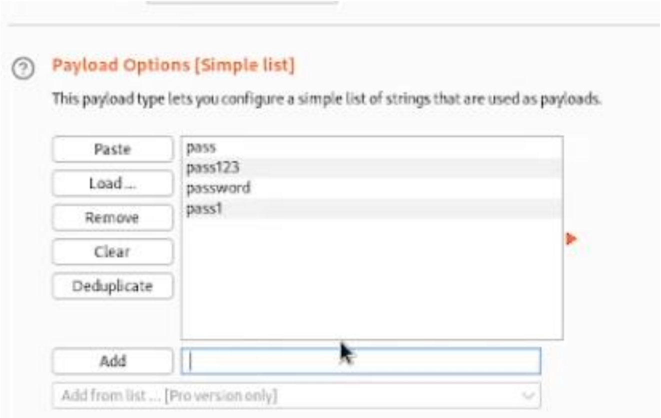
Step 8: Then go to payload and add random related payload for both username and password for Brute Force



Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

user
users
admin1
admin



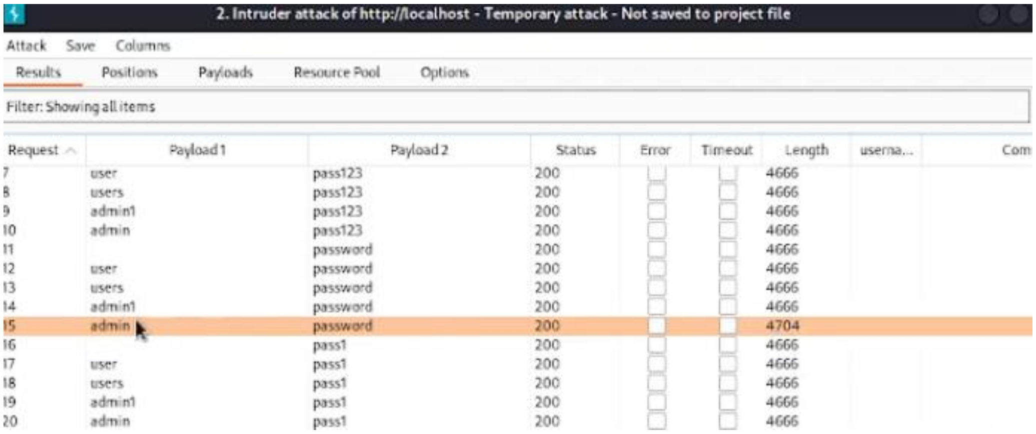
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

pass
pass123
password
pass1

Step 9: click start attack

When the attack is completed, you can get the username & password

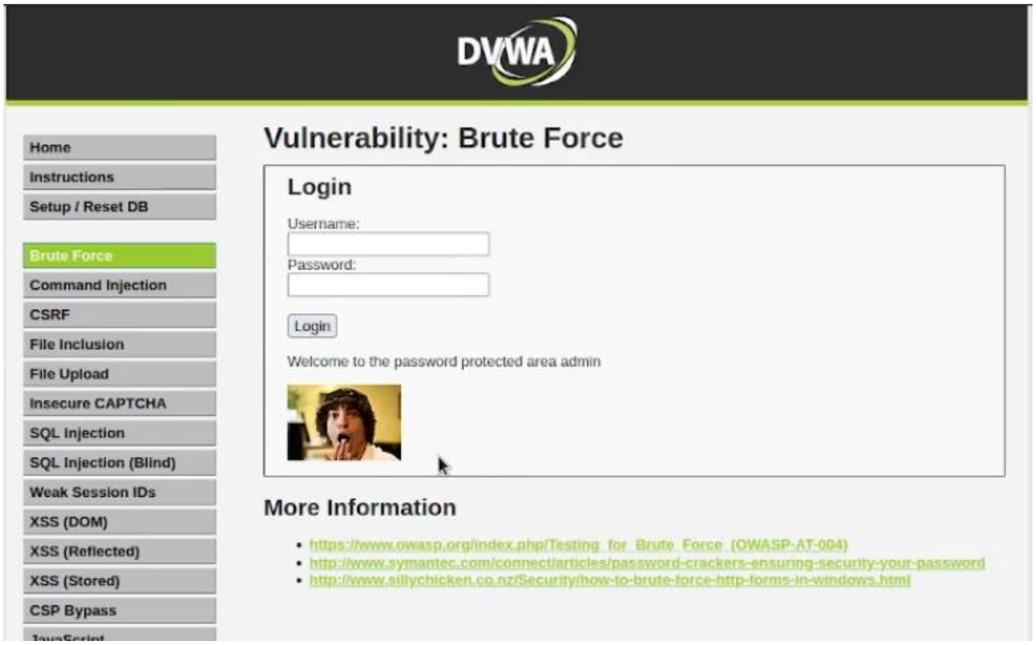


2. Intruder attack of http://localhost - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	userna...	Com
7	user	pass123	200	□	□	4666		
8	users	pass123	200	□	□	4666		
9	admin1	pass123	200	□	□	4666		
10	admin	pass123	200	□	□	4666		
11		password	200	□	□	4666		
12	user	password	200	□	□	4666		
13	users	password	200	□	□	4666		
14	admin1	password	200	□	□	4666		
15	admin	password	200	□	□	4704		
16		pass1	200	□	□	4666		
17	user	pass1	200	□	□	4666		
18	users	pass1	200	□	□	4666		
19	admin1	pass1	200	□	□	4666		
20	admin	pass1	200	□	□	4666		

Step 10: To confirm enter the username & password



Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area admin

More Information

- https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004)
- http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html