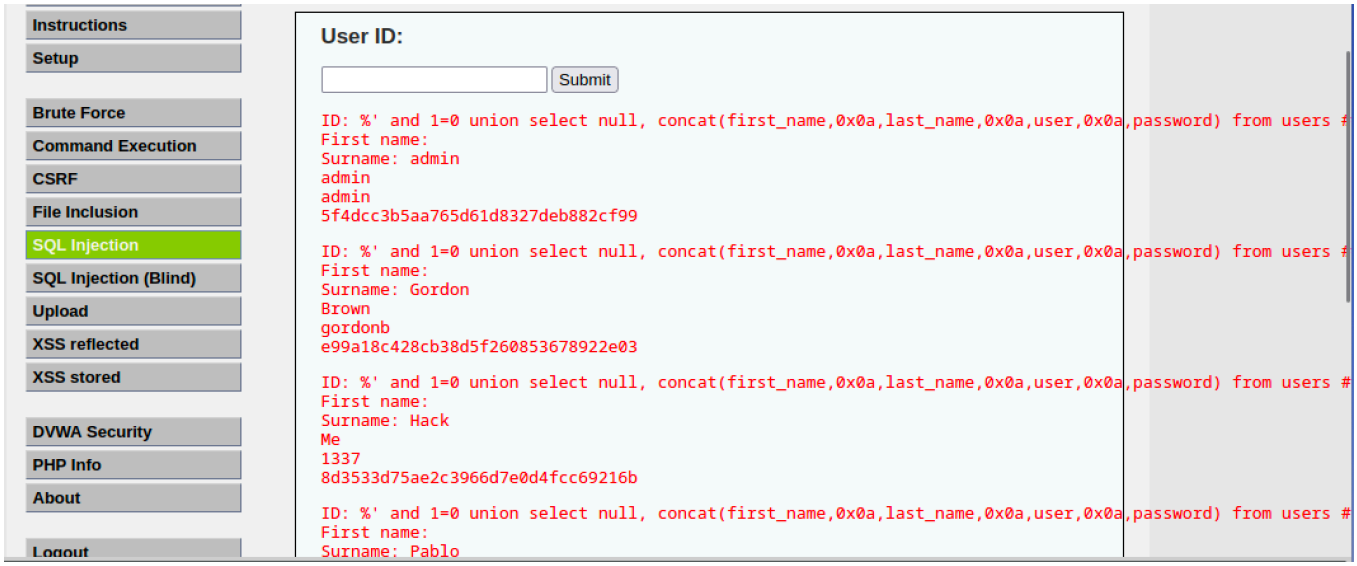
Progetto settimanale
Web application hacking

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



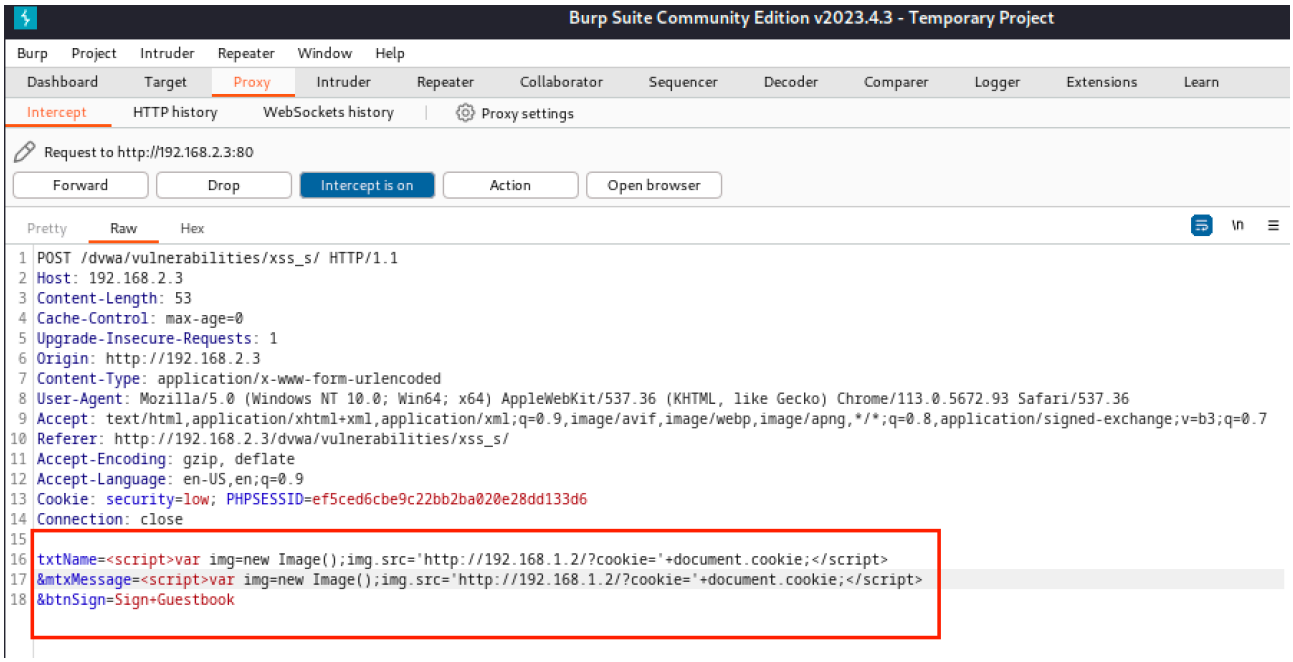
Successivamente con il tool johntheripper decodifichiamo gli has delle password per poterle leggere in chiaro

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --wordlist=rockyou.txt passwd.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
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 rel
iably
Session completed.
```

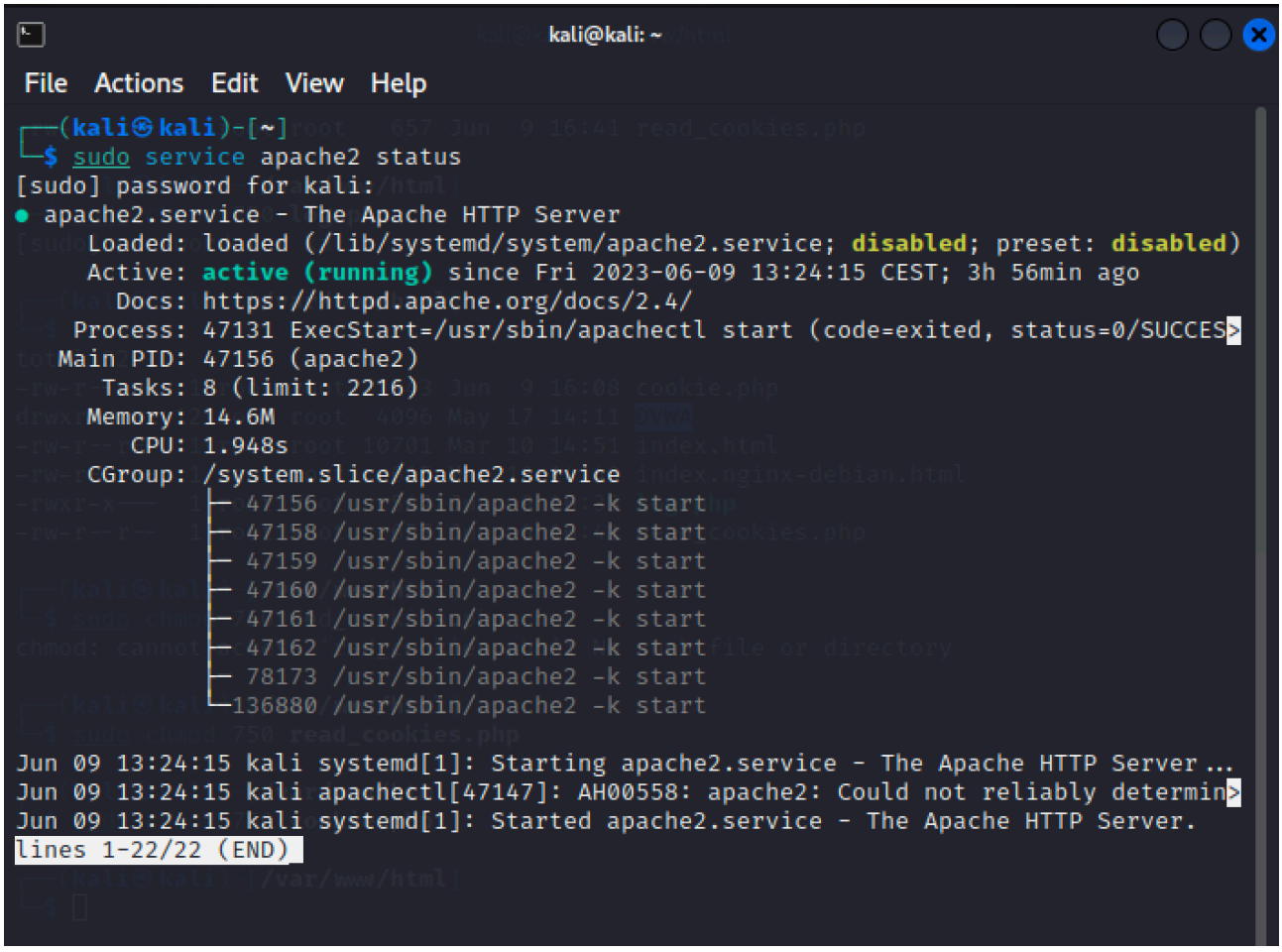
```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --show --format=raw-md5 passwd.txt
admin:password
gordon:abc123
hack:charley
pablo:letmein
bob:password

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