Van Zwam Arjen

Password cracking

#ByteRebels

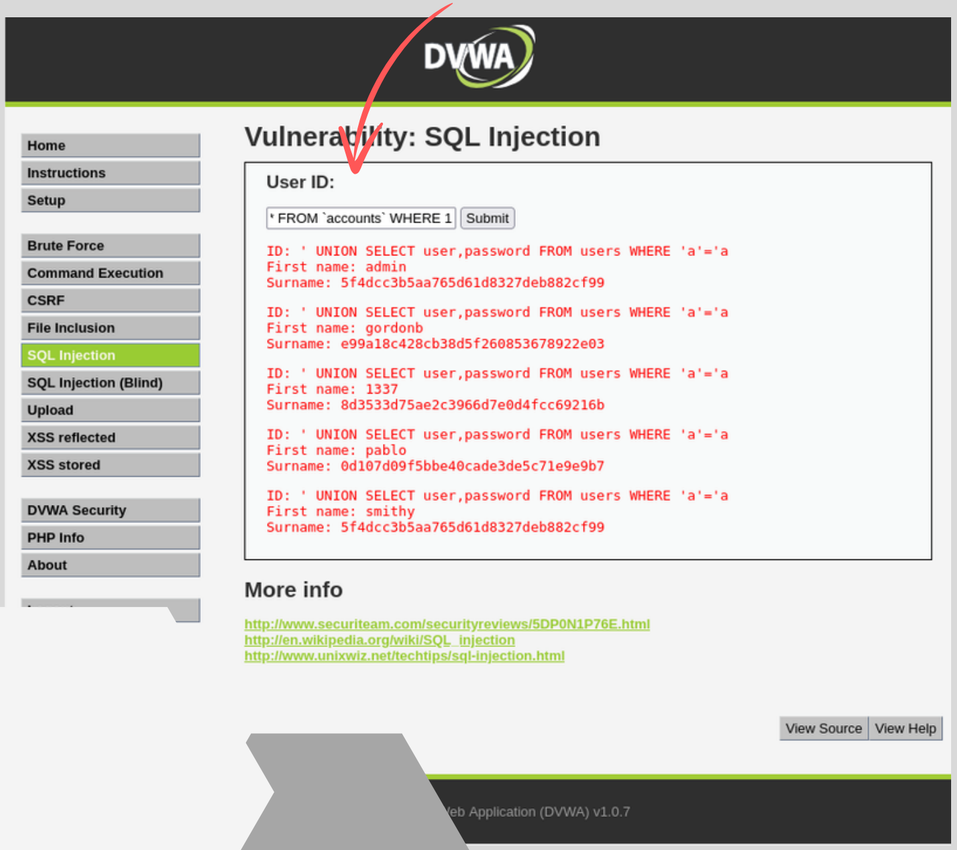
Traccia

Se guardiamo meglio le password, della lezione precedente, non hanno l’aspetto di password in chiaro, ma sembrano più hash di password MD5. Recuperate le password dal DB e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro. Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica. L’obiettivo dell’esercizio di oggi è craccare tutte le password.

Ricerca password MD5

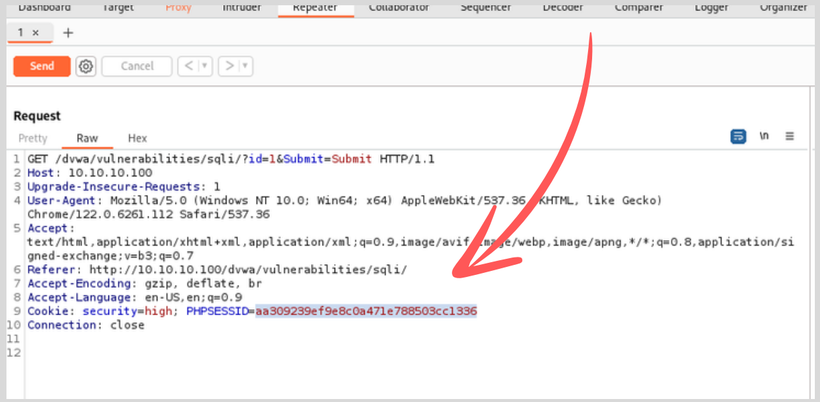
Come prima cosa, ho dovuto recuperare le password cifrate in **MD5** dal Database della DVWA semplicemente inserendo come stringa:

SELECT * FROM `accounts` WHERE 1



Avrei comunque potuto svolgere già in autonomia tutto l'esercizio con **sqlmap** poiché esso oltre ad ottenere i database, tabelle, colonne e ID, può decifrare le password MD5.

Stando attenti a recuperare correttamente i **cookie** tramite **BurpSuite**



John The Ripper

Decifrazione da MD5

Uno dei metodi migliori per vedere in chiaro le password dalla cifratura **MD5** è l'uso del tool **John The Ripper**

john --format=raw-md5 --wordlist=/usr/share/nmap/nselib/data/passwords.lst /home/kali/Desktop/pass.txt

```
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=/usr/share/nmap/nselib/data/passwords.lst  /home/kali/Desktop/pass.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
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         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2024-04-03 03:45) 200.0g/s 144000p/s 144000c/s 182400C/s alvarez..beanie
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.
```

In dettaglio:

john | richiama il tool che andiamo ad utilizzare
--format=raw-md5 | Il tipo di formato HASH da decifrare
--wordlist= | File contenente il dizionario
/Desktop/pass.txt | File contenente le password in MD5

Altri metodi

Per password “gettonate” e facili esistono tool online dove si possono **decifrare** le password

Ayen Van Zwam