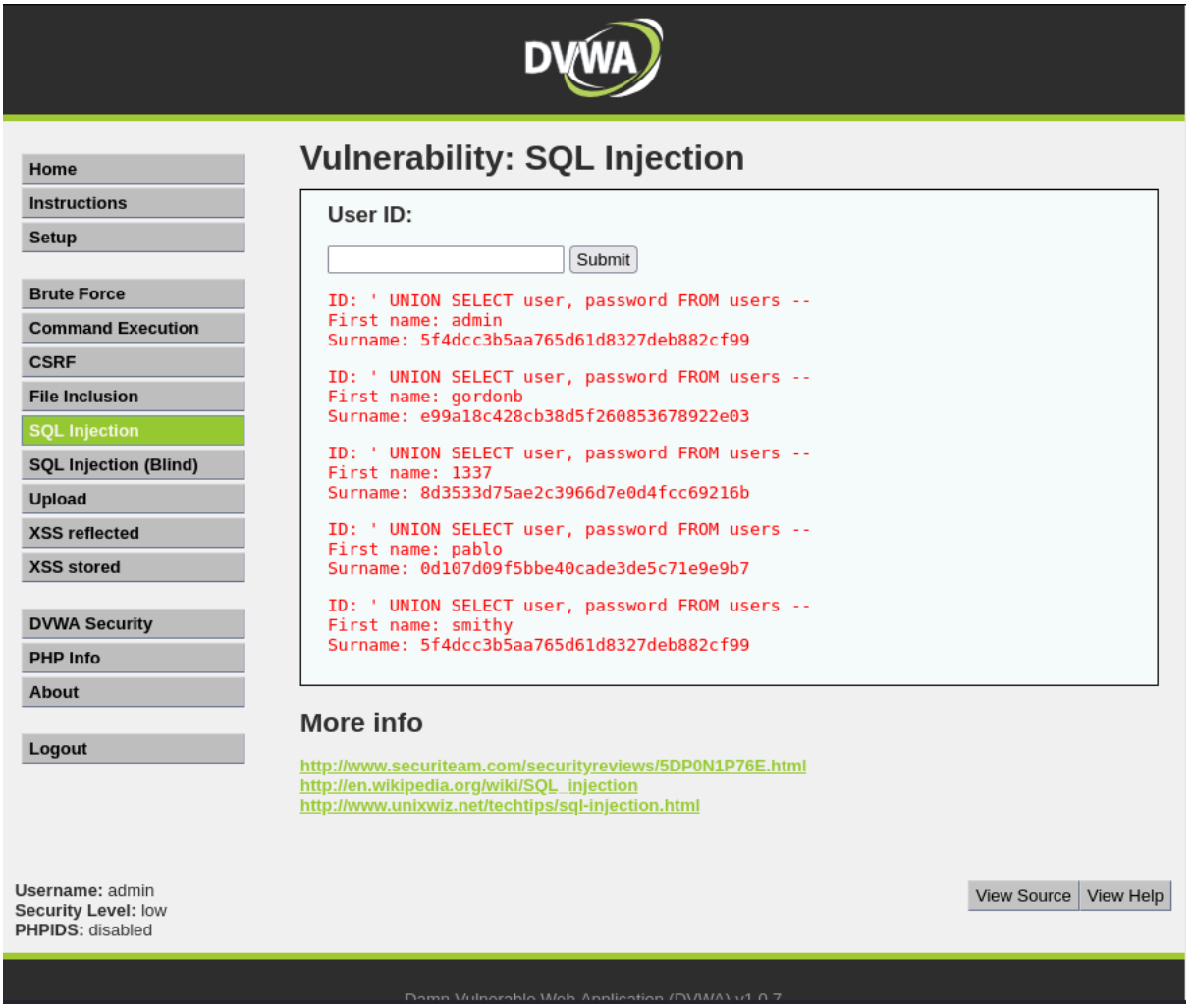
Nell’esercizio di oggi eseguiremo la simulazione di un attacco SQL injection sul server dvwa di metasploitable. La SQL injection è un tipo di attacco di code injection usata contro i database o qualsiasi applicativo che ne fa uso. Consiste nell'iniezione di codice malevolo che, sfruttando una vulnerabilità di mancato controllo dell’input, permette ad un malintenzionato di eseguire una query senza autorizzazione. Grazie a questo meccanismo è possibile eseguire comandi dall’alterazione dei dati (modificarli, cancellarli, creare nuovi utenti,ecc.) fino al download completo del contenuto del database. Per questo motivo è molto pericoloso, fra l’altro non è necessario nemmeno avere strumenti particolari.
Nell’esercizio di oggi vedremo come sfruttare questa vulnerabilità per ottenere le password presenti in dvwa.
Dopo aver acceso le due macchine virtuali (kali e metasploitable) apriamo il nostro browser preferito su kali e digitiamo nella barra degli indirizzi l’indirizzo ip di metasploitable. Entriamo in dvwa con le credenziali di default e andiamo nella sezione di SQL injection.
A questo punto basterà digitare la query che vogliamo far eseguire all’applicazione:

‘ UNION SELECT user, password FROM users - -

Analizziamo la query. Il comando SELECT ci consente di recuperare le informazioni dal database, in questo caso user e password, e il comando UNION ci consente di avere in output entrambi. Il comando FROM invece indica da quale tabella vogliamo recuperare le informazioni. I due trattini finali sono dei commenti.



Come possiamo vedere dall'immagine sopra con la query che abbiamo appena visto siamo stati in grado di ricavare gli username e le password in formato hash dal database di dvwa.
A questo punto tramite john the ripper possiamo provare a ricavare le password dagli hash.

```
┌──(root💀kali)-[/home/kali]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 hash
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2024-01-18 15:17) 133.3g/s 102400p/s 102400c/s 153600C/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.
```

Adesso riusciamo a capire la pericolosità di questa vulnerabilità che ci ha permesso di rubare degli account che possiamo usare per i nostri scopi.