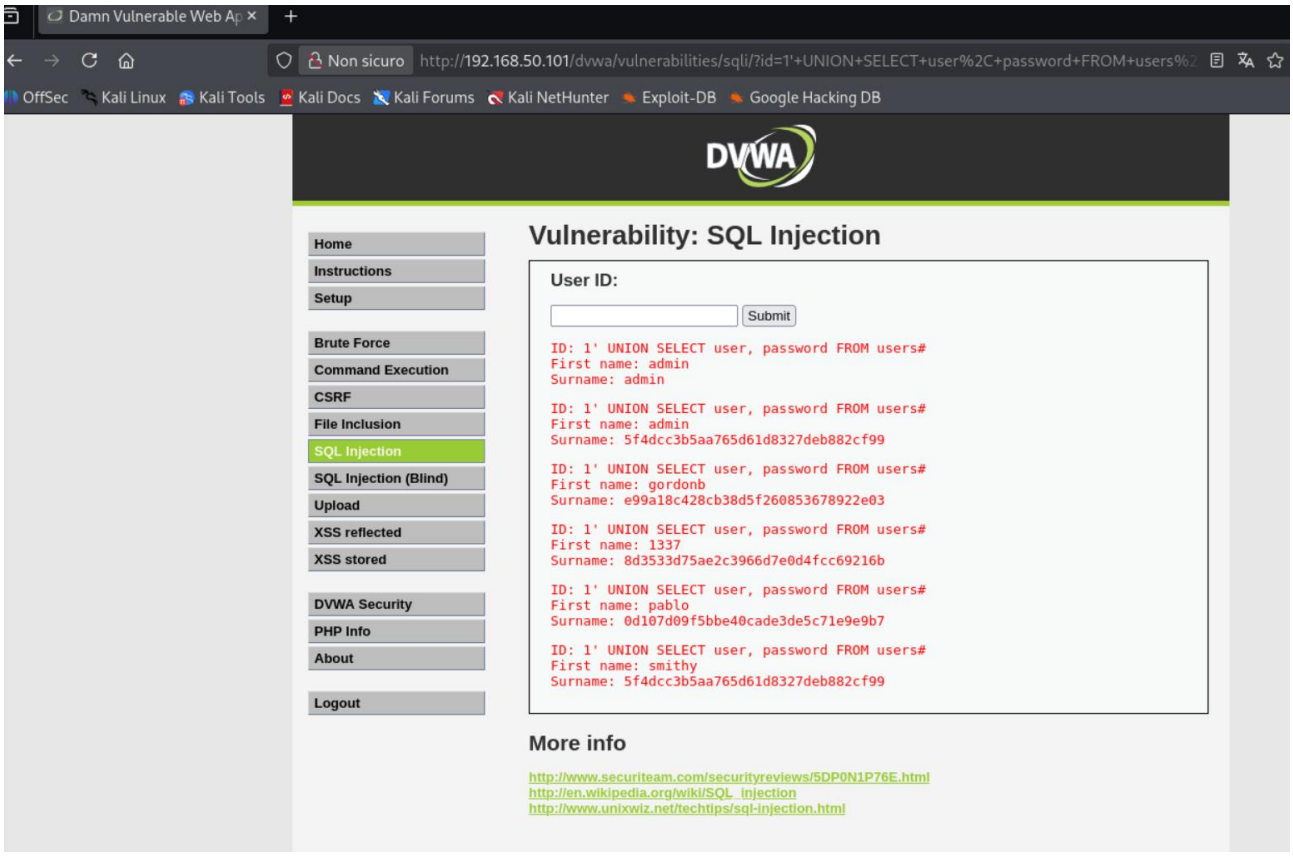

Report: Cracking con John the Ripper e rockyou.txt del precedente SQL Injection

Obiettivo

Password cracking
Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema. Se guardiamo meglio le password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5. Recuperate le password dal DB come visto e provate ad eseguire delle sessioni di cracking sulla password con John the Ripper per recuperare la loro versione in chiaro.
L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

Problemi riscontrati e soluzioni adottate

1. Uso del dizionario compresso (rockyou.txt.gz)

- **Errore:** John non può leggere file .gz direttamente.
- **Soluzione:** Decompressione manuale:

  ```
  gunzip /usr/share/wordlists/rockyou.txt.gz
  ```

---

2. Encoding errato nel dizionario

- **Errore:** John ha rilevato UTF-16 BOM, impedendo la lettura corretta.
- **Tentativo fallito:** Conversione con iconv ha generato errore:

  iconv: illegal input sequence at position ...

- **Soluzione efficace:** Pulizia con dos2unix:

  ```
  dos2unix /usr/share/wordlists/rockyou.txt ~/rockyou_clean.txt
  ```

---

3. Formato hash non compatibile

- **Errore sospetto:** John non trovava password, anche se gli hash erano validi.
- **Verifica:** Controllo del contenuto:

  ```
  head -n 5 /home/kali/Desktop/hash.txt
  ```

- **Soluzione:** Estrazione degli hash (senza username):

  ```
  cut -d ':' -f2 /home/kali/Desktop/hash.txt > ~/clean_hashes.txt
  ```

---

4. File .pot interferiva

- **Errore:** John diceva "No password hashes left to crack".
- **Soluzione:** Rimozione del file .pot:

  ```
  rm ~/.john/john.pot
  ```

---

5. Hash duplicati o sporchi

- **Errore:** Alcuni hash erano duplicati o contenevano caratteri invisibili.

- **Soluzione:** Pulizia rigorosa e deduplicazione:

  cat ~/clean_hashes.txt | tr -d '\r' | grep -E '^[a-fA-F0-9]{32}$' | sort -u > ~/clean_hashes_strict.txt

---

Risultato finale

Comando eseguito:

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt ~/clean_hashes_strict.txt

Output:

password (?)
abc123 (?)
letmein (?)
charley (?)

Hash craccati:

Hash	Password
5f4dcc3b5aa765d61d8327deb882cf99	password
e99a18c428cb38d5f260853678922e03	abc123
0d107d09f5bbe40cade3de5c71e9e9b7	letmein
8d3533d75ae2c3966d7e0d4fcc69216b	charley

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt ~/clean_hashes_strict.txt
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=5
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2025-11-05 14:19) 200.0g/s 153600p/s 153600c/s 230400C/s my3kids..dangerous
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```