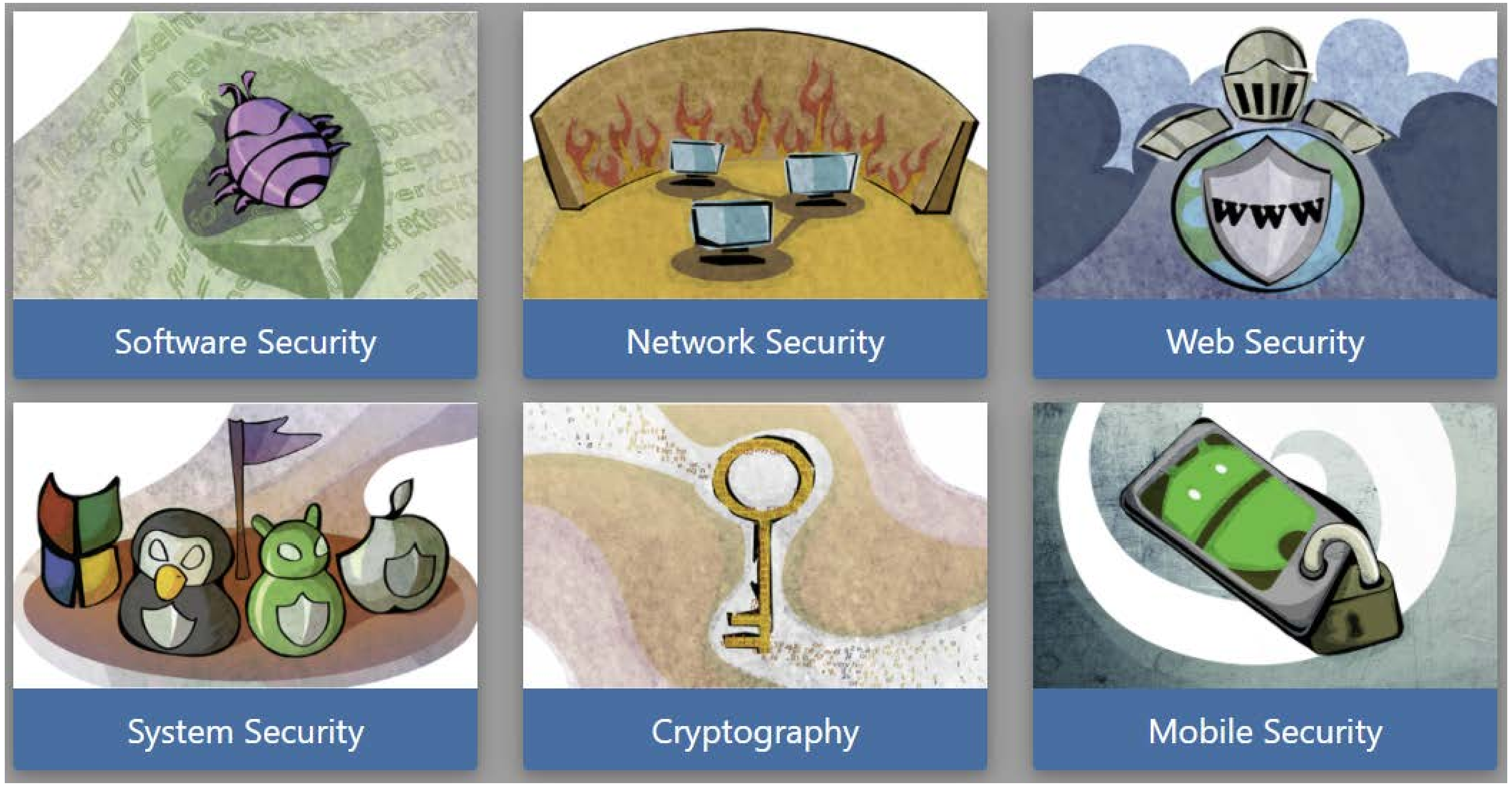
Project #3

SQL injection Setup Instruction

SEED Security Labs

- You can explore existing security problems in form of labs



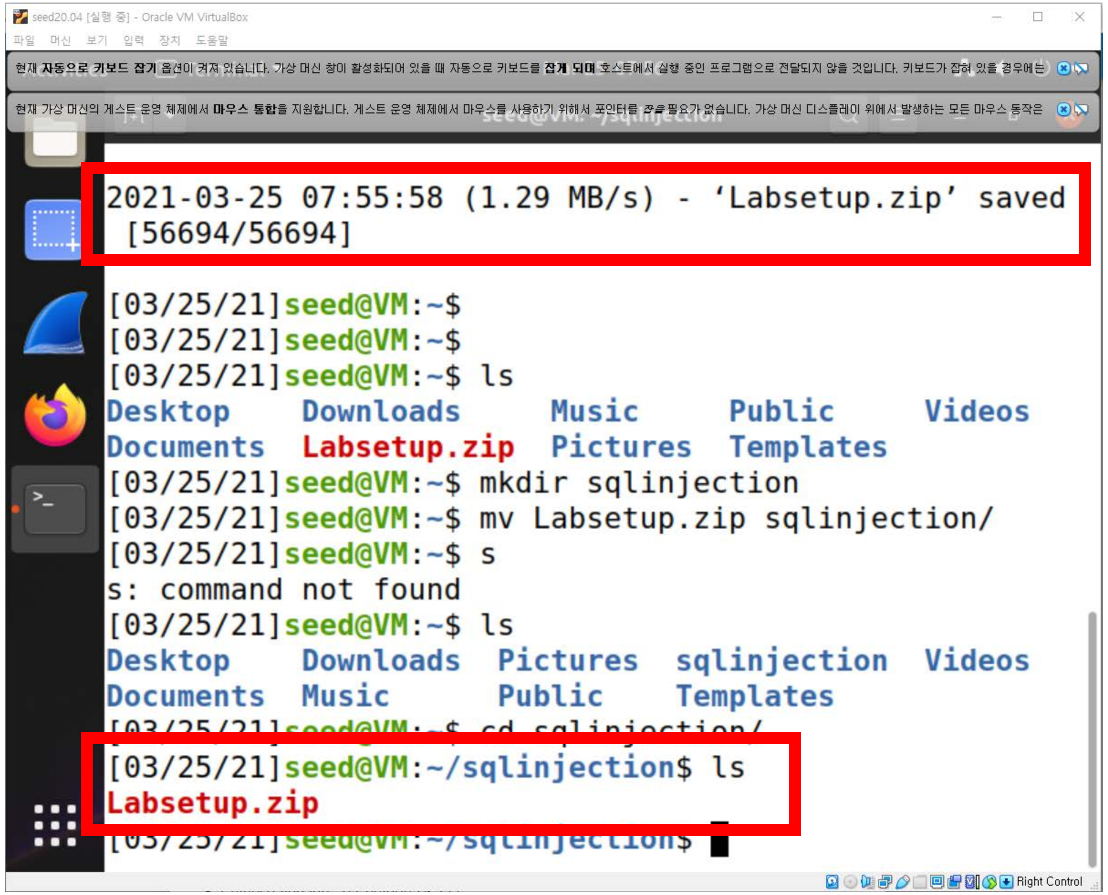
SQL Injection Attack Lab

- [SEED 2.0] – [Web Security] – [SQL Injection Attack Lab]
  - Lab page: https://seedsecuritylabs.org/Labs_20.04/Web/Web_SQL_Injection/
  - **Lab document**: https://seedsecuritylabs.org/Labs_20.04/Files/Web_SQL_Injection/Web_SQL_Injection.pdf
- Prerequisite
  - **Read the lab document before you start the lab!**
  - Build VM and load pre-build SEED VM (you can use cloud instead of using local machine): https://seedsecuritylabs.org/labsetup.html
  - Be familiar with Docker environments: https://github.com/seed-labs/seed-labs/blob/master/manuals/docker/SEEDManual-Container.md

Quick Environment Setup Guideline (1/4)

- Please be familiar with Docker and VM environment! The slides are not sufficient!

1. Setup VM with VirtualBox
2. Download SQL Injection materials



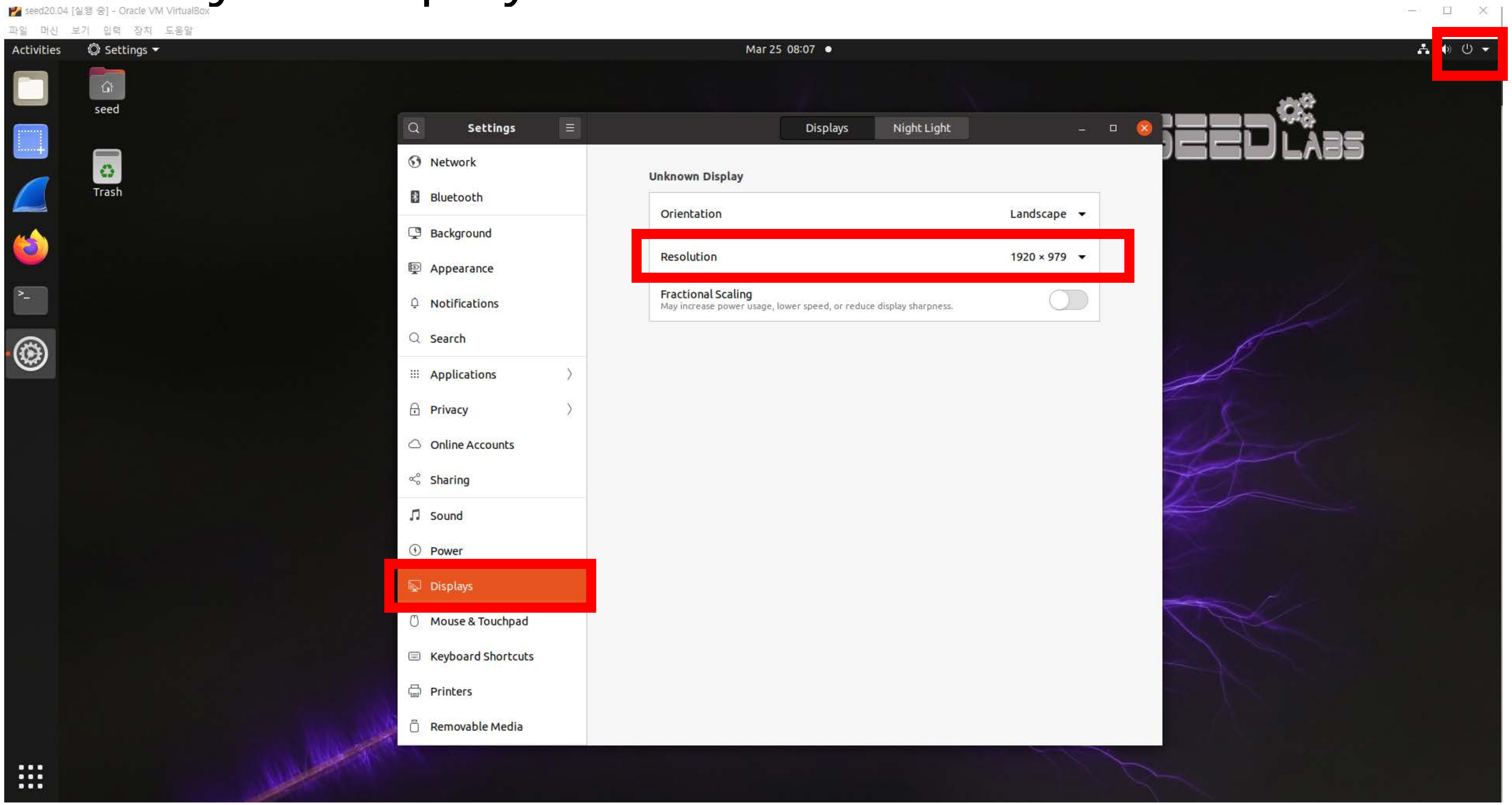
현재 **자동으로 키보드 잡기** 옵션이 켜져 있습니다. 가상 머신 창이 활성화되어 있을 때 자동으로 키보드를 **잡게 되며** 호스트에서 실행 중인 프로그램으로 전달되지 않을 것입니다. 키보드가 잡혀 있을 경우에는

현재 가상 머신의 게스트 운영 체제에서 **마우스 통합**을 지원합니다. 게스트 운영 체제에서 마우스를 사용하기 위해서 포인터를 *잡을* 필요가 없습니다. 가상 머신 디스플레이 위에서 발생하는 모든 마우스 동작은

```
2021-03-25 07:55:58 (1.29 MB/s) - ‘Labsetup.zip’ saved
 [56694/56694]

[03/25/21]seed@VM:~$
[03/25/21]seed@VM:~$
[03/25/21]seed@VM:~$ ls
Desktop    Downloads     Music     Public     Videos
Documents  Labsetup.zip  Pictures  Templates
[03/25/21]seed@VM:~$ mkdir sqlinjection
[03/25/21]seed@VM:~$ mv Labsetup.zip sqlinjection/
[03/25/21]seed@VM:~$ s
s: command not found
[03/25/21]seed@VM:~$ ls
Desktop    Downloads  Pictures  sqlinjection  Videos
Documents  Music      Public    Templates
[03/25/21]seed@VM:~$ cd sqlinjection/
[03/25/21]seed@VM:~/sqlinjection$ ls
Labsetup.zip
[03/25/21]seed@VM:~/sqlinjection$ 
```

Quick Environment Setup Guideline (2/4)

- You can adjust display resolution or use SSH connection.



Unknown Display

Orientation: Landscape

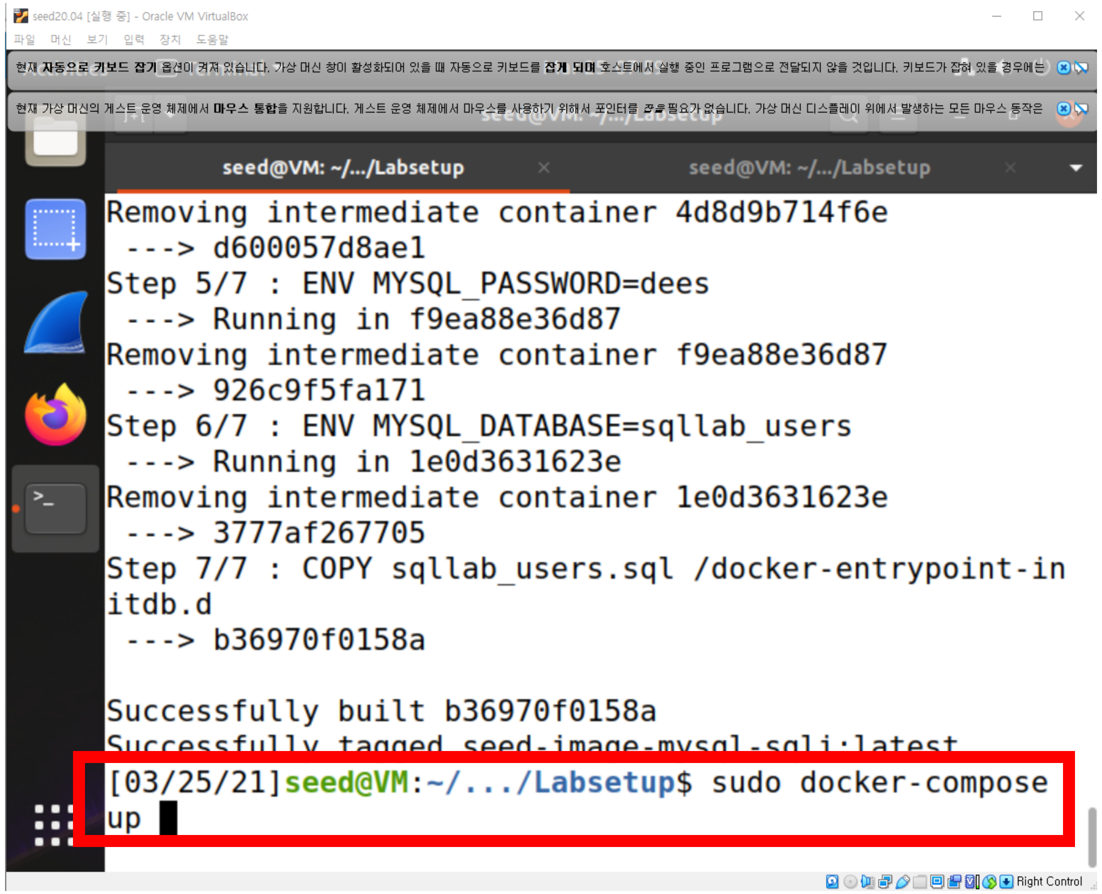
Resolution: 1920 × 979

Fractional Scaling

May increase power usage, lower speed, or reduce display sharpness.

Quick Environment Setup Guideline (3/4)

- Run Docker environment using *docker-compose build (dcbuild)* and *docker-compose up (dcup)*
  - https://github.com/seed-labs/seed-labs/blob/master/manuals/docker/docker.md
  - https://github.com/seed-labs/seed-labs/blob/master/manuals/docker/docker-commands.md



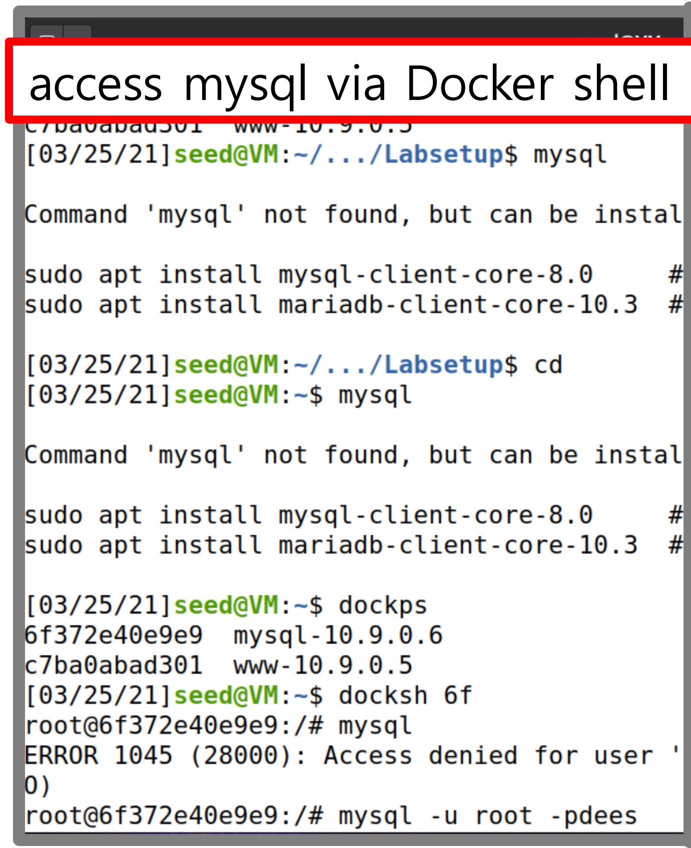
현재 **자동으로 키보드 잡기** 옵션이 켜져 있습니다. 가상 머신 창이 활성화되어 있을 때 자동으로 키보드를 **잡게 되며** 호스트에서 실행 중인 프로그램으로 전달되지 않을 것입니다. 키보드가 잡혀 있을 경우에는

현재 가상 머신의 게스트 운영 체제에서 **마우스 통합**을 지원합니다. 게스트 운영 체제에서 마우스를 사용하기 위해서 포인터를 *잡을* 필요가 없습니다. 가상 머신 디스플레이 위에서 발생하는 모든 마우스 동작은

```
Removing intermediate container 4d8d9b714f6e
 ---> d600057d8ae1
Step 5/7 : ENV MYSQL_PASSWORD=dees
 ---> Running in f9ea88e36d87
Removing intermediate container f9ea88e36d87
 ---> 926c9f5fa171
Step 6/7 : ENV MYSQL_DATABASE=sqllab_users
 ---> Running in 1e0d3631623e
Removing intermediate container 1e0d3631623e
 ---> 3777af267705
Step 7/7 : COPY sqllab_users.sql /docker-entrypoint-in
itdb.d
 ---> b36970f0158a

Successfully built b36970f0158a
Successfully tagged seed-image-mysql-sqli:latest
[03/25/21]seed@VM:~/.../Labsetup$ sudo docker-compose
up
```

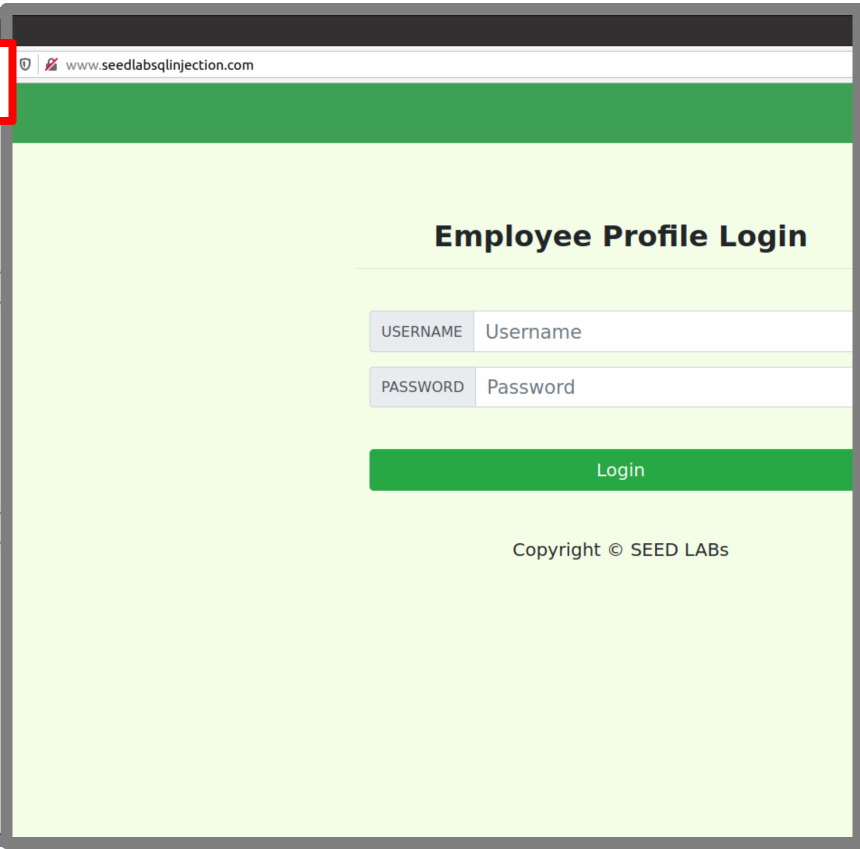
Quick Environment Setup Guideline (4/4)

- Check the database schema, find vulnerabilities in web code, and conduct SQL injection!



access mysql via Docker shell

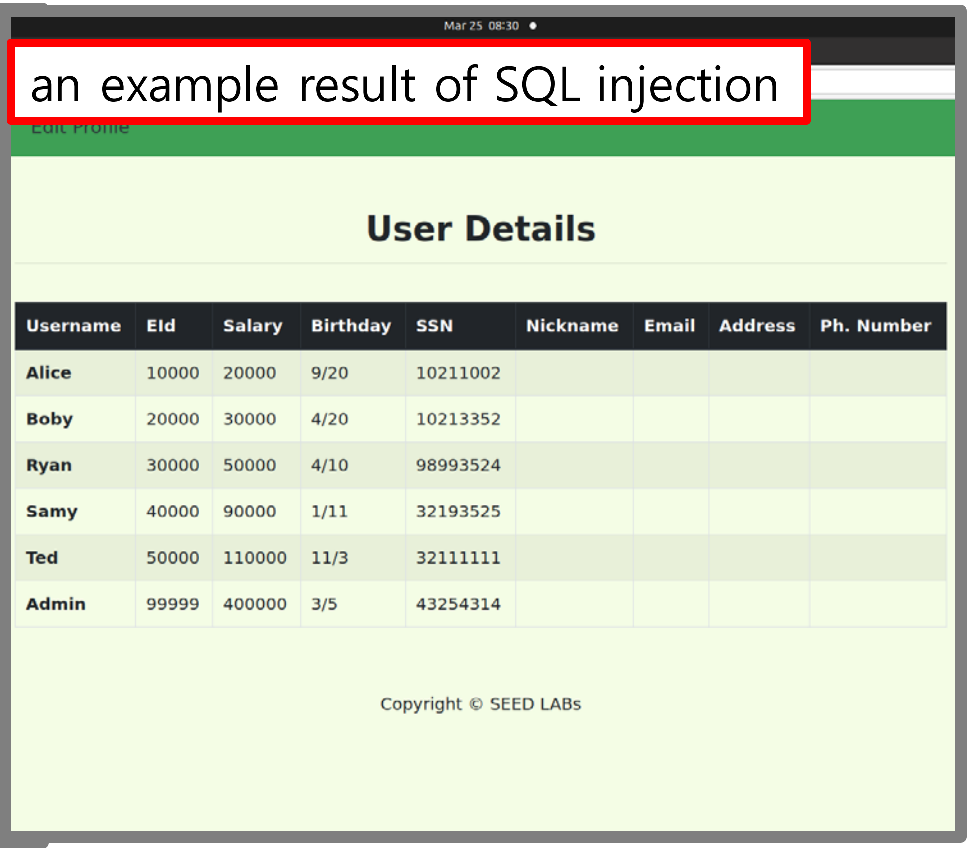
```
c7ba0abad301  www-10.9.0.5
[03/25/21]seed@VM:~/.../Labsetup$ mysql

Command 'mysql' not found, but can be instal

sudo apt install mysql-client-core-8.0     #
sudo apt install mariadb-client-core-10.3  #

[03/25/21]seed@VM:~/.../Labsetup$ cd
[03/25/21]seed@VM:~$ mysql

Command 'mysql' not found, but can be instal

sudo apt install mysql-client-core-8.0     #
sudo apt install mariadb-client-core-10.3  #

[03/25/21]seed@VM:~$ dockps
6f372e40e9e9  mysql-10.9.0.6
c7ba0abad301  www-10.9.0.5
[03/25/21]seed@VM:~$ docksh 6f
root@6f372e40e9e9:/# mysql
ERROR 1045 (28000): Access denied for user '
O)
root@6f372e40e9e9:/# mysql -u root -pdees
```



Employee Profile Login

USERNAME	Username
PASSWORD	Password

Copyright © SEED LABs



an example result of SQL injection

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				

Copyright © SEED LABs

Submission Guideline

- Report
  - Up to Task 3
  - Inputs and outputs (if needed screenshot).
  - Your analysis
- Due date
  - Apr. 5th