**Lab 5. SQL Injection**

SQL injection is a code injection technique that exploits the vulnerabilities in the interface between web applications and database servers. The vulnerability is present when user’s inputs are not correctly checked within the web applications before being sent to the back-end database servers

**Submission:**

You will compose a lab report that documents each step you take, including screenshots to illustrate the effects of commands you type, and describing your observations. Simply attaching code without any explanation will not receive credits

Prepare:

* Pre-built Ubuntu VM (download from the SEED Website)

LAB GUIDE:

1. Review the lab environment



#vi /etc/host

# /etc/ apache2/sites-available/ 000-default.conf

1. Get Familiar with SQL Statements

.

we have already created the Users database for you, you just need to load this existing database using the following command:



you can use the following command to print out all the tables of the selected database



After running the commands above, you need to use a SQL command to print all the profile information of the employee Alice. Please provide the screenshot of your results

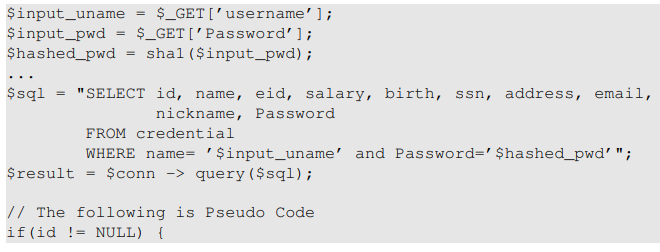
1. SQL Injection Attack on SELECT Statement

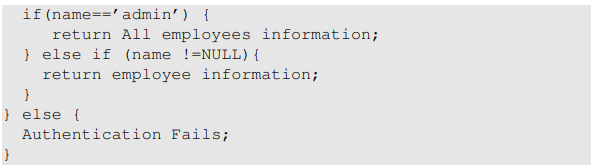
We will use the login page from www.SEEDLabSQLInjection.com for this task



The web application authenticate users based on these two pieces of data, so only employees who know their passwords are allowed to log in. Your job, as an attacker, is to log into the web application without knowing any employee’s credential.

To help you started with this task, we explain how authentication is implemented in the web application. The PHP code unsafe home.php, located in the **/var/www/SQLInjection** directory, is used to conduct user authentication. The following code snippet show how users are authenticated



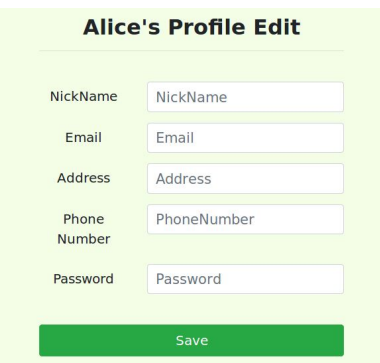
. 

1. SQL Injection Attack from webpage.

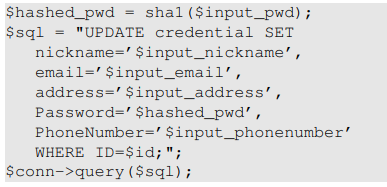
Your task is to log into the web application as the administrator from the login page, so you can see the information of all the employees. We assume that you do know the administrator’s account name which is admin, but you do not the password. You need to decide what to type in the Username and Password fields to succeed in the attack.

1. **SQL Injection Attack on UPDATE Statement**

If a SQL injection vulnerability happens to an UPDATE statement, the damage will be more severe, because attackers can use the vulnerability to modify databases. In our Employee Management application, there is an Edit Profile page that allows employees to update their profile information, including nickname, email, address, phone number, and password



When employees update their information through the Edit Profile page, the following SQL UPDATE query will be executed. The PHP code implemented in unsafe edit backend.php file is used to update employee’s profile information. The PHP file is located in the /var/www/SQLInjection directory



• Task 5.1: Modify your own salary. As shown in the Edit Profile page, employees can only update their nicknames, emails, addresses, phone numbers, and passwords; they are not authorized to change their salaries. Assume that you (Alice) are a disgruntled employee, and your boss Boby did not increase your salary this year. You want to increase your own salary by exploiting the SQL injection vulnerability in the Edit-Profile page. Please demonstrate how you can achieve that. We assume that you do know that salaries are stored in a column called ’salary’.

• Task 5.2: Modify other people’ salary. After increasing your own salary, you decide to punish your boss Boby. You want to reduce his salary to 1 dollar. Please demonstrate how you can achieve that.

• Task 5.3: Modify other people’ password. After changing Boby’s salary, you are still disgruntled, so you want to change Boby’s password to something that you know, and then you can log into his account and do further damage. Please demonstrate how you can achieve that. You need to demonstrate that you can successfully log into Boby’s account using the new password. One thing worth mentioning here is that the database stores the hash value of passwords instead of the plaintext password string. You can again look at the unsafe edit backend.php code to see how password is being stored. It uses SHA1 hash function to generate the hash value of password.