|  |  |
| --- | --- |
| **Họ và tên**: Bùi Lê Thủy Tiên  **Mssv**: 22162048  **LAB 05**:  SQL Injection  **Giảng viên**: TS. Huỳnh Nguyên Chính | **Nhận xét giáo viên** |

**Chuẩn bị:**

Cài Ubuntu16-04 32 bit theo link (https://seedsecuritylabs.org/lab\_env.html)

**LAB GUIDE:**

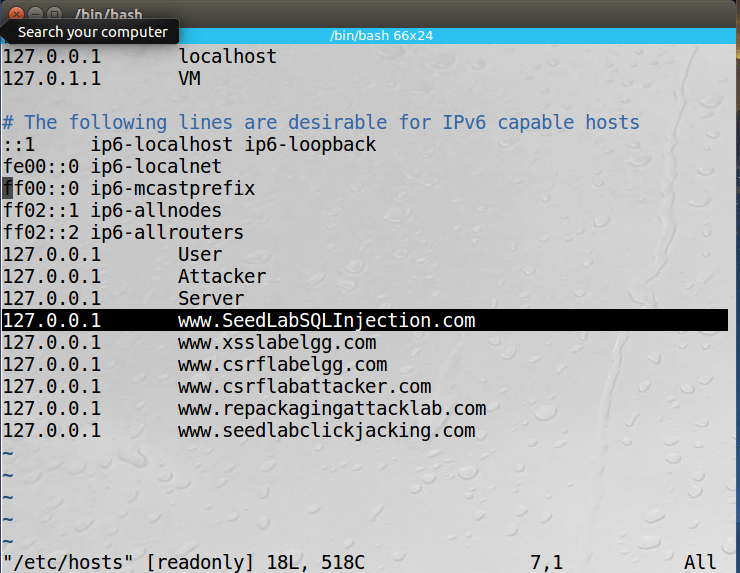
Review the lab environment

A close up of a sign

Description automatically generated

**#vi /etc/hosts**:

File /etc/hosts là một tập tin văn bản đơn giản nằm trong thư mục /etc của hệ điều hành Linux. Nó được sử dụng để ánh xạ các tên miền (domain names) sang địa chỉ IP (IP addresses) tương ứng

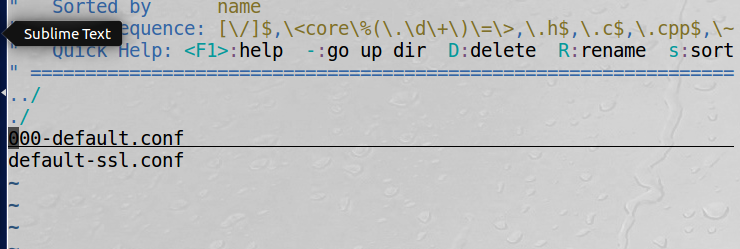


🡪 Những dòng này ánh xạ các tên miền giả mạo sang địa chỉ IP 127.0.0.1. Khi bạn truy cập vào một trong những tên miền này, trình duyệt web của bạn sẽ kết nối với máy tính cục bộ thay vì máy chủ web thực tế. Điều này có thể được sử dụng cho các mục đích khác nhau, chẳng hạn như cho việc kiểm tra bảo mật, trong bài là lỗi SQL Injection.

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

- Các tệp trong /etc/apache2/conf-available là các tệp mà quản trị viên có thể tự do tạo, đổi tên, xóa, điền nội dung phù hợp, v.v.

- Chọn option này nhấn Enter



A screen shot of a computer

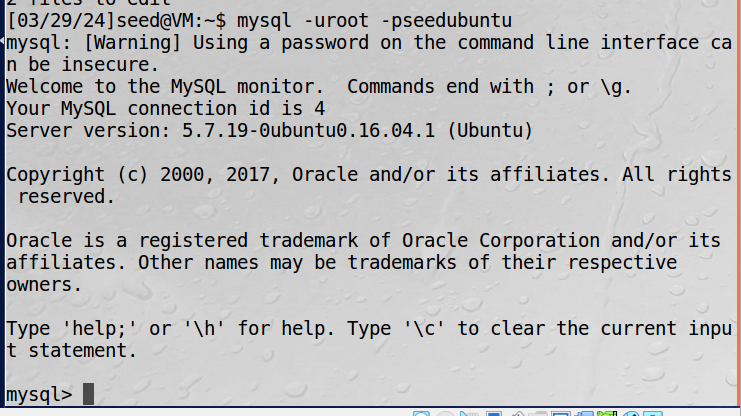
Description automatically generated

**Get Familiar with SQL Statements**.

Database trong bài cụ thể là Users đã được cài sẵn trong môi trường, ta chỉ cần load các cơ sở dữ liệu thông qua việc sử dụng các command.

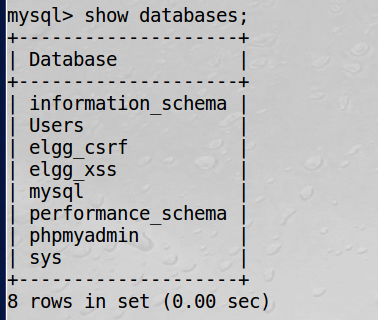
***- Truy cập vô sql***





**mysql> show databases;**

**-** Dùng để hiển thị các cơ sở dữ liệu tồn tại trong hệ thống, ta có thể thấy trong hệ thống đã có sẳn database Users





- Ta sẽ sử dụng database mang tên Users:



- Hiển thị ra các bảng của Users bằng



A white background with black text

Description automatically generated

**Describe Credential:** Xem cấu trúc của table credential

mysql > describe credential;

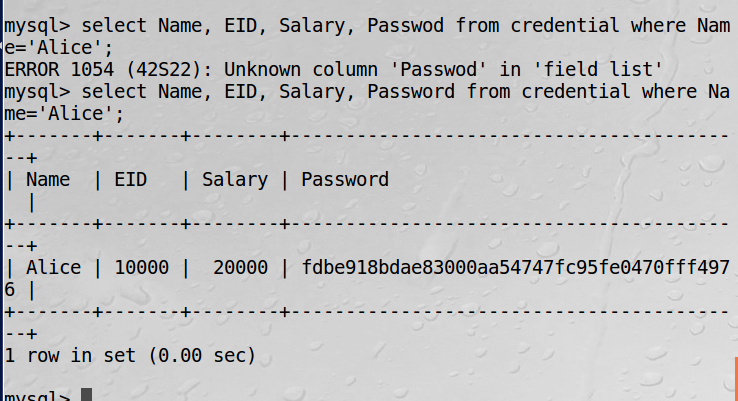
A screenshot of a computer screen

Description automatically generated

🡪 Ta thấy có 11 thuộc tính và các kiểu dữ liệu cũng như các ràng buộc... của credential.

Task: Sau khi chạy xong những câu lệnh trên thì dùng SQL command (không phan biệt chữ hoa thường) để in ra tất cả các thông tin của nhân viên ***Alice***

Solve: bằng lệnh **select Name, EID, Salary, Password from credential where name=’Alice’;**



- In ra các thông tin Tên, Mã nhân viên, Lương, Mật khẩu của tất cả các nhân viên trong bảng credential

**Select Name, EID, Salary, birth, Password from credential;**

A computer screen shot of a computer screen

Description automatically generated

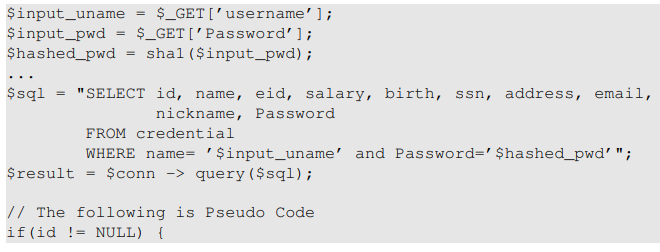
🡪 Ta có thể tiến hành thực hiện thêm các lệnh để nghiên cứu thông tin của database, sau khi chạy thì ta xác định được rằng, các password đã được lưu dưới dạng mã, được băm ra(hashing). Đây là thông tin quan trọng để thực hiện các bước tiếp theo

**3. SQL Injection Attack on SELECT Statement**

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



- Ứng dụng web xác thực người dùng dựa trên hai phần dữ liệu này, vì vậy chỉ những nhân viên biết mật khẩu của họ mới được phép đăng nhập. Công việc của bạn, với tư cách là kẻ tấn công, là đăng nhập vào ứng dụng web mà không cần biết thông tin xác thực của bất kỳ nhân viên nào.

- Để giúp bạn bắt đầu nhiệm vụ này, chúng tôi giải thích cách triển khai xác thực trong ứng dụng web. Mã PHP không an toàn home.php nằm trong thư mục /var/www/SQLInjection được sử dụng để tiến hành xác thực người dùng. Đoạn mã sau đây cho thấy cách người dùng được xác thực

🡪 Tại bước này ta thấy khi chúng ta tiến hành nhập pass thì hệ thống sẽ mả hóa sang sha1 và dùng mật khẩu đó để kiểm tra

. A computer screen shot of a computer code

Description automatically generated

🡪 Tại bước này thì ta thấy nếu tên đăng nhập là admin thì sẽ show ra thông tin của toàn bộ nhân viên

**4. SQL Injection Attack from webpage.**

Task: Nhiệm vụ của bạn là đăng nhập vào ứng dụng web với tư cách quản trị viên từ trang đăng nhập để có thể xem thông tin của tất cả nhân viên. Chúng tôi cho rằng bạn biết tên tài khoản của quản trị viên là quản trị viên nhưng bạn không biết mật khẩu. Bạn cần quyết định nhập gì vào trường Tên người dùng và Mật khẩu để cuộc tấn công thành công.

Tìm kiếm trang: <http://www.seedlabsqlinjection.com/> trên Ubuntu

- Tiến hành đăng nhập vào với tư cách admin thông qua việc nhập username: admin ‘# (sau # các lệnh sẽ không được thực thi do # là kí hiệu của comment nó sẽ ẩn hết những nội dung phía sau dẫn đến password không được check như ta đã nghiên cứu về cách thực hiện xác thực ở trên)

A screenshot of a computer

Description automatically generated

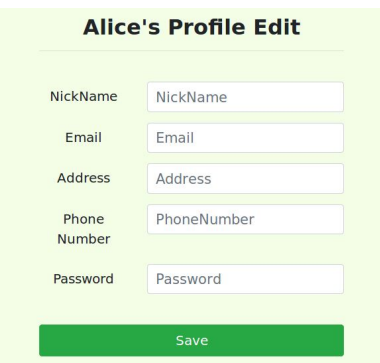
- Ấn login xem thông tin nhân viên

A screenshot of a computer

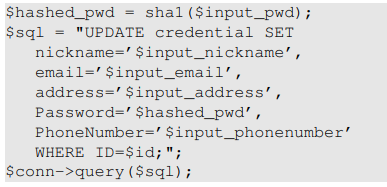
Description automatically generated

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

Nếu lỗ hổng SQL SQL xảy ra với câu lệnh UPDATE, thiệt hại sẽ nghiêm trọng hơn vì kẻ tấn công có thể sử dụng lỗ hổng này để sửa đổi cơ sở dữ liệu. Trong ứng dụng Employee Management có trang Edit Profile cho phép nhân viên cập nhật thông tin hồ sơ của mình, bao gồm biệt danh, email, địa chỉ, số điện thoại và mật khẩu.



- Khi nhân viên cập nhật thông tin của họ thông qua trang Edit Profile, truy vấn SQL UPDATE sau sẽ được thực thi. Mã PHP được triển khai trong tệp backend.php chỉnh sửa không an toàn được sử dụng để cập nhật thông tin hồ sơ của nhân viên. Tệp PHP nằm trong thư mục /var/www/SQLInjection



Task 5.1: Sửa đổi mức lương của riêng bạn. Như được hiển thị trong trang Edit Profile, nhân viên chỉ có thể cập nhật biệt hiệu, email, địa chỉ, số điện thoại và mật khẩu của mình; họ không được phép thay đổi mức lương của mình. Giả sử bạn (Alice) là một nhân viên bất mãn và sếp Boby của bạn không tăng lương cho bạn trong năm nay. Bạn muốn tăng lương cho mình bằng cách khai thác lỗ hổng SQL trong trang Edit Profile. Hãy chứng minh làm thế nào bạn có thể đạt được điều đó. Chúng tôi giả định rằng bạn biết rằng tiền lương được lưu trữ trong một cột có tên là ‘salary’.

**Bước 1: Xem “Salary” của Alice:**

Ta thấy rằng lương ban đầu của Alice là 20000

A screenshot of a graph

Description automatically generated

**Bước 2: Tiến hành tìm kiếm và đăng nhập:**

Vào trang: <http://www.seedlabsqlinjection.com/>

Đăng nhập: Ta có thể dùng SQL injection để đăng nhập vào hệ thống với quyền admin bằng username là: ***admin’#***

A screenshot of a computer

Description automatically generated



**Bước 3: Tiến hành để thay đổi “Salary” của Alice**

Click vào khung nickname và nhập lệnh

**‘, salary = 77000 where Name = ‘Alice’; #**

**🡪 Lệnh này sẽ là thay đổi salary do khi ấn button save thì câu lệnh sql này sẽ được thực hiện**

sql = “update credential set nickname=’$input\_nickname’,

nickname=’$input\_nickname’,

email=’$input\_email’,

address=’$input\_address’,

Password=’$input\_password’,

Phonenumber=’$input\_phoneNumber,

Where id = $id”

Khi ta nhập lệnh **‘, salary = 77000 where Name = ‘Alice’; #** thì câu sql trở thành

sql = “update credential set nickname=’ **‘, salary = 77000 where Name = ‘Alice’; #**

nickname=’$input\_nickname’,

email=’$input\_email’,

address=’$input\_address’,

Password=’$input\_password’,

Phonenumber=’$input\_phoneNumber,

Where id = $id”

🡪 Tất cả câu lệnh sau # thành comment nên sql cuối cùng sẽ thực hiện là sql = “update credential set nickname=’ **‘, salary = 77000 where Name = ‘Alice’; 🡪 *thành công cập nhật lương***

A screenshot of a computer screen

Description automatically generated

- Sau đó ấn save, xem thông tin đã bị thay đổi

A screenshot of a computer screen

Description automatically generated

A white surface with black text

Description automatically generated

🡪 Như 2 ảnh trên, kết quả của việc chỉnh sửa lương Alice đã thành công.

• Task 5.2: Sửa đổi mức lương của người khác. Sau khi tăng lương cho chính mình, bạn quyết định trừng phạt sếp Boby của mình. Bạn muốn giảm lương của anh ấy xuống còn ***100 đô la***. Hãy chứng minh làm thế nào bạn có thể đạt được điều đó.

**Bước 1: Xem “Salary” của Boby:**

A white surface with black text

Description automatically generated

**Bước 2: Tiến hành tìm kiếm và đăng nhập:**

- Vào trang: <http://www.seedlabsqlinjection.com/>

- Đăng nhập: Ta có thể dùng SQL injection để đăng nhập vào hệ thống với quyền admin bằng username là: admin’#

A screenshot of a computer

Description automatically generated

**Bước 3: Tiến hành để thay đổi “Salary” của Boby**

Click vào khung nickname và nhập lệnh

**‘, salary = 100 where Name = ‘Boby; #**

A screenshot of a computer

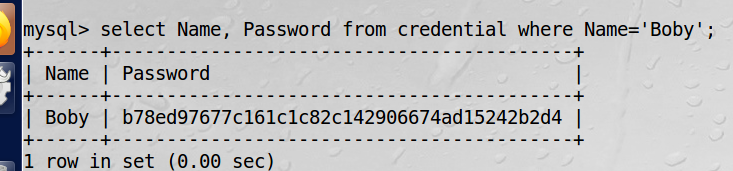
Description automatically generated

A snow with black text

Description automatically generated

• Task 5.3: Sửa đổi mật khẩu của người khác. Sau khi đổi lương cho Boby, bạn vẫn bất bình nên muốn đổi mật khẩu của Boby thành mật khẩu nào đó mà bạn biết, sau đó bạn có thể đăng nhập vào tài khoản của anh ấy và gây thêm thiệt hại. Hãy chứng minh làm thế nào bạn có thể đạt được điều đó. Bạn cần chứng minh rằng bạn có thể đăng nhập thành công vào tài khoản của Boby bằng mật khẩu mới. Một điều đáng nói ở đây là cơ sở dữ liệu lưu trữ giá trị băm của mật khẩu thay vì chuỗi mật khẩu văn bản gốc. Bạn có thể xem lại mã chỉnh sửa backend.php không an toàn để xem mật khẩu đang được lưu trữ như thế nào. Nó sử dụng hàm băm SHA1 để tạo giá trị băm của mật khẩu.

- Xem mật khẩu của Boby, mật khẩu ở dạng 1 bảng băm



Chúng ta sẽ sửa đổi lại mật khẩu của Boby:

**Bước 1: Vào Edit Profile tiến hành đổi password, giả sử ta đặt password mới cho Boby là *“lataone”* thông qua lệnh:**

**‘, password=’lataone’ where Name=’Boby’; #**

A screenshot of a computer

Description automatically generated

- Check pass đã đổi chưa

A close up of a white surface

Description automatically generated

🡪 Mật khẩu mới đã được cập nhật thành công

- Bắt đầu đăng nhập vào hệ thống với username là Boby và mật khẩu mới vừa cập nhật

A screenshot of a login screen

Description automatically generated

A screenshot of a computer

Description automatically generated

🡪 Ta thấy không thể đăng nhập vào được khi ta nhập mật khẩu “lataone” bởi vì nó đã được băm ra thành chuỗi kí tự khác thông qua quá trình hashing.

**Bước 2: ta vào Ubuntu mở Terminater chuyển mật khẩu “lataone” thành giá trị hash thông qua SHA1 hash function.**

**echo -n ‘<lataone>’ | openssl sha1**

A close up of a number

Description automatically generated

- Thực hiện edit profile đặt mật khẩu là chuỗi kí tự này

A screenshot of a computer

Description automatically generated

- Đã cập nhật thành công

A screen shot of a computer

Description automatically generated

**Bước 3: Sau đó tiến hành đăng nhập lại trên trang**

Đăng nhập lại vào hệ thống với username “Boby” và password là “lataone”

A screenshot of a login screen

Description automatically generated

A screenshot of a computer

Description automatically generated

🡪 Đã đăng nhập vào được vào tài khoản của Boby.

🡪 Việc sử dụng hashing mật khẩu là một phần quan trọng của bảo mật hệ thống và ngăn chặn việc truy cập trái phép vào thông tin cá nhân của người dùng. Khi ta cập nhật mật khẩu và lưu trữ chúng dưới dạng chuỗi băm, sẽ giúp tăng cường bảo mật và đảm bảo rằng người quản trị hệ thống không thể dễ dàng biết được mật khẩu ban đầu của người dùng.