

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN – ĐHQG_HCM
KHOA CÔNG NGHỆ THÔNG TIN



An ninh máy tính

Lab 5

Giảng viên: Huỳnh Nguyên Chính
Nguyễn Văn Quang Huy
Ngô Đình Hy

MSSV	Họ và tên
20120083	Nguyễn Trọng Hiếu

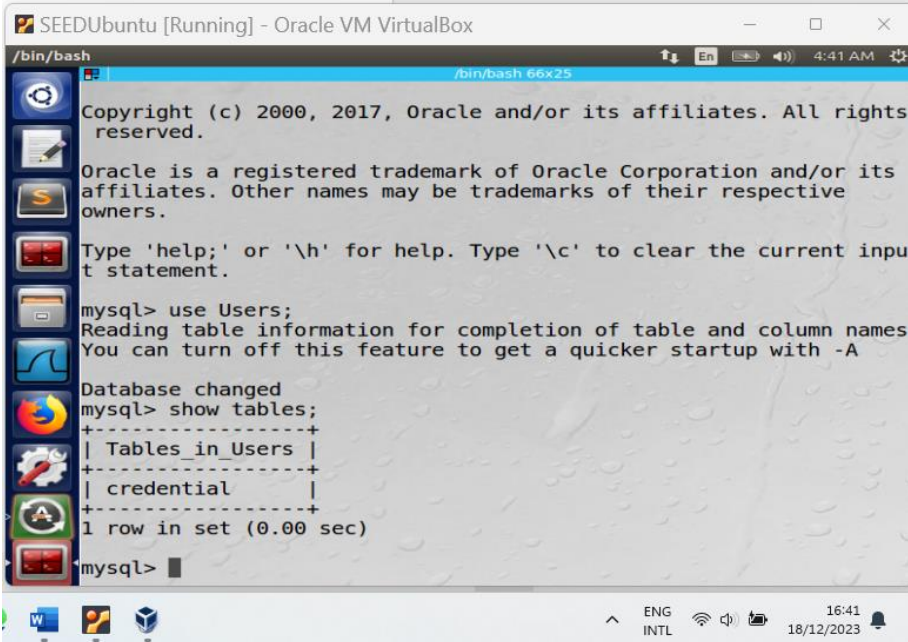
Mục Lục

1. SQL injection [1]	3
1.1 Get familiar with SQL Statement.....	3
1.2 SQL Injection Attack on SELECT Statement.....	3
1.3 SQL Injection Attack on UPDATE Statement.....	5
1.4 Countermeasure — Prepared Statement	5
2. Cross-site Scripting Attack [2].....	5
3. Cross-site Request Forgery [3]	5
4. Cấu hình Website để truy cập qua giao thức HTTPS	5
Bước 1. Tạo CA_SERVER.....	7
Bước 2. Máy WEB_SERVER: www.cntt.vn.....	8
5. Tham khảo:	9

1. SQL injection [1]

1.1 Get familiar with SQL Statement

Kiểm tra các lệnh trong lab



```
SEEDUbuntu [Running] - Oracle VM VirtualBox
/bin/bash
Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

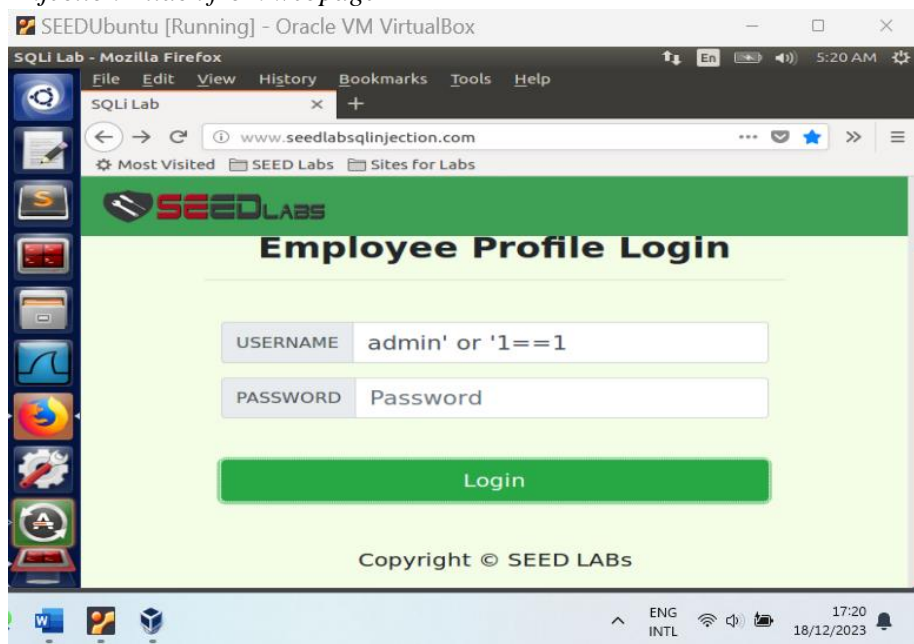
mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

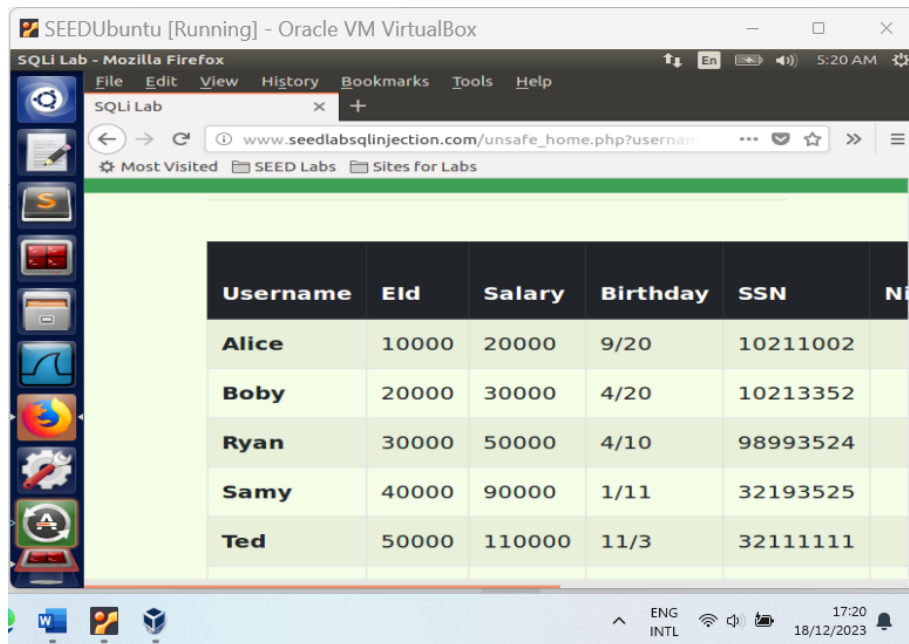
Database changed
mysql> show tables;
+-----+
| Tables_in_Users |
+-----+
| credential      |
+-----+
1 row in set (0.00 sec)

mysql>
```

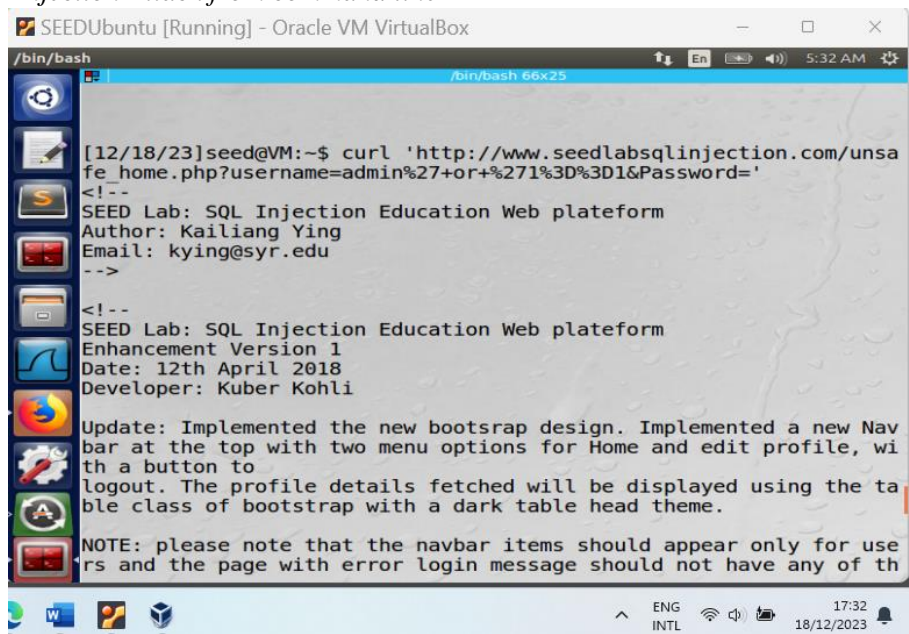
1.2 SQL Injection Attack on SELECT Statement

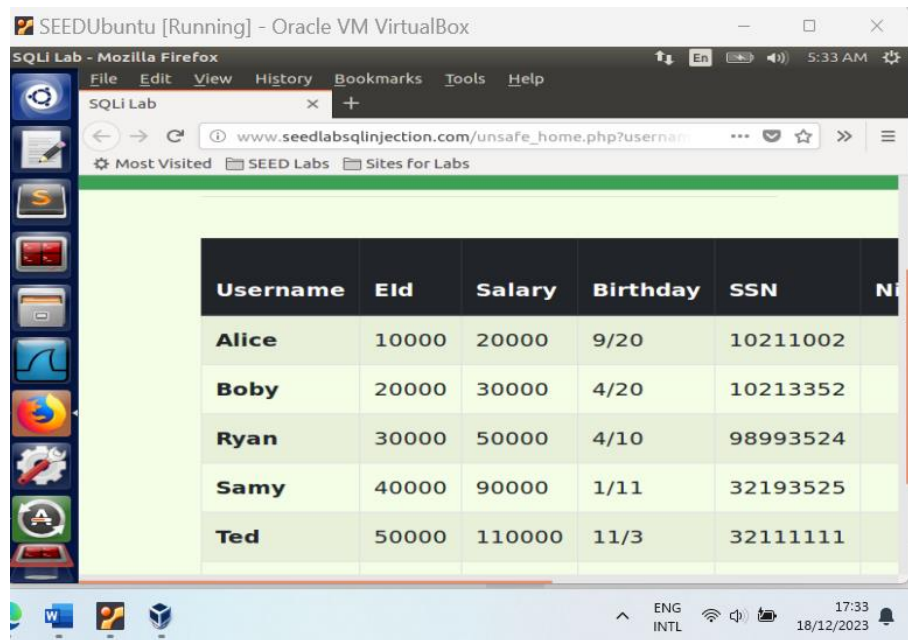
- *SQL Injection Attack from webpage*





- *SQL Injection Attack from command line*





- *Append a new SQL statement*

Không yêu cầu trong lab, tuy nhiên cần nhắc với kích thước của request get trong html mà có thể thiết kế thêm lệnh vào input trong username của trang web khi kết hợp với source code.

1.3 SQL Injection Attack on UPDATE Statement

Kiến thức đọc thêm

- *Modify your own salary*
- *Modify other people's salary*
- *Modify other people's password*

1.4 Countermeasure — Prepared Statement

2. Cross-site Scripting Attack [2]

Cross-Site Scripting (XSS) là một loại tấn công web phổ biến, trong đó kẻ tấn công chèn mã JavaScript hay các mã khác có thể thực thi vào trang web được hiển thị cho người dùng khác. Tấn công XSS thường xuyên xảy ra khi ứng dụng web không kiểm tra đầu vào người dùng đúng cách.

Hậu quả của tấn công XSS có thể rất nghiêm trọng, bao gồm đánh cắp thông tin người dùng, thực hiện hành động thay thế cho người dùng, hoặc thậm chí là kiểm soát toàn bộ trang web.

Biện pháp ngăn chặn tấn công XSS, các nhà phát triển cần kiểm tra và xử lý đầu vào người dùng, mã hóa dữ liệu đầu ra, và sử dụng các biện pháp bảo mật như Content Security Policy (CSP).

3. Cross-site Request Forgery [3]

Cross-Site Request Forgery (CSRF hoặc XSRF) là một loại tấn công mạng, trong đó kẻ tấn công lừa đảo người dùng hoặc trình duyệt của họ để thực hiện các hành động không mong muốn trên một trang web mà họ đã đăng nhập. Tấn công này thường xuyên liên quan đến việc sử dụng các yêu cầu HTTP không mong muốn được gửi từ trình duyệt của người dùng đến máy chủ mục tiêu mà họ đã xác thực.

Hậu quả có thể kể đến như sau:

- Thực hiện các Hành động Không Mong Muốn
- Đánh Cắp Thông Tin Nhạy Cảm
- Thực Hiện Hành động Thay Thế

- Phá Hoại Thương Hiệu và Uy Tín
- Tồn Thất Tài Chính
- Mở Rộng Tấn Công

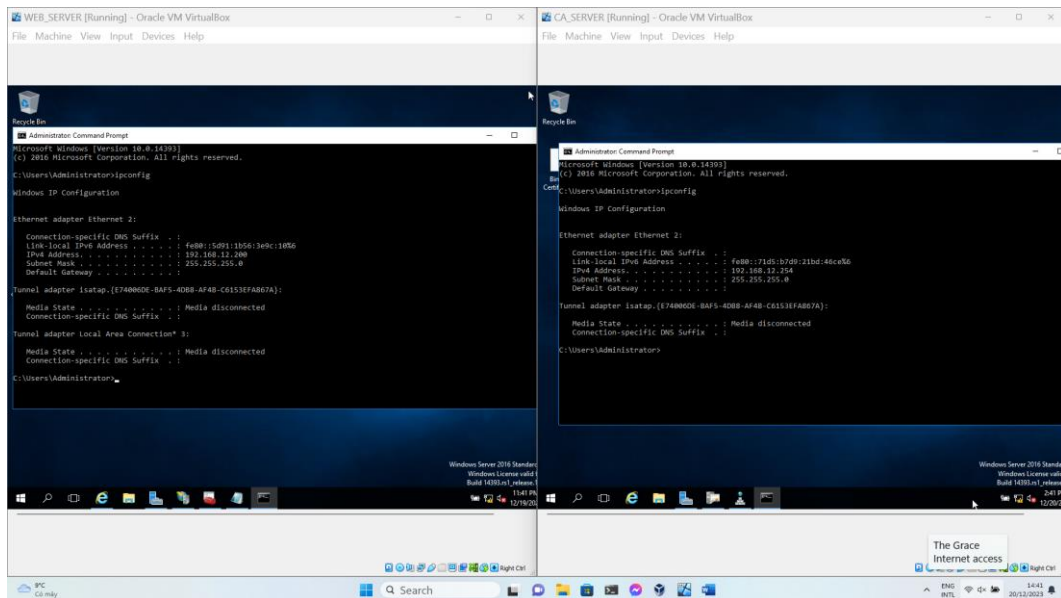
Các biện pháp bảo mật có thể được triển khai, bao gồm sử dụng token chống CSRF (CSRF token), kiểm tra nguồn gốc yêu cầu (Origin header), sử dụng SameSite cookies, và thực hiện kiểm soát chặt chẽ đối với các hành động cực kỳ quan trọng như thay đổi thông tin cá nhân hay thực hiện các giao dịch quan trọng.

4. Cấu hình Website để truy cập qua giao thức HTTPS

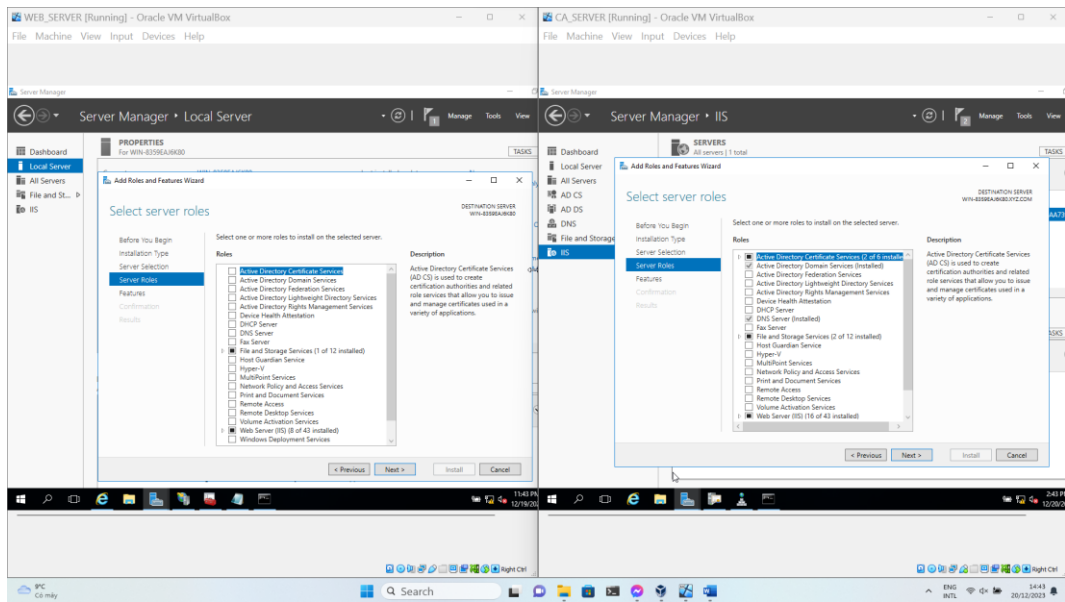
Mô hình Lab:

CA server	-----	Web Server
192.168.216.10		192.168.216.1

- **Quy trình thực hiện theo hướng dẫn của giáo viên bộ môn.**

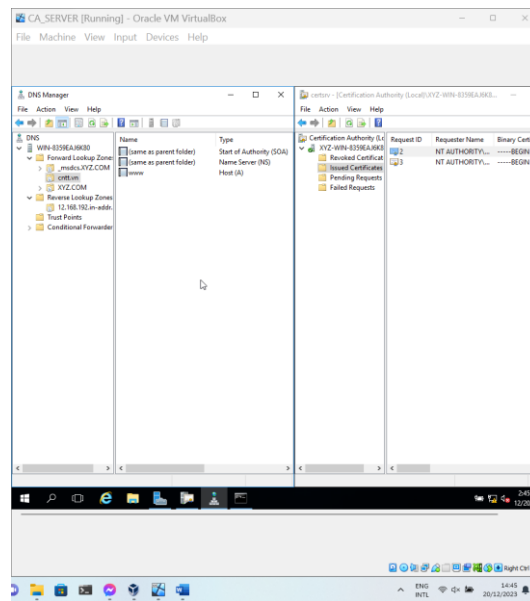


Hình 1: Địa chỉ ip tương ứng của các server.



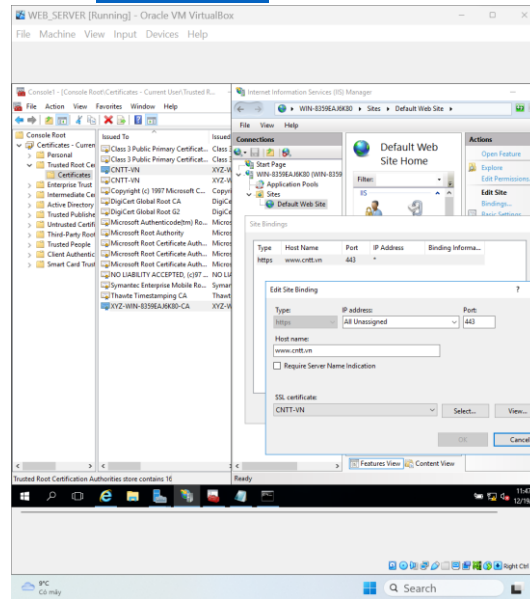
Hình 2: Các Dịch vụ được cài và đang chạy trên từng server.

Bước 1. Tạo CA_SERVER

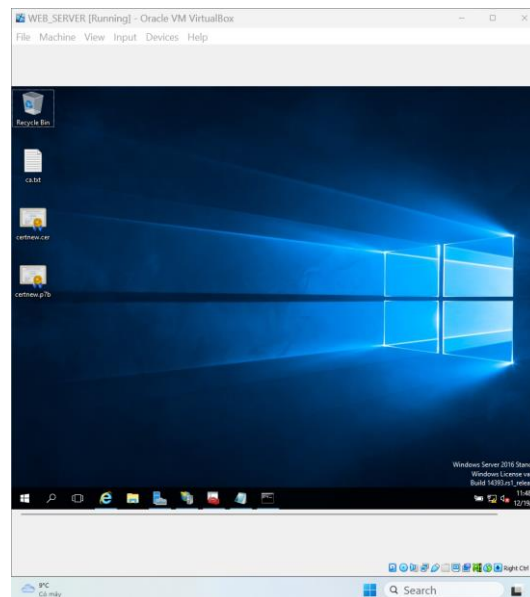


Hình 3: Thông tin thiết lập trên 2 dịch vụ của CA_SERVER

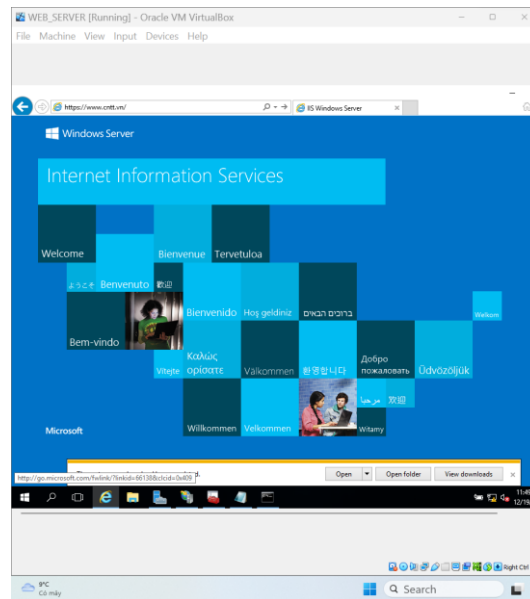
Bước 2. Máy WEB_SERVER: www.cntt.vn



Hình 4: Thông tin được thiết lập trên WEB_SERVER



Hình 5: Các file liên quan đến quá trình chứng thực SSL



Hình 6: Truy cập website với https

5. Tham khảo:

- [1] [SEED Project \(seedsecuritylabs.org\)](https://seedsecuritylabs.org)
- [2] [Cross Site Scripting \(XSS\) | OWASP Foundation](#)
- [3] [Cross Site Request Forgery \(CSRF\) | OWASP Foundation](#)