BÁO CÁO BÀI THỰC HÀNH SỐ 9

KIỂM THỬ LỖ HỔNG XSS và CSRF

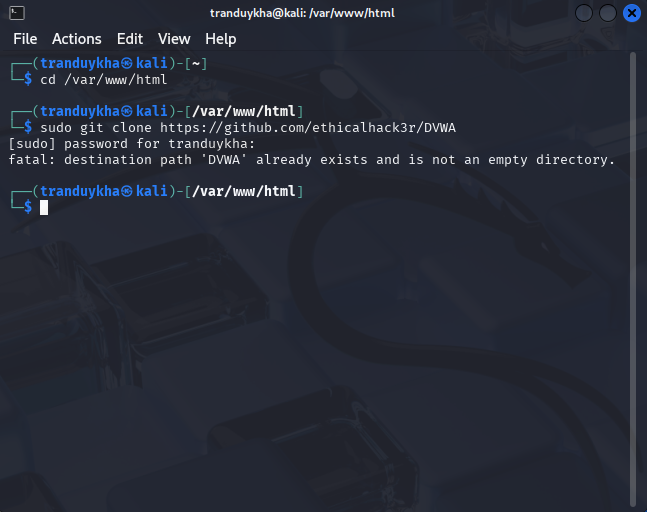
Họ và tên: Trần Duy Kha 1050080139

Link Youtube: <https://youtu.be/4RYov9SvrLI>

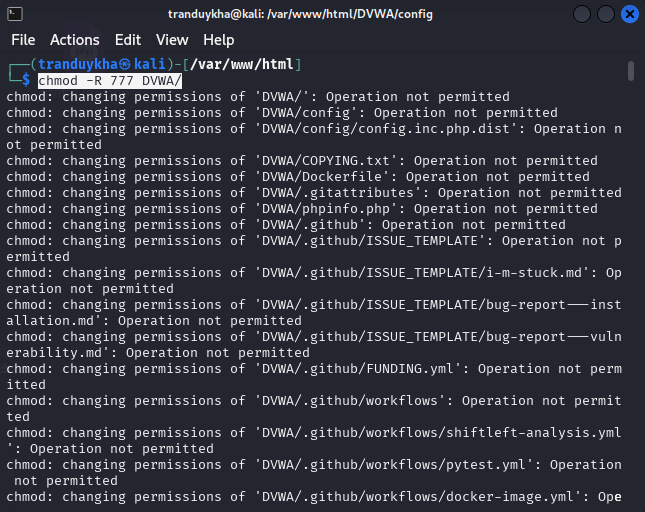
Cài đặt môi trường

cd /var/www/html

sudo git clone <https://github.com/ethicalhack3r/DVWA>

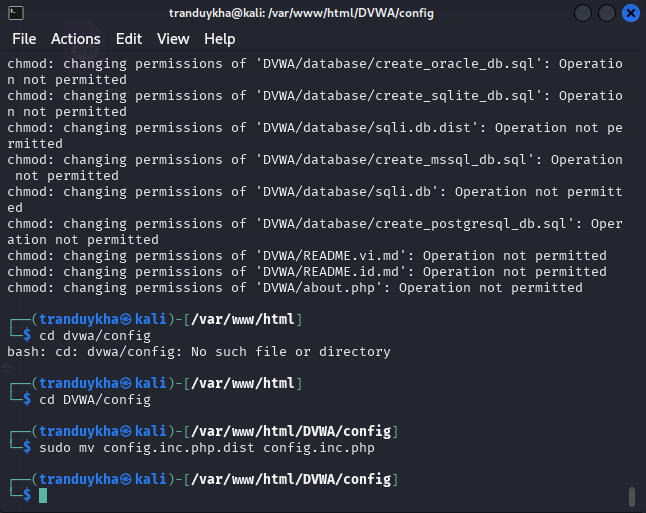


chmod -R 777 DVWA/

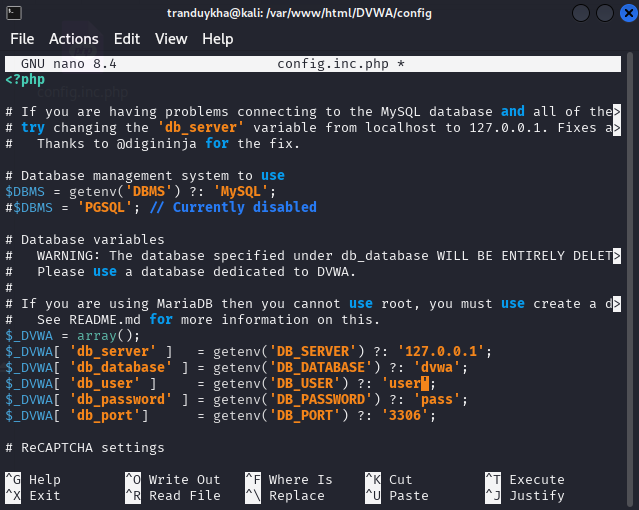


cd DVWA/config

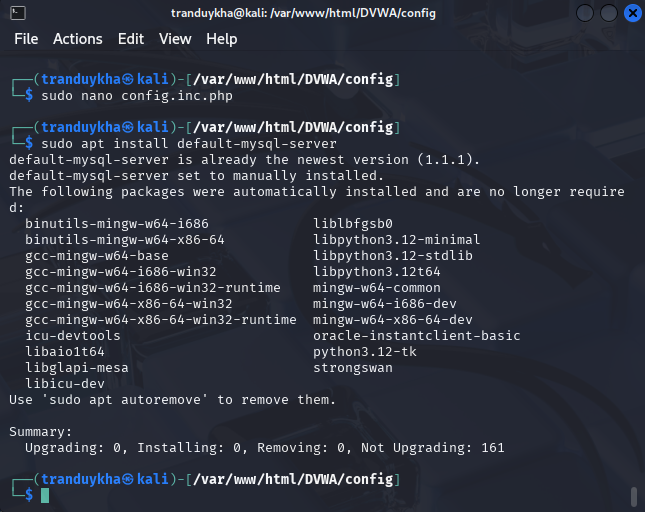
sudo mv config.inc.php.dist config.inc.php



sudo nano config.inc.php

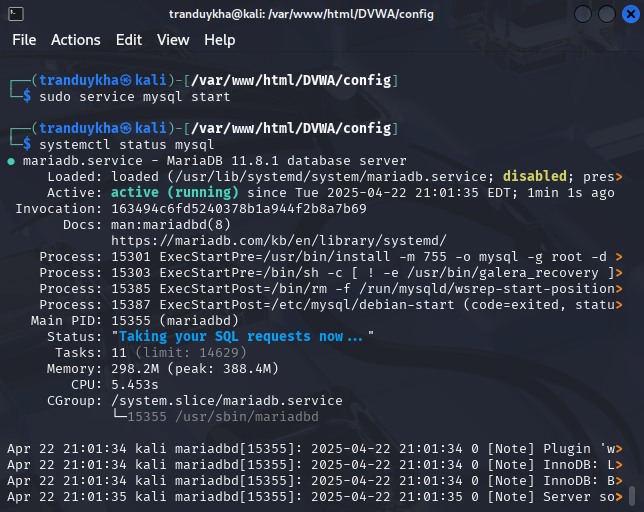


sudo apt install default-mysql-server

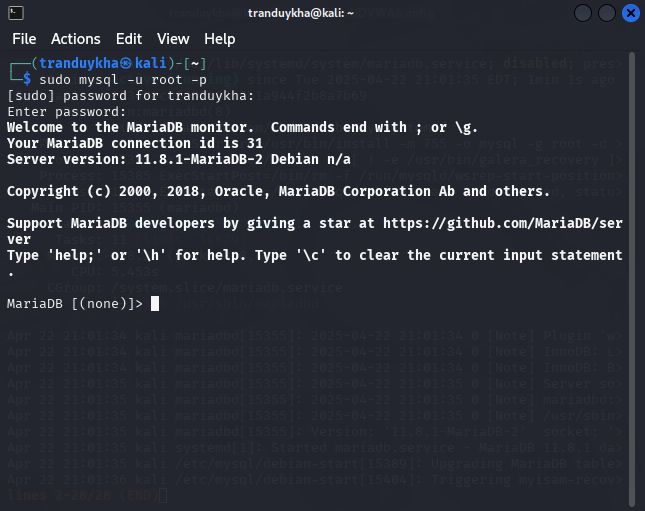


sudo service mysql start

systemctl status mysql



sudo mysql -u root -p

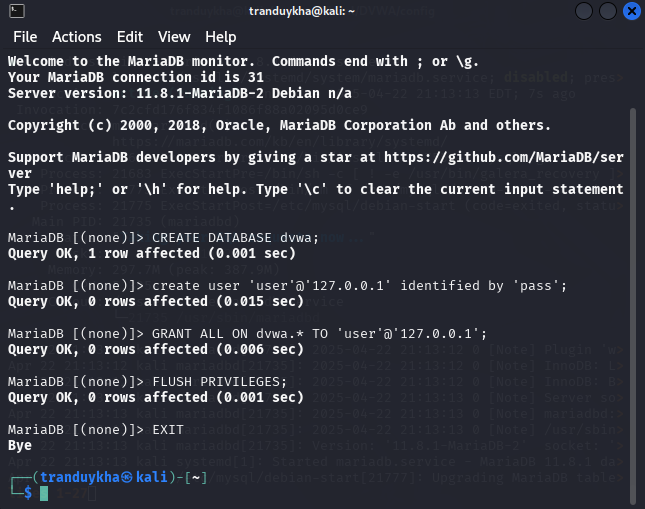


CREATE DATABASE dvwa;

create user 'user'@'127.0.0.1' identified by 'pass';

GRANT ALL ON dvwa.\* TO 'user'@'127.0.0.1';

FLUSH PRIVILEGES;  
EXIT

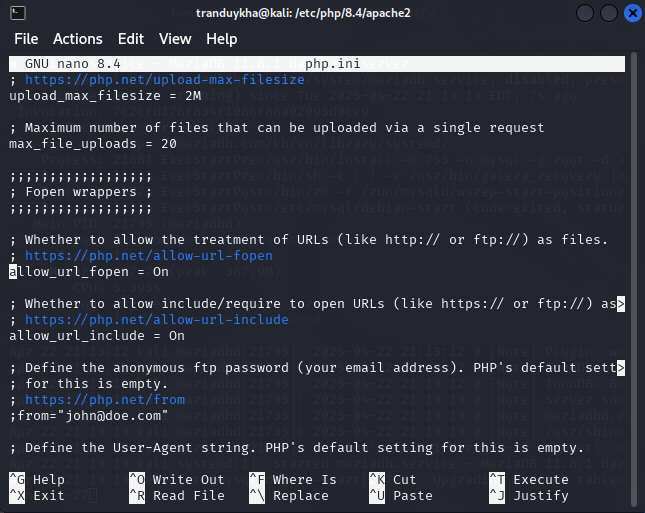


ls /etc/php



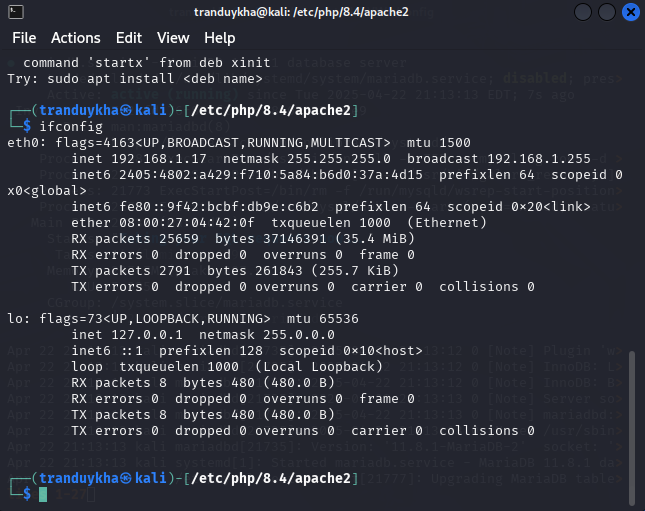
cd /etc/php/7.4/apache2

sudo nano php.ini

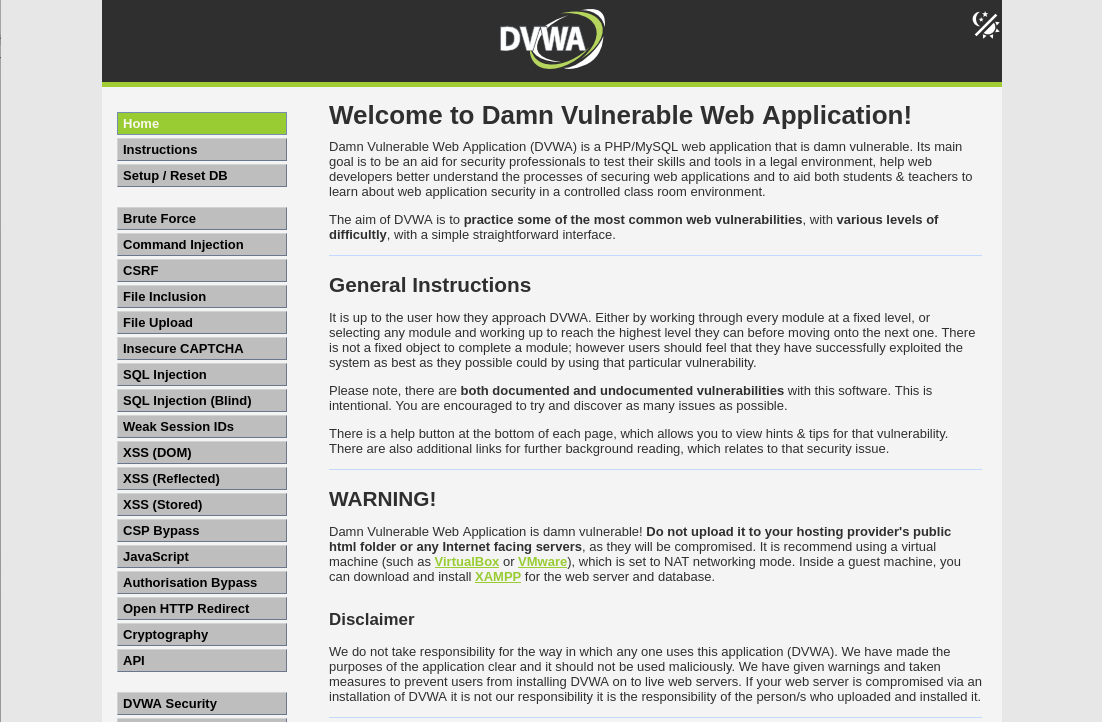


service apache2

ifconfig



<http://127.0.0.1/DVWA/>



Phần 1: Kiểm thử XSS

Thực hiện kiểm thử lỗ hổng XSS trên website: chọn 1 trong các trang sau để thử nghiệm

1. http://demo.testfire.net`

2. http://php.testsparker.com

3. http://testasp.vulnweb.com

4. http://testasp.vulnweb.com

5. http://testphp.vulnweb.com

6. http://www.webscantest.com

7. http://testhtml5.vulnweb.com

8. http://aspnet.testsparker.com

9. http://zero.webappsecurity.com

Câu 1

Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa 4 số cuối MSSV.

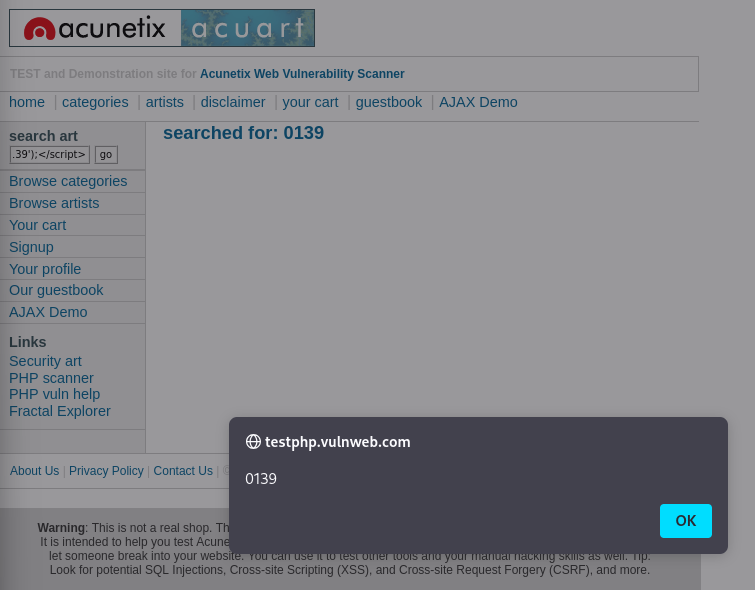
Hãy giải thích:

- Xác định các tham số đầu vào: 0.25 điểm

- Xác định giá trị đầu vào xuất hiện trong trang kết quả: 0.25 điểm

- Các bước kiểm thử và phán đoán: 0-1 điểm theo các bước kiểm thử và logic trong phán đoán

- Giá trị kiểm thử cho thấy lỗ hổng và giải thích: 0.5 điểm



Câu 2

Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa tên của sinh viên.

Điểm cho mỗi tham số đầu vào đã kiểm thử được:

- Xác định các tham số đầu vào: 0.25 điểm

- Xác định giá trị đầu vào xuất hiện trong trang kết quả: 0.25 điểm

- Các bước kiểm thử và phán đoán: 0-1 điểm theo các bước kiểm thử và logic trong phán đoán

- Giá trị kiểm thử cho thấy lỗ hổng và giải thích: 0.5 điểm

Câu 3

Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa 4 số cuối MSSV.

Hãy giải thích:

- Xác định các tham số đầu vào: 0.25 điểm

- Xác định giá trị đầu vào xuất hiện trong trang kết quả: 0.25 điểm

- Các bước kiểm thử và phán đoán: 0-1 điểm theo các bước kiểm thử và logic trong phán đoán

- Giá trị kiểm thử cho thấy lỗ hổng và giải thích: 0.5 điểm