BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Lab 6

GVHD: Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Văn Hào	20521293	20521293@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Yêu cầu 1: Thực hiện lấy flag.png

- Code util.py, để lấy flag phải vượt qua đoạn mã kiểm tra:

```
try:
    if is_inner_ipaddress(socket.gethostbyname(domain)):
        return flash('IP not allowed', 'danger')
    return serve_screenshot_from(url, domain)
except Exception as e:
    return flash('Invalid domain', 'danger')
```

- Giải thích: Xác minh xem tên miền có nằm trong phạm vi bị chặn hay không bằng cách phân giải tên miền thành địa chỉ IP và kiểm tra hàm **is_inner_ipaddress**.

```
def is_from_localhost(func):
    @functools.wraps(func)
    def check_ip(*args, **kwargs):
        if request.remote_addr != '127.0.0.1':
            return abort(403)
        return func(*args, **kwargs)
    return check_ip
```

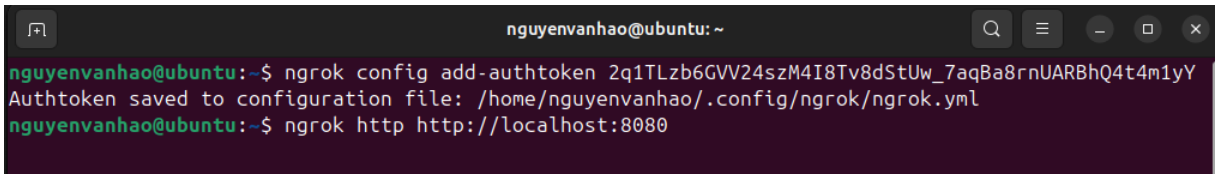
- Giải thích: Hàm **is_from _localhost** là một decorator dùng để kiểm tra xem request có đến từ localhost (127.0.0.1) hay không.

- Ta tải apache và ngrok:

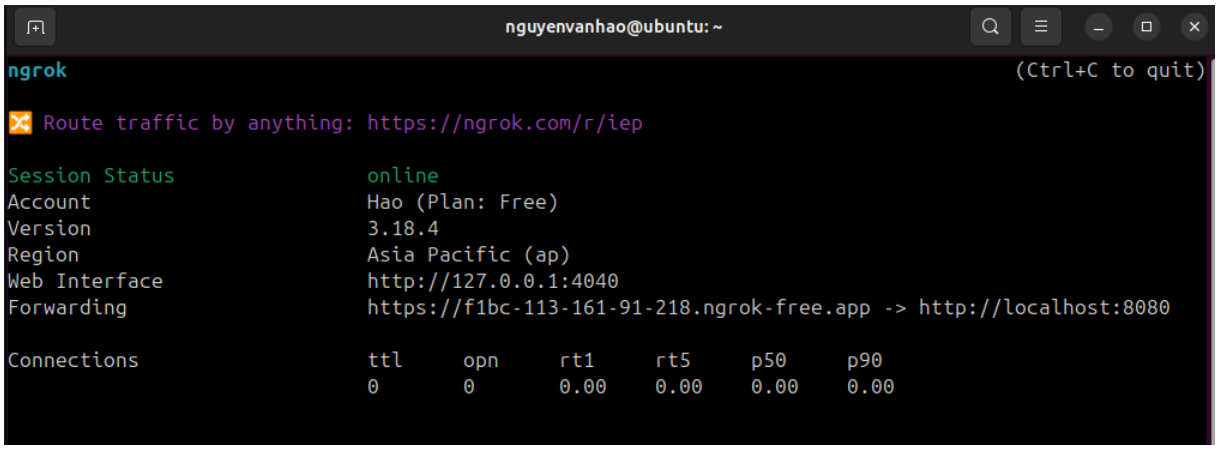
```
nguyenvanhao@ubuntu:~$ apache2 -v
Server version: Apache/2.4.58 (Ubuntu)
Server built:   2024-10-02T12:40:51
nguyenvanhao@ubuntu:~$ ngrok -v
ngrok version 3.18.4
nguyenvanhao@ubuntu:~$
```

- Tạo một file PHP sử dụng header redirec để chuyển hướng apache_web đến **http://127.0.0.1:1337/flag**

- Cấu hình Ngrok bằng Auth Token (mã Auth Token lấy trong lúc tạo tài khoản) và khởi chạy Ngrok trên cổng 8080:



- Ngrok tạo một URL công khai từ internet đến server Apache chạy trên máy cục bộ.



- URL Ngrok công khai: **https://f1bc -113-161-91-218.ngrok-free.app**

- Ta nhập vào URL: **https://f1bc -113-161-91-218.ngrok-free.app/bhin.php** , ta có kết quả như hình: