BÁO CÁO BÀI TẬP

**Môn học: Bảo mật web và ứng dụng**

**Tên chủ đề: Thi thực hành kỹ năng giữa kỳ theo hình thức jeopardy (CTF)**

*GVHD: Nguyễn Công Danh*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT213.O21.ANTT

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Phạm Ngọc Thiện | 21522627 | [21522627@gm.uit.edu.vn](mailto:21522627@gm.uit.edu.vn) |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-2)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Botcheck as a service | 100% |
| 2 | Router emulator | 100% |
| 3 | Smart contract | 100% |

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

BÁO CÁO CHI TIẾT

1. **Botcheck as a service**

- Ta thấy rằng muốn đọc được flag thì user account phải có trường premium là 1:

**A screen shot of a computer program

Description automatically generated**

- Ngoài ra còn có botcheck có thể truy cập các url bằng curl\_exec():

A screen shot of a computer code

Description automatically generated

- User chỉ có thể truyền vào các url có scheme http hoặc https:

**A screen shot of a computer program

Description automatically generated**

- Có 1 cách để user có thể upgrade trường premium của account lên 1 bằng cách gửi một POST request đến /manager/index.php với username = “user\_account” kèm với giá trị upgrade (1/true….)

**A screen shot of a computer program

Description automatically generated**

→ Tuy nhiên, user thông thường không thể trực tiếp gửi yêu cầu từ xa. Do đó, chúng ta lợi dụng bot trong cùng hệ thống để thực hiện ssrf nhằm upgrade user account mong muốn.

#### **\* Khai thác:**

**A diagram of a system

Description automatically generated**

- Host một form autosubmit với username = “testabc” và upgrade = “true” gửi đến /manager bằng phương thức POST:

****

- Truy cập vào router, sau đó tùy chỉnh port forwarding.

Tại ô Start Port/End Port điền số port(80/443 …) mà đã thiết lập trên IIS trước đó.

Ở ô LAN Host IP Address, điền địa chỉ IP hiện tại của máy host trang web.

Xem địa chỉ IP của router (có thể vào trang <https://whatismyipaddress.com/> hoặc một số trang khác để thấy được địa chỉ IPv4 hiện tại của router).

Có thể truy cập vào trang web bằng địa chỉ của router.

- Đây là thông tin IP router của nhóm lúc làm:

A screenshot of a computer

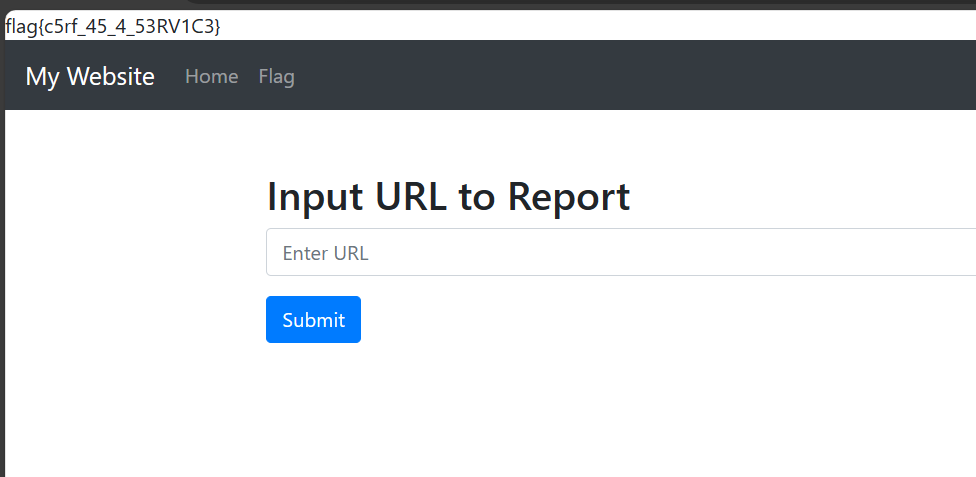
Description automatically generated

- Điền url và tiến hành submit:

A screenshot of a computer

Description automatically generated

- Lợi dụng bot để thực hiện csrf nhằm autosubmit form để năng quyền premium của user lên.



→ Kết quả thành công nâng lên premium và xem được flag.

**flag{c5rf\_45\_4\_53RV1C3}**

1. **Router emulator**

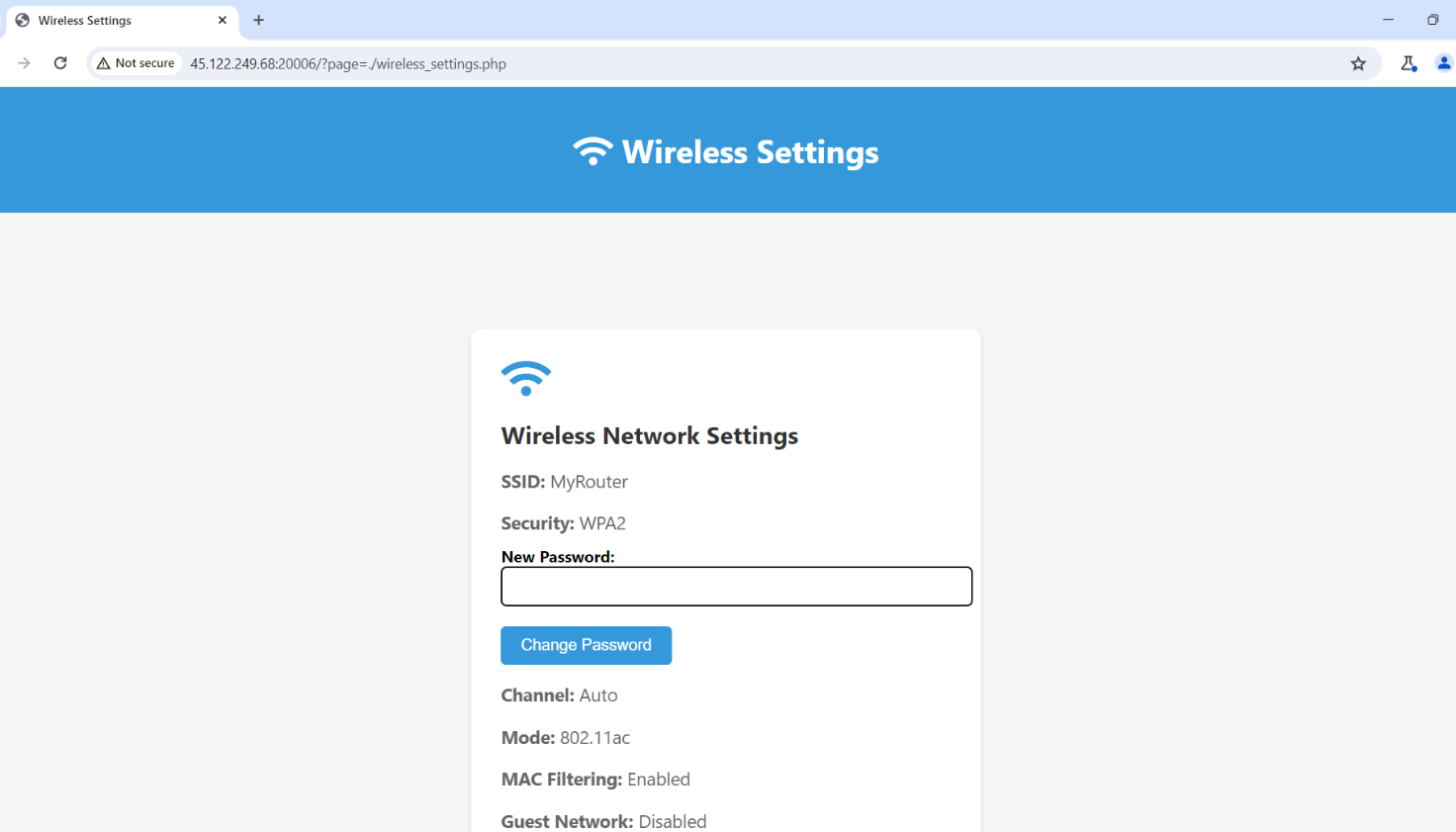
- Đoạn code bên dưới cố gắng ngăn cản người dung truy cập vào trang config của firewall và wireless\_settings từ bên ngoài mạng nội bộ.

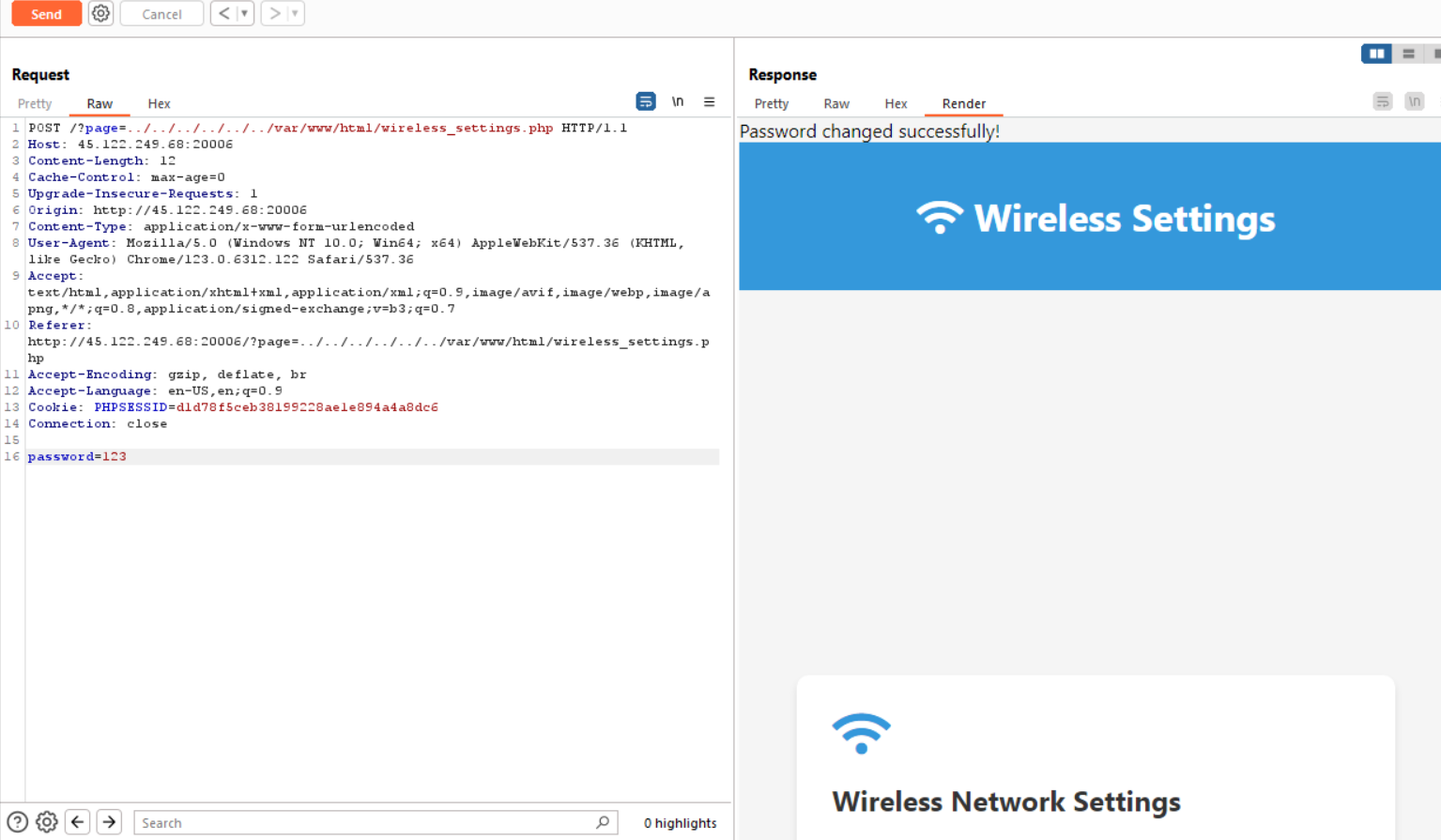
**A computer code on a black background

Description automatically generated**

→ Tuy nhiên attacker vẫn có thể bypass bằng path traversal.

Attacker chỉ cần thêm đường dẫn vào phía trước tên file firewall.php hoặc wireless\_settings.php là có thể bypass và truy cập vào 2 trang trên.





- Trang wireless\_settings.php có chức năng change password và ghi encrypted password mới vào file ./passwd

**A computer screen with text and images

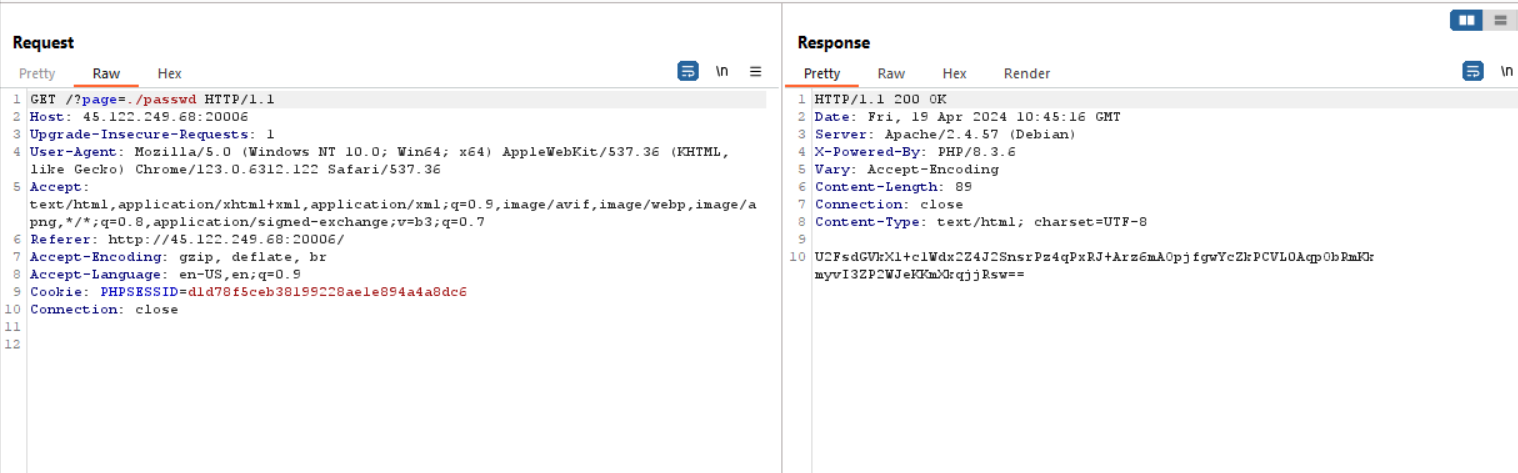
Description automatically generated**

- Hàm encrypt\_password() sử dụng shell\_exec() và không sanitize input -> có thể thực hiện command injection

**A screenshot of a computer program

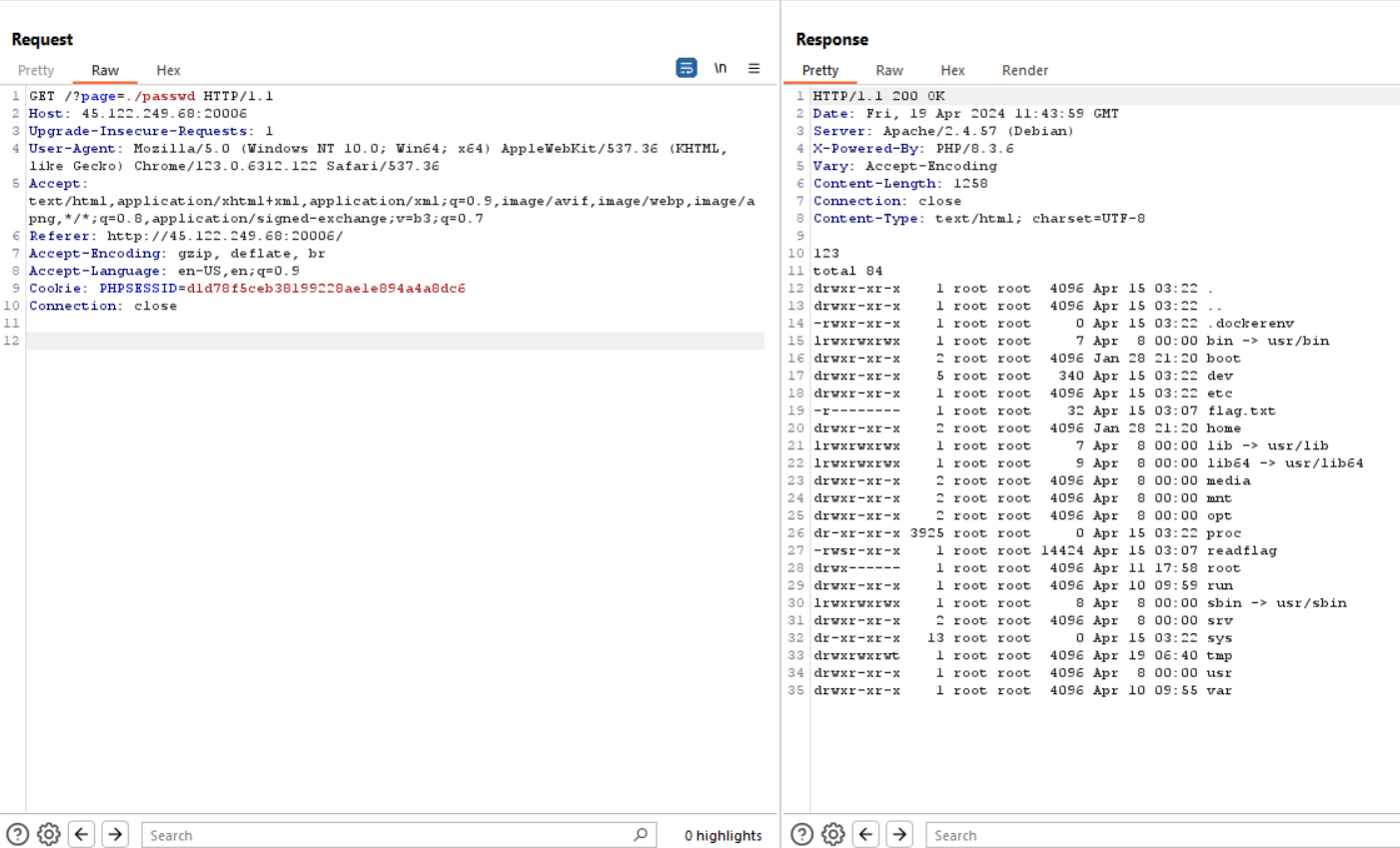
Description automatically generated**

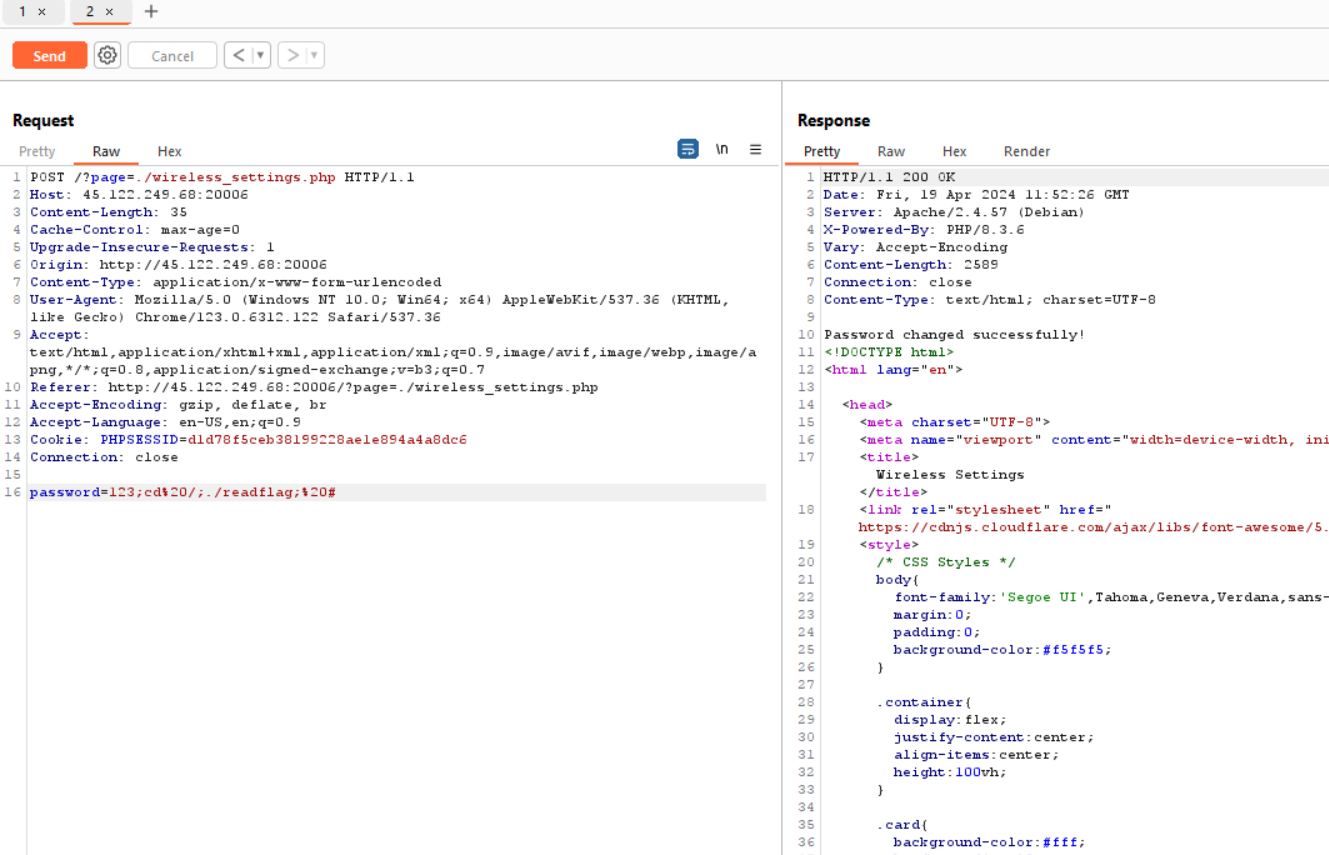
- Ngoài ra, ta còn có thể truy cập và đọc nội dung file ./passwd

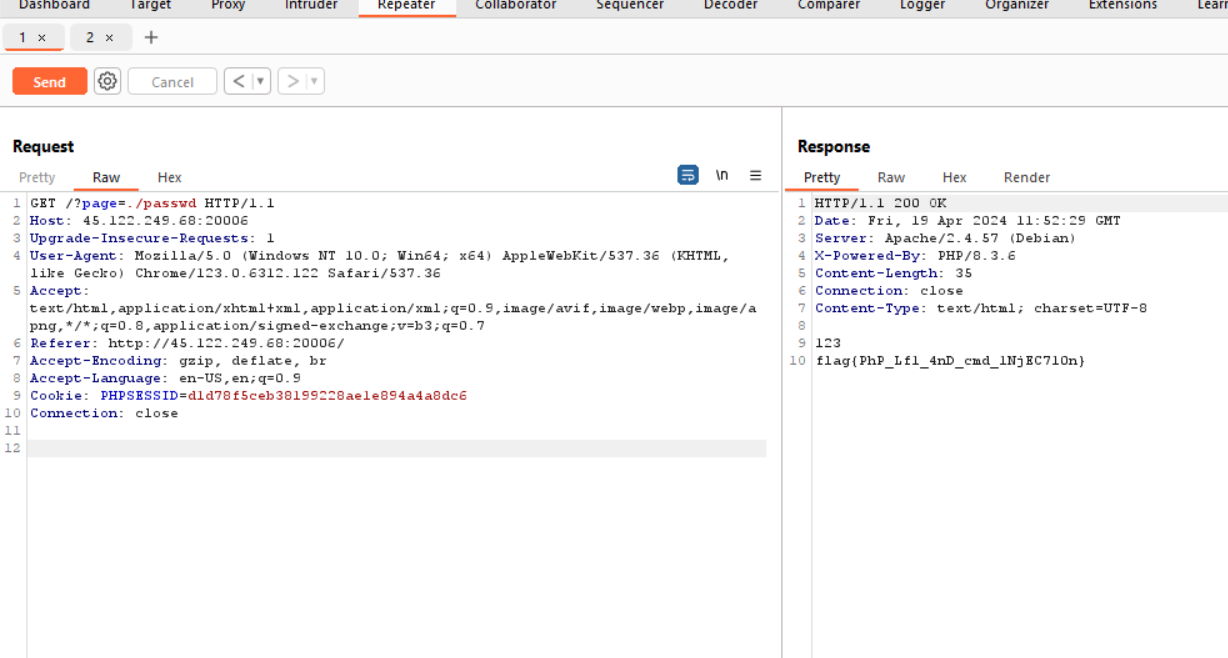


#### **\* Khai thác:**

- Command injection và đọc kết quả trả về từ file ./passwd





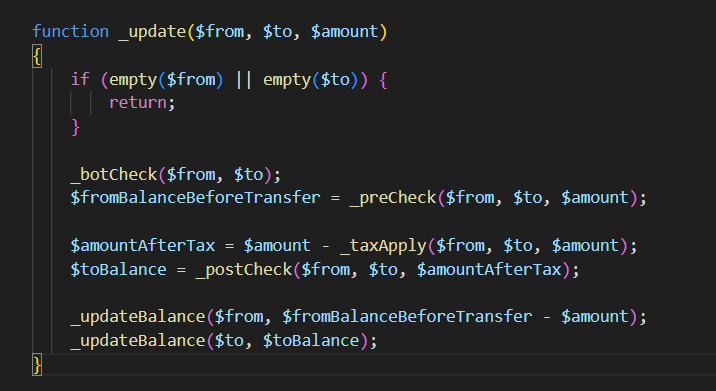


→ Thành công thu được flag:

**flag{PhP\_Lf1\_4nD\_cmd\_1NjEC710n}**

1. **Smart contract**

- Lỗi logic code xử lý ở hàm \_update khi không có trường hợp riêng biệt khi user tự chuyển tiền cho chính mình:



- Khi user tự chuyển tiền cho chính mình thì hàm \_update() gọi \_updateBalance() 2 lần nhằm cập nhật số dư của người gửi và sau đó là người nhận.

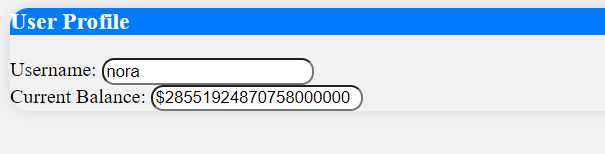
→ Do không có trường hợp xử lý riêng biệt khi người nhận và người gửi cùng là 1 người, do đó khi tự gửi tiền cho chính mình → số tiền sẽ được tăng lên.

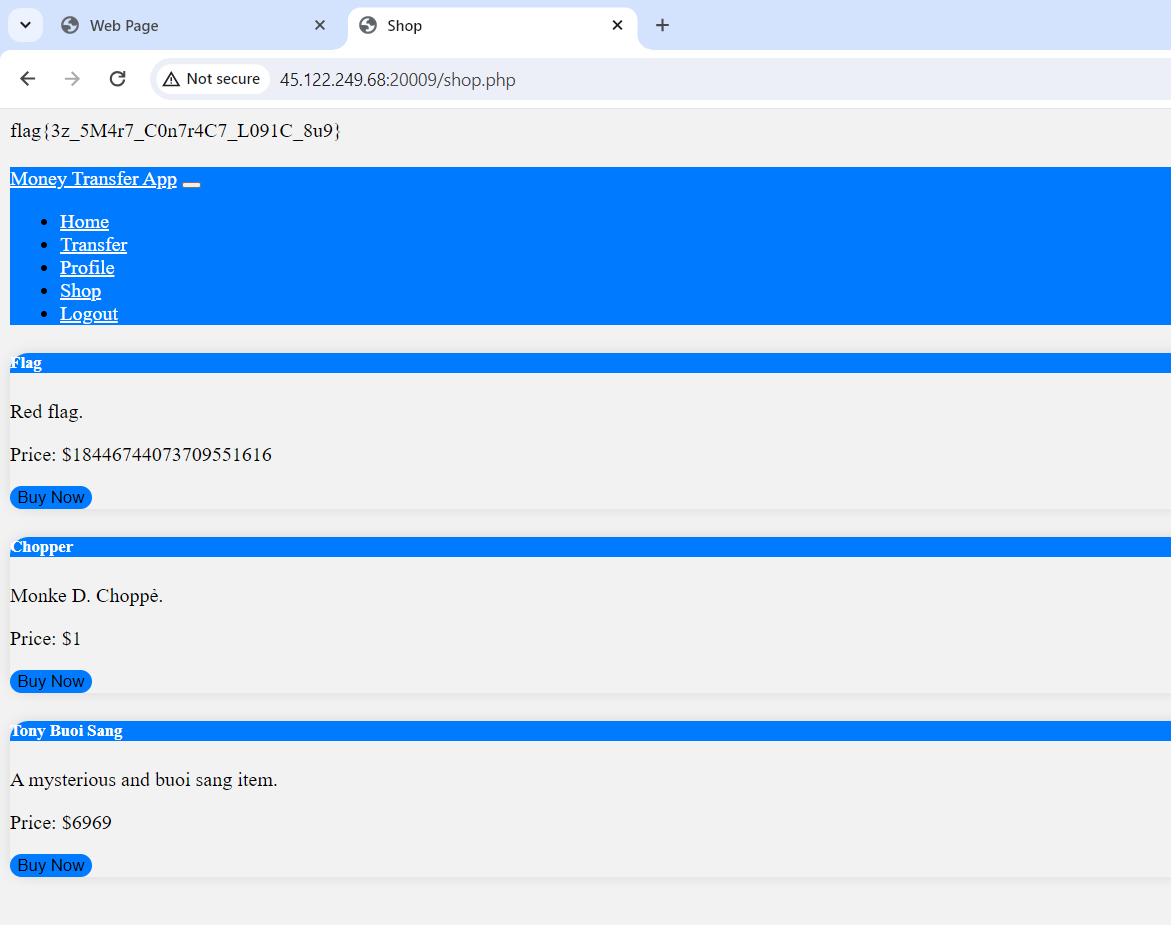
#### **\* Khai thác:**

- Tạo 1 request bằng python và dung vòng lặp để thực hiện việc tự chuyển tiền vào tài khoản:

A screenshot of a computer program

Description automatically generated





→ Thành công thu được flag:

**flag{3z\_5M4r7\_C0n7r4C7\_L091C\_8u9}**

--- **HẾT** ---

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-2)