BÁO CÁO THỰC HÀNH

**Môn học: Bảo mật web và ứng dụng**

**Tên chủ đề: Lab 06 Challenge CTF**

*GVHD: Ngô Đức Hoàng Sơn*

**Nhóm: 09**

1. **THÔNG TIN CHUNG:**

Lớp: NT213.P12.ANTT.1

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Hồ Vỉ Khánh | 22520633 | 22520633@gm.uit.edu.vn |
| 2 | Trần Tiễn Nhật | 22521030 | 22521030@gm.uit.edu.vn |
| 3 | Trần Hoàng Tuấn Kiệt | 22520724 | 22520724@gm.uit.edu.vn |

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

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung | Tình trạng | Trang |
| 1 | Empty | 100% | 2 - 3 |
| 2 | 2FA | 100% | 3 - 7 |
| 3 | Mark Editor | 100% | 8 - 13 |
| Điểm tự đánh giá | | | **10/10** |

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

BÁO CÁO CHI TIẾT

# Empty

**Empty** : <http://a1d5d5bd6fa04226b42eb446992ec172-3ba9019e-server-10001.vlab.uit.edu.vn>.

Giao diện ban đầu của challenge:

A black screen with a black background

Description automatically generated with medium confidence

Gợi ý là có thể truy cập vào một số file public ở đường dẫn /assets/??????????/

Ta tìm được một đường dẫn OpenAPI schema mô tả cấu trúc của các endpoint:

A screenshot of a computer

Description automatically generated

Có một đường dẫn được định nghĩa /assets/{file\_path}: Đây là một đường dẫn động, trong đó {file\_path} là một tham số mà có thể thay thế bằng bất kỳ giá trị nào mình muốn. API sẽ hiểu rằng file\_path là một phần của URL, và có thể truyền vào bất kỳ giá trị nào thay cho {file\_path} trong yêu cầu HTTP.

Tìm kiếm các file thông qua đường dẫn /assets/...

Sau một hồi tìm kiếm đường dẫn đọc được app.py với đường dẫn /assets/..app.py:

A screenshot of a computer

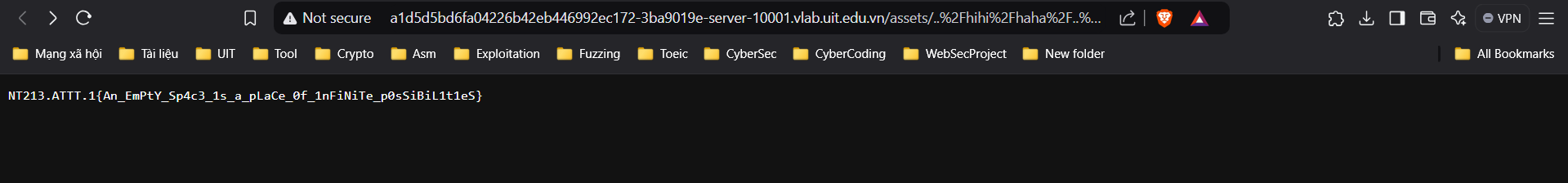
Description automatically generated

Thử với flag.txt:

A screenshot of a computer

Description automatically generated

Ta thấy được đường dẫn của real flag. Truy cập đường dẫn /assets/../hihi/haha/../../hihi/huhu/../huhu/hihi/hihi.txt ta có được flag:



* Flag: **NT213.ATTT.1{An\_EmPtY\_Sp4c3\_1s\_a\_pLaCe\_0f\_1nFiNiTe\_p0sSiBiL1t1eS}**

# 2FA

**2FA** : <http://a1036c268d464f208db857806d482624-9465c6bd-server-10002.vlab.uit.edu.vn>.

Trang giao diện ban đầu của challenge:

A screenshot of a computer

Description automatically generated

Tiến hành tạo 1 tài khoản mới:

A screenshot of a computer

Description automatically generated

Sau khi tạo xong tài khoản, web chuyển hướng đến bước xác thực Email:

A screenshot of a computer

Description automatically generated

Khi bấm nút Resend code, bắt gói tin Response thấy được một mã code ẩn là **AIJBEWG3:**

A screenshot of a computer

Description automatically generated

Ta thử nhập đoạn code trên vào trang Verify, một mã QR được hiện ra:

A screenshot of a qr code

Description automatically generated

Quét mã QR bằng app Google Authenticator:

A screenshot of a social media account

Description automatically generated

Nhập mã 6 chữ số vừa tìm được, ta đã đăng nhập thành công:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Sau một hồi tìm kiếm, ta thấy trong danh sách cookies ta thấy có trường **vuot muc pickleball** với giá trị false. Thử sửa lại thành **true**. Ta có được flag.

A screenshot of a computer

Description automatically generated

Kết quả:

A screenshot of a computer

Description automatically generated

* Flag: **NT213.ATTT.1{d4p\_BaNh\_DaP\_b4nH\_d3n\_3m\_M4nH\_v4o}**

# Mark Editor

**Mark Editor**: <http://a1036c268d464f208db857806d482624-9465c6bd-server-10003.vlab.uit.edu.vn>.

Trang giao diện ban đầu của challenge:

A screenshot of a computer

Description automatically generated

Dùng burpsuite để bắt các request

A screenshot of a computer

Description automatically generated

Tìm thử với các URL như \_root.txt nhưng không thấy gì trong response

A screenshot of a computer

Description automatically generated

Tìm kiếm thấy một vài nguồn đề cập đến lỗ hỏng liên quan Markdown

A screenshot of a computer

Description automatically generated

<https://github.com/simonhaenisch/md-to-pdf/issues/99>

A screenshot of a computer

Description automatically generated

<https://github.com/gatsbyjs/gatsby/security/advisories/GHSA-7ch4-rr99-cqcw>

Thử một đoạn code javascript để tiêm CSS vào ô input ta thấy hiển thị cảnh báo cho thấy

rằng WAF (tường lửa) đã chặn một số từ khóa hoặc chuỗi nhất định  
A screenshot of a computer

Description automatically generated

Từ khóa “js” có thể nằm trong danh sách cấm vì nó được liên kết với mã độc hoặc payload phổ biến. Nên có thể nằm trong danh sách cấm của WAF. Thay vì dùng “js” ta thay bằng “javascript” có thể bypass được WAF

A screenshot of a computer

Description automatically generated

Viết một payload javascript khác để liệt kê các file hoặc thư mục hiện tại

A screenshot of a computer

Description automatically generated

Dễ dàng thấy các file có thể chứa flag như **flag.txt** và **flag.zip**

Viết payload đọc file **flag.txt** nhưng không phải, có thể nằm trong file .zip  
A screenshot of a computer

Description automatically generated

Giải nén file zip yêu cầu phải có mật khẩu.

Tìm đường dẫn của trang web ta thấy với URL /robots.txt có chứa một đoạn mã gì đó

A screenshot of a computer

Description automatically generated

Truy cập đường dẫn tới /robots.txt thấy 1 dòng gì đó được mã hóaA screen shot of a video

Description automatically generated

Copy đoạn mã trên crackstation.net thấy được mã được hash loại sha512 và kết quả của đoạn mã hash trên là **hackmepls**

A screenshot of a computer

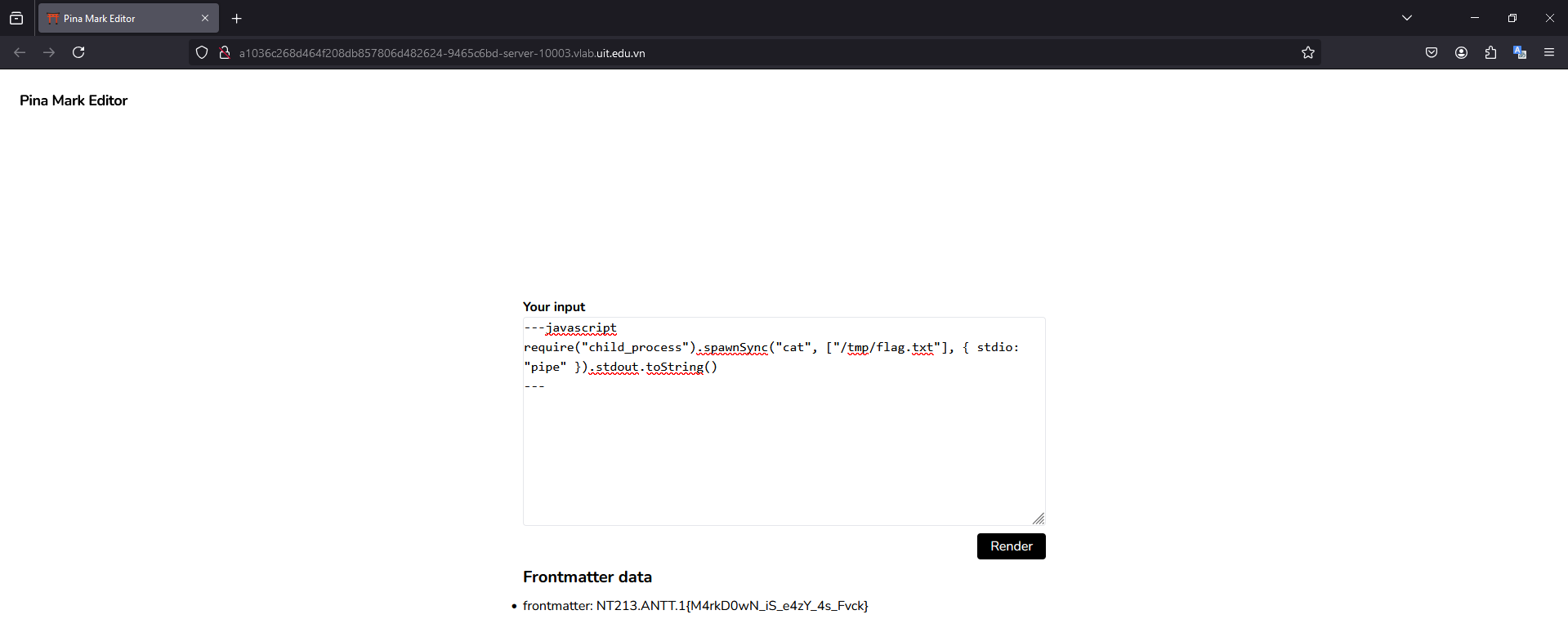
Description automatically generated

Thực hiện giải nén file **flag.zip** với mật khẩu hash đã được tìm thấy trong file *robots.txt* và lưu trong /**tmp**

A screenshot of a computer

Description automatically generated

Tiếp tục cat /tmp/flag.txt để xem được flag



* Flag: **NT213.ANTT.1{M4rkD0wN\_iS\_e4zY\_4s\_Fvck}**

-- HẾT --

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