BÀI TẬP CTF

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

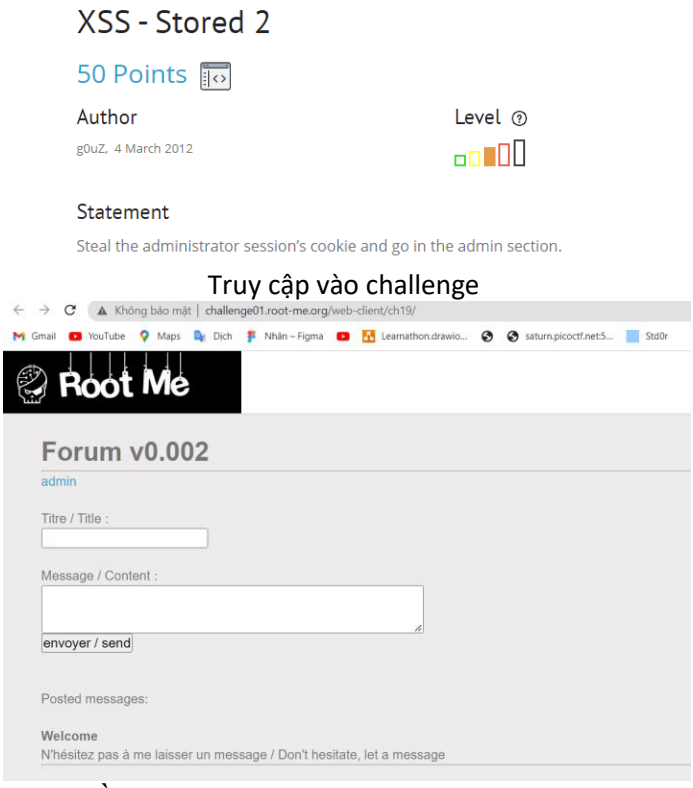
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

Challenge 6: XSS - Stored 2 (level medium)

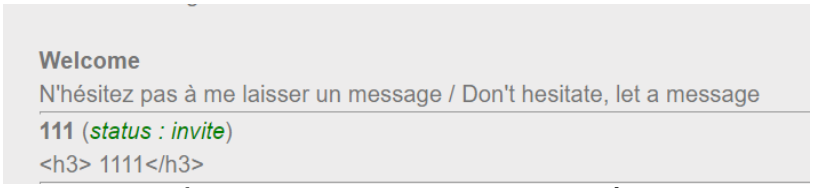
Link challenge: https://www.root-me.org/en/Challenges/Web-Client/XSS-Stored-2

- ✓ Challenge yêu cầu ta lấy session cookie của admin và truy cập vào section admin

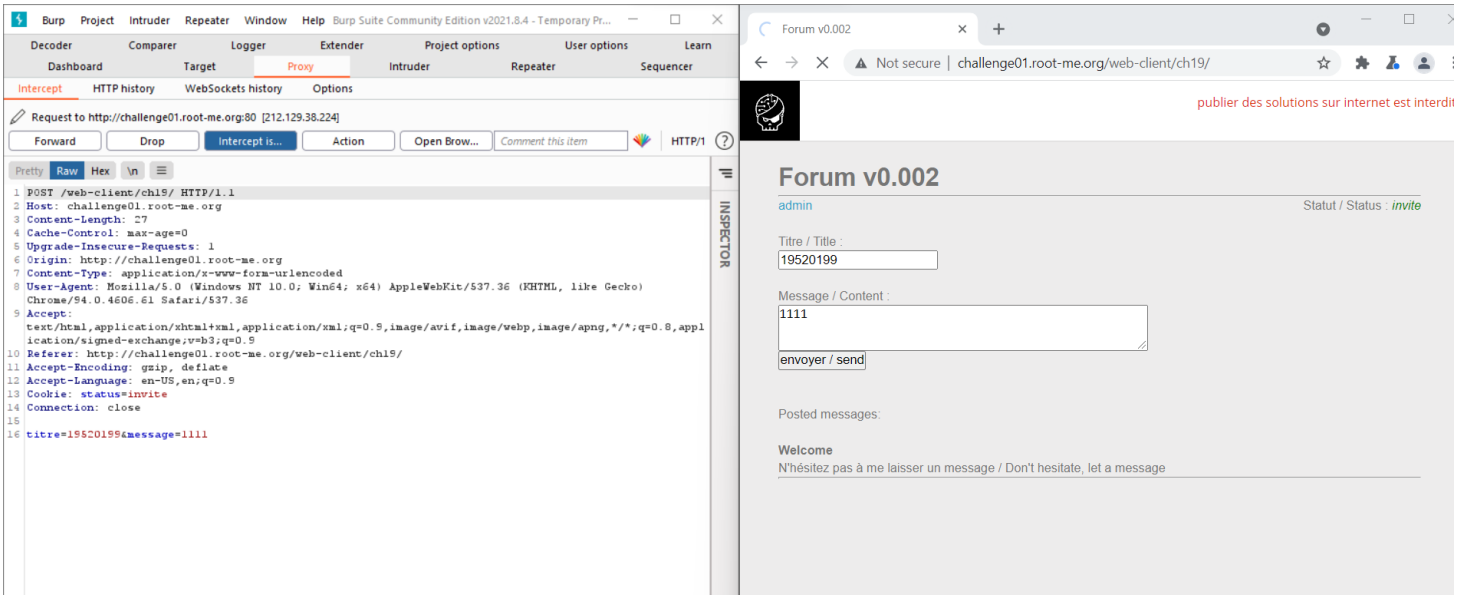


Truy cập vào challenge

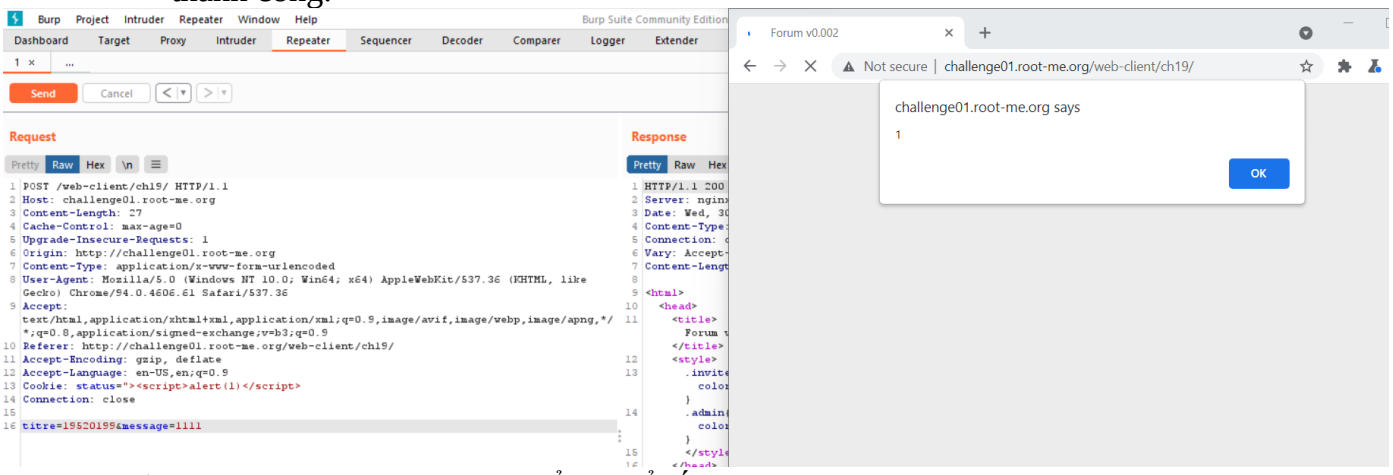
- ✓ Chương trình có 2 đầu vào là tille và message
- ✓ Thử nhập vào, ta thấy sau khi nhấn send, trang web sẽ hiển thị cho ta ba nội dung là tiêu đề đã nhập, tin nhắn đã nhập và trạng thái ở bên phải tiêu đề



✓ Sử dụng Burp Suite để chặn gói tin request lên thì thấy có 1 vị trí status có thể chỉnh sửa được, cho thấy đây là điểm chèn XSS

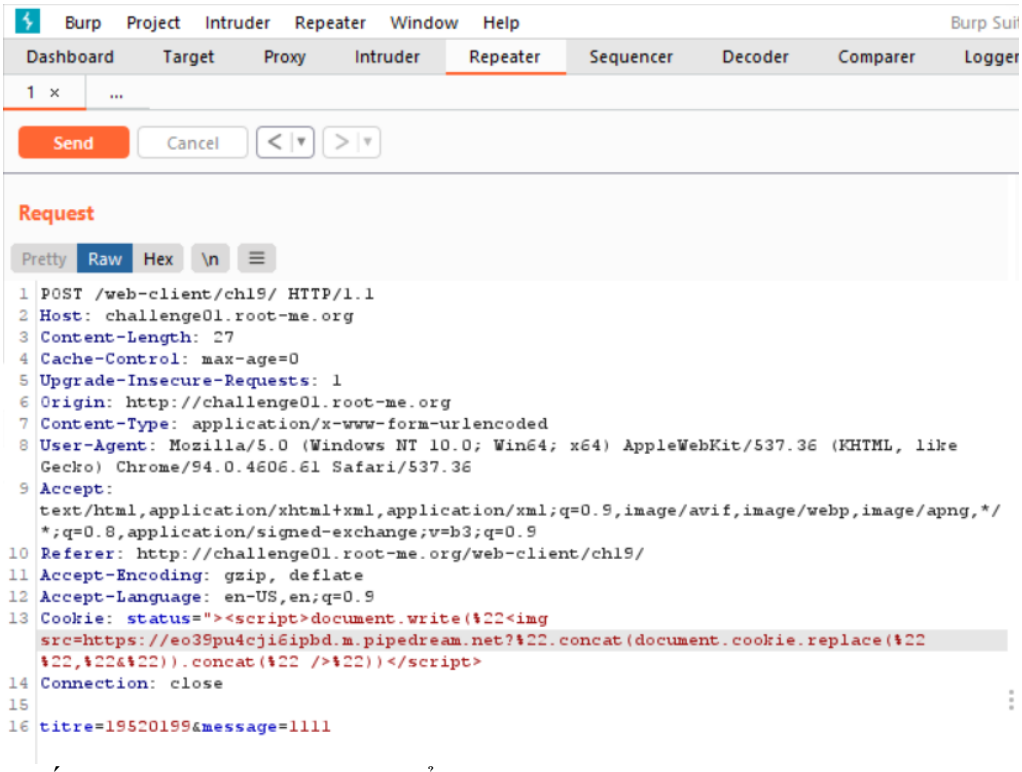


✓ Thử tạo payload: **"> <script> alert (1) </script>** (đóng thẻ <i> và đưa vào <script>). Ta thấy một hộp thoại cảnh báo bật lên trên trang và quá trình tiêm đã thành công.

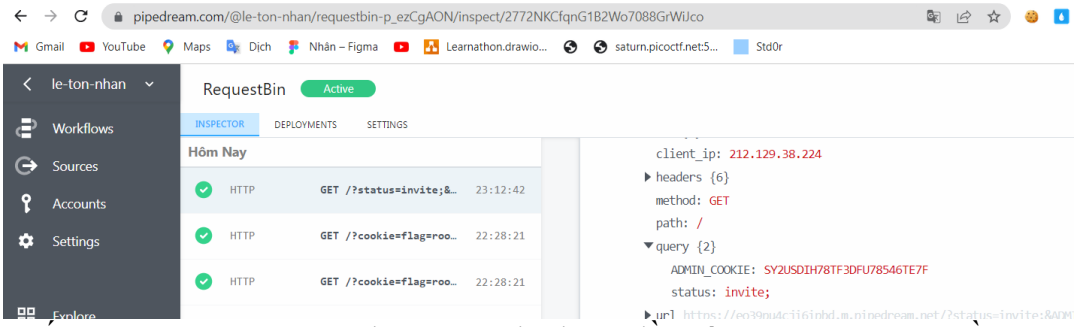


✓ Ta sẽ chèn đoạn code sau để có thể lấy cookie session của admin.

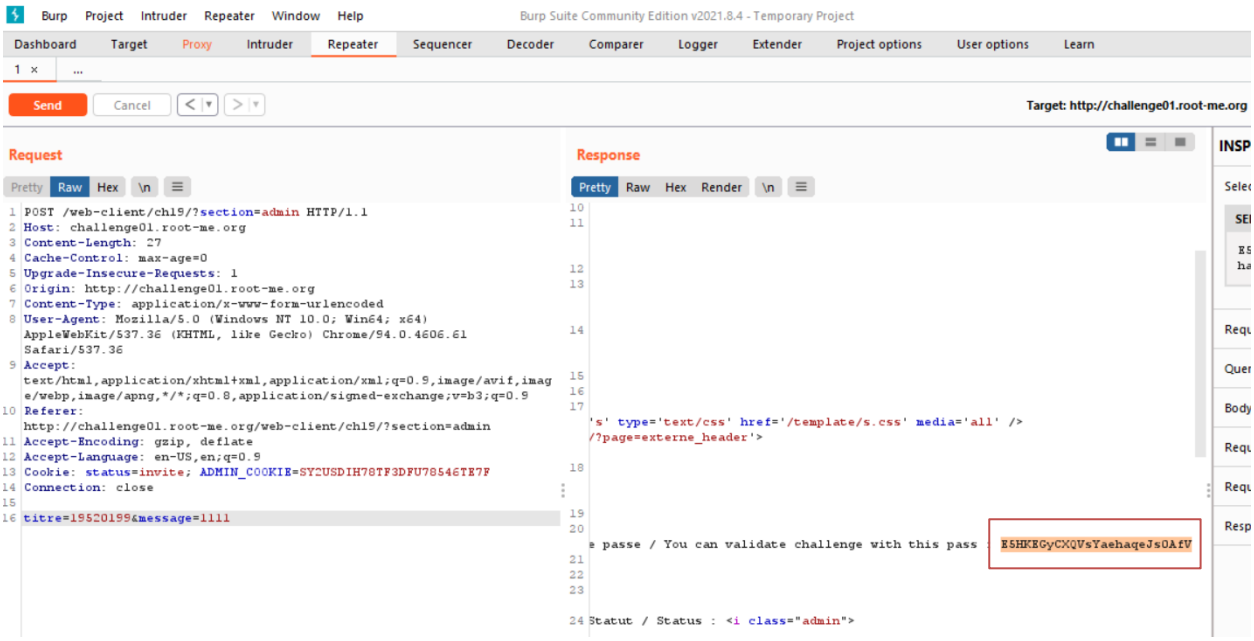
"><script>document.write(%22%22))</script>



✓ Ta tiếp tục sử dụng burp suite để chặn gói tin trên và thay đoạn code ở trên vào vào để nhận request chứa cookie của chương trình. Cookie nhận được là: ADMIN_COOKIE: SY2USDIH78TF3DFU78546TE7F



✓ Tiếp tục chặn request từ chương trình nhưng lần này ta thay cookie bằng admin mà chúng ta lấy được. Với referer là http://challenge01.root-me.org/web-client/ch19/?section=admin.



- ✓ Gửi gói tin và ta thu được Flag

FLAG: E5HKEGyCXQVsYaehaqeJs0AfV