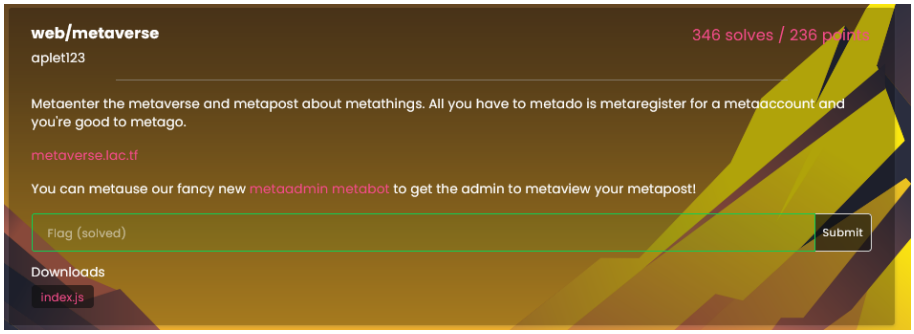
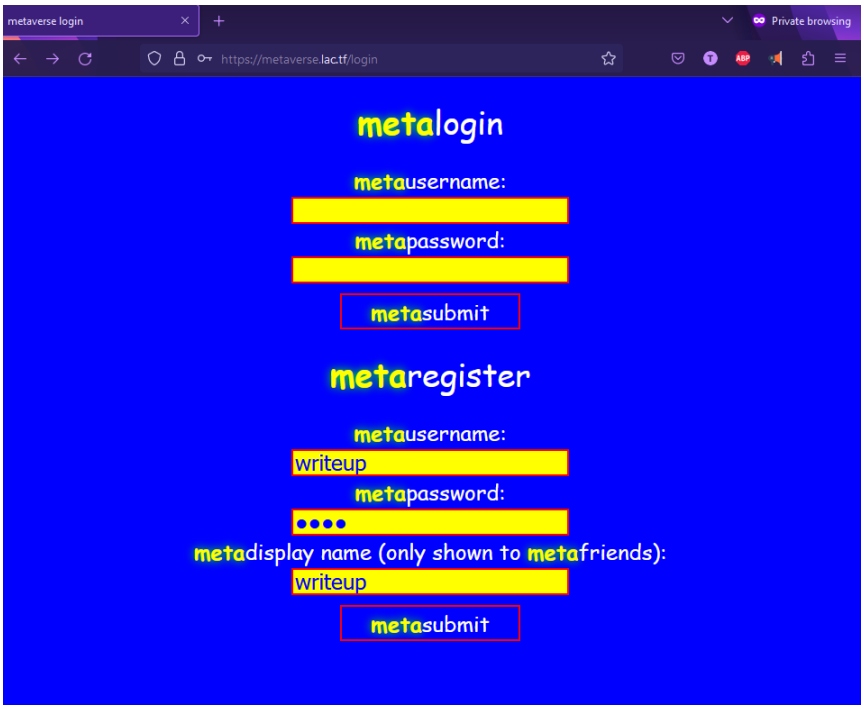
This web challenge comes from LACTF 2023.

We get a website and an admin bot that can “metaview our metapost”. These admin bot challenges are usually some sort of XSS challenge, but let’s check it out.

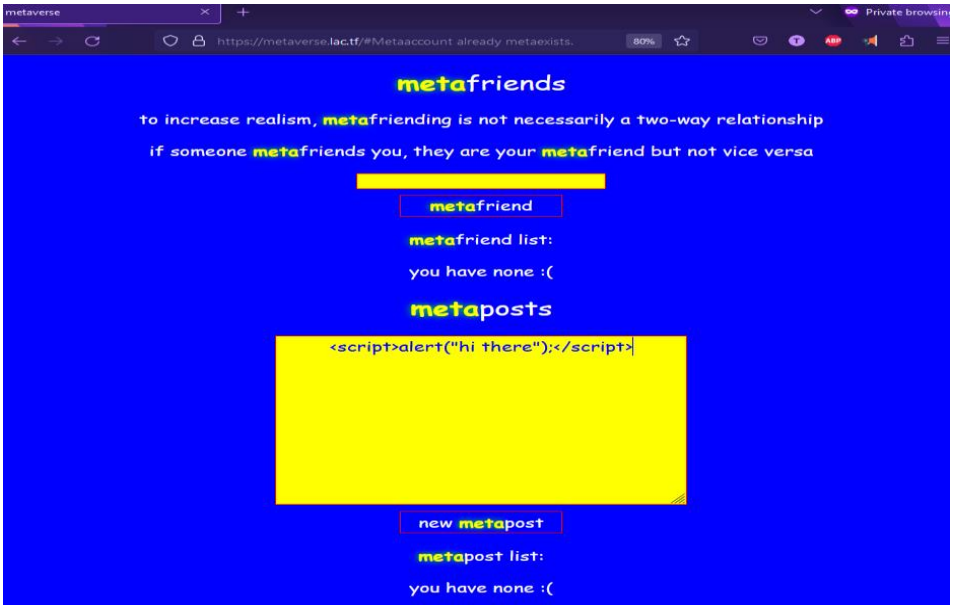


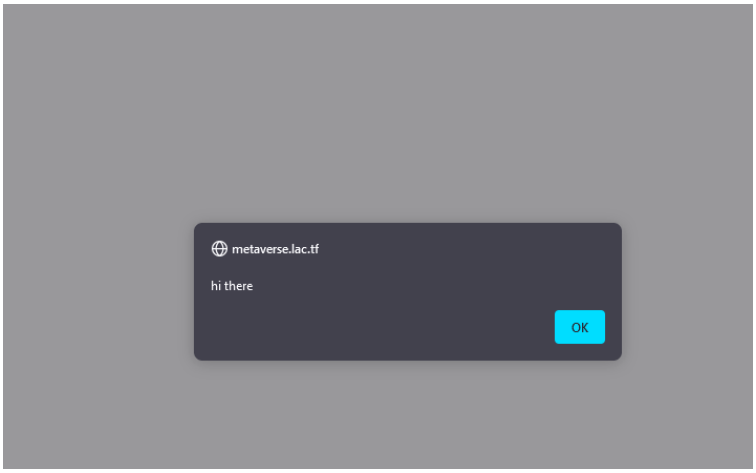


We get a very beautiful website. Another example of amazing design from LACTF. So we get a login section and a registration section, let’s just go ahead and make a new account for this writeup.

Alright, it looks like we have a nice social media platform here. We can add friends (but they have to add us back) and we can make some posts.

So, let’s see if the post section is properly sanitized for xss.

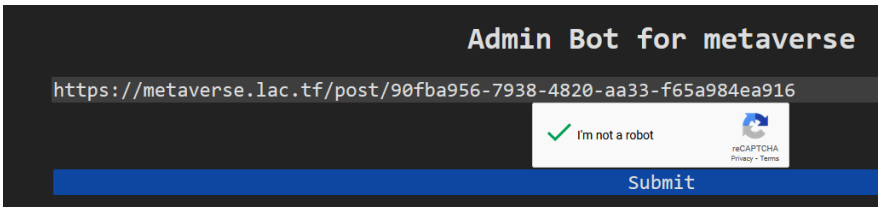




Nice! Next, let's consider that the challenge description didn't say anything about cookies, so we don't want to be doing cookie stealing with this XSS. My guess is that because "friending" someone on this website is a two way interaction, we just need to get the admin to befriend us. When we send a friend request, we hit the /friend endpoint in the code, so we just need to send the admin there with our username as the parameter.

We can have the page run our function on load such that when someone views our post, the script will make a post request to the /friend endpoint with our username as the content of the request. We can get the request sent using an Ajax XMLHttpRequest.

Perfect! We are our own friend because we viewed the post and made a request to be friends with user "writeup"! Now, we just need to take the URL of the post and have the admin visit it!



Nice! This was cool!