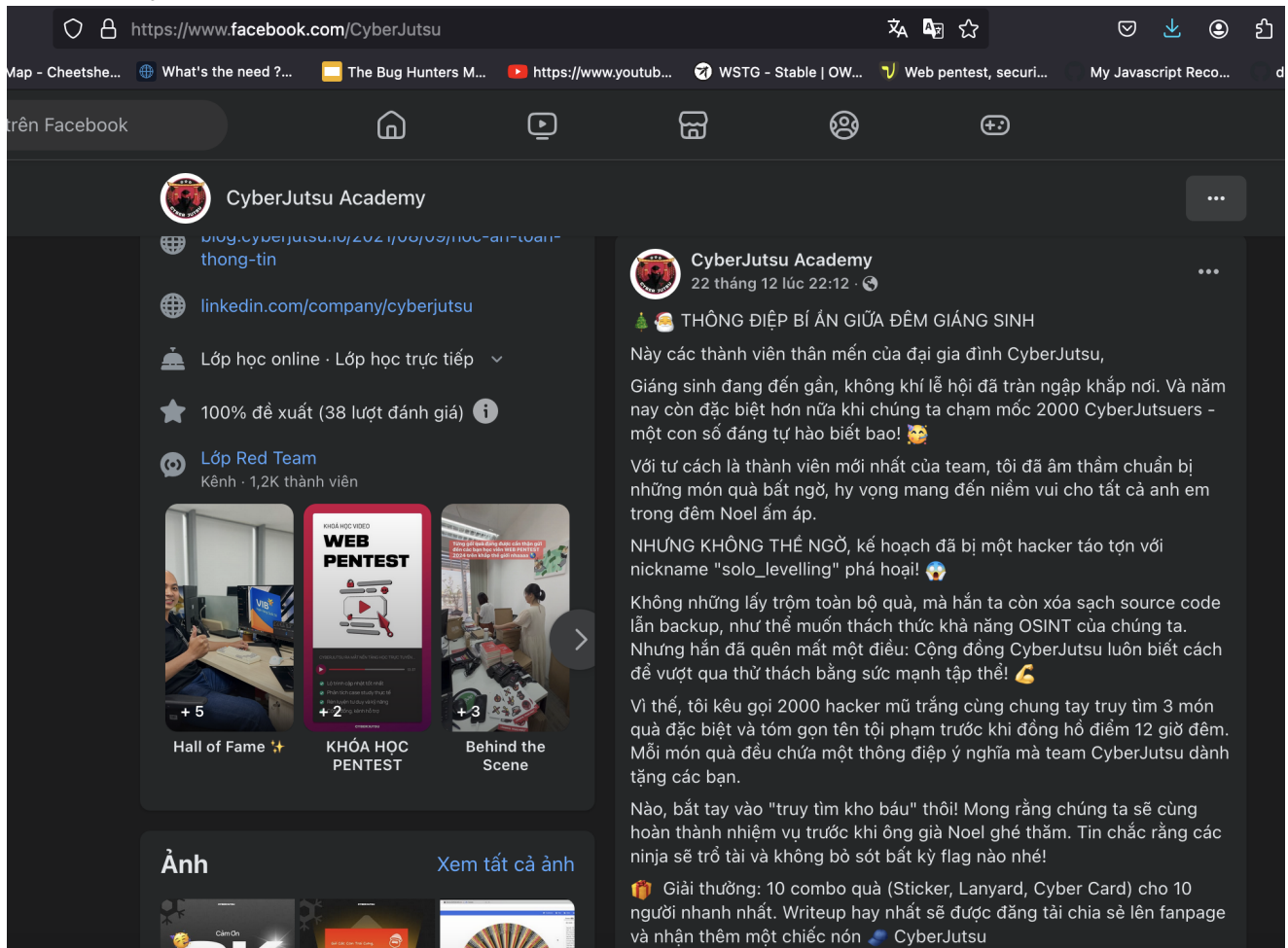


OSINT Challenge Writeup

Christmas OSINT Challenge từ CBJs

Thứ 2 mở đầu với challenge OSINT đến từ CBJs. Mình đó giờ cũng chưa OSINT nhiều nên cũng phải thử tay mới biết.



=> Từ thông tin stt chúng ta biết được username của Hacker là `solo_levelling`

Đọc trên Github biết được có vài tools thú vị dành cho việc tìm kiếm username, ở đây mình chọn Sherlock: <https://github.com/sherlock-project/sherlock>

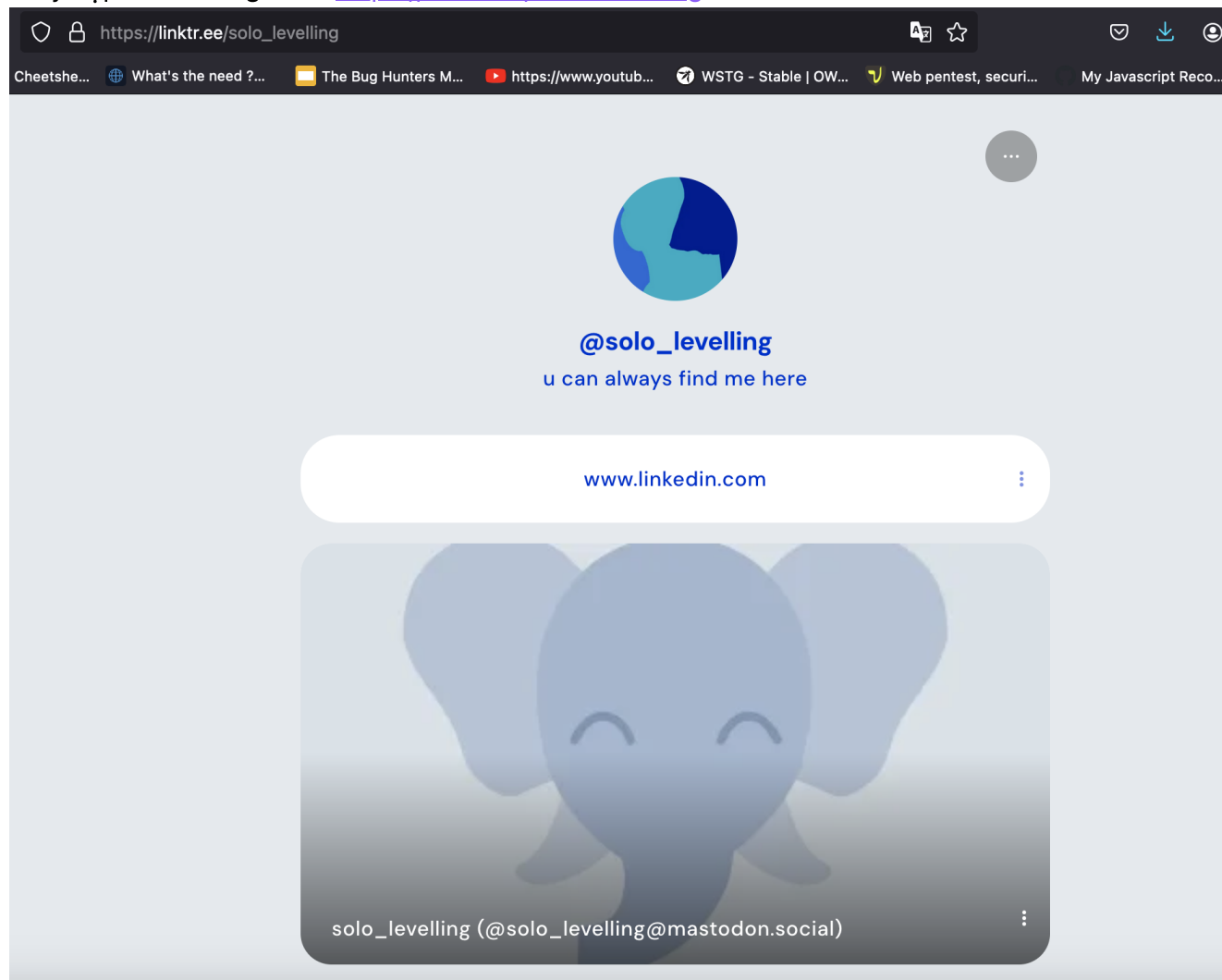
Tool trả về cho mình một số kết quả, trong đó có phần LinkTree khá thú vị, có vẻ liên quan đến vị hacker này:

```
> sherlock solo_levelling
[*] Checking username solo_levelling on:

[+] Codechef: https://www.codechef.com/users/solo_levelling
[+] Codeforces: https://codeforces.com/profile/solo_levelling
[+] Discord: https://discord.com
[+] Duolingo: https://www.duolingo.com/profile/solo_levelling
[+] HackenProof (Hackers): https://hackenproof.com/hackers/solo_levelling
[+] HackerOne: https://hackerone.com/solo_levelling
[+] HackerRank: https://hackerrank.com/solo_levelling
[+] Instagram: https://instagram.com/solo_levelling
[+] Lichess: https://lichess.org/@/solo_levelling
[+] Linktree: https://linktr.ee/solo_levelling
[+] MyAnimeList: https://myanimelist.net/profile/solo_levelling
[+] Pokemon Showdown: https://pokemonshowdown.com/users/solo_levelling
[+] ProductHunt: https://www.producthunt.com/@solo_levelling
[+] PyPi: https://pypi.org/user/solo_levelling
[+] Reddit: https://www.reddit.com/user/solo_levelling
[+] Roblox: https://www.roblox.com/user.aspx?username=solo_levelling
[+] SlideShare: https://slideshare.net/solo_levelling
[+] Snapchat: https://www.snapchat.com/add/solo_levelling
[+] Strava: https://www.strava.com/athletes/solo_levelling
[+] Telegram: https://t.me/solo_levelling
[+] TradingView: https://www.tradingview.com/u/solo_levelling/
[+] Twitch: https://www.twitch.tv/solo_levelling
[+] Twitter: https://x.com/solo_levelling
[+] YouTube: https://www.youtube.com/@solo_levelling
[+] mastodon.cloud: https://mastodon.cloud/@solo_levelling
[+] mastodon.social: https://mastodon.social/@solo_levelling
[+] npm: https://www.npmjs.com/~solo_levelling
[+] osu!: https://osu.pysh/users/solo_levelling

[*] Search completed with 28 results
```

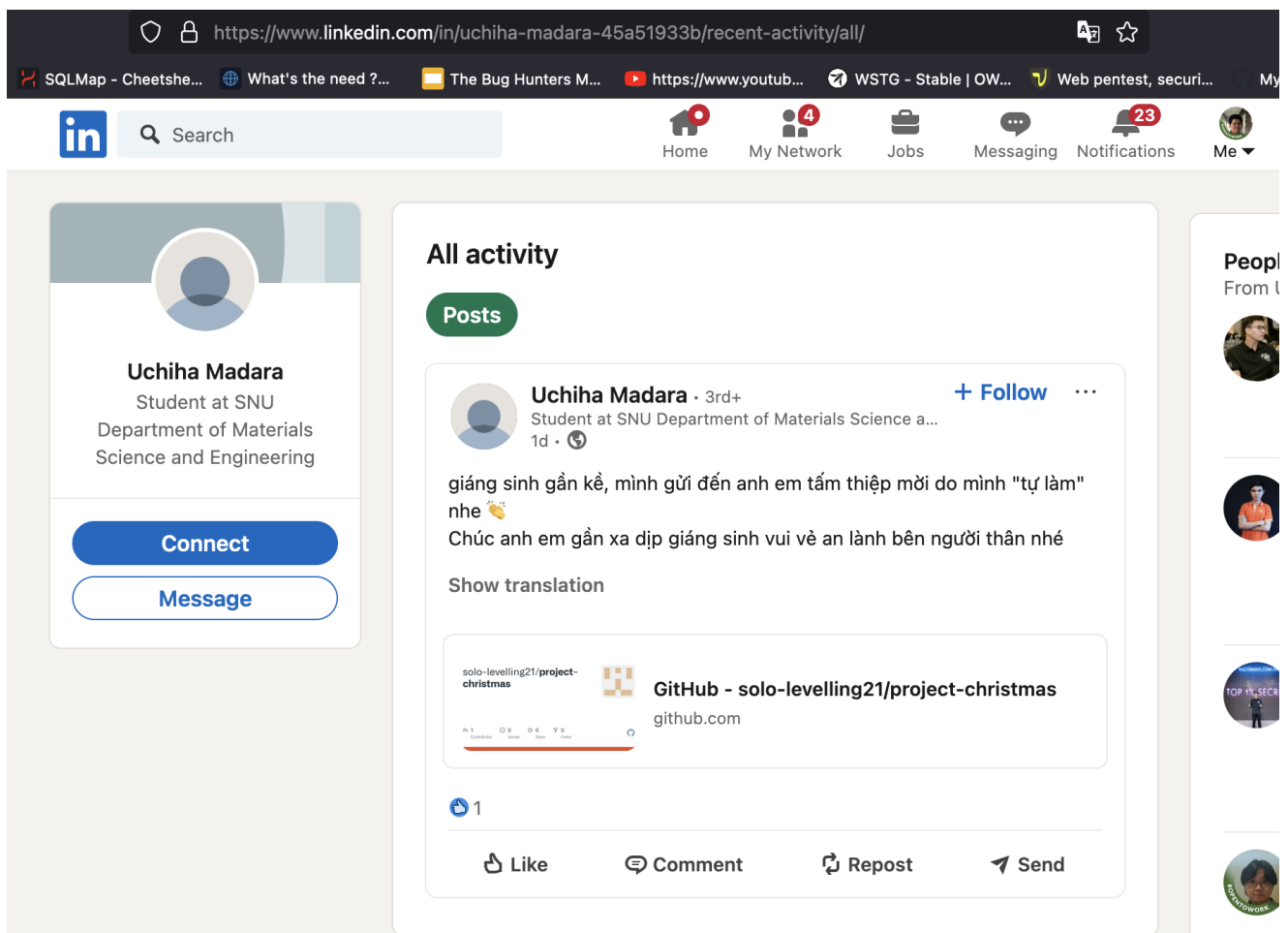
Truy cập vào đường Link: https://linktr.ee/solo_levelling



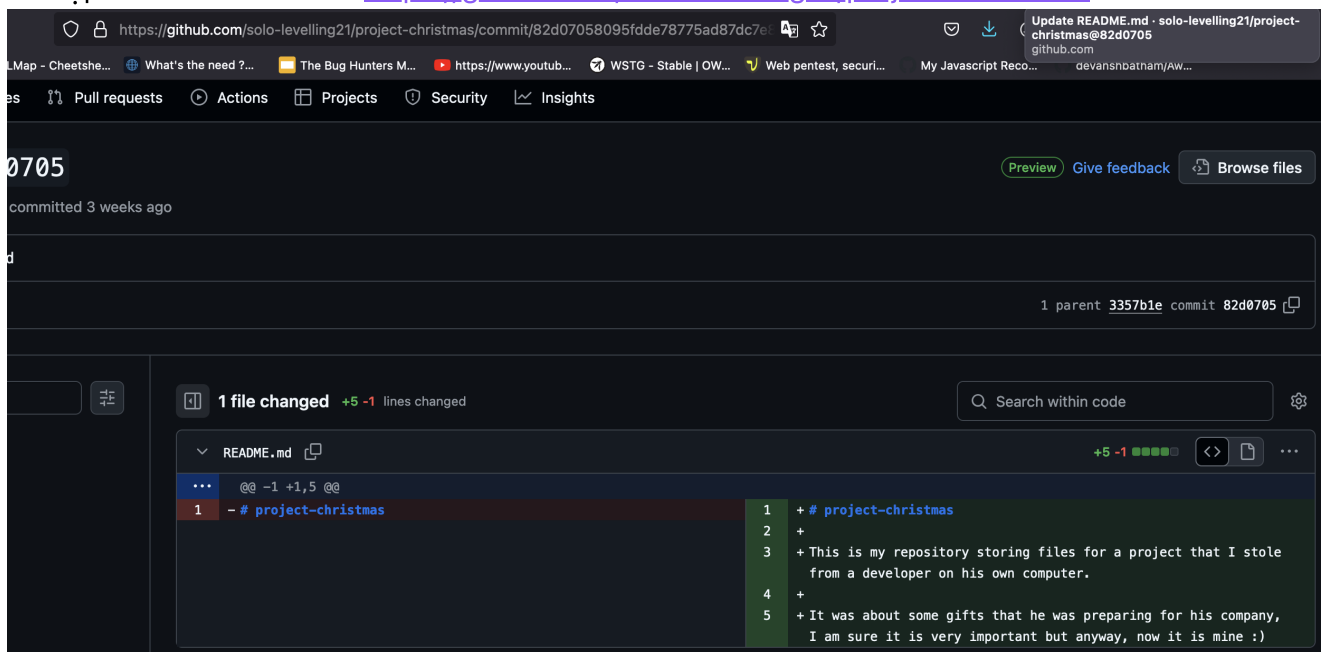
Tìm được 2 đường dẫn tới 2 profile ở Linkedin và Mastodon.

1st Flag

Trong profile Linkedin, mình tìm được 1 bài viết dẫn đến 1 link github đặt tên là project_christmas



Ngồi đọc qua các thông tin trong repo, có lẽ đây chính là phần source code bị đánh cắp được đề cập trên stt của CBJS. <https://github.com/solo-levelling21/project-christmas>



Lướt qua hết các commits của bạn này mình tìm được flag đầu tiên:

1 file changed +6 -6 lines changed

↑ Top Search within code

a.html +6 -6

121	<div class="snow"></div>	121	<div class="snow"></div>
		122 +	<div class="message">
		123 +	Chúc Mừng Giáng Sinh!
		124 +	Merry Christmas!
		125 +	</div>
122	<div class="tree">	126	<div class="tree">
123	<div class="star"></div>	127	<div class="star"></div>
124	<div class="ornaments ornament1"></div>	128	<div class="ornaments ornament1"></div>
125	<div class="ornaments ornament2"></div>	129	<div class="ornaments ornament2"></div>
126	<div class="ornaments ornament3"></div>	130	<div class="ornaments ornament3"></div>
127	</div>	131	</div>
128 -	<div class="message">		
129 -	Chúc Mừng Giáng Sinh! 		
130 -	Merry Christmas!		
131 -	</div>		
132	</div>	132	</div>
133	</body>	133	</body>
134	</html>	134	</html>

Comments 1

solo-levelling21 3 days ago

Owner Author ...

CBJS{hehehee_ban_co_de_lai_gi_trong_github_commit_hong???!}

Flag 1

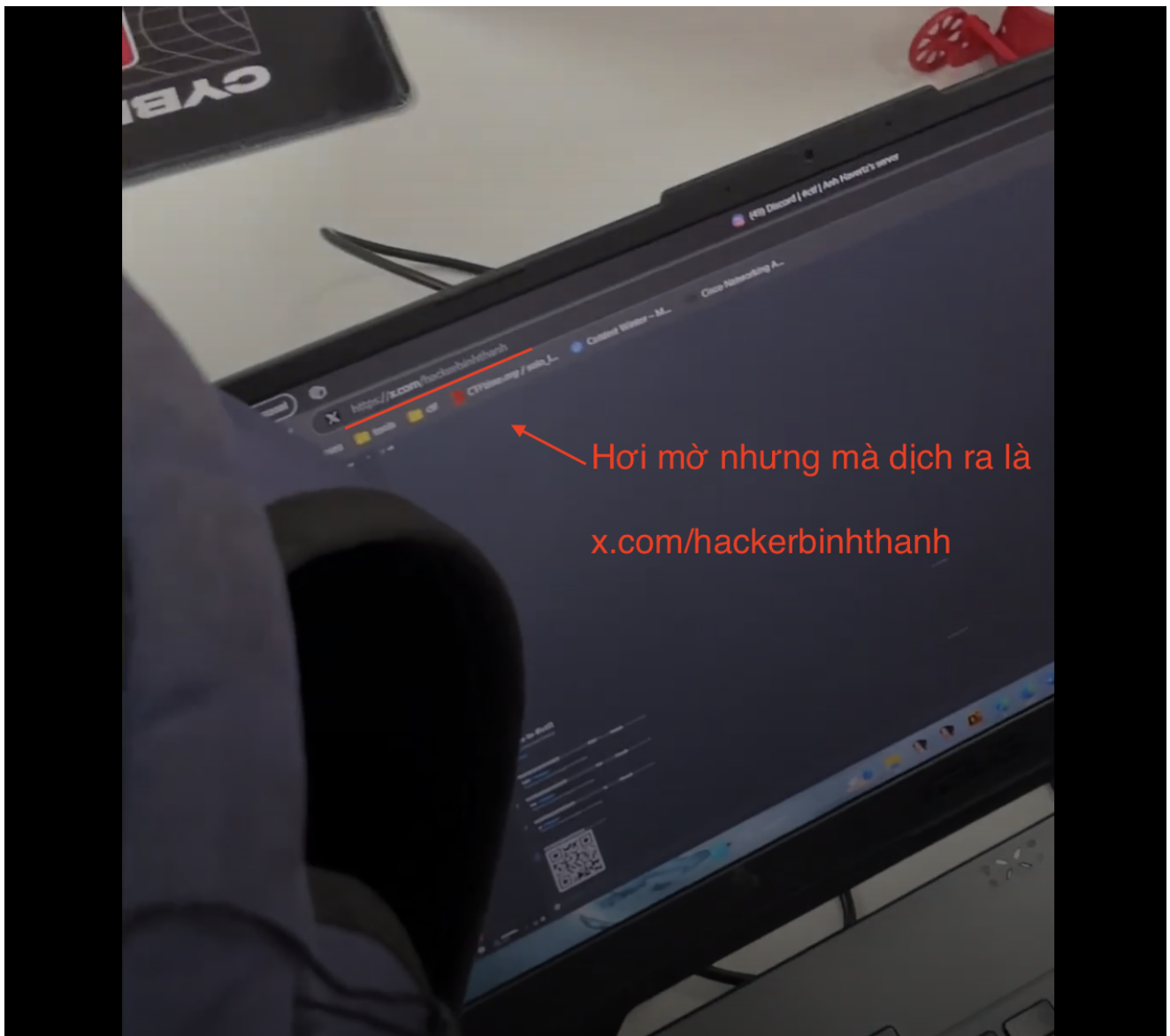
CBJS{hehehee_ban_co_de_lai_gi_trong_github_commit_hong???!}

2nd Flag

Lần này truy cập vào Mastodon: https://mastodon.social/@solo_levelling

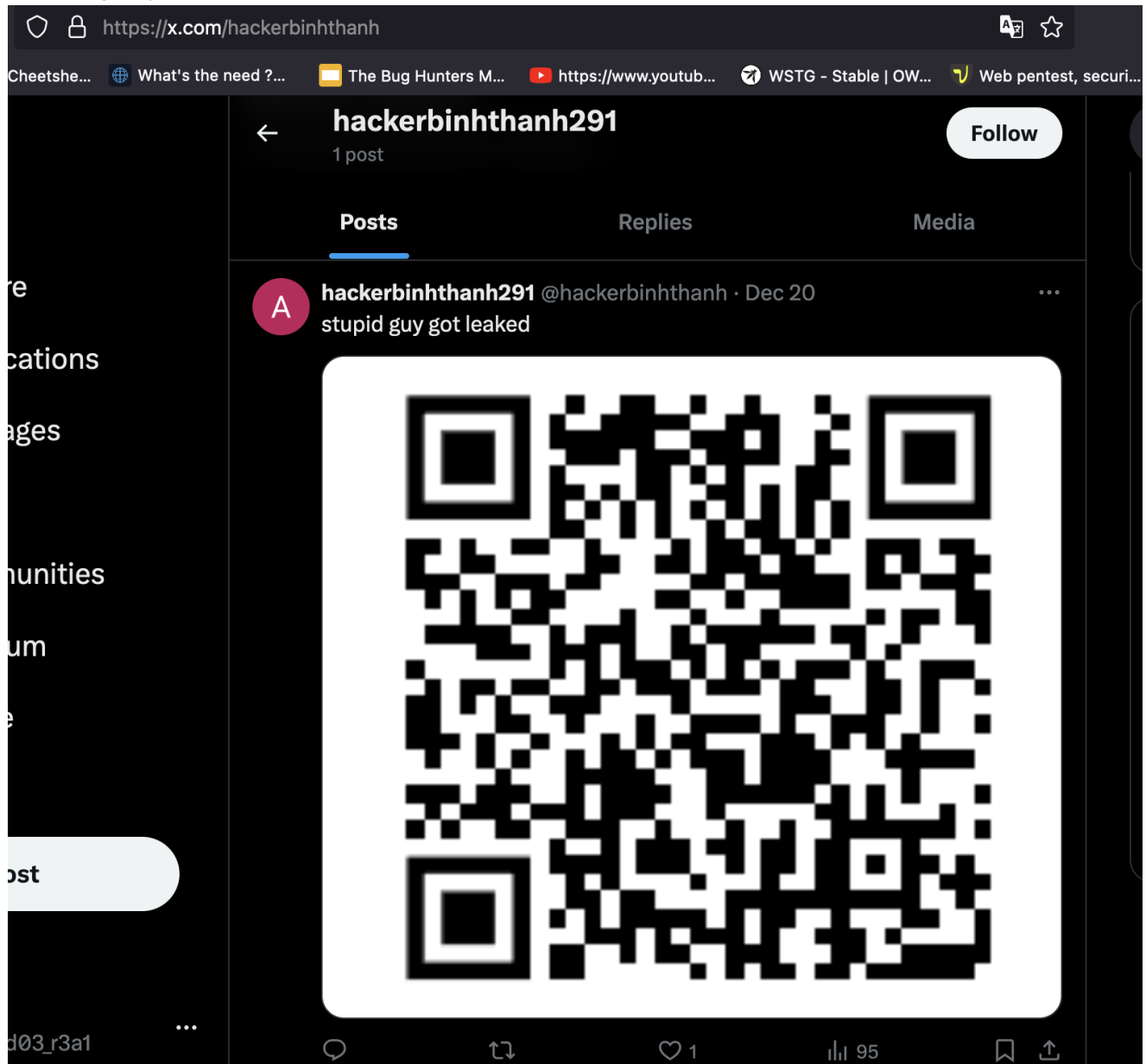
The screenshot shows the Mastodon profile page for the user **solo_levelling** (@solo_levelling) on the **mastodon.social** server. The browser address bar displays the URL https://mastodon.social/@solo_levelling. The profile header includes a back arrow, the username **solo_levelling**, the handle **@solo_levelling**, and the server **mastodon.social**. The bio states "I am the besst hackerr in the world". The user joined on Dec 21, 2024, and has 3 posts, 0 following, and 0 followers. The profile tabs are "Posts", "Posts and replies", and "Media", with "Posts" selected. The first post, from 2 days ago, contains the text "ui does matter, what doesnt look good on computer may better on phone" and has 0 replies, 0 retweets, and 0 favorites. The second post, also from 2 days ago and marked as a favorite, contains the text "today is so fun, i have recorded a video for this day: drive.google.com/file/d/1TtV_I...". Below the text is a video player showing a Google Docs interface with the filename **xmas.MOV**. The left sidebar features a search bar, a welcome message for mastodon.social, a cartoon illustration, and server statistics: "ADMINISTERED BY: Mastodon @Mastodon" and "SERVER STATS: 247K active users". The right sidebar shows the Mastodon logo, navigation links for "Explore" and "Live feeds", a description of Mastodon, and buttons for "Create account" and "Login".

Có vẻ như **Best Hacker** của chúng ta có đăng 1 video tên **xmas.MOV**, hãy xem video đó coi có thông tin gì thú vị không nào.



Có vẻ như Hacker này trong lúc quá vui để lộ thông tin tài khoản twitter của bản thân hehe. Giờ

nền tảng này đổi tên thành X rồi nên mới ra cái URL: <https://x.com/hackerbinhthanh>



Scan mã QR mình tìm được FLAG thứ 2:

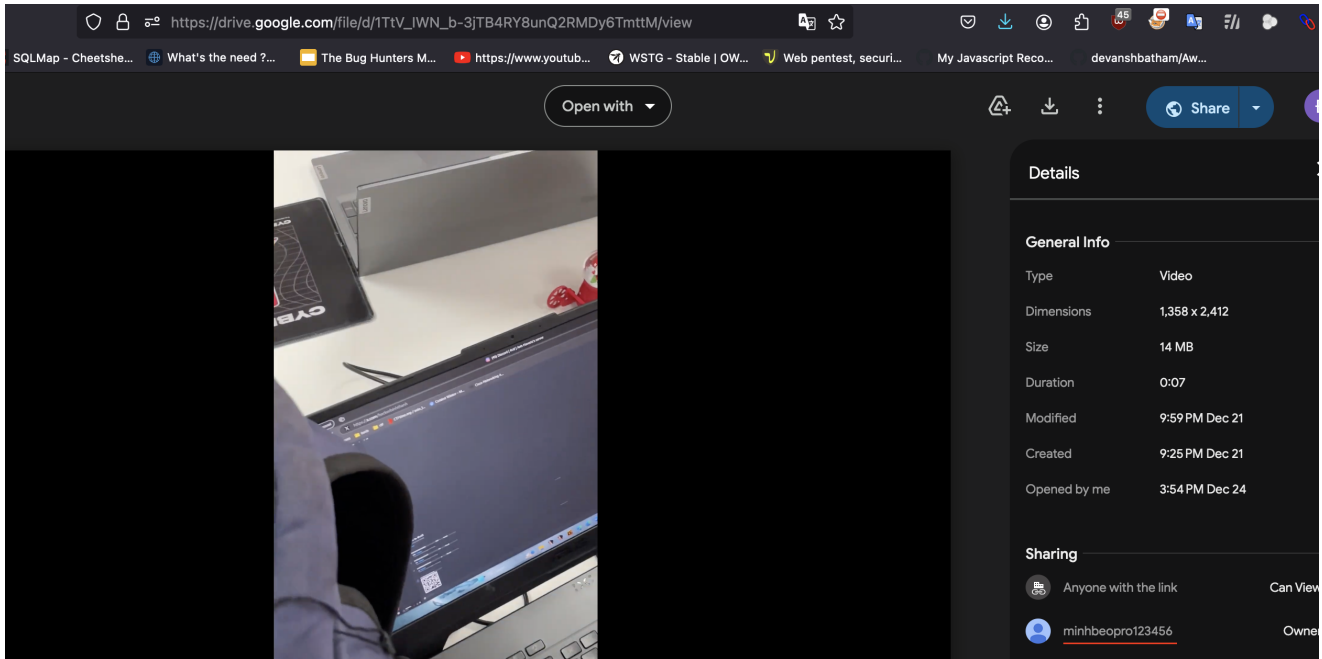
 Flag 2

```
CBJS{tinh_mat_qua_chac_ko_sot_con_bug_ngo_dau:)):D}"
```

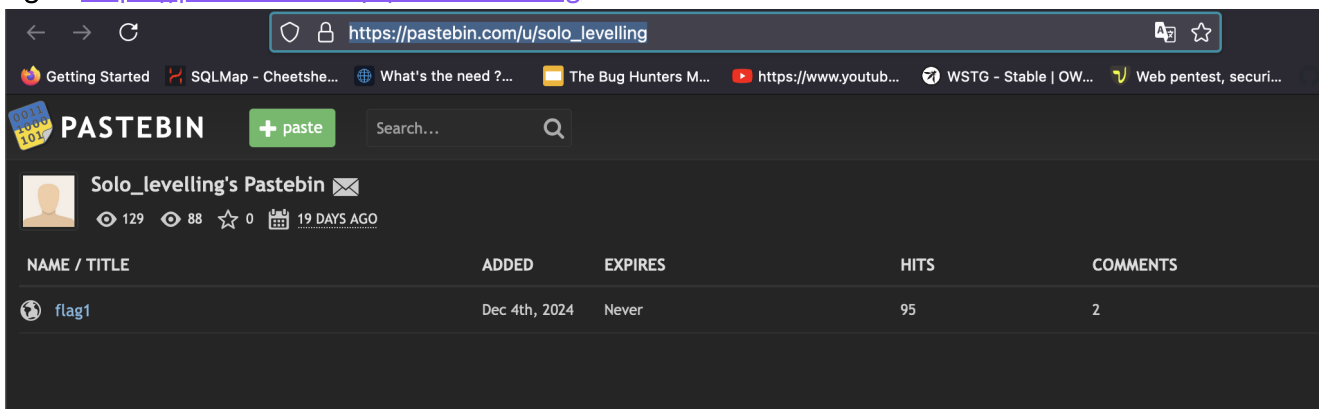
3rd Flag

Quê mò xong 2 Flags rồi cái bị stuck, mình chả biết có thông tin gì tìm được không nữa ??? Thử tìm qua cả thông tin metadata của video, và owner của nó `minhbeopro123456`, cũng không trả

về kết quả gì, mình tắt máy rồi đi ngủ do cũng nửa đêm rồi hic :<

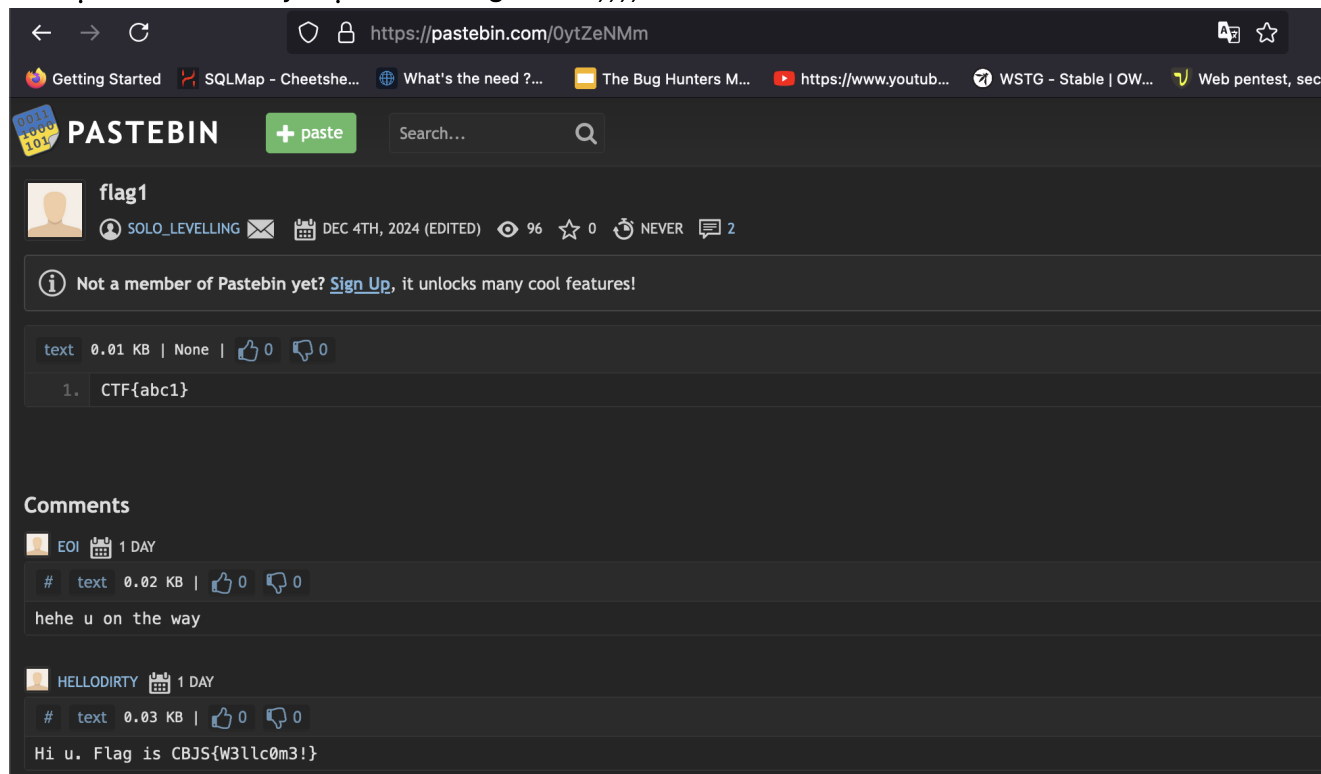


Cái hôm nay thử tìm lại xem sao, chợt nhớ mình có lướt qua 1 cái pastebin trông cũng rất khả nghi: https://pastebin.com/u/solo_levelling



Đọc quả flag này vào hôm thứ 2 thì không có gì cả, nội dung của nó là: `CTF{abc1}` lại không match format `CBJS{}` của CBJS nên mình cứ để đó thôi.

Cái tự nhiên hôm nay hiện ra cái flag hehe :)))



The screenshot shows a web browser at <https://pastebin.com/0ytZeNMm>. The page displays a Pastebin post titled "flag1" by user "SOLO_LEVELLING", dated "DEC 4TH, 2024 (EDITED)". The post content is a list with one item: "1. CTF{abc1}". Below the post, there are two comments. The first comment is from user "EOI" (posted 1 DAY ago) with the text "hehe u on the way". The second comment is from user "HELLODIRTY" (posted 1 DAY ago) with the text "Hi u. Flag is CBJS{W3llc0m3!}". The browser's address bar and tabs are visible at the top.

 Flag 3

CBJS{W3llc0m3!}

Final

Rất vui vì bản thân đã hoàn thành challenge của CBJS, từ challenge mình cũng học được nhiều kiến thức về phương pháp OSINT. Bản thân đi tìm bug bounty cũng khá nhiều nhưng chưa có kết quả gì hay ho, có lẽ đây sẽ là 1 khởi đầu tuyệt vời cho năm mới 2025 của mình. Tui đang lên sắp viết Writeup đây hehe :>.

Merrrryyyy ChristMas CBJS và mn nhé.