

# CBSJ Christmas 2024

## Write-up Osint Challenge



Author: **Ren**

### CONTACT

 [Facebook](#) |  [linkedin.com](#)

### Challenge Overview

Thử thách này là một cuộc điều tra OSINT (Thu thập thông tin từ nguồn mở) đòi hỏi việc phát hiện nhiều flag trên các nền tảng trực tuyến khác nhau. Điểm khởi đầu được cung cấp thông qua tên người dùng: `solo_levelling`.

**CyberJutsu Academy**  
11 giờ · 

🎄👤 THÔNG ĐIỆP BÍ ẨN GIỮA ĐÊM GIÁNG SINH

Này các thành viên thân mến của đại gia đình CyberJutsu,

Giáng sinh đang đến gần, không khí lễ hội đã tràn ngập khắp nơi. Và năm nay còn đặc biệt hơn nữa khi chúng ta chạm mốc 2000 CyberJutsuers - một con số đáng tự hào biết bao! 🥳

Với tư cách là thành viên mới nhất của team, tôi đã âm thầm chuẩn bị những món quà bất ngờ, hy vọng mang đến niềm vui cho tất cả anh em trong đêm Noel ấm áp.

NHƯNG KHÔNG THỂ NGỜ, kế hoạch đã bị một hacker táo tợn với nickname "solo\_levelling" phá hoại! 🤖

Không những lấy trộm toàn bộ quà, mà hắn ta còn xóa sạch source code lẫn backup, như thể muốn thách thức khả năng OSINT của chúng ta. Nhưng hắn đã quên mất một điều: Cộng đồng CyberJutsu luôn biết cách để vượt qua thử thách bằng sức mạnh tập thể! 💪

Vì thế, tôi kêu gọi 2000 hacker mũ trắng cùng chung tay truy tìm 3 món quà đặc biệt và tóm gọn tên tội phạm trước khi đồng hồ điểm 12 giờ đêm. Mỗi món quà đều chứa một thông điệp ý nghĩa mà team CyberJutsu dành tặng các bạn.

Nào, bắt tay vào "truy tìm kho báu" thôi! Mong rằng chúng ta sẽ cùng hoàn thành nhiệm vụ trước khi ông già Noel ghé thăm. Tin chắc rằng các ninja sẽ trở tài và không bỏ sót bất kỳ flag nào nhé!

🎁 Giải thưởng: 10 combo quà (Sticker, Lanyard, Cyber Card) cho 10 người nhanh nhất. Writeup hay nhất sẽ được đăng tải chia sẻ lên fanpage và nhận thêm một chiếc nón 🧢 CyberJutsu

THỂ LỆ CUỘC THI:

- 🎄 Flag format: CBSJ{...}
- 🎄 Thời gian: 22:12 22/12/2024 - 23:59 25/12/2024
- 🎄 Độ khó cao, hãy để ý các chi tiết nhỏ nhất!
- 🎄 Người tham gia cần share bài viết này ở chế độ public và Submit 3 flag + writeup qua inbox fanpage CyberJutsu

#HappyHoliHacking #OSINT #OSINTchallenge #CTF #CyberJutsu

Sử dụng công cụ OSINT để liệt kê tên người dùng, tôi đã tiến hành tìm kiếm toàn diện trên nhiều nền tảng. Cuộc điều tra đã cho kết quả hai hướng đi tiềm năng:

1. Hồ sơ Mastodon: [https://mastodon.social/@solo\\_levelling](https://mastodon.social/@solo_levelling)
2. Hồ sơ Linktree: [https://linktr.ee/solo\\_levelling](https://linktr.ee/solo_levelling)

Các url khác false positive.

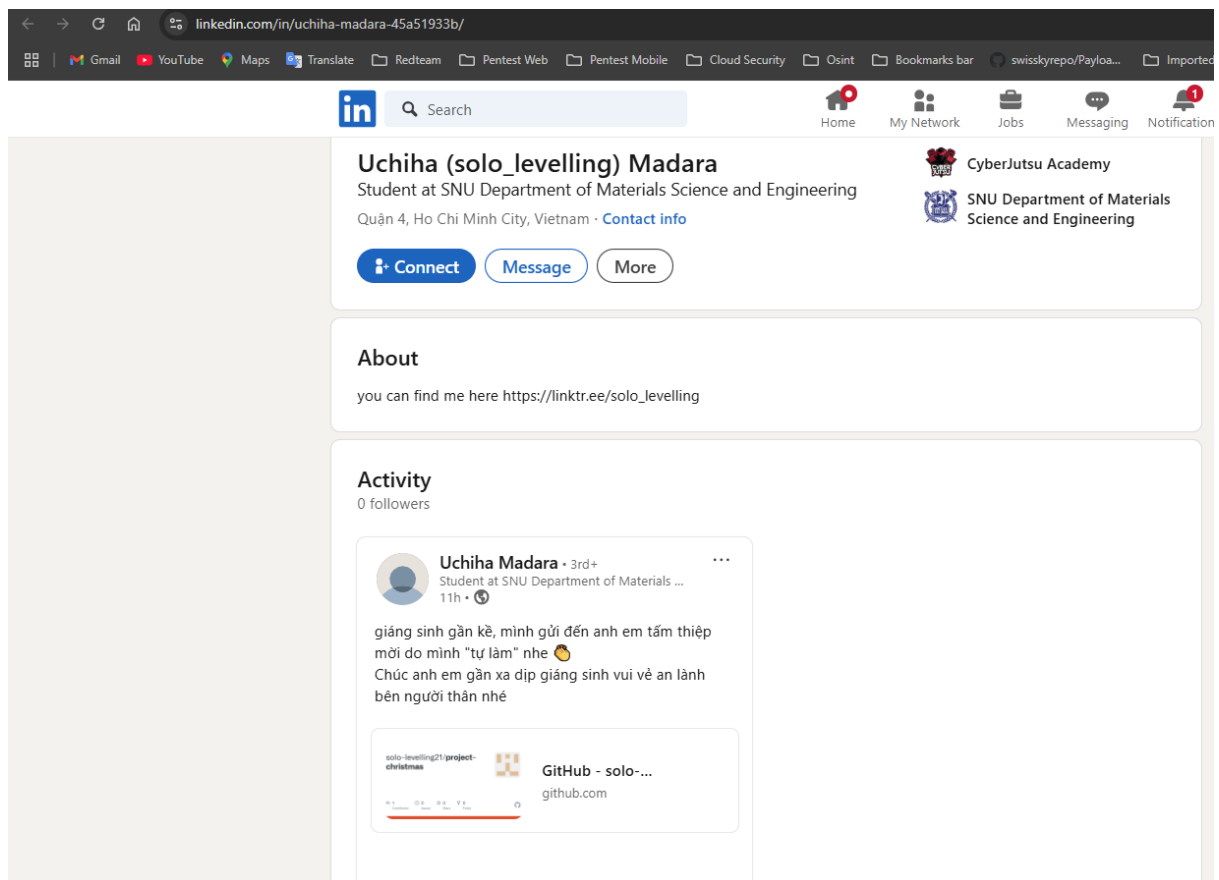
```
(venv)-(kali㉿kali)-[~/Tools/blackbird]
$ python blackbird.py --username solo_levellling
/home/kali/Tools/blackbird/src/modules/core/email.py:65: SyntaxWarning: invalid escape sequence '\['
f" ✓ \[[cyan]\{site['name']}\[/cyan]\] [bright_white]{response['url']}\[/bright_white]"

██████████BLACKBIRD██████████

    Made with ♥ by Lucas 'Pingulin0' Antoniacci
📁 Downloading site list
▶ Enumerating accounts with username "solo_levellling"
✓ [BandLab] https://www.bandlab.com/api/v1.3/users/solo_levellling
✓ [Chess.com] https://api.chess.com/pub/player/solo_levellling
✓ [character.ai] https://character.ai/profile/solo_levellling
✓ [Duolingo] https://www.duolingo.com/2017-06-30/users?username=solo_levellling&=1628308619574
  = Avatar: https://sig-sql.duolingo.com/avatar/default_2
  = Name: waad
  = Courses:
    ● Chinese
    ● English
✓ [Codeforces] https://codeforces.com/profile/solo_levellling
✓ [Folkd] https://www.folkd.com/?app=core&module=system&controller=ajax&do=usernameExists&input=solo_levellling
✓ [GOG] https://www.gog.com/u/solo_levellling
✓ [Instagram (Imginn)] https://imginn.com/solo_levellling/
✓ [Internet Archive User Search] https://archive.org/advancedsearch.php?q=solo_levellling&output=json
✓ [Linktree] https://linktr.ee/solo_levellling
✓ [Kik] https://kik.me/solo_levellling
✓ [Lichess] https://lichess.org/@/solo_levellling
✓ [Mastodon API] https://mastodon.social/api/v2/search?q=solo_levellling&limit=1&type=accounts
✓ [Mastodon-mastodon] https://mastodon.social/@solo_levellling
✓ [MyAnimeList] https://myanimelist.net/prorate/solo_levellling
✓ [npm] https://www.npmjs.com/~solo_levellling
✓ [npm] https://www.npmjs.com/~solo_levellling
✓ [Reddit] https://www.reddit.com/user/solo_levellling/about/.json
✓ [Roblox] https://auth.roblox.com/v1/usernames/validate?username=solo_levellling&birthday=2019-12-31T23:00:00.000Z
✓ [RblxTrade] https://rblx.trade/p/solo_levellling
✓ [Snapchat] https://www.snapchat.com/add/solo_levellling
✓ [Telegram] https://t.me/solo_levellling
✓ [TikTok] https://www.tiktok.com/oembed?url=https://www.tiktok.com/@solo_levellling
  = Name: Solo Levellling PUBG
✓ [Tradingview] https://www.tradingview.com/u/solo_levellling/
✓ [Twitch] https://twitchtracker.com/solo_levellling
✓ [Twitter archived tweets] http://archive.org/wayback/available?url=https://twitter.com/solo_levellling/status/*
✓ [Twitter] https://nitter.privacydev.net/solo_levellling
  = Avatar: https://nitter.privacydev.net/pic/pbs.twimg.com%2Fprofile_images%2F1764329071696392192%2FcXyoo4gS_400x400.jpg
  = Name: Domingo Oliva
✓ [YouTube User2] https://www.youtube.com/@solo_levellling
▶ Check completed in 53.2 seconds (668 sites)
```

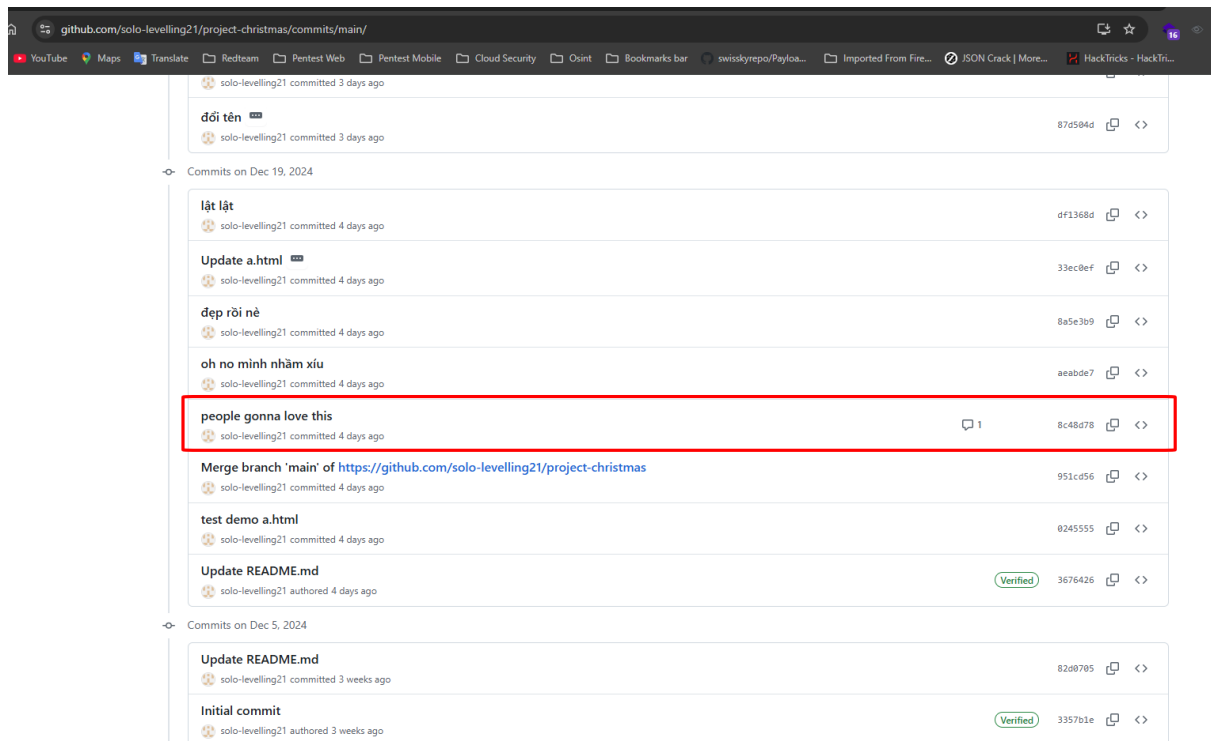
## Phase 1: First Flag Discovery

Hồ sơ Linktree dẫn đến một tài khoản LinkedIn ( <https://www.linkedin.com/in/uchiha-madara-45a51933b> ), chứa một bài đăng duy nhất tham chiếu đến một kho lưu trữ GitHub. Điều này mở rộng bề mặt tấn công của chúng ta đến: <https://github.com/solo-levelling21>



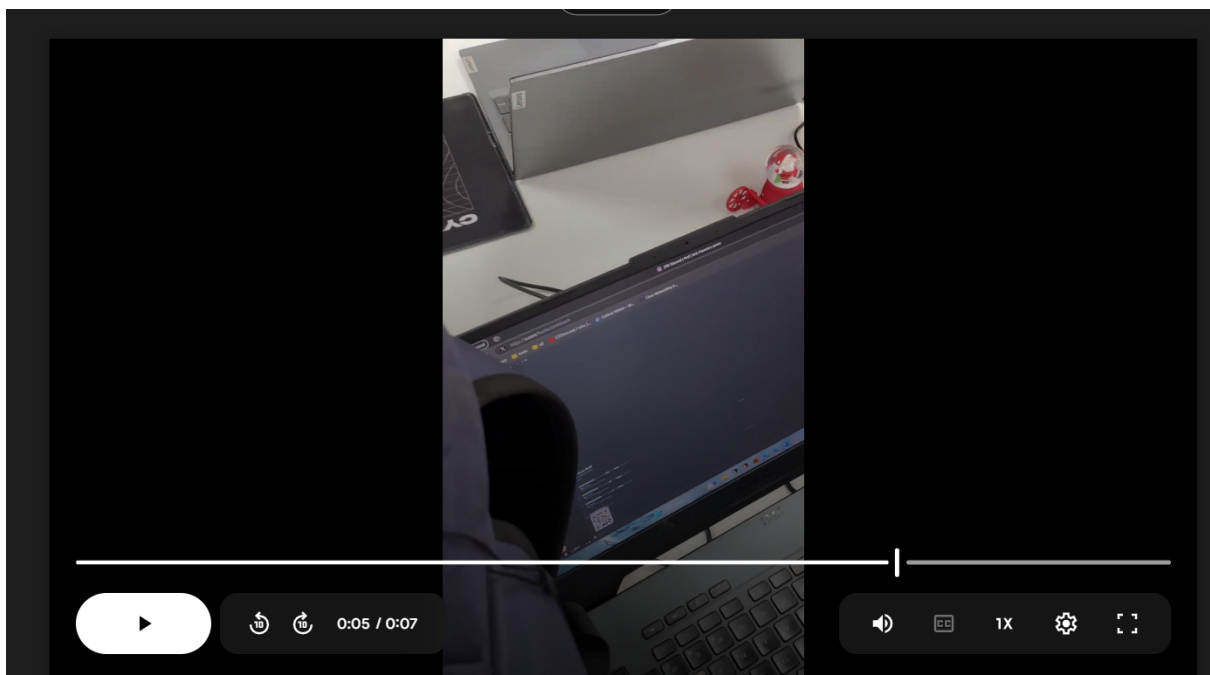
Khi kiểm tra lịch sử commit của kho lưu trữ `project-christmas`, tôi đã xác định được một commit đáng ngờ có tiêu đề "people gonna love this". Phân tích commit này đã tiết lộ flag đầu tiên trong phần bình luận:

```
CBJS{hehehee_ban_co_de_lai_gi_trong_github_commit_hong???!}
```



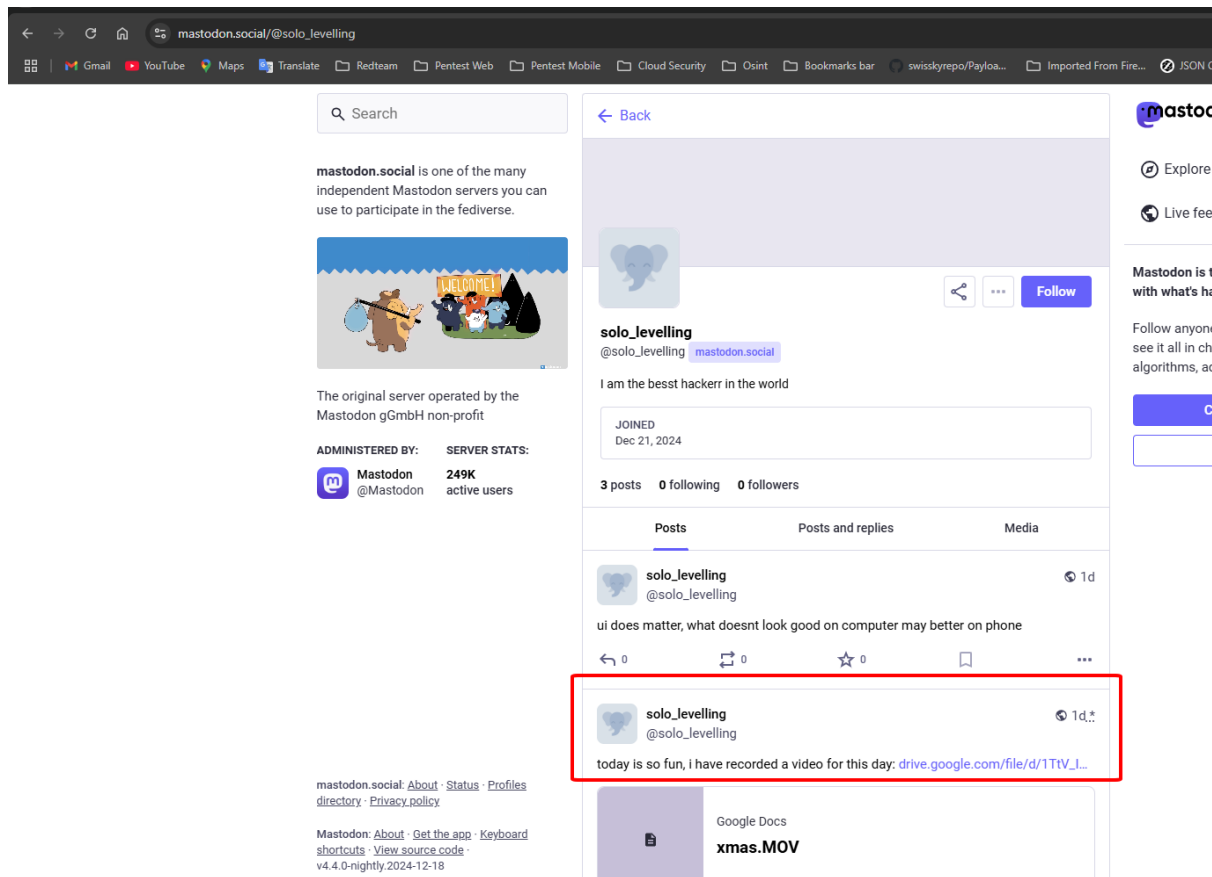
## Phase 2: Video Analysis

Quay trở lại hồ sơ Mastodon, tôi phát hiện ba bài đăng, một trong số đó chứa liên kết Google Drive đến một tệp có tên `xmas.MOV`. Phân tích khung hình của video tại thời điểm 00:05 đã tiết lộ URL hồ sơ Twitter/X: <https://x.com/hackerbinhthanh>



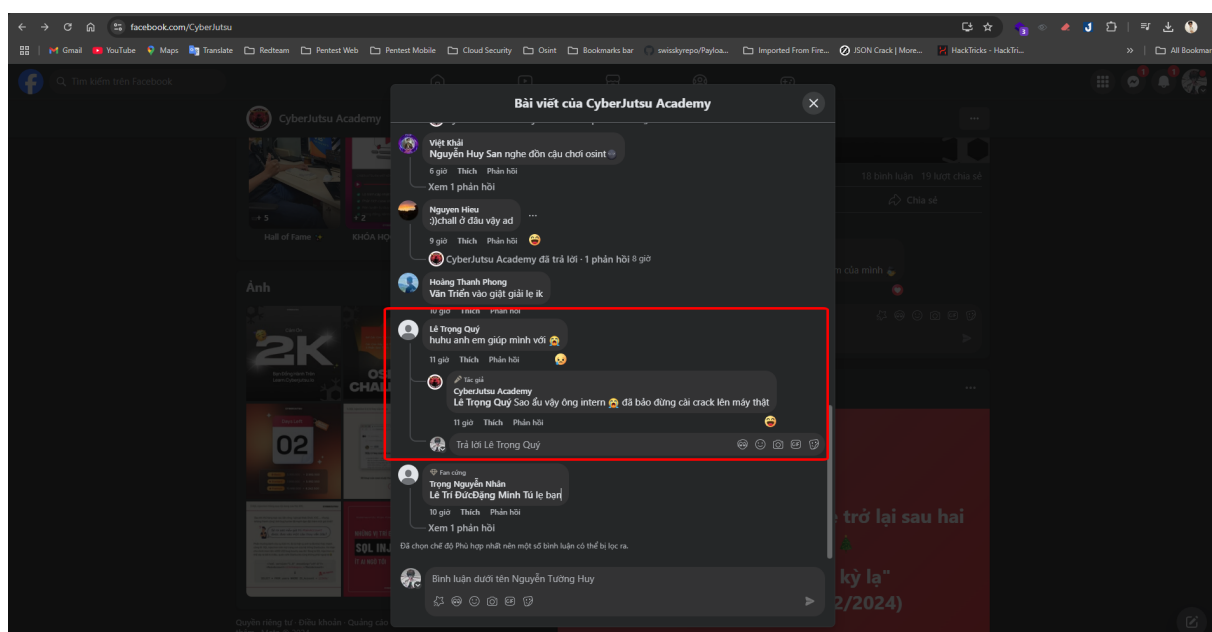
Hồ sơ này chứa một mã QR, khi giải mã đã cho ra flag thứ hai:

```
CBJS{tinh_mat_qua_chac_ko_sot_con_bug_nao_dau:)):D}
```

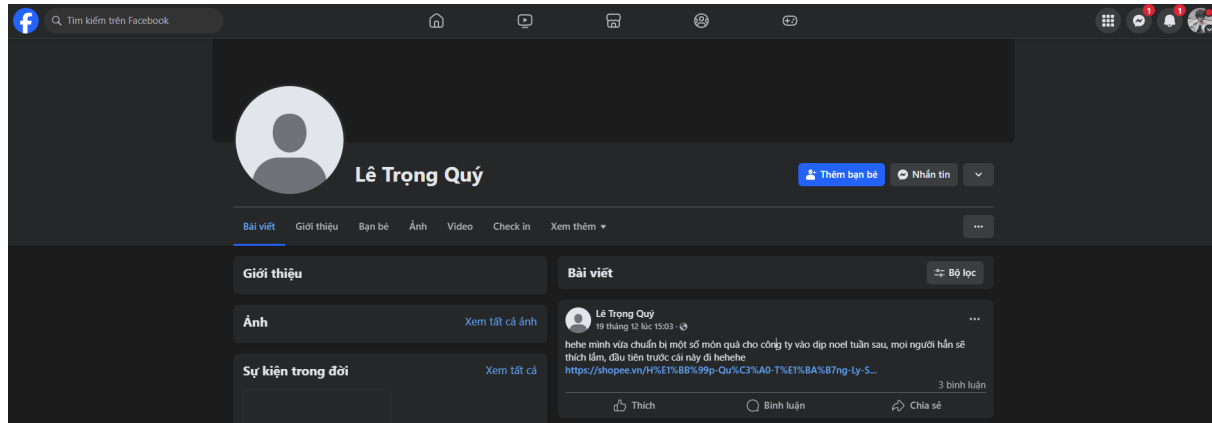


## Phase 3: Social Engineering Analysis

Một mảnh cuối cùng nằm trong comment bài POST Challenge ( **khảy giấu kỹ quá** ).

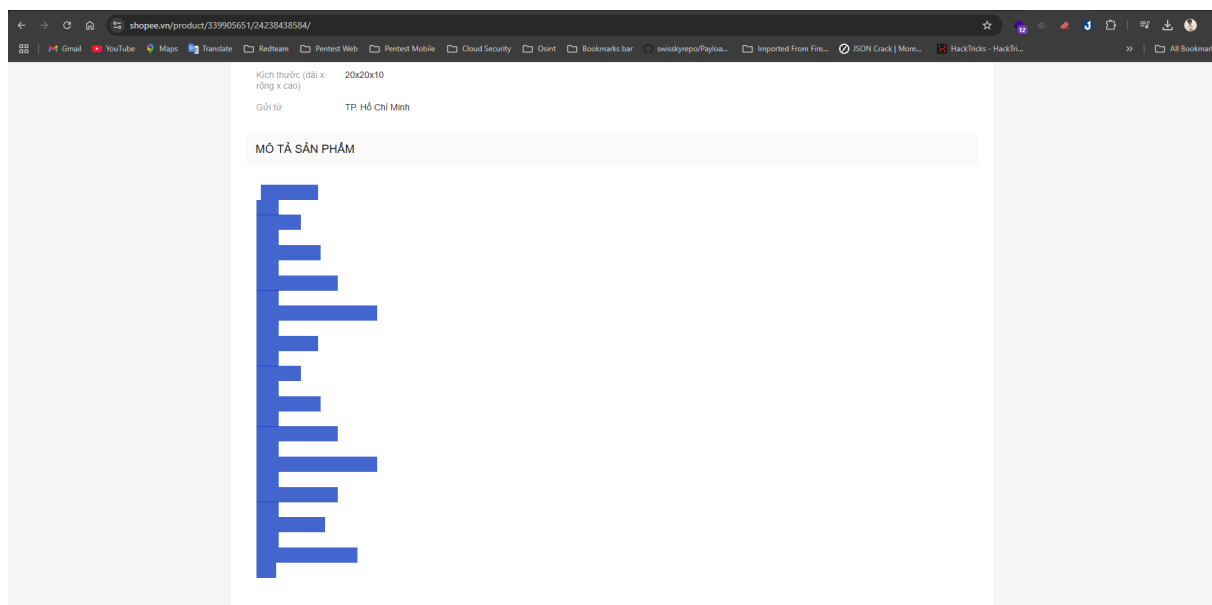


Điều này dẫn đến việc phát hiện một hồ sơ Facebook với một bài đăng đã được chỉnh sửa chứa liên kết sản phẩm Shopee: <https://shopee.vn/product/339905651/24238438584/>



## Phân Tích Steganography

Phần mô tả sản phẩm chứa một đoạn khoảng trắng bất thường lớn. Khi kiểm tra kỹ hơn, phát hiện ra việc sử dụng ngôn ngữ lập trình bí mật Whitespace. Sử dụng bộ giải mã Whitespace (<https://dcode.fr/whitespace-language>), tôi đã trích xuất được flag cuối cùng:



```
CBJS{CBJS_chuc_anh_em_giang_sinh_an_lanh!!!<33}
```

## Technical Tools Used

- blackbird, Automation Dork...
- history commit Git
- [www.dcode.fr](https://www.dcode.fr)

## Platform Coverage

Cuộc điều tra trải rộng trên nhiều nền tảng:

- Hệ thống quản lý phiên bản (GitHub)
- Mạng xã hội (Mastodon, Twitter/X, Facebook)
- Mạng chuyên nghiệp (LinkedIn)
- Nền tảng thương mại điện tử (Shopee)
- Tổng hợp nội dung (Linktree)

## Conclusion

Thử thách CTF này đã thể hiện tầm quan trọng của phương pháp luận OSINT toàn diện và tương quan giữa các nền tảng. Thử thách tích hợp nhiều khía cạnh của điều tra số bao gồm:

- Điều tra pháp y kho lưu trữ
- Phân tích phương tiện truyền thông
- Kỹ thuật xã hội
- Steganography
- Thu thập thông tin đa nền tảng

Mỗi flag đòi hỏi một cách tiếp cận và bộ kỹ năng kỹ thuật khác nhau, làm cho nó trở thành một bài tập xuất sắc trong kỹ thuật điều tra OSINT toàn diện.