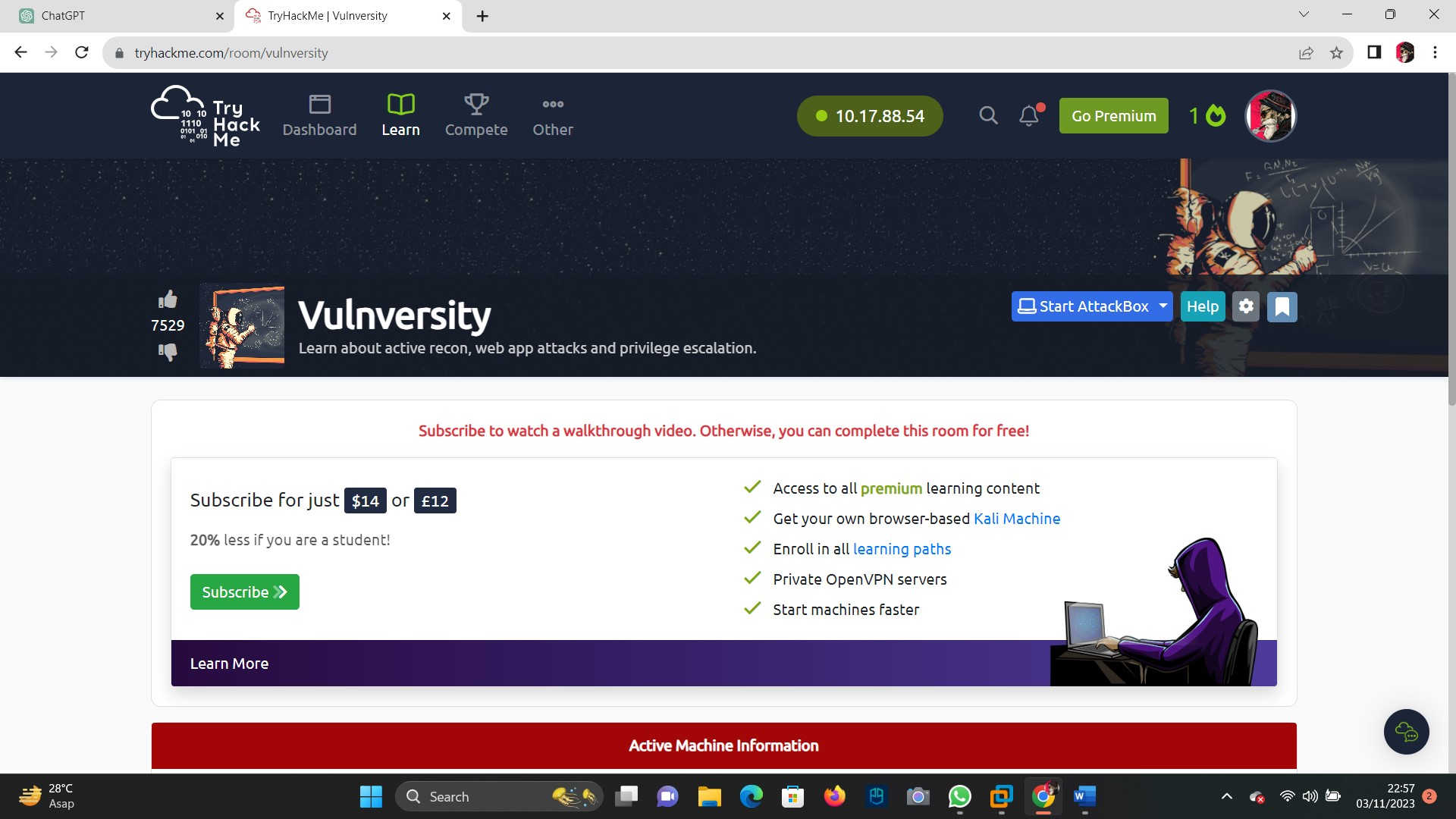
Berikut adalah laporan tentang langkah-langkah awal hingga solusi terhadap kerentanan yang ditemukan dalam TryHackMe room "Vulnversity":



Laporan Pentesting - TryHackMe Vulnversity

Penulis: Andrian Zola & Faris Alqhaniyyu

Tanggal: 3 November 2023

1. Ringkasan

Basic pentesting, juga dikenal sebagai uji penetrasi dasar, adalah proses yang dilakukan oleh para profesional keamanan komputer untuk mengevaluasi kelemahan sistem dan aplikasi, serta mengidentifikasi kerentanan yang dapat dieksploitasi oleh penyerang. Tujuan utama dari basic pentesting adalah menguji sejauh mana sistem, jaringan, dan aplikasi dapat tahan terhadap serangan dan risiko keamanan. Berikut adalah pemahaman yang lebih mendetail tentang basic pentesting:

* Tujuan Pentesting:
* Identifikasi Kerentanan: Pentesting bertujuan untuk menemukan dan mengidentifikasi kerentanan dalam sistem yang dapat dieksploitasi oleh penyerang.
* Evaluasi Keamanan: Pentesting digunakan untuk mengevaluasi tingkat keamanan sistem dan aplikasi, serta mengukur sejauh mana perangkat lunak dan perangkat keras dapat bertahan terhadap serangan.

Laporan ini berfokus pada pentesting yang telah saya lakukan di room TryHackMe "Vulnversity." Saya akan memberikan rincian langkah-langkah awal, kerentanannya yang ditemukan, dan solusi yang disarankan untuk mengatasi kerentanan tersebut.

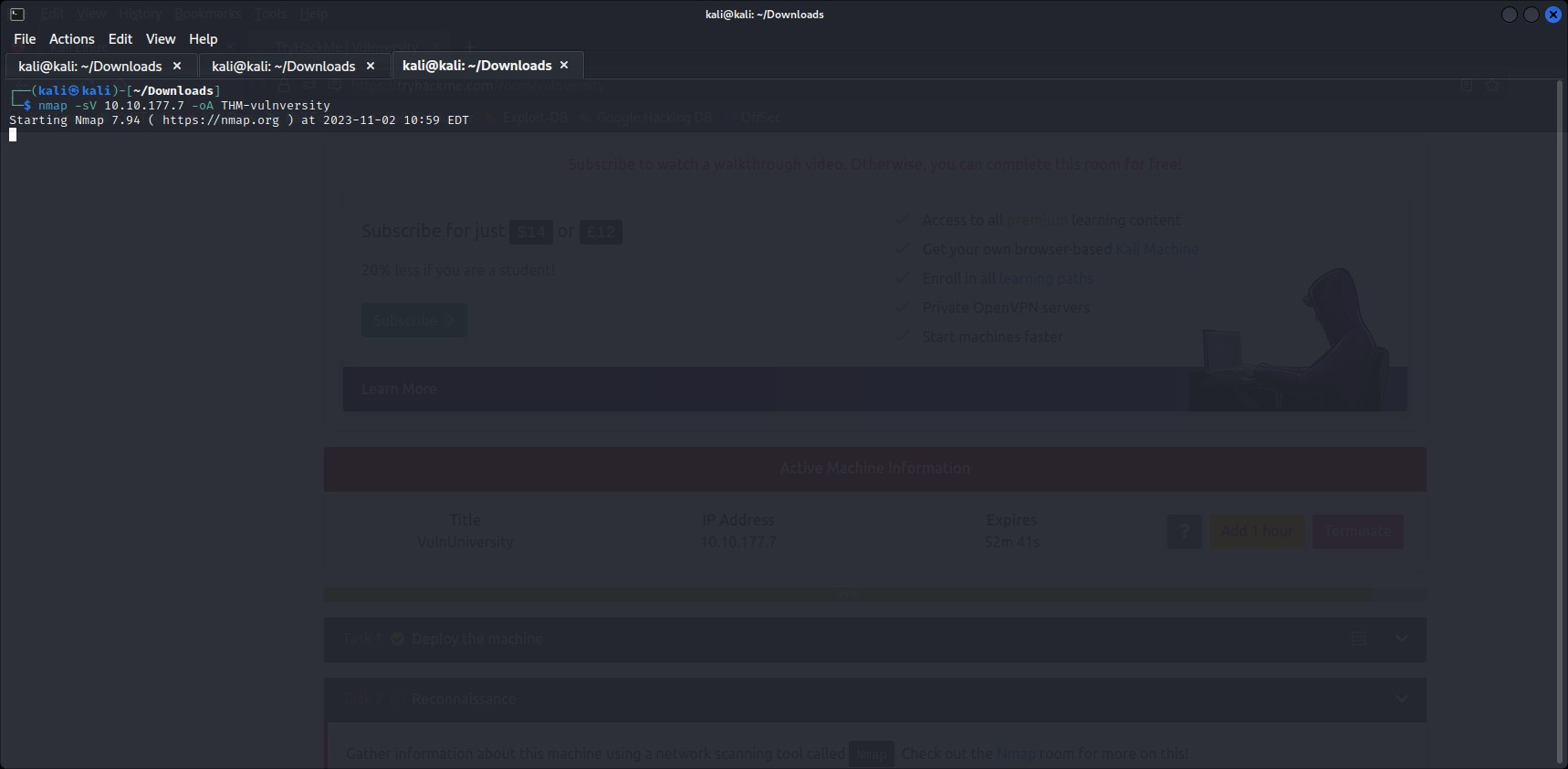
1. Lingkungan Tes

* Nama Room: Vulnversity
* URL Room: <https://tryhackme.com/room/vulnversity>

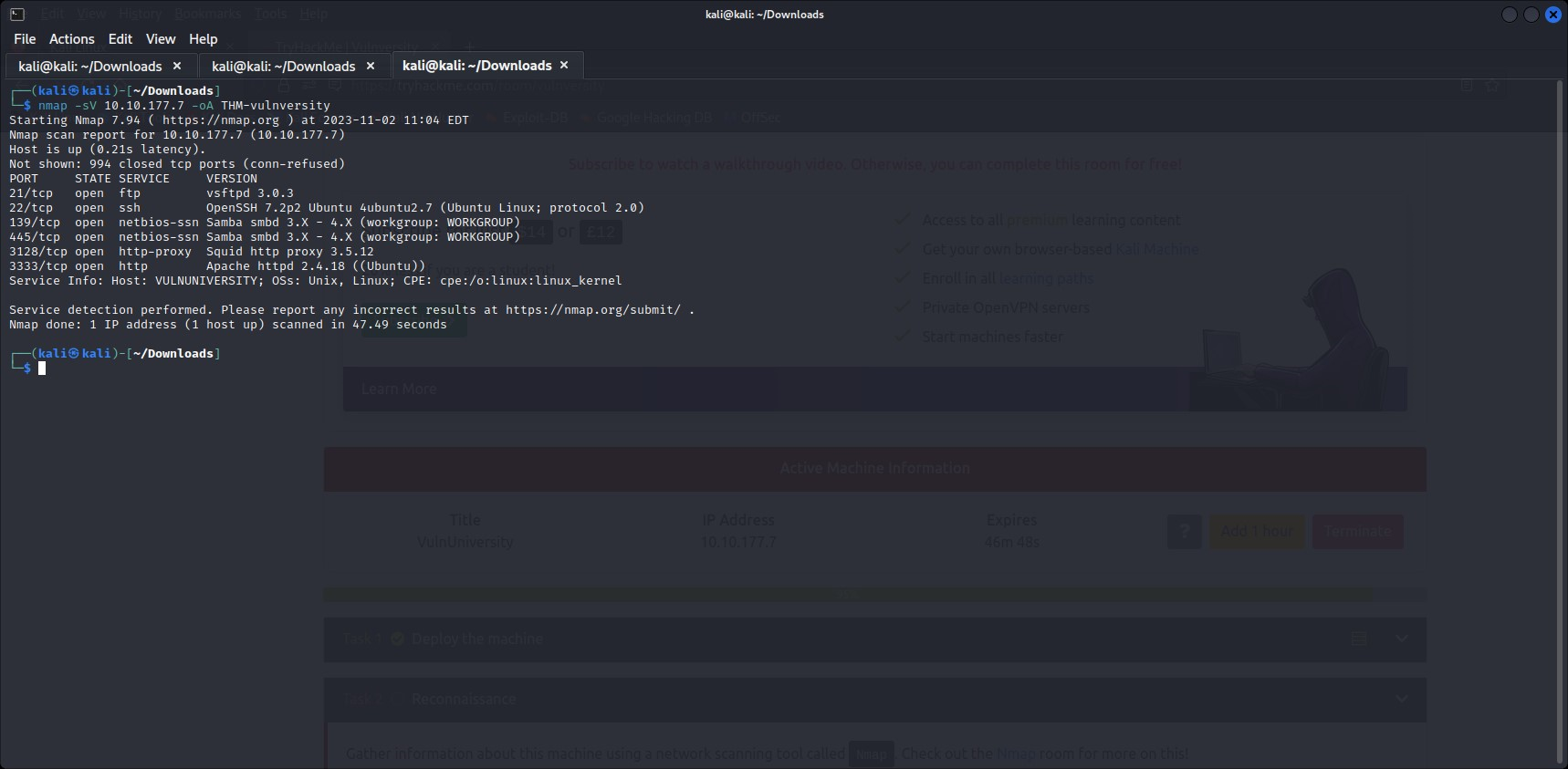
1. Langkah-Langkah Pentesting
2. Identifikasi Host

Penting untuk memahami target Anda. Saya mengidentifikasi host target dengan perintah nmap sebagai berikut:

1. **nmap -sV 10.10.177.7**



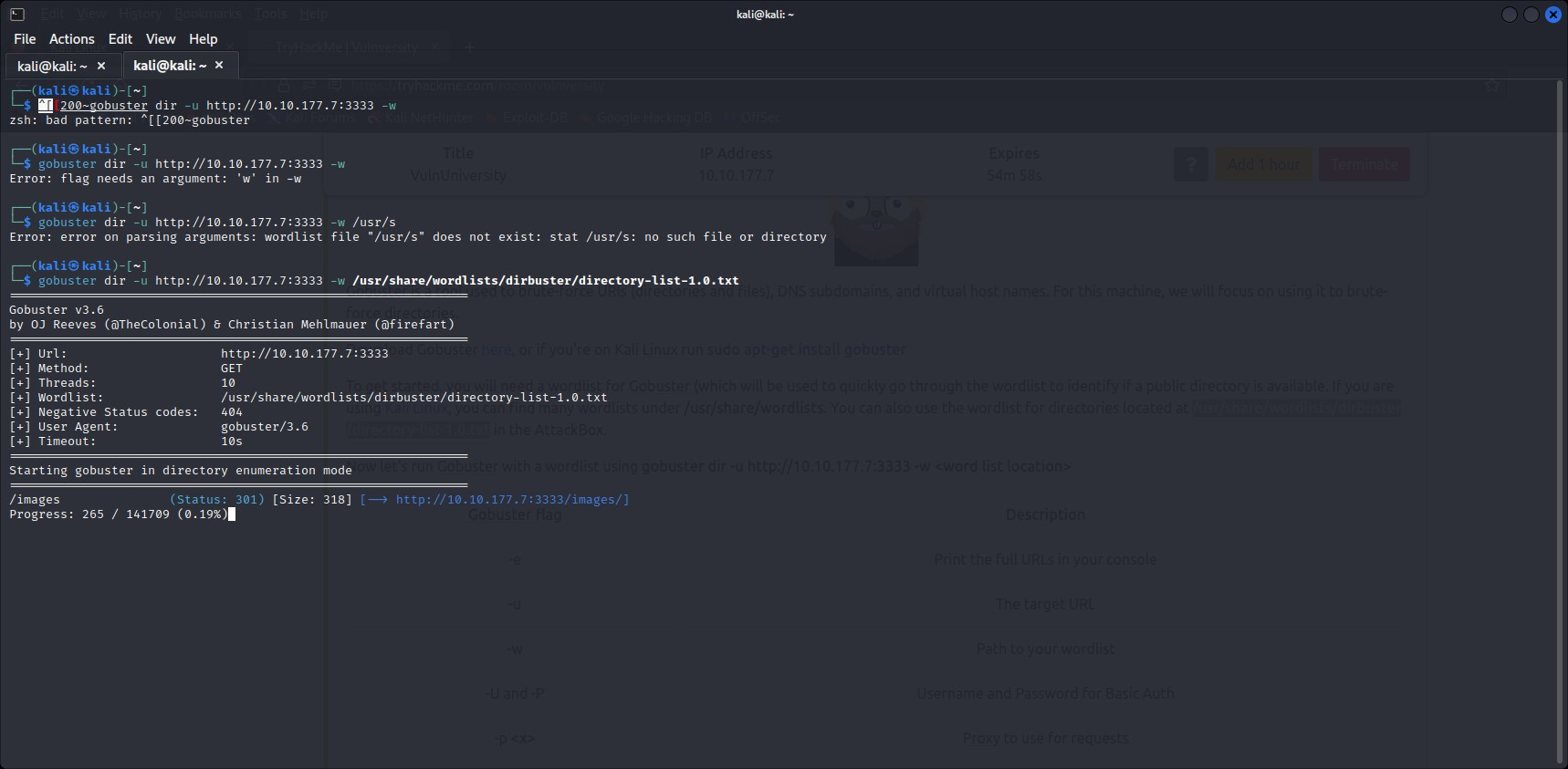
1. Hasil pemindaian nmap:



1. Pemindaian Fuzzing Direktori

Saya melanjutkan dengan melakukan pemindaian fuzzing direktori dengan menggunakan `gobuster` untuk mencari direktori tersembunyi.

* + 1. **gobuster dir -u** [**http://10.10.177.7:3333**](http://10.10.177.7:3333) **-w /usr/share/wordlists/dirbuster/directory-list-1.0.txt**



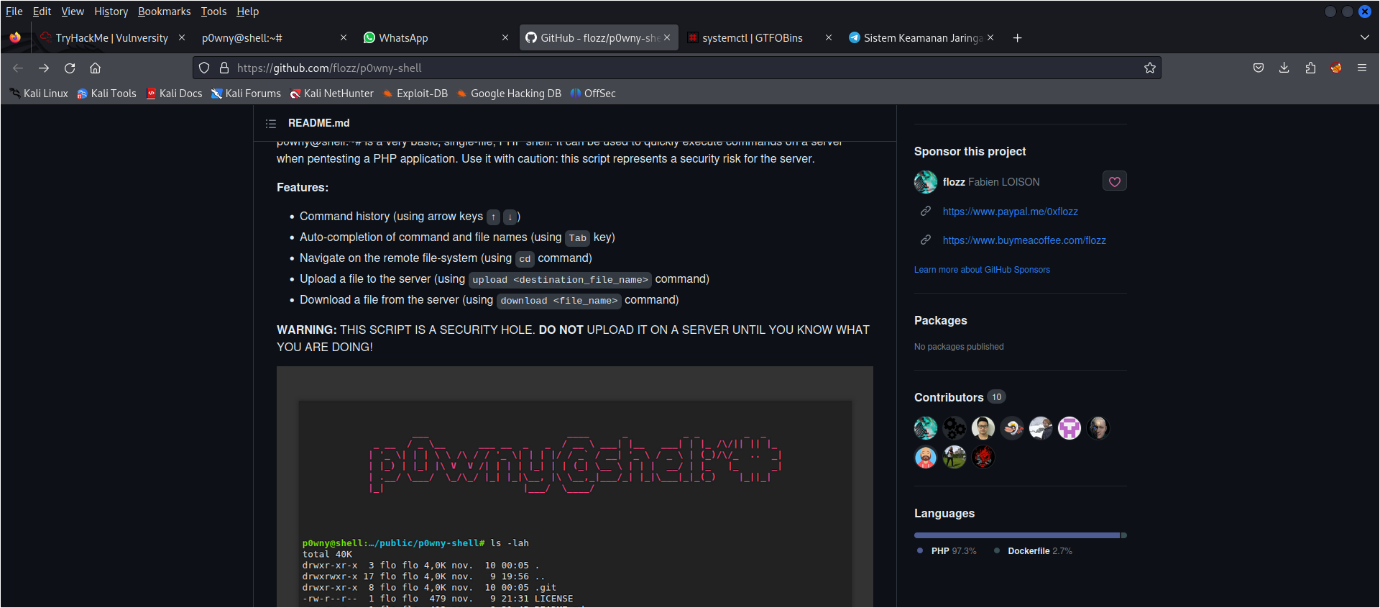
1. Temuan Kerentanan

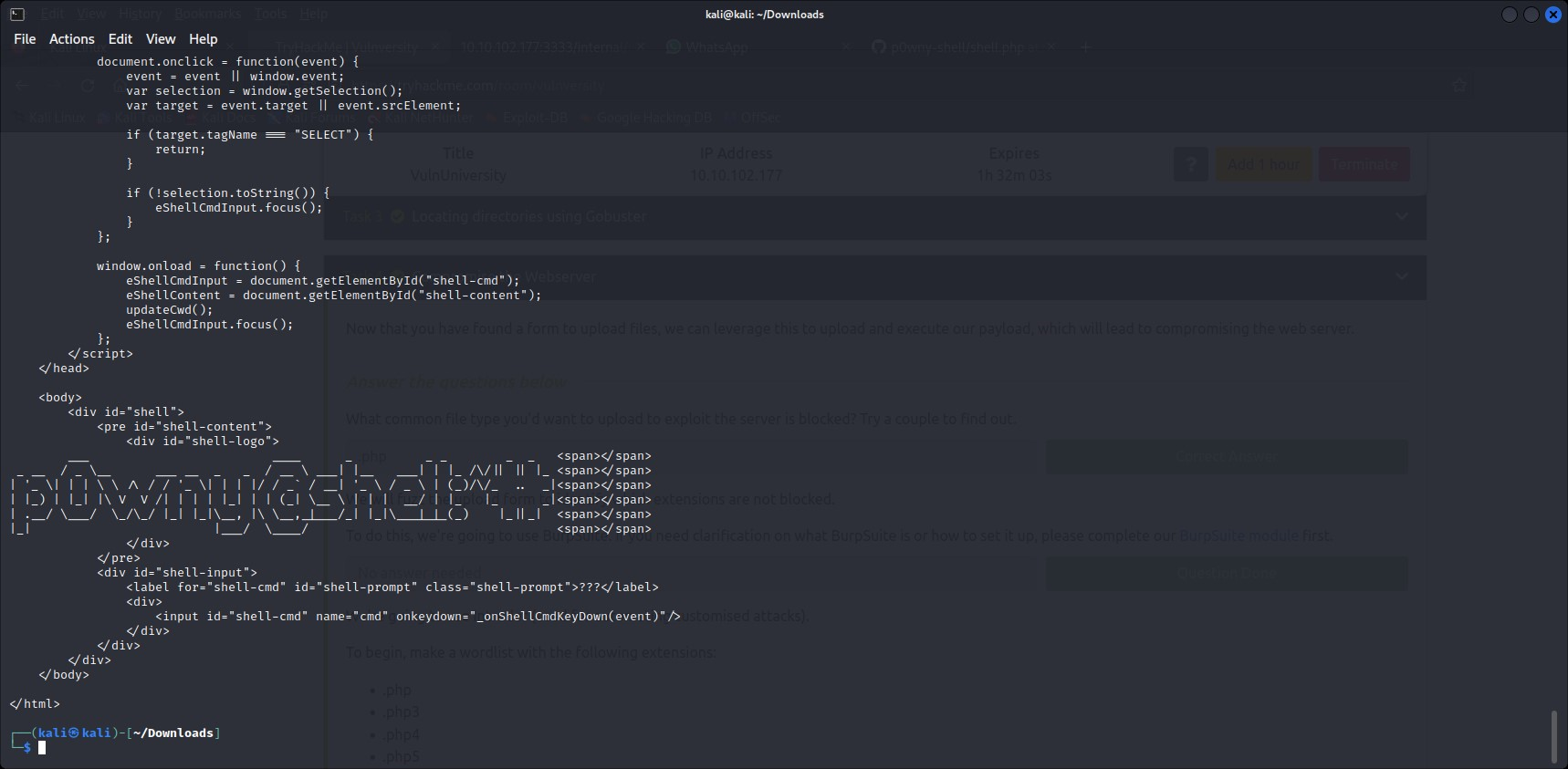
* Kerentanan yang ditemukan adalah Local File Inclusion (LFI) pada halaman `http://[Alamat IP Target]/etc/...`. Saya dapat mengakses file sistem sensitif melalui LFI.

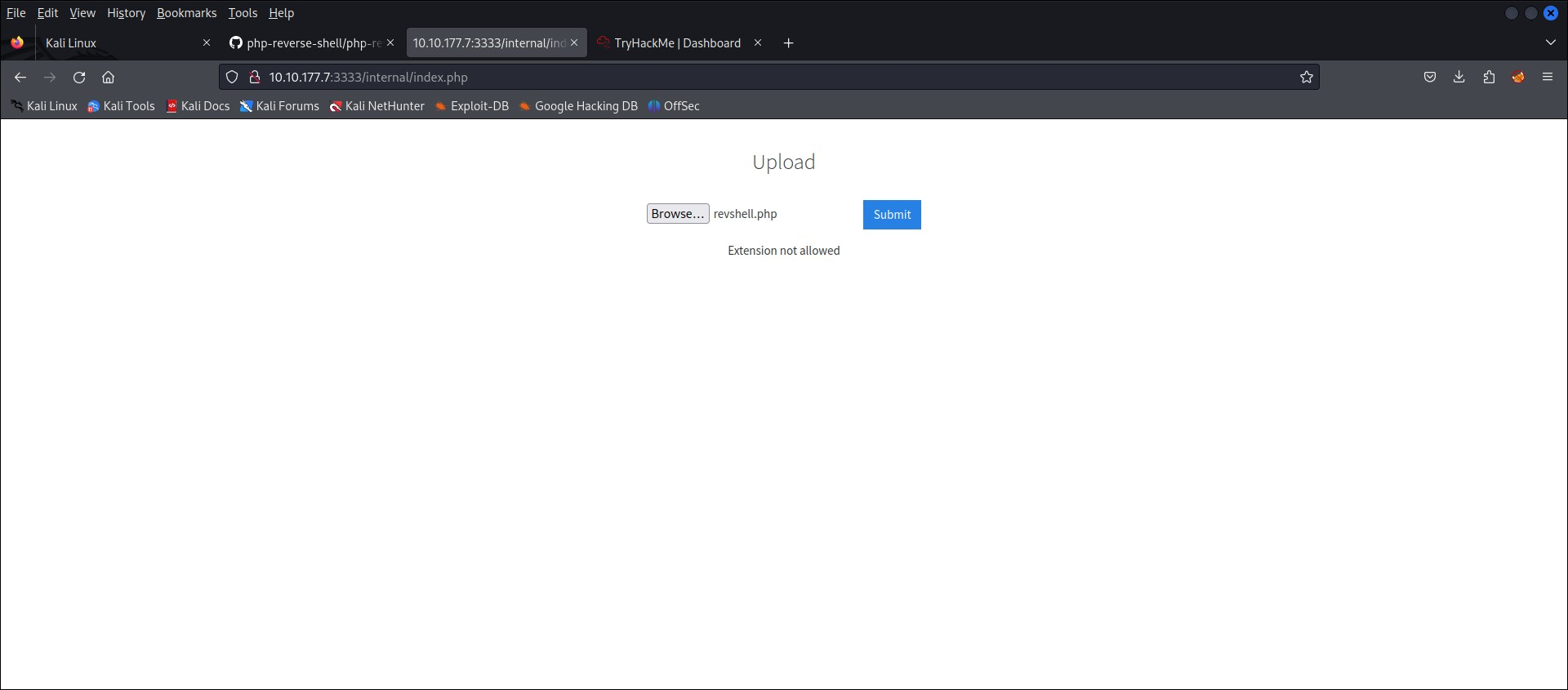
1. Mendapatkan Akses Shell

Setelah mengeksploitasi kerentanan LFI, saya berhasil mendapatkan akses shell pada sistem target. Saya menggunakan `nc` (Netcat) untuk berkomunikasi dengan shell.

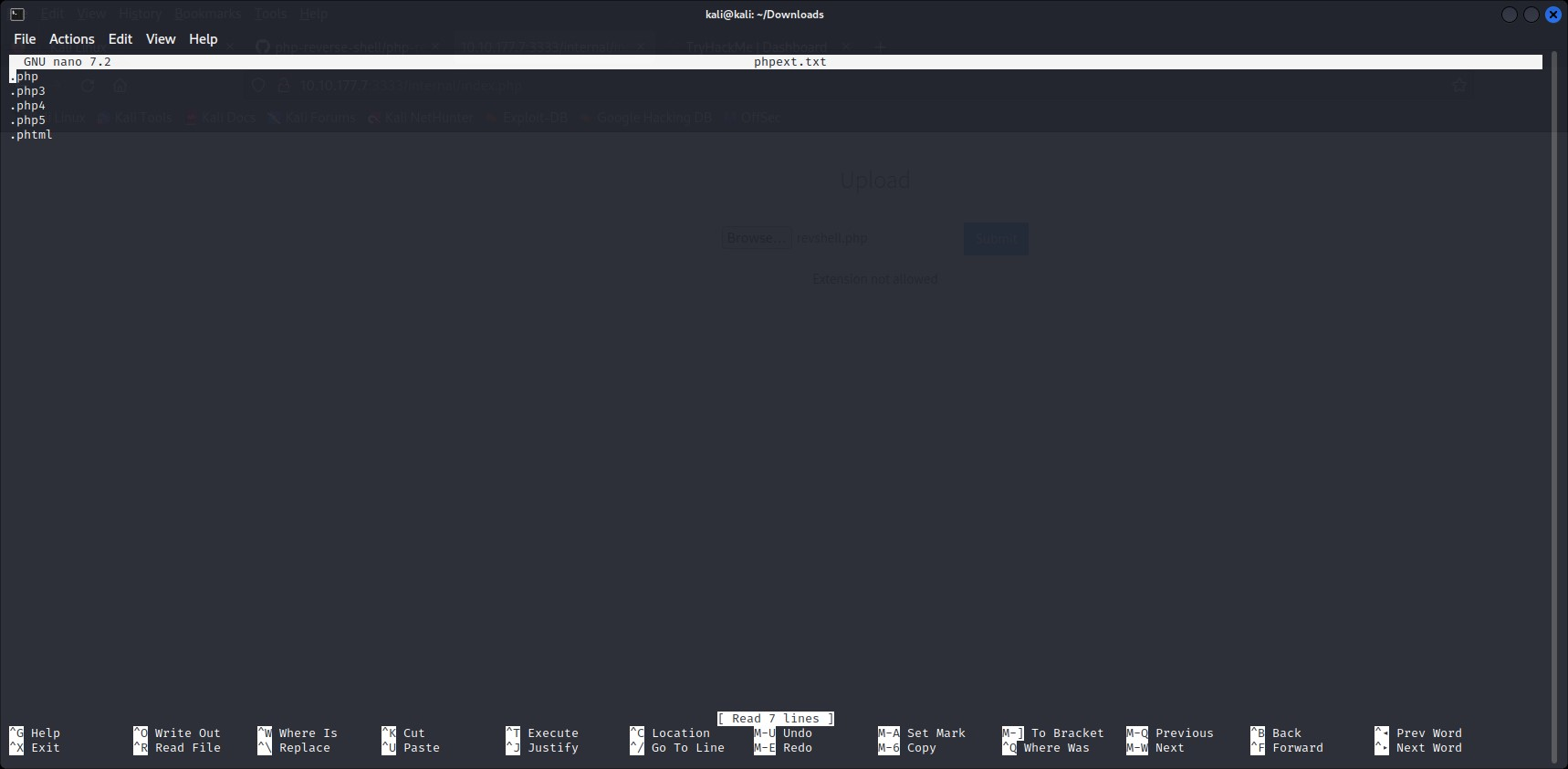
* + 1. Mendownload p0wny-shell di <https://github.com/flozz/p0wny-shell>





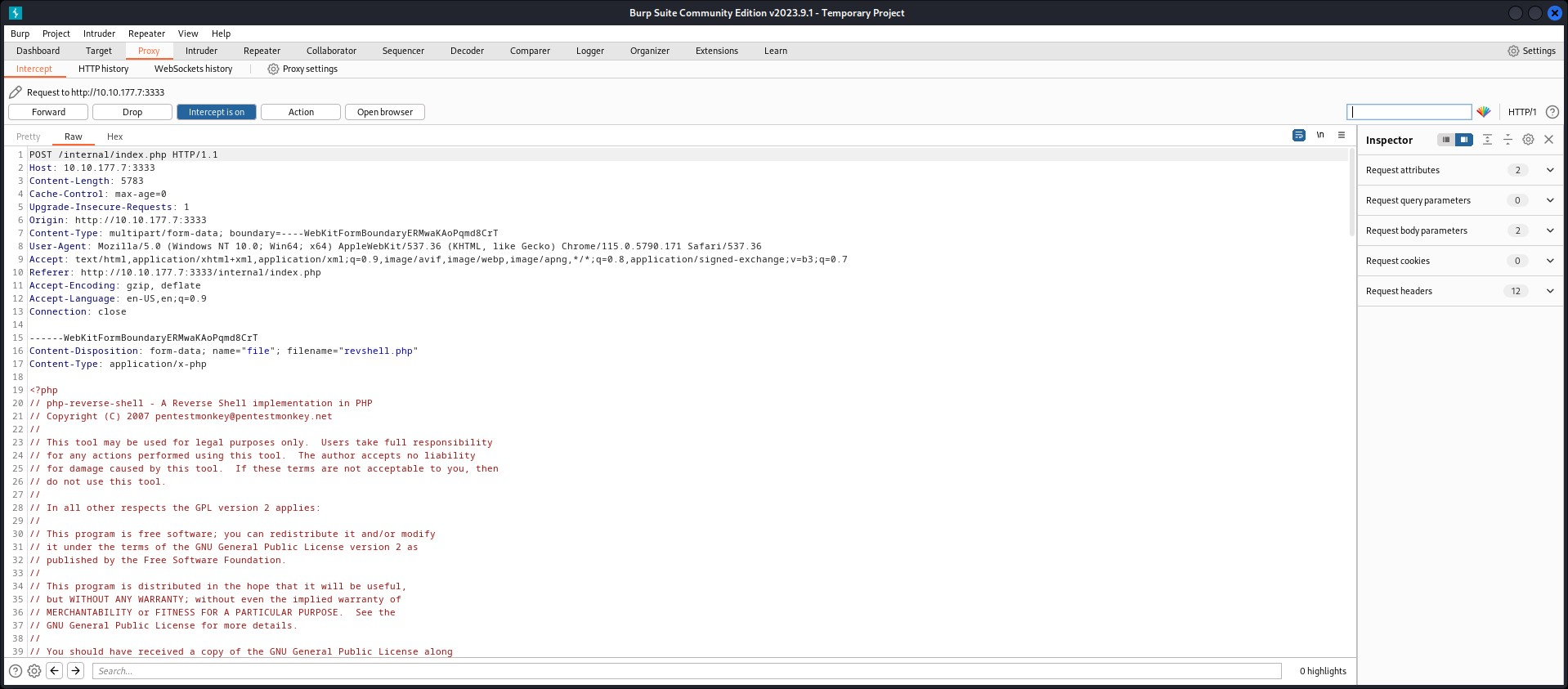


* + 1. Menggunakan Intruder (digunakan untuk mengotomatiskan serangan khusus) “**nano phpext.txt**”

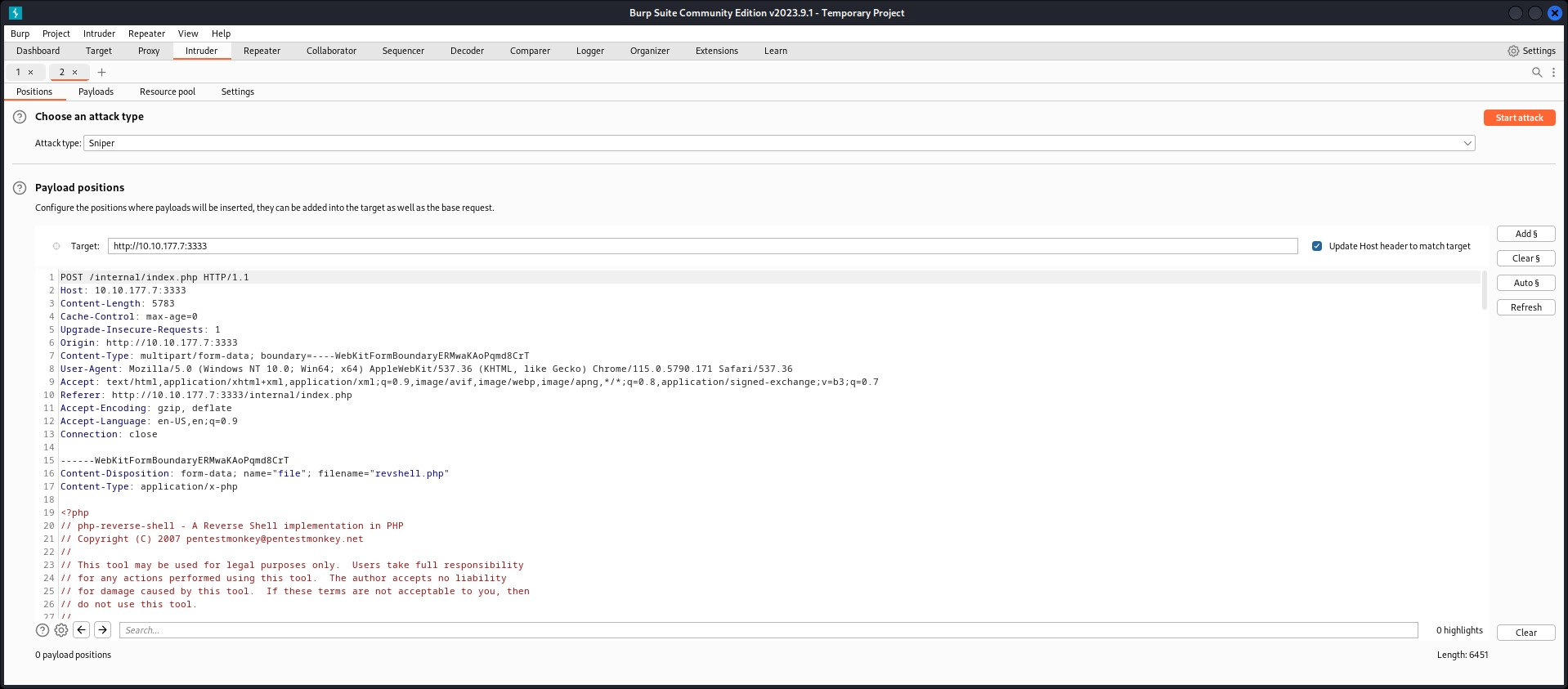


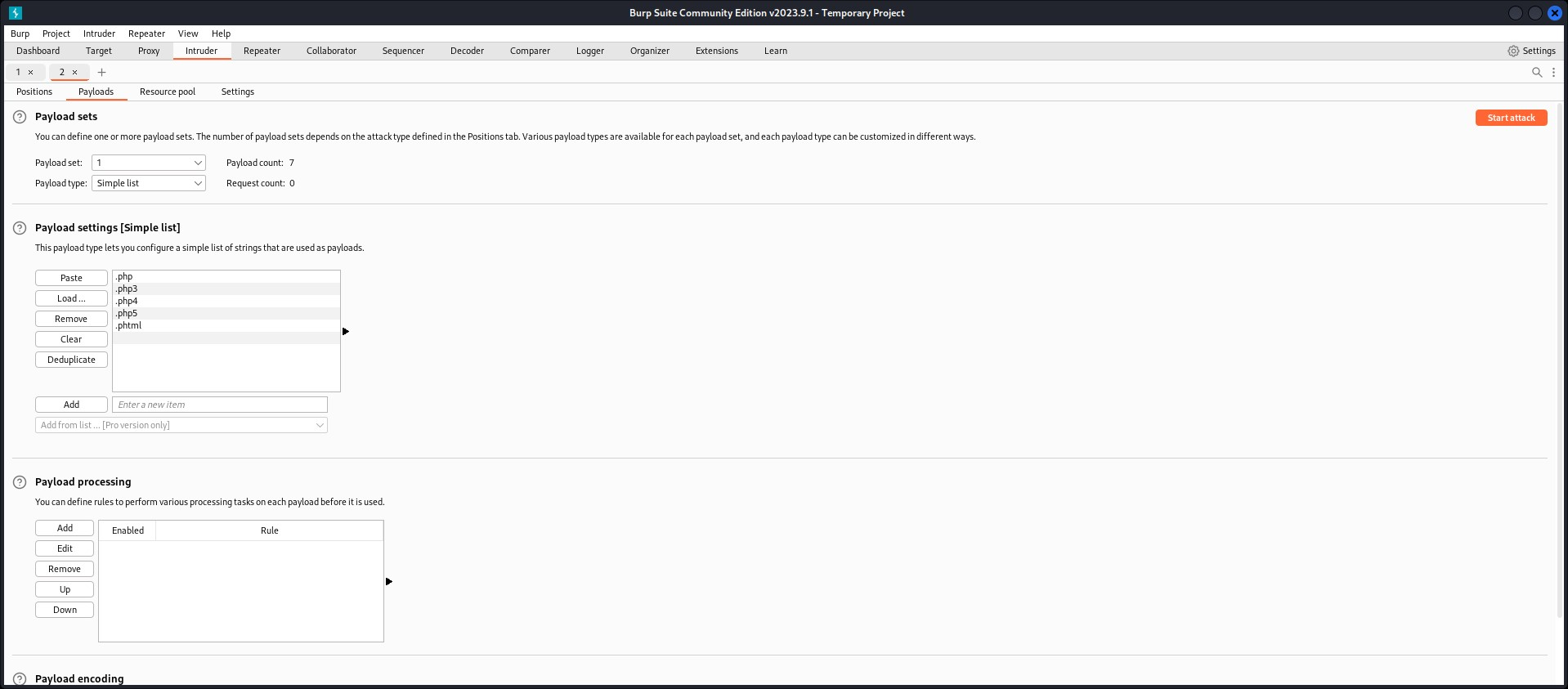
* + 1. Membuka **Burp Suite** dan memasukkan file “**revshell.php**” ke dalam aplikasi tersebut.



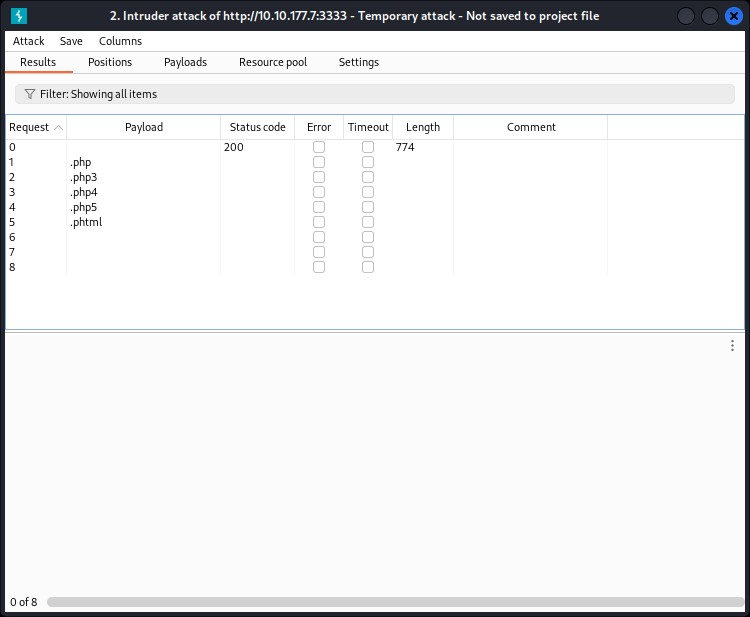


* + 1. Memindahkan **Proxy** ke **Intruder**

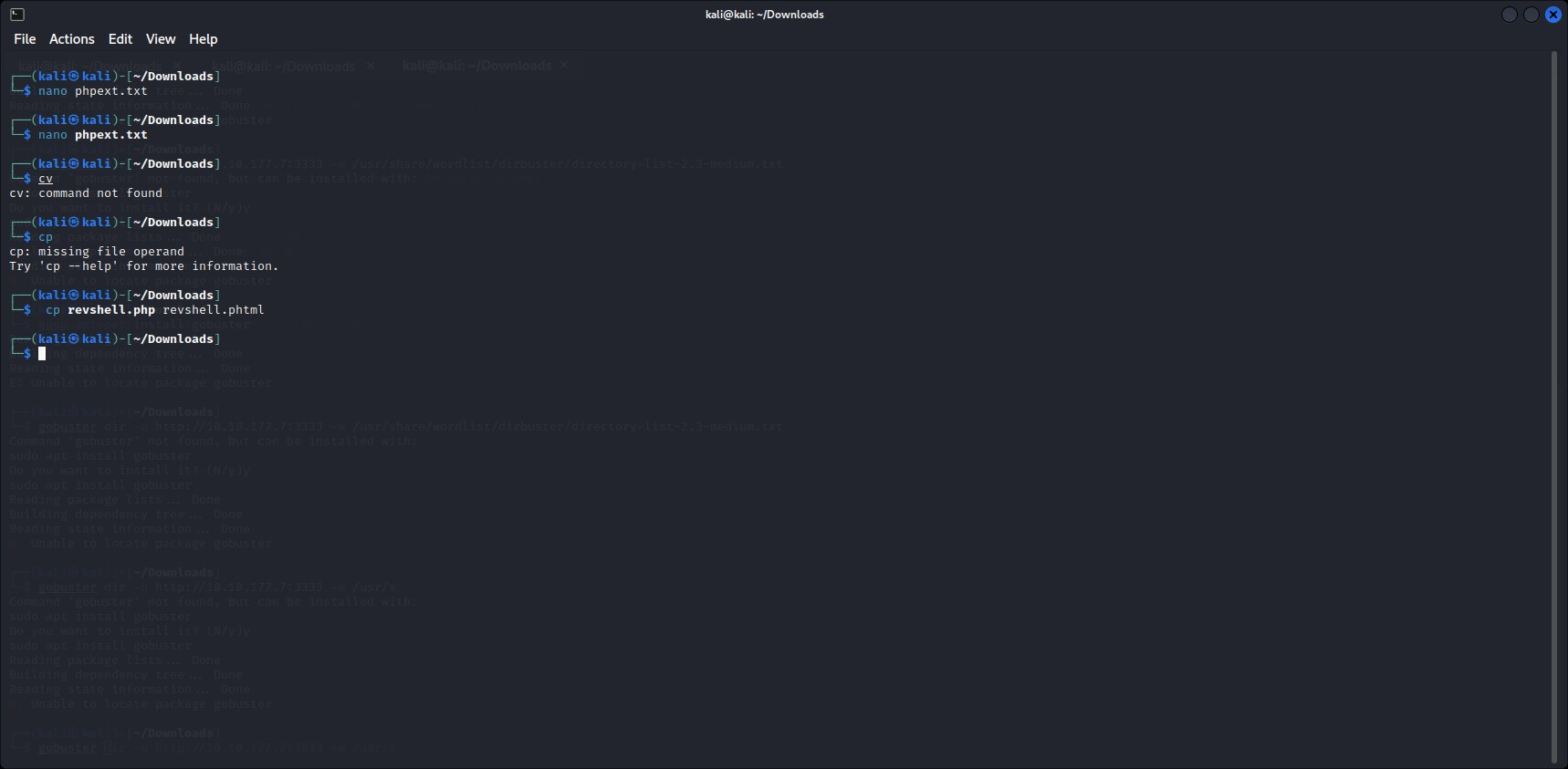


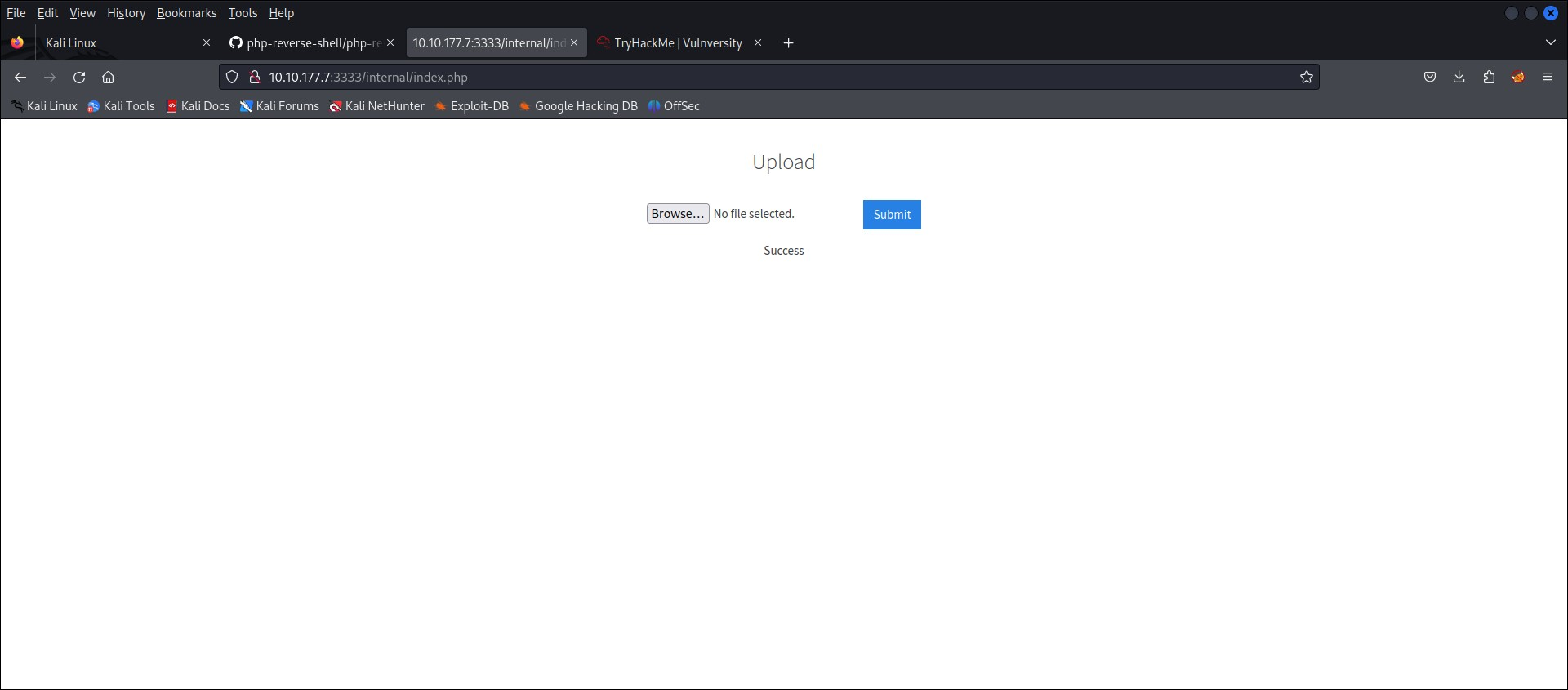


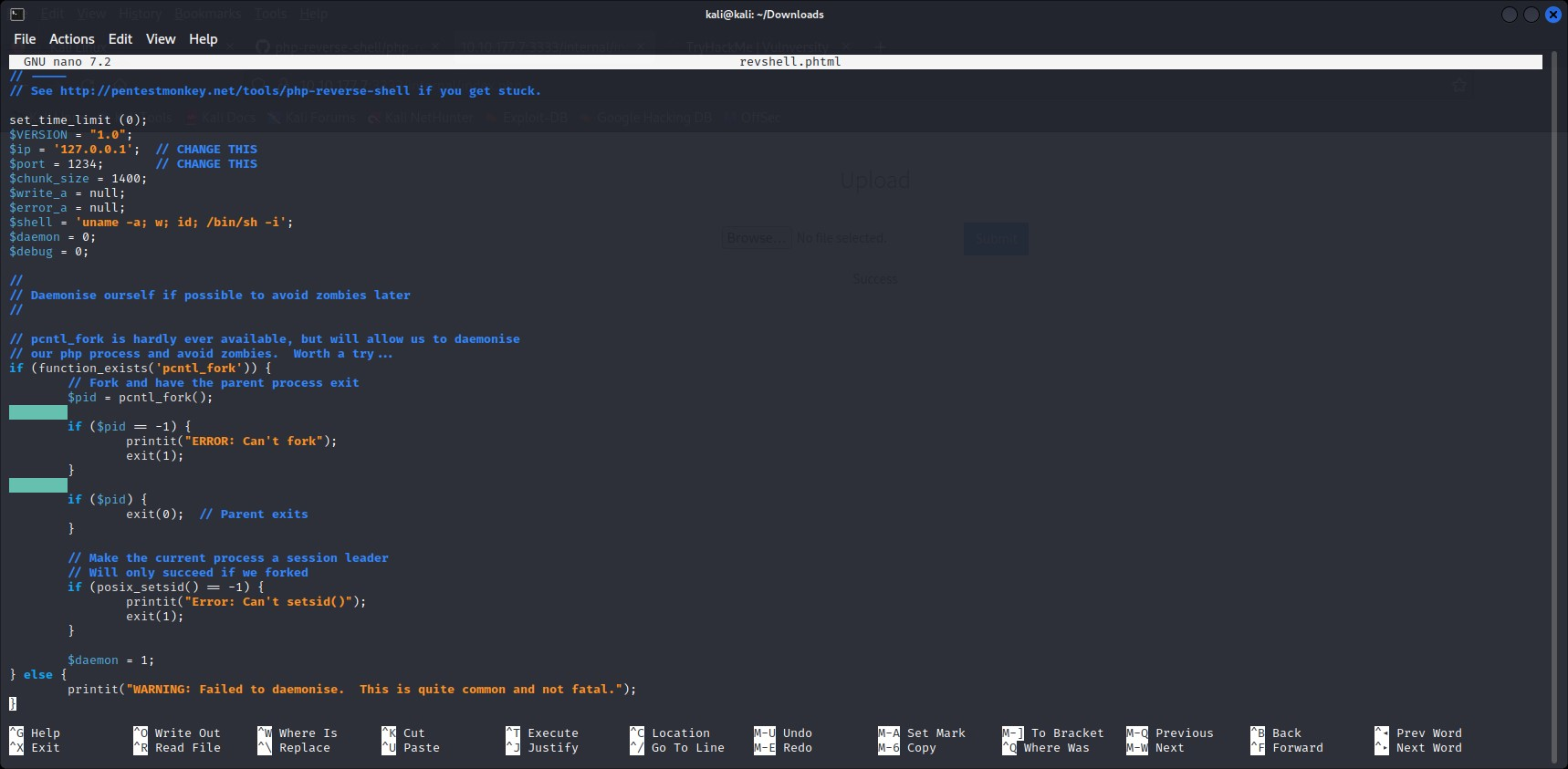
* + 1. Lalu mulai Start Attack



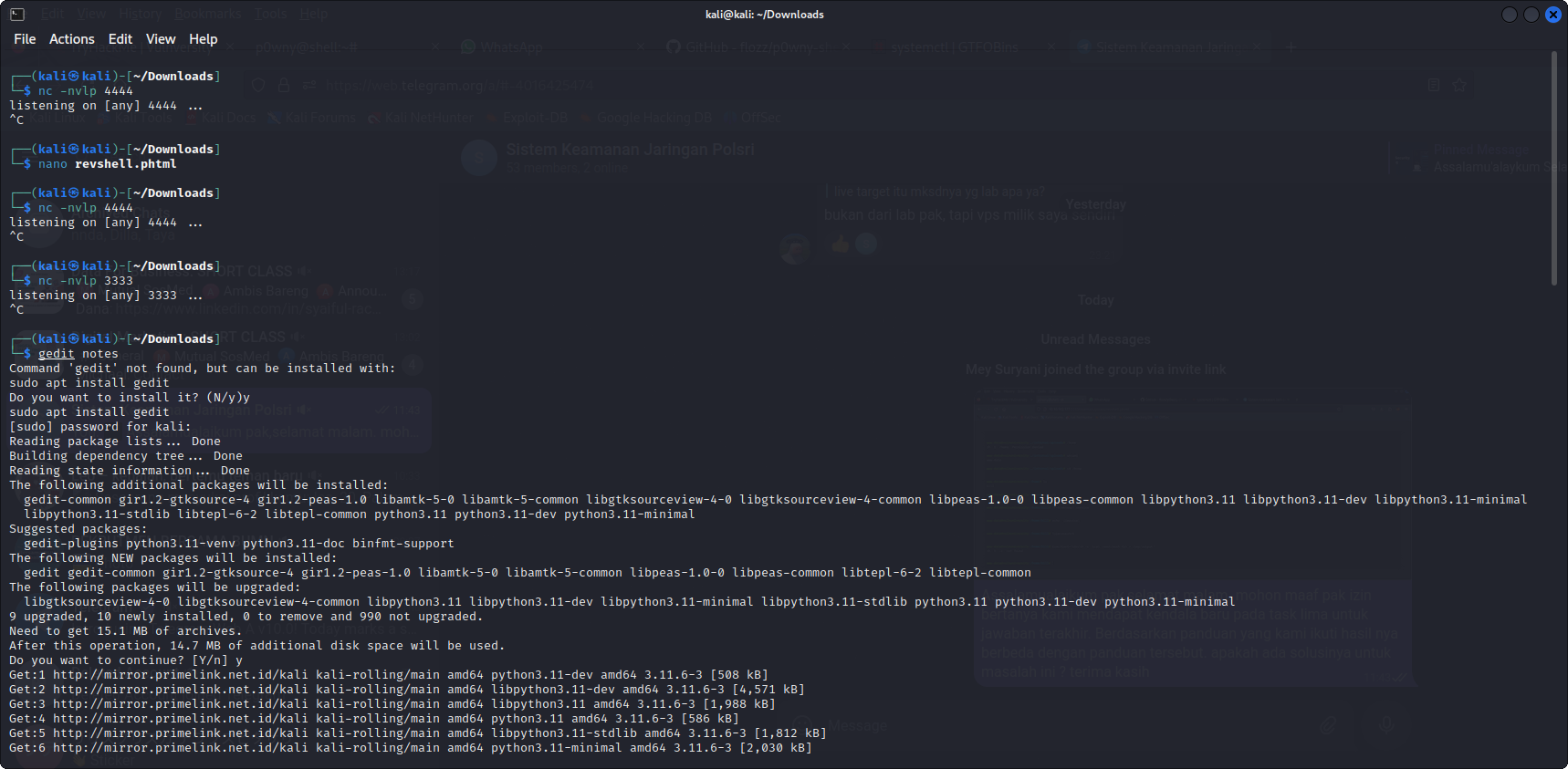
* + 1. Memindahkan format **php** ke **phtml**

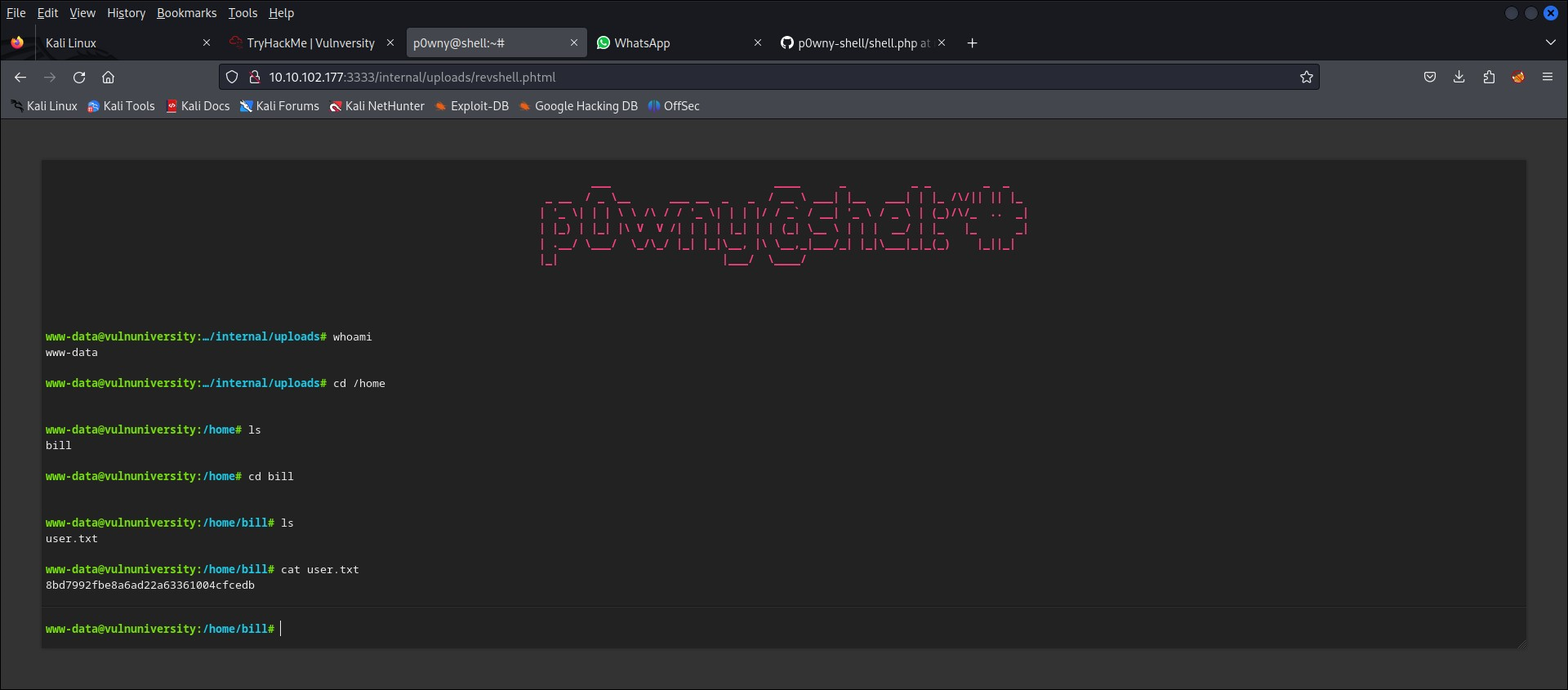






* + 1. Kemudian, di shell yang berhasil didapatkan:





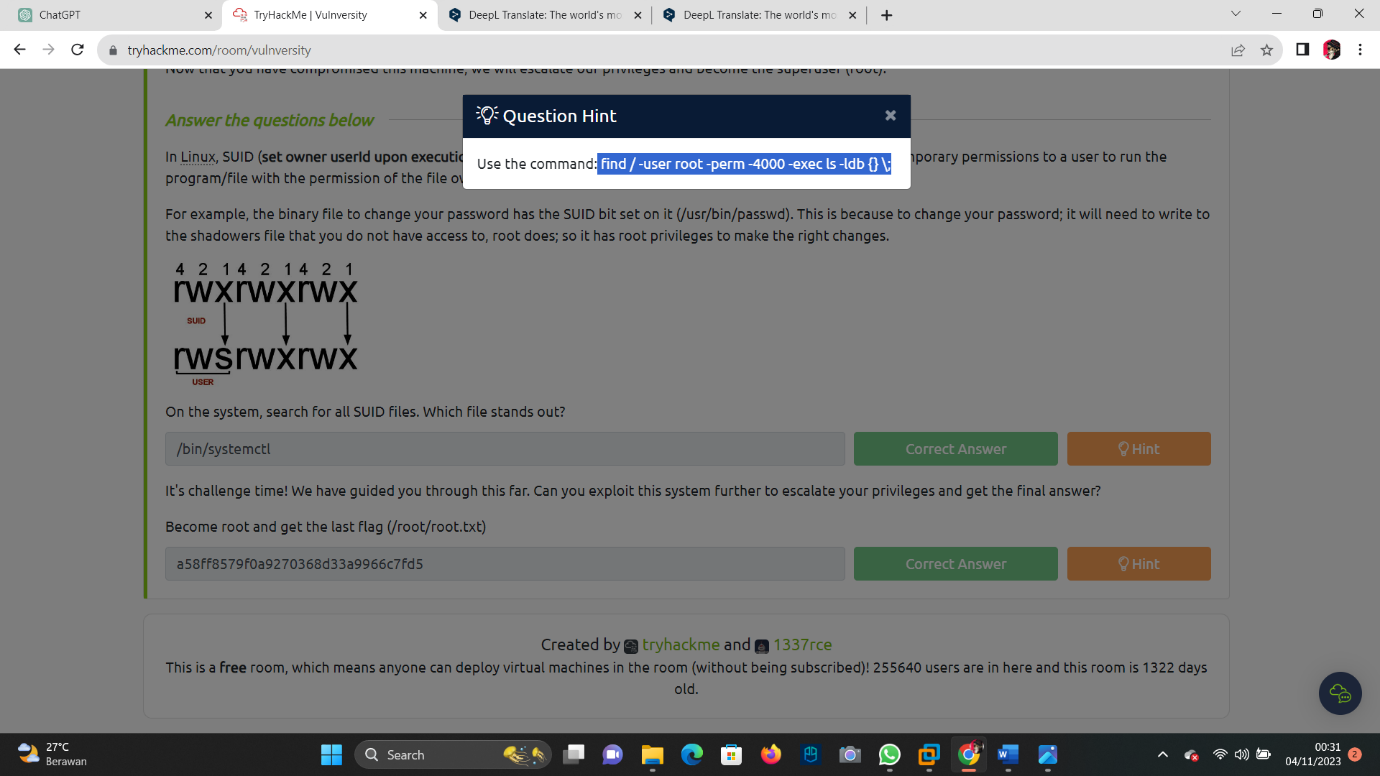
1. Eskalasi Hak Istimewa ( Privilege Escalation )

Sekarang setelah Anda membobol mesin ini, kami akan meningkatkan hak istimewa kami dan menjadi pengguna super (root).

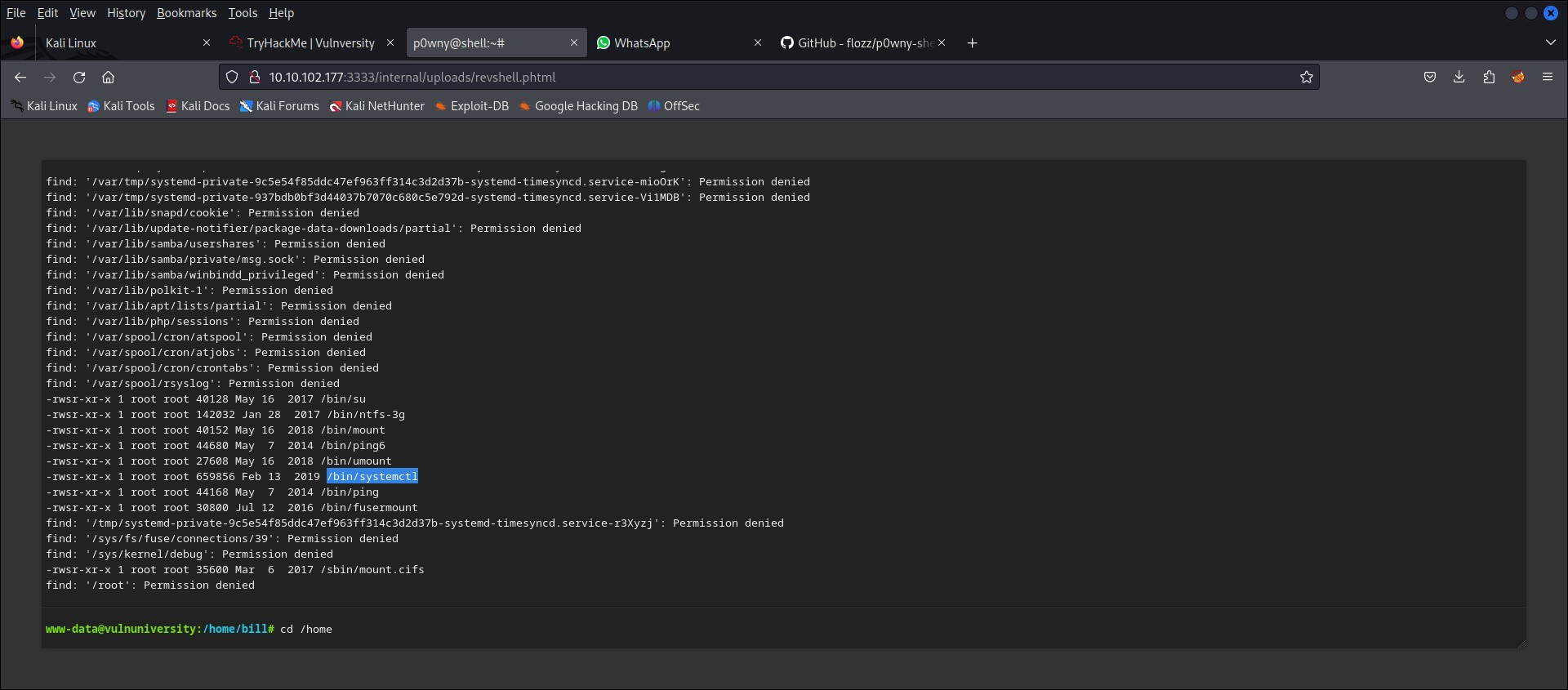
Pada Linux, SUID (set owner userId saat eksekusi) adalah jenis izin file tertentu yang diberikan pada sebuah file. SUID memberikan izin sementara kepada pengguna untuk menjalankan program/file dengan izin dari pemilik file (bukan pengguna yang menjalankannya).

1. Pada sistem, cari semua file SUID. File mana yang menonjol

* Ketik *python3 -c 'import pty; pty.spawn("/bin/bash")'* pada **p0wny-shell** setelah selesai lanjut dengan mengcopy pada soalan tryhackme tersebut



* Hasilnya akan seperti ini



1. Solusi terhadap Kerentanan

* Kerentanan LFI yang ditemukan memerlukan tindakan perbaikan berikut:
* Perbarui Perangkat Lunak

Selalu perbarui semua perangkat lunak dan sistem operasi. Pastikan tidak ada kerentanan yang telah diperbaiki oleh pembaruan terbaru.

* Konfigurasi Keamanan

Periksa dan optimalkan konfigurasi server web untuk mencegah akses tidak sah ke file sistem. Pastikan hanya file yang benar-benar diperlukan dapat diakses.

* Manajemen Hak Akses

Terapkan manajemen hak akses yang ketat pada server dan aplikasi Anda. Ini akan membantu mengurangi risiko kerentanan LFI.

* Pemantauan Keamanan

Gunakan alat pemantauan keamanan dan log untuk mendeteksi aktivitas mencurigakan dan tangani kerentanan dengan cepat.

1. Kesimpulan

Pentesting di room "Vulnversity" di TryHackMe memberikan pemahaman mendalam tentang kerentanan LFI dan langkah-langkah yang dapat diambil untuk meningkatkan keamanan sistem.