1. nmap untuk mencari open ports

2. lakukan gobuster untuk mencari directory

3. ketemu directory /admin dan ada login page

4. coba mencari-cari usernya

5. lalu pada gobuster ketemu /todo.txt dan mendapatkan potential usernya fergus

6. pada about, terdapat hint kalau pembuat web ini menyimpan seluruh fakta di web ini

7. gunakan tool cewl untuk membuat wordlist dari fakta-fakta pada web ini

6. gunakan burp untuk melakukan bruteforce login page yang ditemukan

7. ketemu credential fergus:RolandDeschain

8. gunakan credential tersebut untuk login ke /admin

Asumsi saya, bludit memiliki validasi seperti berikut untuk file upload:

- Pertama, memvalidasi apakah file tersebut memiliki extension php secara client side, jika iya maka akan ditolak langsung.

- Kedua, pada saat file sudah terkirim dari client side ke server side, server side memvalidasi jika file yang diupload memiliki extension png, maka akan dimasukkan ke dalam directory uploads/pages. Jika file tersebut memiliki extension php, maka akan dimasukan ke dalam directory tmp

https://github.com/bludit/bludit/issues/1079

9. membuat file php-reverse-shell.png lalu gunakan burp untuk merubah extension menjadi php

10. membuat file htaccess.png lalu gunakan burp untuk merubah nama file menjadi .htaccess

11. akses file php-reverse-shell.php pada directory /bl-content/tmp/php-reverse-shell.php

USER FLAG

1. pada directory /var/www terdapat versi bludit yang lain yaitu versi 3.10.0a

2. lakukan enumerating dengan command

3. ketemu user baru dengan credential hugo:Password120

4. switch user hugo denga ncommand su hugo

5. ambil user.txt

ROOT FLAG

1. gunakan sudo -l

2. user bisa melakukan (ALL, !root) /bin/bash https://www.exploit-db.com/exploits/47502

3. gunakan command sudo -u#-1 /bin/bash

4. ambil root.txt