ISCC2016-BASIC、WEB、MISC简单writeup

转载

weixin_30646505 于 2016-05-25 13:36:00 发布 128 收藏
文章标签： 网络 php
原文链接：http://www.cnblogs.com/xiao3c/p/5526656.html

RE和PWN题目的wp有大神已经放出来了，我也不擅长，就不搬了。bin求带。

BASIC

BASIC-1 50

仿射函数，百度“仿射加密法”，它讲的够清楚了。

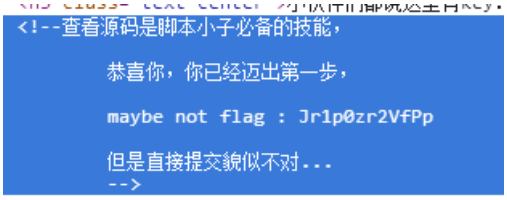
BASIC-2 50

```
Vm0wd2QyVkhVWGhVYmxKV1YwZDRXRmxVUm5kVlJscHpXa2M1
VjFKdGVGWlZNbmhQWVd4YWMxZHViRmROYWxaeVdWZDRZV01
4WkhGU2JlQk9VbTVDZVZkV1pEUlRNazE0Vkc1T2FWSnVRazlWY
WtwdlZWWmtWMWt6YUZSTlZUVkpWbTEwYzJGV1NuVlJiR2hYWW
xSV1JGcFdXbXRXTVZwMFpFWlNUbFp1UWpaV2Fra3hVakZaZVZO
cmJGSmlWR3hXVm01d1lyUldjRmhsUjBacVZtczFNVmt3WkRSVk1ER
kZWbXBXVjFKc2NGaFdha3BlVTBaYWRWSnNTbGRTTTAwMQ==
```

结尾的“=”这个特征很明显，base64解密，需要解多次，直到出现flag。

BASIC-3 50

题目说在这个页面却看不到，那么应该是藏在页面的某个地方，F12进入调试模式，找到下图的内容：



提示直接提交貌似不对，那么应该是有加密。ROT13加密，解密一下就OK了。

BASIC-1 100 心灵鸡汤

丢进OD搜了一下，发现了一个字符串。卡了一会，甚至连它的出处都搜到了。然后看了看这串字符只有大小写区别，可能是培根加密，然后解密出来得到flag。

BASIC-1 100 小伟密码

一个老旧无用的加密工具加密了文件，百度上有很多针对它的攻击方法。注意版本问题。（值得一提：如果不是专业的人员，不要自己乱搞什么加密，这就是例证。）

BASIC 200 JJ

文档是JFf*ck编码，不确定代码具体是什么，还是最好解码一下。然后找到网盘地址，下载。然后又是编码（泥煤）。查了一圈，是JJencode，然后在github上找到了脚本，解密出来，是一个JS压缩加密，再解一下吧。最后是一个alert。早知道就放进<script>标签里让它弹出了。

解密脚本获取：github搜索JJencode，第一个就是decoder，复制那个html代码，然后.....

WEB

WEB100

注入，burp拦截一下，转存之后用sqlmap可以跑出来。（自己的电脑一直被banIP，换了别人没问题，郁闷）

WEB300

代码审计。真是ping出问题了.....题目修改前交的flag，当时用&&dir就可以了，然后打开代码看一下，然后就是绕过去打flag。

WEB350-1 double kill

上传问题。测试了一下，上传的代码应该是过滤了后缀并检查了文件头。给php一句话加了图片头传上去之后，在uploads找到了但是不解析。之后用加了头的JS一句话再传，还是没访问到。注意包含地址，最后加了00截断，成功。（目的不是连接，只要能被解析就可以了。）

http://101.200.145.44/web5/index.php?page=uploads/图片ID.gif%00

http://101.200.145.44/web5/index.php?page=uploads/图片ID.jpg%00

WEB350-2 simple injection

注入问题。测试了可以注入的地方应该是用户名，用户名应该是admin了，有报错。盲注。在freebuf上有一篇类似的文章，用mid()逐位测试。也没有写脚本，用burpsuite上的暴力破解，爆出password字段的32位MD5值，解密，登陆后台即得到flag。

WEB500

这个有点费劲，先看代码。先用双向代理，曝出文件。第一次看了都没认出来是干嘛的。然后理了理，这几句是编码的流程，最后爆出来一句话的密码。然后构造payload完成注册，注意这里需要绕一下。最后带上cookie访问即可。

```php
function checkpassword($user,$pwd,$pdo){
    if($user!='admin'){
        exit('you are not admin!');
    }
    $query="SELECT password FROM user WHERE username='admin'";
    $result=$pdo->query($query);
    if ($result!=null&&$result->rowCount()!==0){
        while($row = $result->fetch()){
            if ($row['password']===$pwd){
                return 1;
            }
        }
    }
    return 0;
```

MISC

MISC 100

Wireshark打开，查看TCP包，追踪TCP流。看起来应该是一个图片。猜测出题者应该是让提取出文件然后操作的，不过在TCP追踪流中已经可以看到FLAG。

```
M:DocumentID="xmp.did:fafea4d3-3c83-2d43-9da5-c8f6f0b834ad"
M:OriginalDocumentID="xmp.did:fafea4d3-3c83-2d43-9da5-c8f6f0b834ad" photoshop:ColorMode="3"
oshop:ICCProfile="sRGB IEC61966-2.1" dc:format="image/jpeg"> <xmpMM:History> <rdf:Seq> <rdf:li
t:action="created" stEvt:instanceID="xmp.iid:fafea4d3-3c83-2d43-9da5-c8f6f0b834ad"
t:when="2015-08-14T07:08:07+08:00" stEvt:softwareAgent="Adobe Photoshop CC (Windows)"/> <rdf:li
t:action="saved" stEvt:instanceID="xmp.iid:b87042de-8708-be43-83af-8851384adf34"
t:when="2015-08-14T07:08:07+08:00" stEvt:softwareAgent="Adobe Photoshop CC (Windows)"
t:changed="/"/> </rdf:Seq> </xmpMM:History> <photoshop:TextLayers> <rdf:Bag> <rdf:li
oshop:LayerName="flage{w23e3 6ktr04}" photoshop:LayerText="flage{w23e3 6ktr04}"/> </rdf:Bag> </
oshop:TextLayers> </rdf:Description> </rdf:RDF> </x:xmpmeta>
acket end="w"?>...XICC_PROFILE......HLino....mntrRGB XYZ .....    ...1..acspMSFT....IEC
.....-HP  .....cprt...P...
c.....lwtpt.....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued.
```

去掉空格提交。flag：w23e36ktr04

MISC 200

先用16进制编辑器查看一下吧。搜索常见的ASCII，搜到pass时，找到了密码：bfsiscc2016。

```
4 6D 03 97 18 37 D5 F4 A9 87 CE 32 E7 03 03 44 6F 01 40 J\..2tm...7.....2...Do.@
2 AA 80 99 9C 25 DD 04 85 54 22 14 6F 84 B2 B9 0C 4C 2C .v.TN.....%...T".o....L,
D A2 D2 C8 EC ED 41 E1 EC D6 35 17 B7 D9 26 E7 7F F2 FF :L...}.....A...5...&....
F D7 A9 68 FF 5E 94 FD 68 FE A8 C8 AE 8E 45 BA 95 9B A2 ..cs.o..h.^..h.....E....
0 70 61 73 73 3A 62 66 73 69 73 63 63 32 30 31 36 20 20 ...   pass:bfsiscc2016
5 FF FB 92 00 02 00 02 D6 43 58 03 2C 12 E0 5C E8 6B 00 G.............CX.,...\.k.
1 7B A7 88 6D E9 83 13 6B C1 97 A1 28 10 38 83 95 B7 AF a.\...{..m...k...(.8....
0 98 D1 54 3C E1 03 8B 24 C5 BF 1C 63 99 F4 B2 50 4A 8A A.Srs...T<...S...c...PJ.
```

应该是MP3stego了，下载相应的工具，解密出隐藏的txt。

```
Flag is
SkYzWEkOM1JOWlNHWTJTRktKUkdJTVpXRzVSVOU2REdHTVp
HTlpZPQ== ???
```

等号结尾一般是base64补位用的，base64解一次，还有等号。再用base64解，出错.....实在想不到还有别的加密带=号了，就想着有没有base32。结果真有。在国外网站找到base32解密。最后，是这样解出来的：base64一次，之后用base32再解一次。

base64：SkYzWEk0M1JOWlNHWTJTRktKUkdJTVpXRzVSV0U2REdHTVpHT1pZPQ==

base32：JF3Xl43RNZSGY2SFKJRGIMZWG5RWE6DGGMZGOZY=

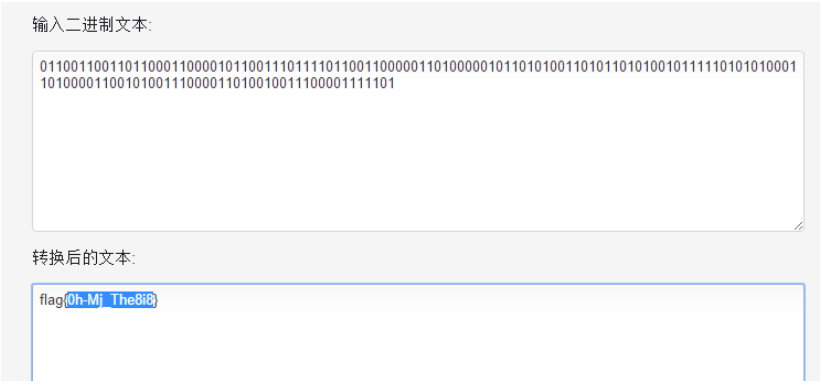
flag：lwtsqndljERbd367cbxf32gg

MISC 300毕业论文

下载得到doc文件，用相应程序打开另保存为docx。改后缀为ZIP，解压，直接找document.xml。用notepad++打开，观察结构：1.spacing有-2和2之分；2.每个spacing之后仅有一个汉字（也就是对应只算一次）

```
<w:rPr>
<w:spacing w:val="-2"/>
<w:sz w:val="10"/>
</w:rPr>
<w:t>
论</w:t>
</w:r>
<w:r>
<w:rPr>
<w:spacing w:val="2"/>
<w:sz w:val="10"/>
</w:rPr>
<w:t>
文</w:t>
</w:r>
```

利用正则将<w:spacing w:val="-2"/>变成0，将<w:spacing w:val="2"/>变成1，利用<.*>清除所有括号。统计出来少了一位。然后8位一行排列一下，每行是一个字符。考虑到最后答案是ASCII字符串，必定不会出现大于0x80的字符。但是字符串中出现了大于0x80的字符，于是人工在第一次出现大于0x80字符的那行的最前面增添了一位0，一次延后一位，所有结果合乎逻辑。转换成字符串得到flag。



MISC300-2加密协议

给了几个txt文档，看样子应该是数据包的转储。用wireshark导入16进制转储，看出来是ISAKMP协议包(主要是IKE协商)。按照次序整理好文件，截获数据对应main模式前4个包，密文对应第五个包。格式wireshark已经整理好了。看出来主要的算法是DES，采用的预共享密钥模式，nonce、双方的公钥还有其他系列的参数都可以提取出来。然后参考RFC2409，http://www.ietf.org/rfc/rfc2409.txt，算出DH的共享密钥、解密。

转载于:https://www.cnblogs.com/xiao3c/p/5526656.html