

安恒赛php_CTF-安恒18年十一月月赛部分writeup

原创

[weixin_39946534](#) 于 2021-01-13 03:47:44 发布 43 收藏

文章标签: [安恒赛php](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_39946534/article/details/112873433

版权

安恒十一月月赛writeup

昨天做了一下十一月的题目, 不才只做出来几道

签到web1

这个是十月的原题, 因为忘了截图所以只能提供思路

Web消息头包含了登陆框的密码

输入密码后进入上传页面, 上传一句话木马1.jpg,

使用burp将上传文件名改为1.php.jpg

然后post数据发现已经getshell

Flag就在上一层目录里所以post数据:system('dir ../');

得出flag为: flag{698539765730b69026796420b9201e03}

具体可以参考: <https://www.jianshu.com/p/e1af7cc3483d>

MISC1-Numeric password

题目:

解题过程:

起初并不知道这是啥, 然后百度了一下下面的名词, 发现

有点意思, 然后进去看看, 发现了对应关系,

然后一个一个找出来, 其中21世纪就是21, 是在其他数字记忆表找到的, 72-企鹅.....

72 78 67 73 93 67 25 20 69 20 20 70 69 68 67 70 24 21 27 67 27 20 25 27 21 72 26 20 18 20 70 70 67 70 72
23 20 95

然后试着去换成ASCII码看看, 发现

出现了不可见的ASCII码，那flag肯定不是这个，既然数字已经给定了，编码最有可能是凯撒移位

Payload:

写个脚本爆破一下

```
exp =
```

```
[72,78,67,73,93,67,25,20,69,20,20,70,69,68,67,70,24,21,27,67,27,20,25,27,21,72,26,20,18,20,70,70,67,70,72,
```

```
flag=""
```

```
for i in range(1,127):for j in exp:
```

```
flag+=chr(j+i)print(flag)
```

```
flag=""
```

flag为: flag{a72c22dcbad639a92793f8202ddadf52}

MISC2-我的公子在何方

题目:

解题过程:

压缩包是加密的，打开password，直接输入提示错误。

Base64解一下

读一下txt内容

他有提示说：其载体图像是24位的BMP格式图像

百度一下：载体图像是24位的BMP格式图像隐写工具

下载这个工具

尝试打开图片发现需要密码

然后txt提示：并且密码是与图片主人公演绎的剧中相关的人物

百度搜图

天仙配...其实我根本不知道相关人物是谁，然后百度一下演员表一个一个试吧

发现dongyong就是密码，

什么也没，那应该还是加密了...

密码也不知道是什么，看了题解才知道是dongyong...

Payload:

所以flag为flag{97db6057a9a113c3e0a2bfb188a92698}

CRYPTO2-仿射

题目:

解题过程:

解一下，已经提示了b=7那这就好办了，直接爆破a就行

网站也提示了a的取值

在a=9的时候出现了flag

题目要求提交md5所以

Payload:

flag为: flag{e8cb7b46bcf72d62e74100dd19bc63c6}

REVERSE2-Generate

题目:

题目要求输入一个数字然后给出flag

解题过程:

到ida看一下程序的逻辑

程序刚开始有一个Getinput，跟进看一下

提示输入信息，输入到DstBuf，输入的数是16字节然后转换为整数，然后传到int型中

无符号整数v11进入循环，循环32次

V8初始值为0，然后与v11异或，再和异或

疑惑的条件即是判断v7的范围是否在@以上Z以下，且不等于”_”,”{”,”}”,如果不满足条件提示错误退出，意思就是结果是有范围的，结果在A-Z 和{ }_

接下来的操作是

最后的结果会赋给byte_408040

并且v8会和bajt_404024再次异或，byte_404020为字节

最后每次循环结束都把v11向后移一字节，然后继续进入循环

然后循环完后用start函数检测一下结果的开头

Start为

Exp

使用Z3约束解决

X=3658134498

Flag为flag:FLAG{__ZZLOZEZ_Z__AAPHTZIZ__}

原创文章，转载请标明出处：<https://www.cnblogs.com/pureqh>