i春秋 “百度杯”CTF比赛 2017 二月场 爆破-1、爆破-2、爆破-3

原创

「已注销」 于 2018-09-06 08:36:26 发布 996 收藏

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82453482

https://www.ichunqiu.com/battalion?t=1

爆破1

题目提示说flag就在某六位变量中

```php
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
  die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

然后我就用`python`写了个爆破的代码，但是每一位有63种可能，一共是63^6，运算量太大了，无奈看了一下writeup，才知道是要输出PHP中的一个特殊变量`$GLOBALS`，在输出结果中查找flag即可

爆破2

题目提示为flag不在变量中

这道题不会做，还是看了writeup，使用`file`或者`get_file_contents`函数来获得`falg.php`文件的内容即可，这两个函数的不同之处在于，使用`file`函数可以把注释语句也数出来，但是使用`file_fet_contents`函数时，由于它把`flag.php`文件作为字符串输出，所以注释语句不会显示出来

爆破3

题目提示为这个真的是爆破

此题的关键在于`substr(md5($value),5,4)==0`

只要绕过了这一个就能做出来了，我想了很久，也没找到解决办法，还是看了writeup，得到了一点提示，说当value为数组的时候该条件就会被满足`value[]=ea`

真的是没想到还能这样提交数据，还是懂的太少