# 暑期练习web1：MISC web1（i春秋）

原创

何家公子 于 2018-07-30 16:35:16 发布 349 收藏

分类专栏： ctf web 文章标签： web ctf php



本文链接：https://blog.csdn.net/qq_41618162/article/details/81287509




ctf 同时被 2 个专栏收录

32 篇文章 0 订阅

订阅专栏


web

32 篇文章 0 订阅

订阅专栏

题目的hint：flag就在某六位变量中。

我们打开题目：

```php
<?php
include "flag.php"; //包含flag.php这个文件
$a = @$_REQUEST['hello'];//$a这个变量请求变量hello的值
if(!preg_match('/^\w*$/',$a )){//正则表达式，匹配字符串，\w表示字符<数字+下划线，*代表有若干个\w字符组成。
  die('ERROR');//不匹配则输出ERROR
}
eval("var_dump($$a);");//如果匹配输出\$\$a的值
show_source(__FILE__);
?>
```

先来一波知识点普及：

1. include"flag.php" :则表示已经固定flag.php,这时候我们要去寻找其他我们能控制的东西，比如a
2. 而$_REQUEST则具有POST[] 和GET[]的功能,但是REQUEST[]比较慢。通过post和get方法提交的所有数据都可以通过REQUEST数组获得
3. if语句中是一个正则匹配，^是这个表达式的起始符号；\w表示任意一个字符(a-z、0-9); * 表示匹配前面的子表达式零次或多次。例如，zo* 能匹配 “z” 以及 “zoo”。 * 等价于{0,}；最后的$表示末尾。所以这个判断语句就是 **输入到a中，的如果全是字符，则为真**
4. var_dump:显示关于一个或多个表达式的结构信息，包括表达式的类型与值。数组将递归展开值，通过缩进的数组形式显示其结构，例如：

```
<?php
$a = array(1, 2, array("a", "b", "c"));
var_dump($a);
?>

以上例程会输出：

array(3) {
  [0]=>
  int(1)
  [1]=>
  int(2)
  [2]=>
  array(3) {
    [0]=>
    string(1) "a"
    [1]=>
    string(1) "b"
    [2]=>
    string(1) "c"
  }
}
```

5.这个

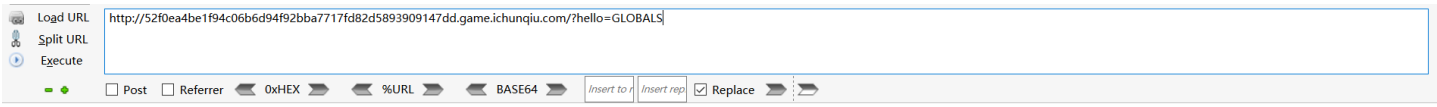
## $$a

估计就有很多同学搞不懂，$$为可变变量，简单说下他的用法就是这样：

```
$a = "b";
$b = "c";
echo $$a;`

结果输出为c
```

由于这题涉及到了可变变量，所以我们很容易就想到了用超全局变量$GLOBALS一次性查询所有的东西
给hello赋值后得到flag




array(9) { ["_GET"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) { } ["_COOKIE"]=> array(8) { ["chkphone"]=> string(33) "acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O" ["UM_distinctid"]=> string(61) "164bd1904bc64e-005e86c29125a38-1262694a-144000-164bd1904be9f2" ["pgv_pvi"]=> string(10) "1249226752" ["Hm_lvt_2d0601bd28de7d49818249cf35d95943"]=> string(43) "1532763486,1532767717,1532789701,1532921912" ["browse"]=> string(55) "CFlZTxUYU0BaWlhAVQJTRFBZSkdeQFFYWVRFR1xRW0RTV1FPWkBLThQ" ["ci_session"]=> string(40) "8c5a691850c311f16f7ec31b20ba2ecd7b0d4a76" ["pgv_si"]=> string(11) "s4336846848" ["Hm_lpvt_2d0601bd28de7d49818249cf35d95943"]=> string(10) "1532935617" } ["_FILES"]=> array(0) { } ["_REQUEST"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["flag"]=> string(38) "flag在一个长度为6的变量里面" ["d3f0f8"]=> string(42) "flag{9a68c759-26b6-4faf-be9a-af10e316d338}" ["a"]=> string(7) "GLOBALS" ["GLOBALS"]=> *RECURSION* } <?php
include "flag.php";



**总结：这题本身难度不大，主要是涉及到了许多陌生的东西，而且，不能看到flag.php就一股脑的想文件包含那些的去了，总之还是学到了许多东西**