

# i春秋 Misc Web 爆破-1 wp

原创

[Garybr0](#) 于 2021-01-10 11:06:17 发布 107 收藏 2

分类专栏: [CTF writeup PHP函数](#) 文章标签: [i春秋 web](#)

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\\_45253216/article/details/112424973](https://blog.csdn.net/weixin_45253216/article/details/112424973)

版权



[CTF writeup](#) 同时被 2 个专栏收录

16 篇文章 0 订阅

订阅专栏



[PHP函数](#)

4 篇文章 0 订阅

订阅专栏

2021.1.10

网安菜鸡今天来划水了!

CTF题目属于萌新入门级, 写下WP仅供自己总结练习, 大佬请自行绕路, 另外如果有师傅愿意有每日轻松一笑环结, 还望不吝赐教。【狗头】

“百度杯” CTF比赛 2017 二月场

分值: 10分 类型: Misc Web 题目名称: 爆破-1 已解答

题目内容: flag就在某六位变量中。

<http://34200c89686940f3b46508a31d3c36253dc197db908540ea.changame.ichunqiu.com:80>

00 : 27 : 38

延长时间(3) 重新创建

Flag:  提交

解题排名: 1 青海长云 2 canic 3 王乙文

提交Writeup获取金币

题目提示:

flag就在某六位变量中。

点开链接，是一段PHP源码:

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

[https://blog.csdn.net/weixin\\_45253216](https://blog.csdn.net/weixin_45253216)

首先第一行 include "flag.php" 表示包含一个flag.php的文件。

第二行 \$a = @\$\_REQUEST['hello'];命名一个变量a，让他接收超全局变量\$\_REQUEST['hello']。这里有一个知识点，就是**什么是超全局变量?**

**超全局变量:**

超全局变量 — 超全局变量是在全部作用域中始终可用的内置变量。

PHP 中的许多预定义变量都是“超全局的”，这意味着它们在一个脚本的全部作用域中都可用。在函数或方法中无需执行 `global $variable`; 就可以访问它们。超全局变量包括：

```
$GLOBALS
$_SERVER
$_GET
$_POST
$_FILES
$_COOKIE
$_SESSION
$_REQUEST
$_ENV
```

本题涉及了两个超全局变量，分别是 `$GLOBALS` 和 `$_REQUEST`。

## `$GLOBALS`

`$GLOBALS` — 引用全局作用域中可用的全部变量。一个包含了全部变量的全局组合数组。变量的名字就是数组的键。

具体使用方法：来自 [PHP Document](#)

### 范例

示例 #1 `$GLOBALS` 范例

```
<?php
function test() {
    $foo = "local variable";

    echo '$foo in global scope: ' . $GLOBALS["foo"] . "\n";
    echo '$foo in current scope: ' . $foo . "\n";
}

$foo = "Example content";
test();
?>
```

以上例程的输出类似于：

```
$foo in global scope: Example content
$foo in current scope: local variable
```

[https://blog.csdn.net/weixin\\_45253216](https://blog.csdn.net/weixin_45253216)

## `$_REQUEST`

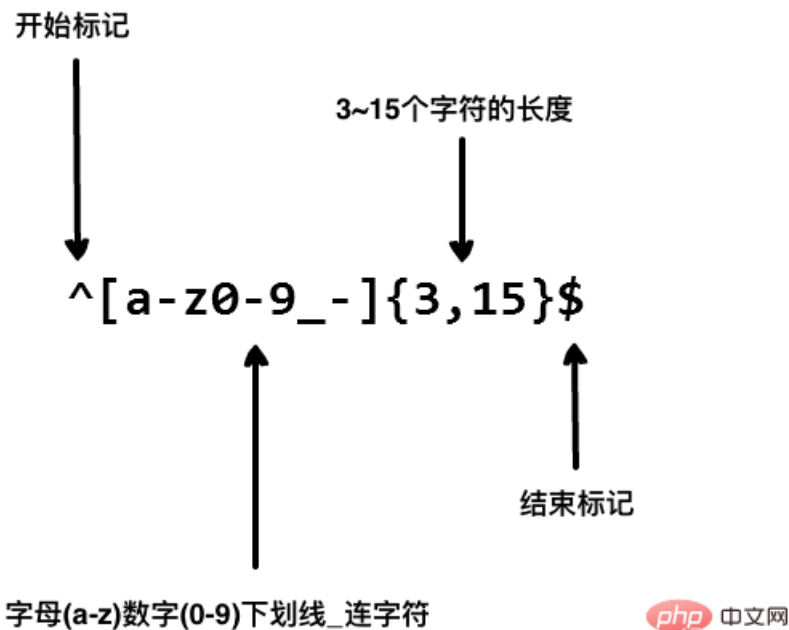
`$_REQUEST` — HTTP Request 变量。默认情况下包含了 `$_GET`，`$_POST` 和 `$_COOKIE` 的数组。

第三行，是用正则表达式过滤，如果传入的参数不符合格式要求，则 `die('error')`;

@写在变量前面，是忽略错误提示的意思。@用于抑制警告输出，通常用在PHP数据库连接数据库或接收网络传参。

### 正则表达式

[PHP中文网](#)



正则表达式在匹配字符串时，遵循以下2个基本原则：

- 1.最左原则：正则表达式总是从目标字符串的最左侧开始，依次匹配，直到匹配到符合表达式要求的部分，或直到匹配目标字符串的结束。
- 2.最长原则：对于匹配到的目标字符串，正则表达式总是会匹配到符合正则表达式要求的最长的部分；即贪婪模式。

### 那么通用原子和元字符有哪些呢？

- `\d`匹配一个数字字符。等价于 `[0-9]`。
- `\D`匹配一个非数字字符。等价于 `^[^0-9]`。
- `\f`匹配一个换页符。等价于 `\x0c` 和 `\cL`。
- `\n`匹配一个换行符。等价于 `\x0a` 和 `\cJ`。
- `\r`匹配一个回车符。等价于 `\x0d` 和 `\cM`。
- `\s`匹配任何空白字符，包括空格、制表符、换页符等等。等价于 `[\f\n\r\t\v]`。
- `\S`匹配任何非空白字符。等价于 `^[^\f\n\r\t\v]`。
- `\t`匹配一个制表符。等价于 `\x09` 和 `\cI`。
- `\v`匹配一个垂直制表符。等价于 `\x0b` 和 `\cK`。
- `\w`匹配包括下划线的任何单词字符。等价于 `[A-Za-z0-9_]`。
- `\W`匹配任何非单词字符。等价于 `^[^A-Za-z0-9_]`。
- `\xn`匹配 `n`，其中 `n` 为十六进制转义值。十六进制转义值必须为确定的两个数字长。例如，`'\x41'` 匹配 "A"。`'\x041'` 则等价于 `'\x04' & "1"`。正则表达式中可以使用 ASCII 编码。
- `\nm`标识一个八进制转义值或一个向后引用。如果 `\nm` 之前至少有 `nm` 个获得子表达式，则 `nm` 为向后引用。如果 `\nm` 之前至少有 `n` 个获取，则 `n` 为一个后跟文字 `m` 的向后引用。如果前面的条件都不满足，若

n 和 m 均为八进制数字 (0-7), 则 `\nm` 将匹配八进制转义值 nm。

• `\nml` 如果 n 为八进制数字 (0-3), 且 m 和 l 均为八进制数字 (0-7), 则匹配八进制转义值 nml。

• `\un` 十六进制数字表示的 Unicode 字符。例如, `\u00A9` 匹配版权符号(?)。

• `.` 匹配除“\n”之外的任何单个字符

[https://blog.csdn.net/weixin\\_45253216](https://blog.csdn.net/weixin_45253216)

### 使用命名子组

```
<?php
$str = 'foobar: 2008';

preg_match('/(?P<name>\w+): (?P<digit>\d+)/', $str, $matches);

/* 下面例子在php 5.2.2(pcre 7.0)或更新版本下工作, 然而, 为了后向兼容, 上面的方式是推荐写法. */
// preg_match('/(?<name>\w+): (?<digit>\d+)/', $str, $matches);

print_r($matches);

?>
```

执行结果如下所示:

```
Array
(
    [0] => foobar: 2008
    [name] => foobar
    [1] => foobar
    [digit] => 2008
    [2] => 2008
)
```

[https://blog.csdn.net/weixin\\_45253216](https://blog.csdn.net/weixin_45253216)

正则表达式是一块非常重要的内容, 稍后要多加练习以熟练运用。

本题目中传入`$REQUEST`就会`ERROR`, 因为`\w`匹配包括下划线的任何单词字符。等价于`[A-Za-z0-9_]`。

接下来是eval("var\_dump(\$\$a);");

代表执行var\_dump这个函数：

var\_dump() 函数用于输出变量的相关信息。

## 实例

### 实例

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

输出结果为：

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

[https://blog.csdn.net/weixin\\_45253216](https://blog.csdn.net/weixin_45253216)

var\_dump() 等价于 print\_r。

最后一行show\_source(\_\_FILE\_\_);代表能把PHP代码打印到网页上，同样能实现这个功能的还有highlight\_file()。

解题过程：把全局变量GLOBALS通过hello赋值给\$a,就变成了\$GLOBALS，然后打印全局变量，就能找到flag：

```
array(9) { ["_GET"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) {} ["_COOKIE"]=> array(7) { ["ci_session"]=> string(40) "9acd59f473adb97bd18eae16d2ff04bdc629d03f" ["UM_distinctid"]=> string(59) "176e9db6ae8133-04ec60f3566911-6313f69-144000-176e9db6ae996b" ["chkphone"]=> string(33) "acWxNpxhQpDiAchhNuSnEqyiQuDIO0000" ["browse"]=> string(55) "CFIZTxUYU0BZWI5GVQJTRFBZSkdeQ1hYWVJFRF9RWUxTUV5PX0BLThQ" ["Hm_lvt_2d0601bd28de7d49818249cf35d95943"]=> string(21) "1610241240,1610243282" ["Hm_lpv_2d0601bd28de7d49818249cf35d95943"]=> string(10) "1610243732" ["_jsluid_h"]=> string(32) "8684d78aac49a784162ba849958d8613" } ["_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{525d4620-9cd2-49df-921b-88482ebe2b28}" ["a"]=> string(7) "GLOBALS" ["GLOBALS"]=> *RECURSION* } }
php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match("/\w*$/", $a )){
    die("ERROR");
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

[https://blog.csdn.net/weixin\\_45253216](https://blog.csdn.net/weixin_45253216)