i春秋 “百度杯”CTF比赛 2017 二月场 分值：10分 类型：MiscWeb题目名称：爆破-1

原创

WeUjie 于 2020-04-06 14:19:37 发布 400 收藏

分类专栏： CTF 文章标签： 信息安全

本文链接：https://blog.csdn.net/u010062917/article/details/105343160

分值：10分 类型：MiscWeb题目名称：爆破-1

题目内容：

flag就在某六位变量中。

http://c04f614f28694cc1a65e93c5daa3f23ed4c100b475394d01.changame.ichunqiu.com

```php
<?php
include "flag.php";  //包含flag.php文件
$a = @$_REQUEST['hello'];  // 请求参数为hello
if(!preg_match('/^\w*$/',$a )){  //从^开头到结尾$ 匹配字符包括下划线\w 匹配字母或数字或下划线或汉字 等价于 '[A-Za-z0-9_]
'
  die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

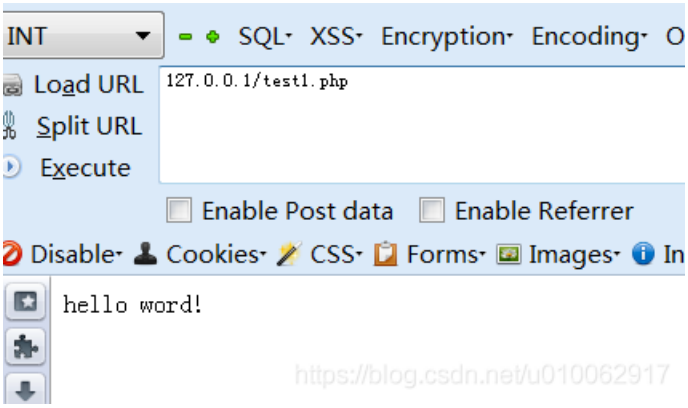
知识点1：$$

php中的$是可以叠加的

例如：

```php
$a = "b";
$b = "Hello world!";
echo $$a;
```

结果：



知识点2：超全局变量

$GLOBALS 的作用：引用全局作用域中可用的全部变量，就可以导出所有的变量。

由此可知 GET传参hello，给a赋值，最后输出值。

http://c04f614f28694cc1a65e93c5daa3f23ed4c100b475394d01.changame.ichunqiu.com/?hello=GLOBALS