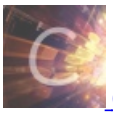
“百度杯” 2017 二月场 Misc Web 爆破-1

原创

白衣w 于 2019-04-15 15:52:58 发布 174 收藏

分类专栏： CTF之Web

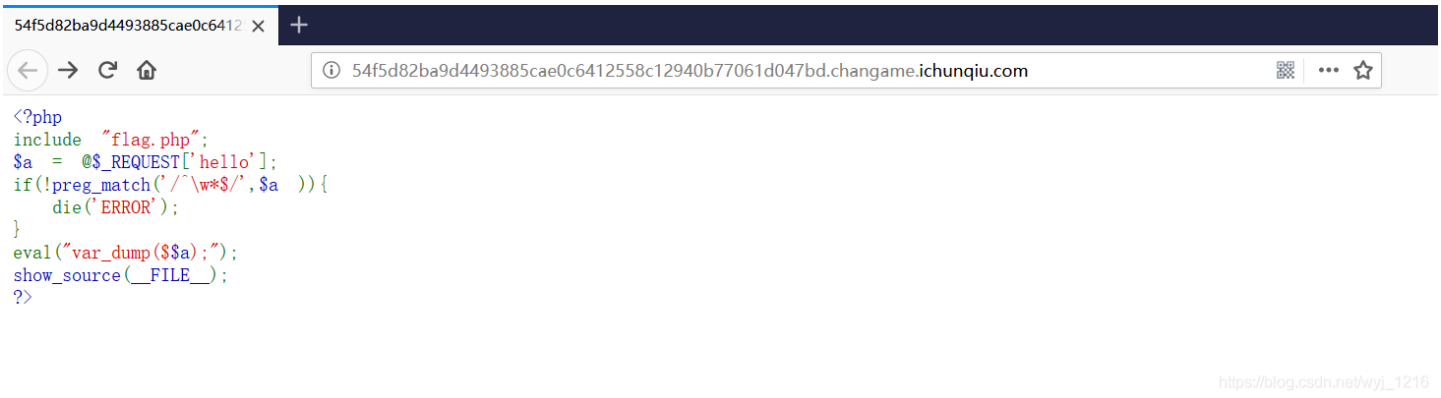
本文链接：https://blog.csdn.net/wyj_1216/article/details/89313668



题目

i春秋CTF题库

flag就在某六位变量中



writeup

知识点

$$

php中 $ 是可以叠加使用的

```
$$a = ${${a}} = ${b} = "Hello world!"
```

例如：

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

就可以打印出 b 的值 “Hello world!”

超全局变量

$GLOBALS — 引用全局作用域中可用的全部变量

$GLOBALS 这种全局变量用于在 PHP 脚本中的任意位置访问全局变量（从函数或方法中均可）。

题解

发送get请求：hello=GLOBALS

查看所有变量

```
?hello=GLOBALS
```