

magic_quotes_gpc魔术引号

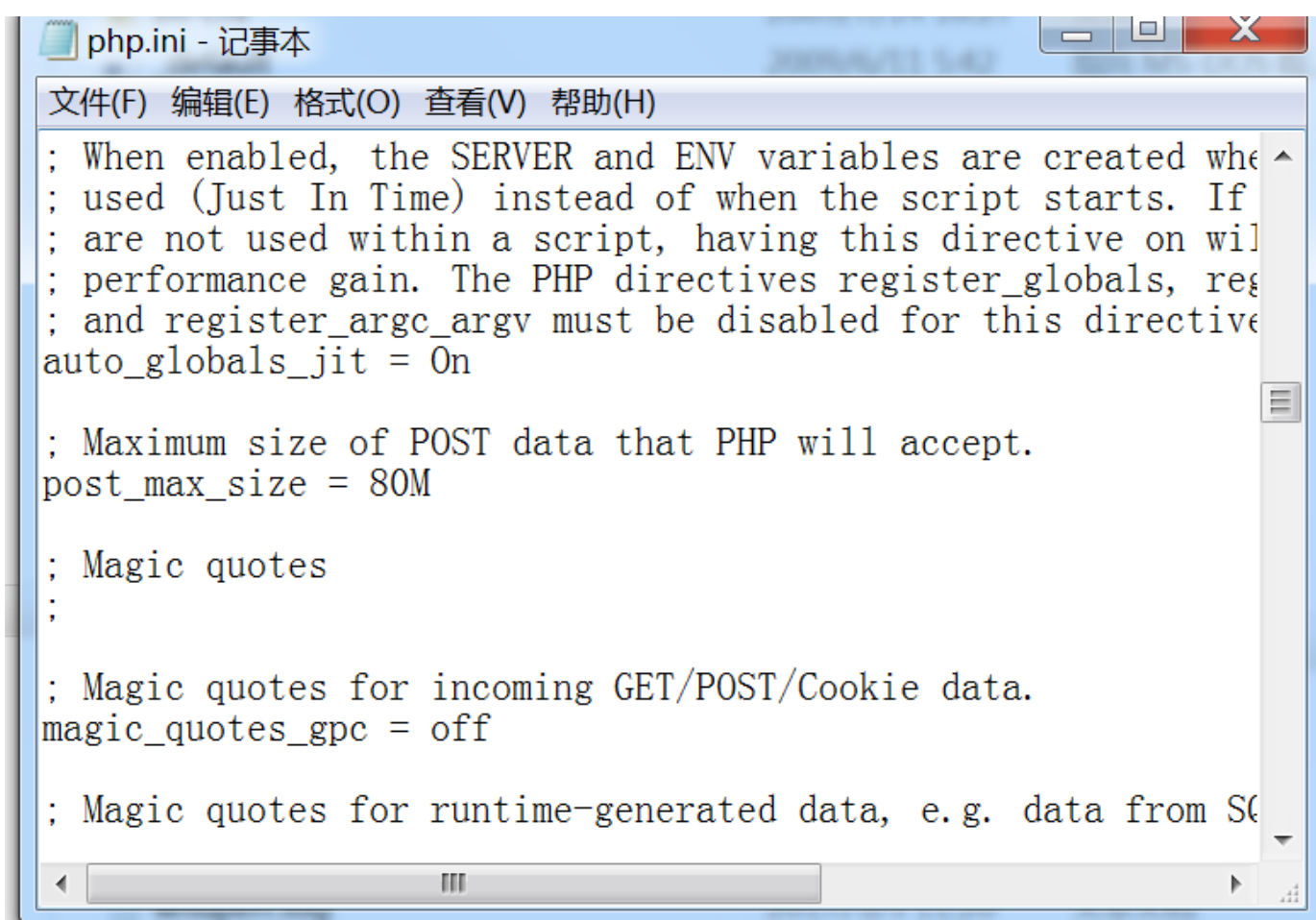
- 在PHP配置文件php.ini中存在magic_quotes_gpc选项，被称为魔术引号。
- 在high级别下，PHP的magic_quotes_gpc被自动设为on。
- 开启之后，可以对所有的GET、POST和COOKIE传值的数据自动运行 addslashes()函数

开启魔术引导(一般不建议采用,可能会造成可移植方面的问题)之后，可以对所有的GET,POST和COOKIE传值的数据自动运行 addslashes()函数;

关闭魔术引导:

关闭魔术引号

- 修改C:\Windows\php.ini文件
magic_quotes_gpc = Off
- 重启Apache服务



high级别下的防御措施:

high级别的防御措施

```
$id = $_GET['id'];  
$id = stripslashes($id);  
$id = mysql_real_escape_string($id);
```

- stripslashes()函数的作用是删除由 addslashes()函数添加的反斜杠，也就是去除addslashes()函数的转义。

I

2.利用is_numeric()函数判断你输入的是不是数字，如果输入的不是字符就不会往下执行!

3.把你输入的数据放于单引号内,作为一个字符型

high级别的防御措施

```
if (is_numeric($id)){  
    $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";  
}
```

- 在执行查询之前，使用了if语句进行判断，判断的条件是is_numeric()函数。
- 判断用户输入的数据是否是数字型，只要不是数字型就一概报错。
- and、or、select等语句都无法执行。

ed151cto.com

如何防御:

如何从代码层面防范SQL注入

- 对于数字型注入，可以使用if语句，并以is_number()函数作为判断条件进行防御。
- 对于字符型注入，对用于接收用户参数的变量，用mysql_real_escape_string()、addslashes()等函数进行过滤。

I

字符型注入里面最关键的就是单引号,怎么闭合单引号,你把单引号转义了,字符型注入就不存在了;

SQL注入的防范措施

- 代码层面
 - 1.对输入进行严格的转义和过滤;
 - 2.使用参数化查询。
- 网络层面
 - 1.通过WAF进行防护;
 - 2.云端防护：安全狗、360网站卫士、阿里云盾等。

在WAF里面主要做过滤!云端防护也一样的原理!

