WooYun-2014-51950(sqli using[slashes斜杠])

在magic\_quotes\_gpc=On的情况下，如果输入的数据有

单引号（’）、双引号（”）、反斜线（）与 NUL（NULL 字符）等字符都会被加上反斜线。这些转义是必须的，如果这个选项为off，那么我们就必须调用addslashes这个函数来为字符串增加转义。

addslashes()

## 定义和用法

addslashes() 函数返回在预定义字符之前添加反斜杠的字符串。

预定义字符是：

* 单引号（'）
* 双引号（"）
* 反斜杠（\）
* NULL

提示：该函数可用于为存储在数据库中的字符串以及数据库查询语句准备字符串。

注释：默认地，PHP 对所有的 GET、POST 和 COOKIE 数据自动运行 addslashes()。所以您不应对已转义过的字符串使用 addslashes()，因为这样会导致双层转义。遇到这种情况时可以使用函数 get\_magic\_quotes\_gpc() 进行检测。

1\' union select user,password from mysql.user #