封神台SQL注入-宽字节

原创

VIP文章 炎凰先生 于 2020-10-05 12:45:48 发布 194 收藏

分类专栏： Web安全微专业 渗透 黑客

本文链接：https://blog.csdn.net/qq_40941912/article/details/108927676

一、原理

magic_quotes_gpc（魔术引号开关）

magic_quotes_gpc函数在php中的作用是判断解析用户提交的数据，如包括有：post、get、cookie过来的数据增加转义字符“\”，以确保这些数据不会引起程序，特别是数据库语句因为特殊字符引起的污染而出现致命的错误。

单引号（’）、双引号（”）、反斜线（\）与 NULL（NULL 字符）等字符都会被加上反斜线

GBK全称《汉字内码扩展规范》,gbk是一种多字符编码。他使用了双字节编码方案，因为双字节编码所以gbk编码汉字，占用2个字节。一个utf-8编码的汉字，占用3个字节。

二、作业

（一） SQL注入-宽字节注入 Rank 1

页面原始URL：http://inject2.lab.aqlab.cn:81/Pass-15/index.php?id=1

任务：

通过宽字节注入获得flag。

对该页面进行GET传参，传参名为id

注意到单引号前加了反斜杠，使我们不能闭合字符串。所以在URL中不能出现单引号。其他和普通的GET注入一样

判断闭合字符

只要出现单引号，前面就会加上反斜杠，有反斜杠就无法实现注入。现在考虑怎么把它加的反斜杠吃掉。反斜杠和前面的一个字符组成一个整体就不会去转义单引号了。这个整体就是宽字节。

对于中文这样的字符集，一个字符是用多个字节表示的。比如GBK编码用两个字节表示，UTF-8用3个字节表示。如