MD5加密下的SQL注入

转载

Ghostlead 于 2017-11-03 18:00:37 发布 5028 收藏
文章标签： sql注入 md5
转自：http://www.joychou.org/index.php/web/SQL-injection-with-raw-MD5-hashes.html?utm_source=tuicool

做题的时候看到下面这个句子：

```
$sql="select password from users where password='".md5($password,true)."'"
```

这里面的md5()函数有两个参数，一个是要加密的字符串，另一个是输出格式，具体是

raw	可选。规定十六进制或二进制输出格式： • TRUE - 原始 16 字符二进制格式 • FALSE - 默认。32 字符十六进制数

但是组成查询语句的时候这个hex会被转成字符串，如果转换之后的字符串包含`'or'<xxx>`，就会和原查询语句一起组成

```
$sql="select password from users where password=''or'<xxx>'"
```

导致了sql注入。

提供一个字符串：ffifdyop

md5后，276f722736c95d99e921722cf9ed621c

再转成字符串： `'or'6<其他字符>`

参考：

http://mslc.ctf.su/wp/leet-more-2010-oh-those-admins-writeup/

http://cvk.posthaven.com/sql-injection-with-raw-md5-hashes
http://www.w3school.com.cn/php/func_string_md5.asp