封神台靶场，为了小芳，冲之——cookie注入

原创

午喻 于 2020-10-30 09:55:54 发布 193 收藏 2

分类专栏： 渗透入门 文章标签： cookie

本文链接：https://blog.csdn.net/Wubuqing/article/details/109379178

渗透入门 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

第二个靶场

打开网站

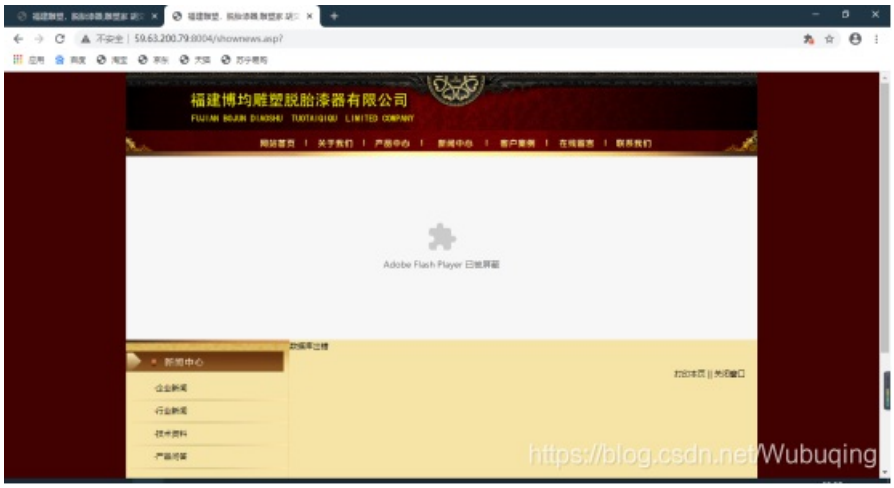
找一下注入点 一般在新闻这种里面点开看看

先判断是否存在注入

有waf

尝试了很多方法绕过都没成功，/and/,aandnd,AnD等一系列都没绕过去，乌鸡鲅鱼

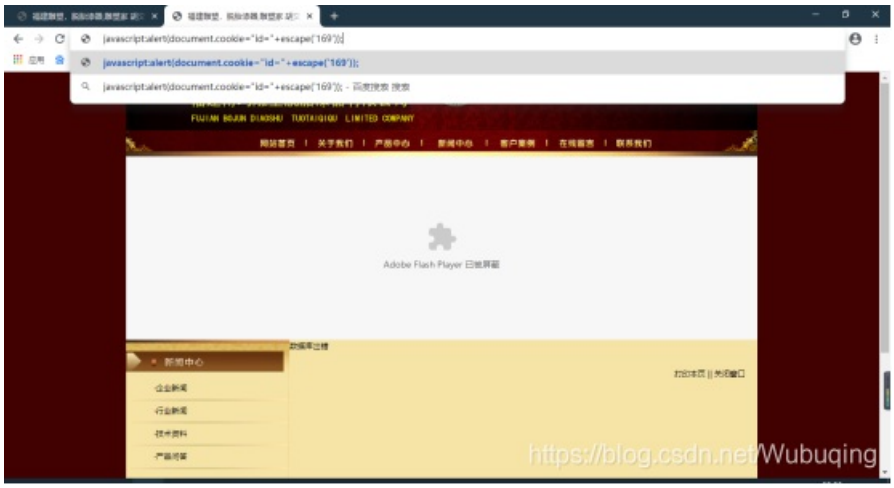
删掉id=169 发现



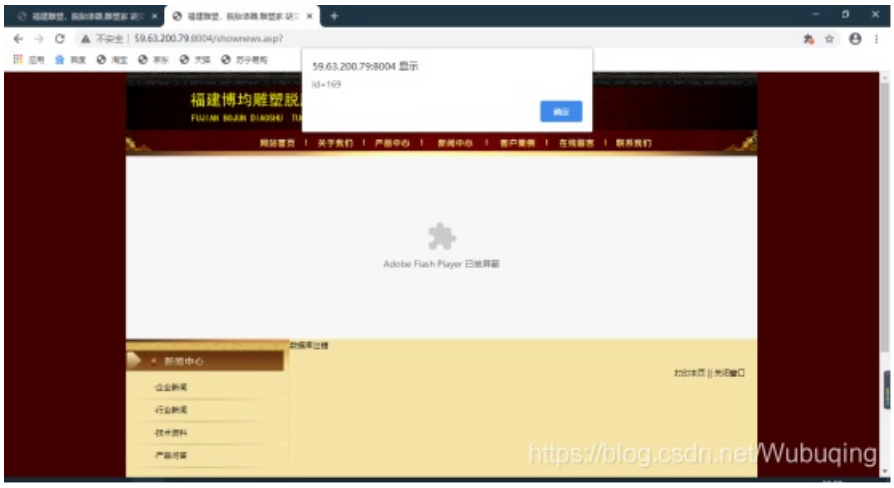
然后判断cookie注入

在搜索框输入

Javascript:alert(document.cookie="id="+escape('169'));

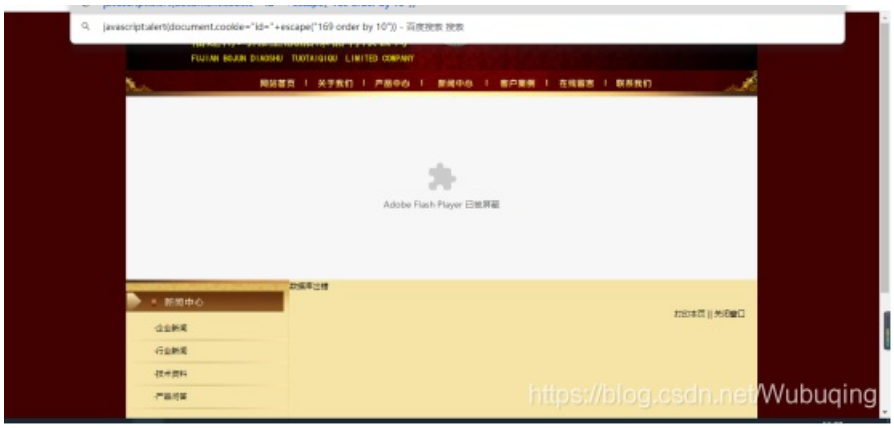


然后弹窗了（其中 "id=" 取决URL中的id= escape中的数值也是URL中id=的值）返回刚刚的页面，把ID删除后一样能正常显示。说明服务器能接收cookie传的id参数。

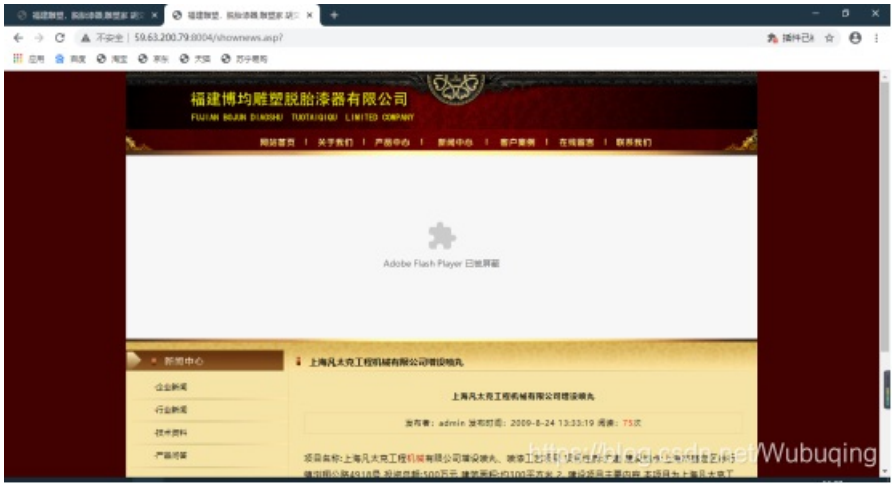


然后利用order by 查询字段数

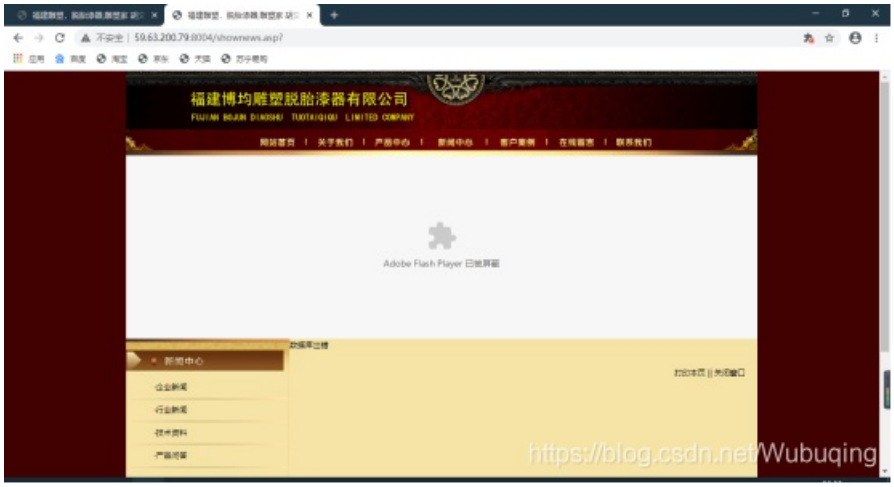
Javascript:alert(document.cookie="id="+escape("169 order by 10"));



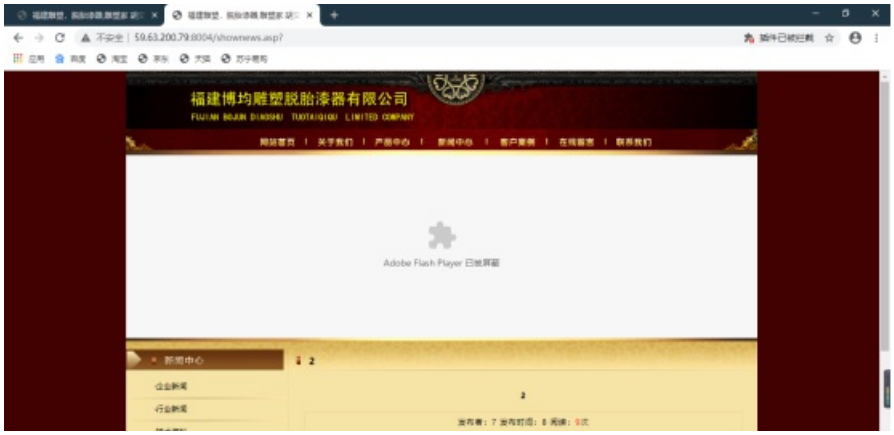
返回后正常



然后order by 11 返回后页面错误，说明只有10个



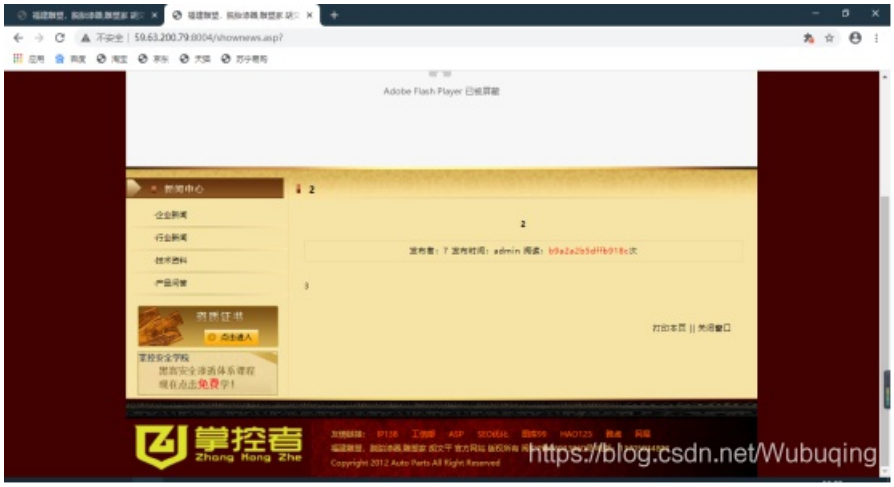
然后利用union select 1,2,3,4,5,6,7,8,9,10 from admin (猜测是admin表)
然后查看回显的位置



有2,3,7,8,9

然后在对应的位置查询

union select 1,2,3,4,5,6,7,username,password,10 from admin

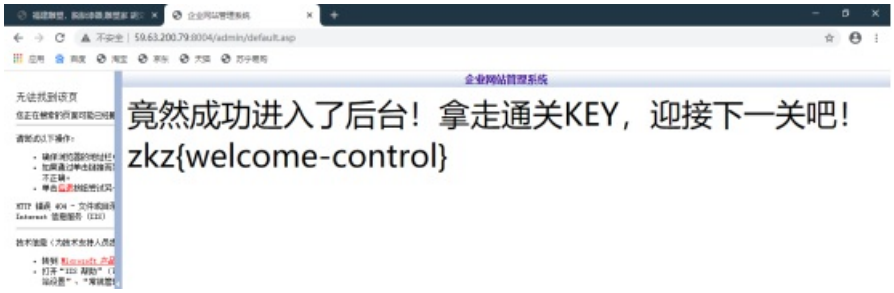


Password 有加密 解一下

我们就知道了 username：admin password：welcome

然后进入后台登录界面

输入密码登录进去



成功拿到key

还有另一个方法，利用burp抓包，然后在url中把id=170删除，加在cookie后面，记得用分号隔开，然后看页面是否报错，如果不报错说明存在cookie注入，然后利用查询语句查询即可，查询语句之间用+连接。