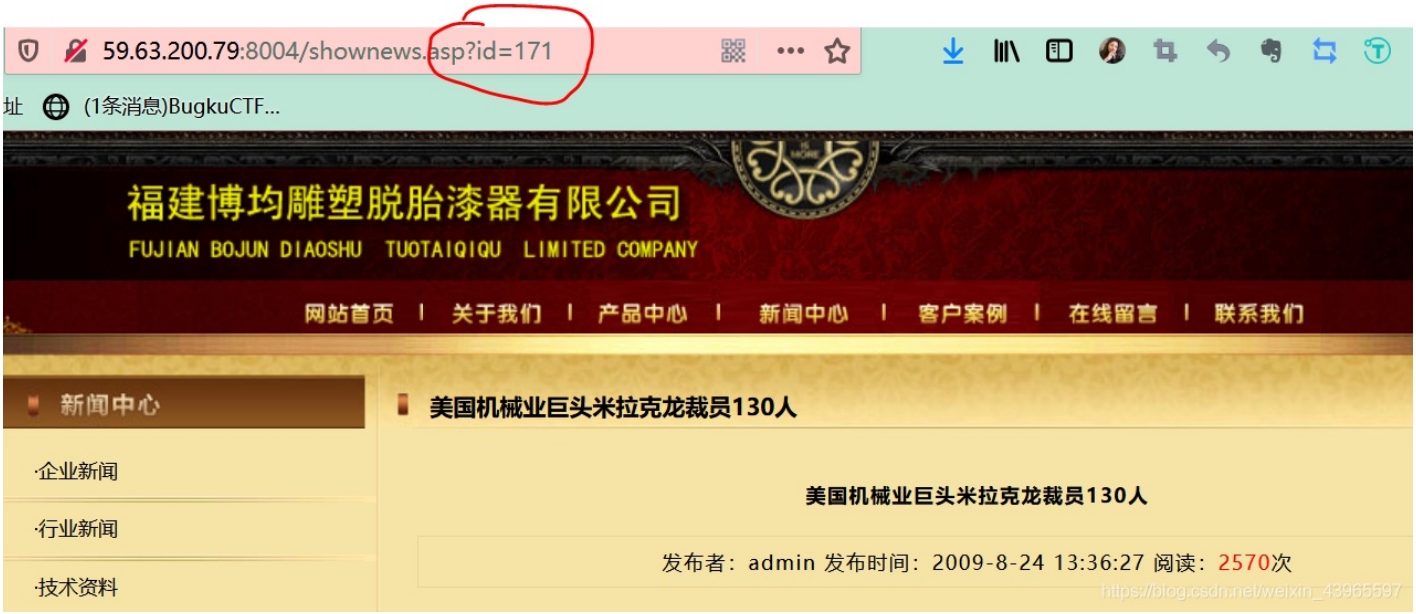
封神台——WAF绕过

原创

Zichel77 于 2020-07-04 12:20:45 发布 390 收藏 2
分类专栏： web学习 封神台 文章标签： WAF

本文链接：https://blog.csdn.net/weixin_43965597/article/details/107122515

没看到id，还是点进一篇新闻看看，因为新闻的页面是和新闻网站数据库产生交互的

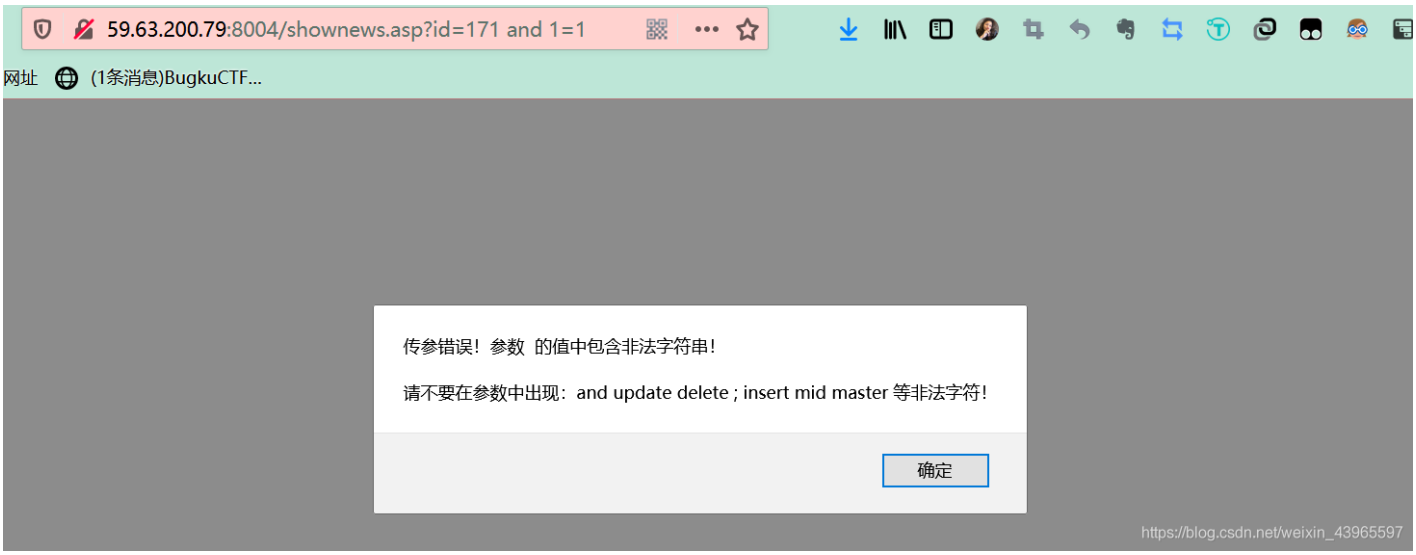


是你呀id

是网站下的shownews.asp这个ASP动态网页文件，与数据库进行交互，并查询出了第171篇（id=171）新闻内容的值。

按照上次的老套路

准备来手工注入，构造 and 1=1



我人都要被吓尿了，感觉自己是不是会被请去喝茶

但是毕竟是练习，已经提醒了会有waf拦截，但是他只阻碍了传参中的一些参数，刚刚的and就被禁了

那我试一下不用and

注意，此题使用的是Access数据库，与MySQL不同的是，它是后差后显示，也就是说不需要要前面的报错，直接查询后面的语句

于是我们直接构造order by 1查询字段数

说明一共有10个字段，因为传参的很多符号都被waf限制

于是用新知识点试一下，用cookie传参

选择插件ModHeader

添加一个cookie,构造value为

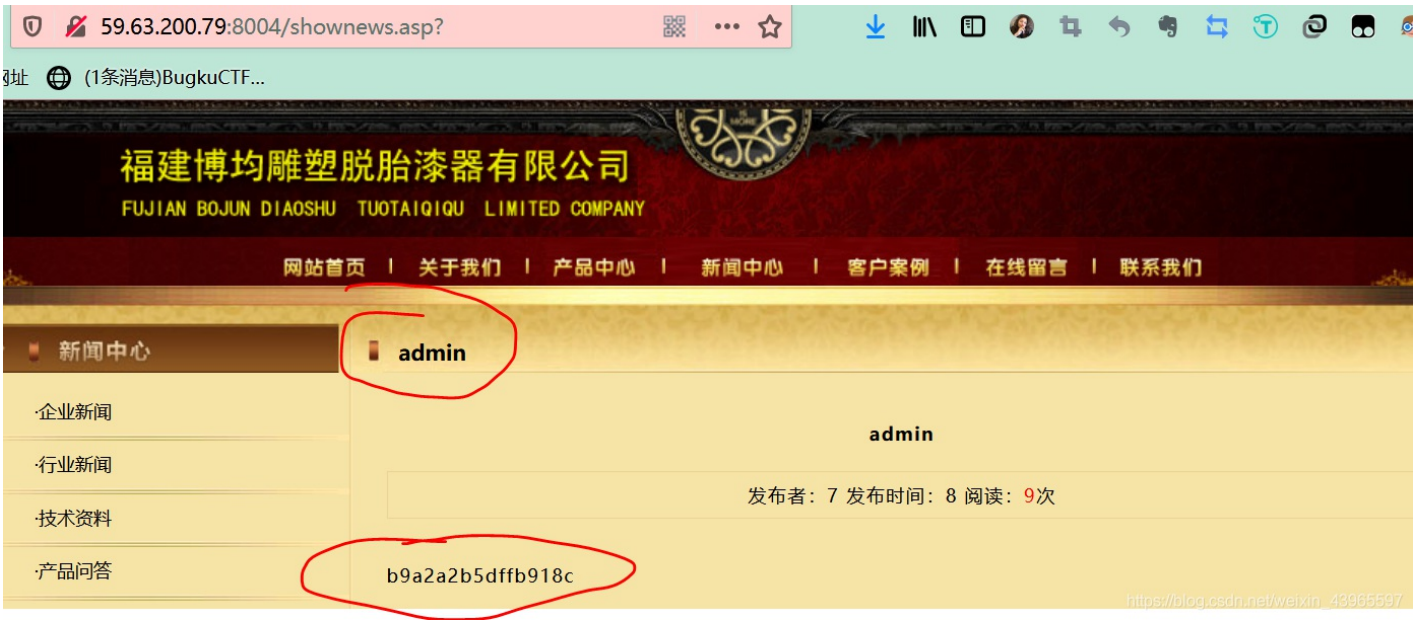
id=171+union+select+1,2,3,4,5,6,7,8,9,10+from+admin

查询到的回显点有这些

然后显示出登录名和密码

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

注意一定要用加号代替空格来连接，否则无法显示结果



这里的密码使用了MD5加密，在线解密一下

然后进入后台登录

这个站貌似是南方的CMS，默认管理员后台是根目录的/admin/

登录即可

记得!

一定要关掉插件啊啊啊啊啊啊!