mbp 封神台靶场 二（笔记）

原创

qq_43558415 于 2020-02-09 17:25:33 发布 1015 收藏 2

分类专栏： 封神台靶场

本文链接：https://blog.csdn.net/qq_43558415/article/details/104237173

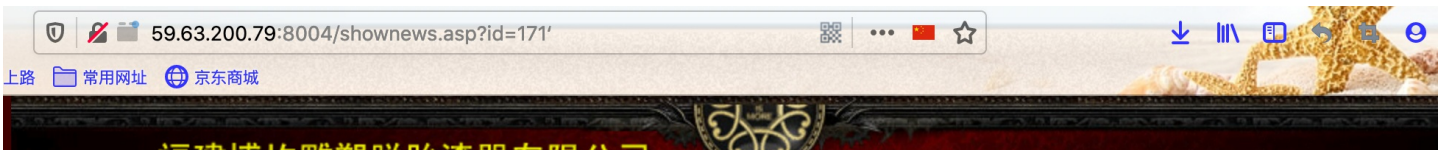
封神台靶场 专栏收录该内容

7 篇文章 4 订阅

订阅专栏

打开第二关的链接，是一个雕塑网页，点开各个链接查看，在新闻动态里点开了一个新闻，发现了熟悉的身影。

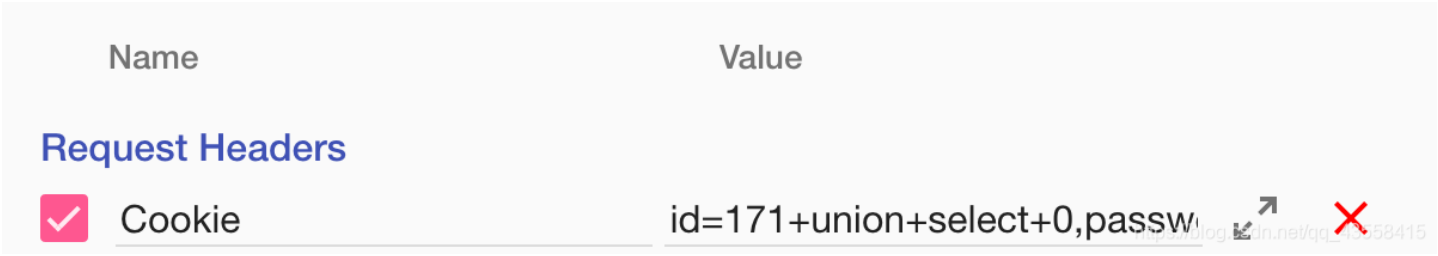
常理，还是用上一关的方法来测试一下，看看有没有注入点，页面显示数据库出错，即可注入。



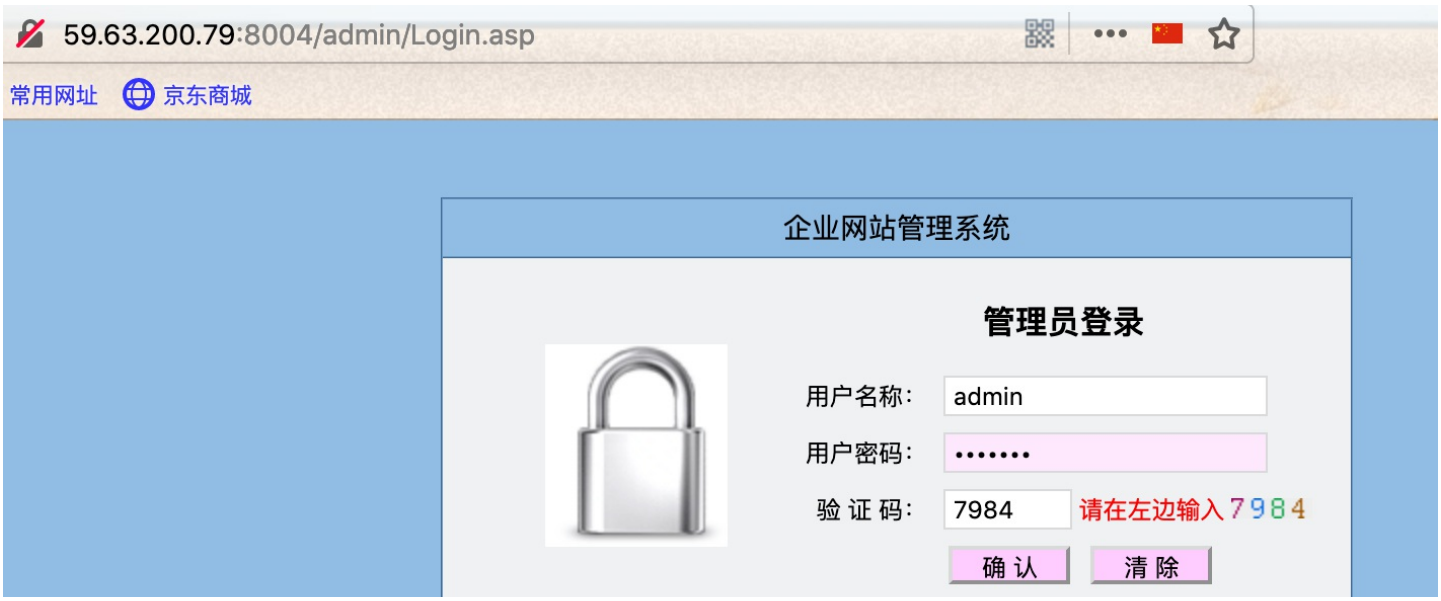
之后order by函数判断字段数,可知字段数为10。

老步骤，知道字段数之后判断回显点，输入`union select 0,1,2,3,4,5,6,7,8,9 from admin`发现传参错误，这就有点麻烦了，说明有waf过滤，众所周知，向网站传送数据不只有post和get两种方式，还有cookie，之后在浏览器里安装了modheader插件，创建了Cookie来查询password，（password和admin字段都是盲猜的，因为使用语句返回的都是数据库出错，难搞）

将`id=171+union+select+0,password,2,3,4,5,6,7,8,9+from+admin`输入得到password



然后对该串编码进行md5解码，得到是welcome,这下好了，开开心心去提交flag发现是错的，于是在原页面又思考了起来，有了用户名和密码，是不是这个网站还有后台，于是尝试着登陆后台。使用常用的后台进行盲猜，最后找到后台并登陆，拿到flag。



总结：本关还是用SQL注入来拿到密码，相对前一关增加了解码和WAF过滤还有寻找后台的这些手段，在公开课听到老师用modheader这个插件帮助了我挺多，还想搞明白如果不知道表名、字段名而注入又返回数据库出错怎么去解决，在找到后台的时候老师说还可以用比较原始的方法：用burp在登陆时使用万能密码对不知道的后台进行尝试。