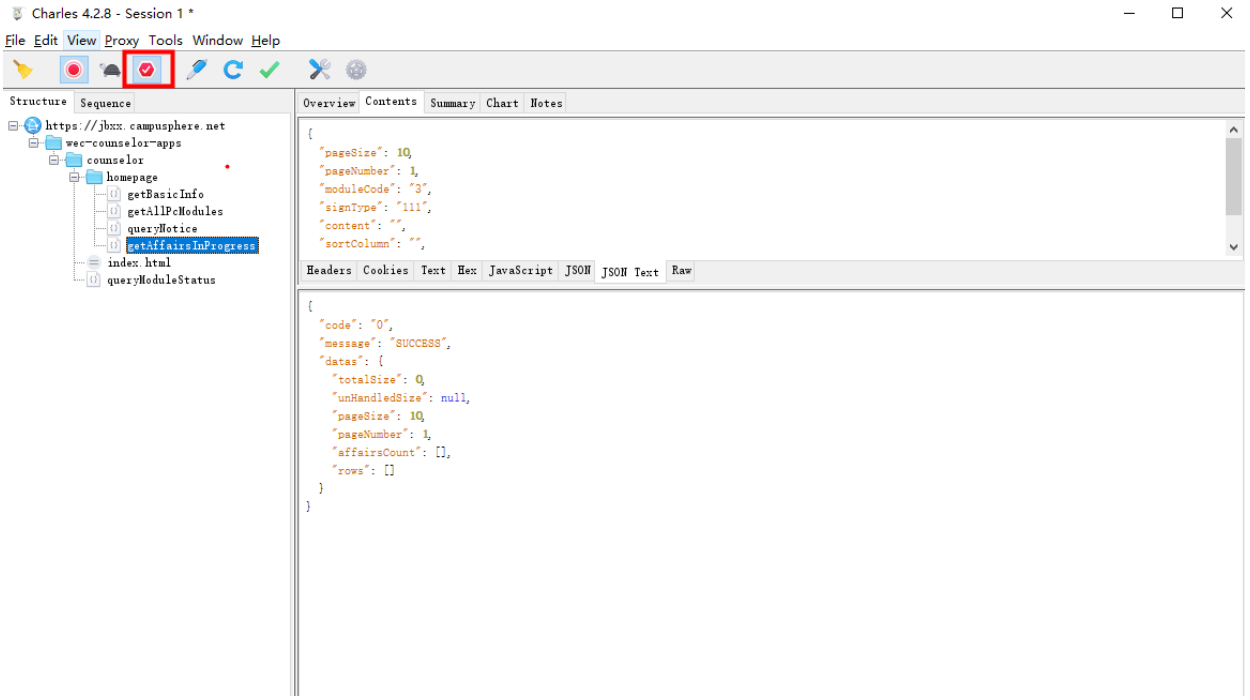
一、断点设置、请求的拦截和修改

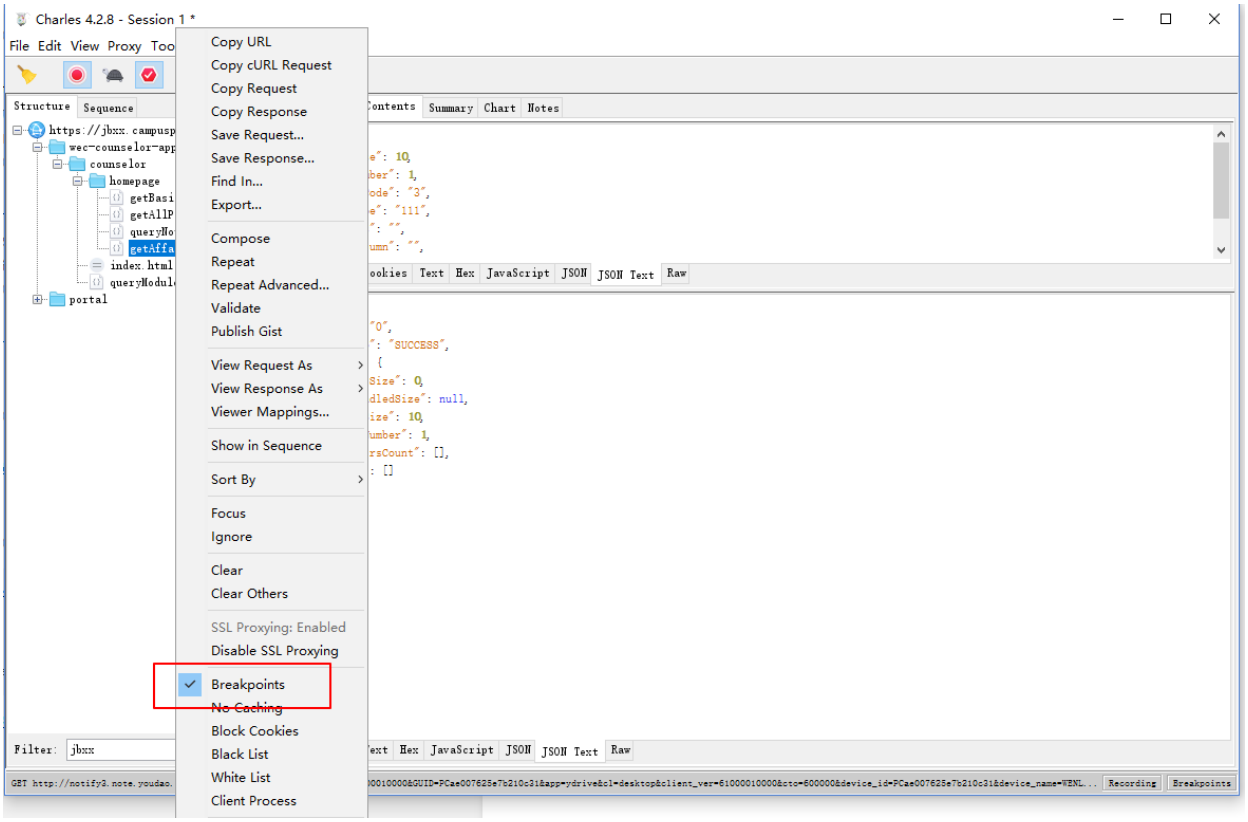
1.1 设置断点

点击下图中红框的“nike对号”图案的按钮开启断点开关



客户端发起请求，捕获到结构/时序视图中，选中要拦截的请求，右键选breakpoints选项

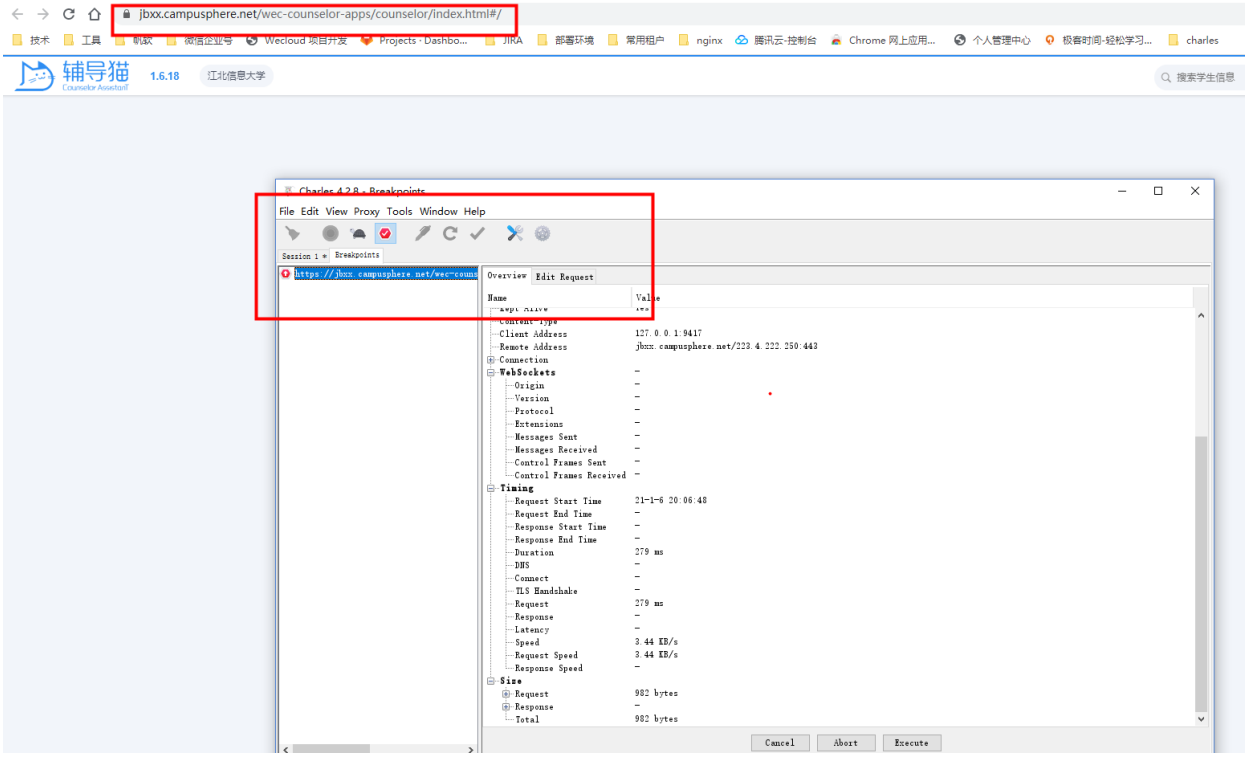
此时，该请求就被标记为断点了，即请求到这里就会停下来，“断在这个点上了”-断点



1.2、拦截请求

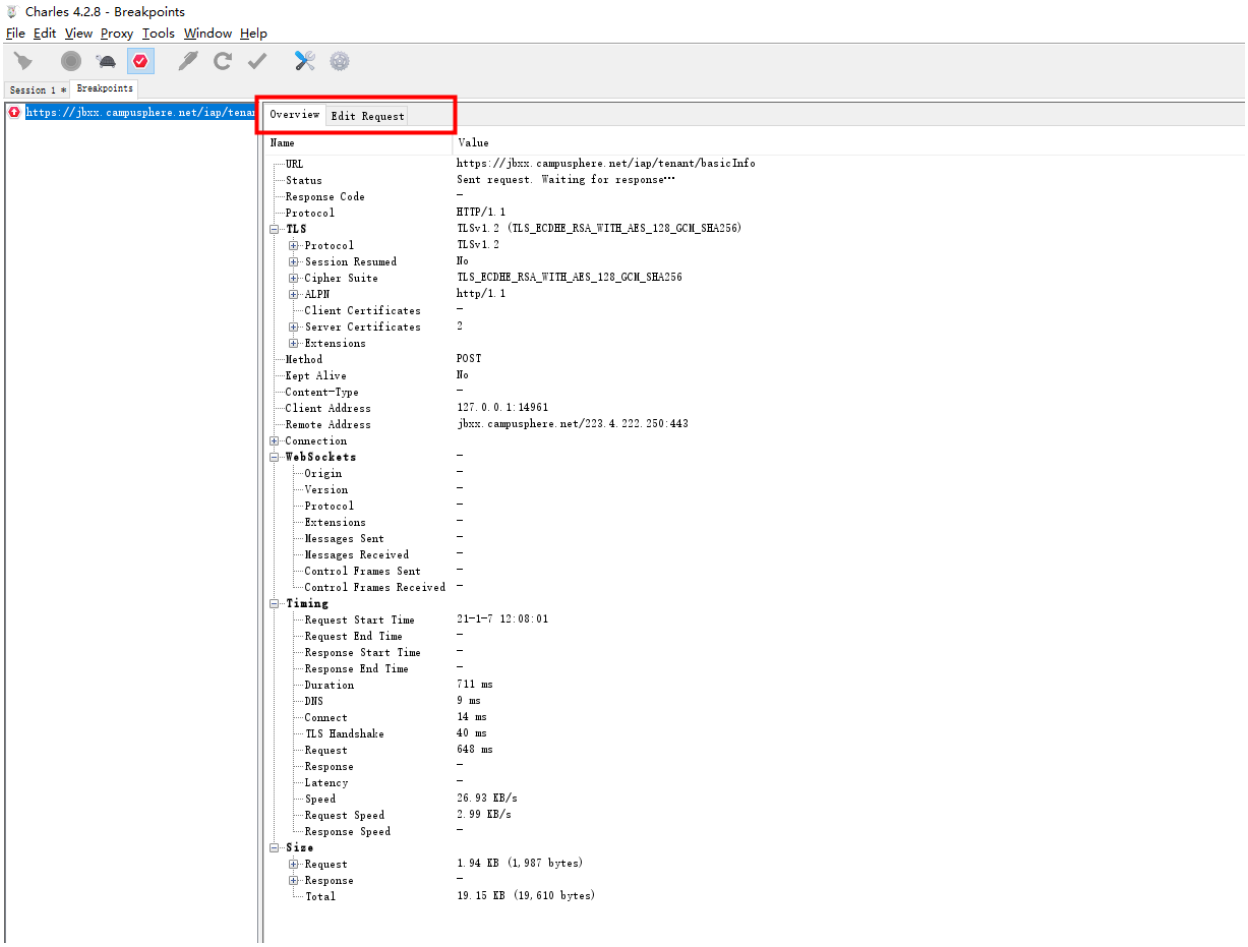
清空之前的请求，再次从客户端发起请求，这时请求就被Charles拦截下来了

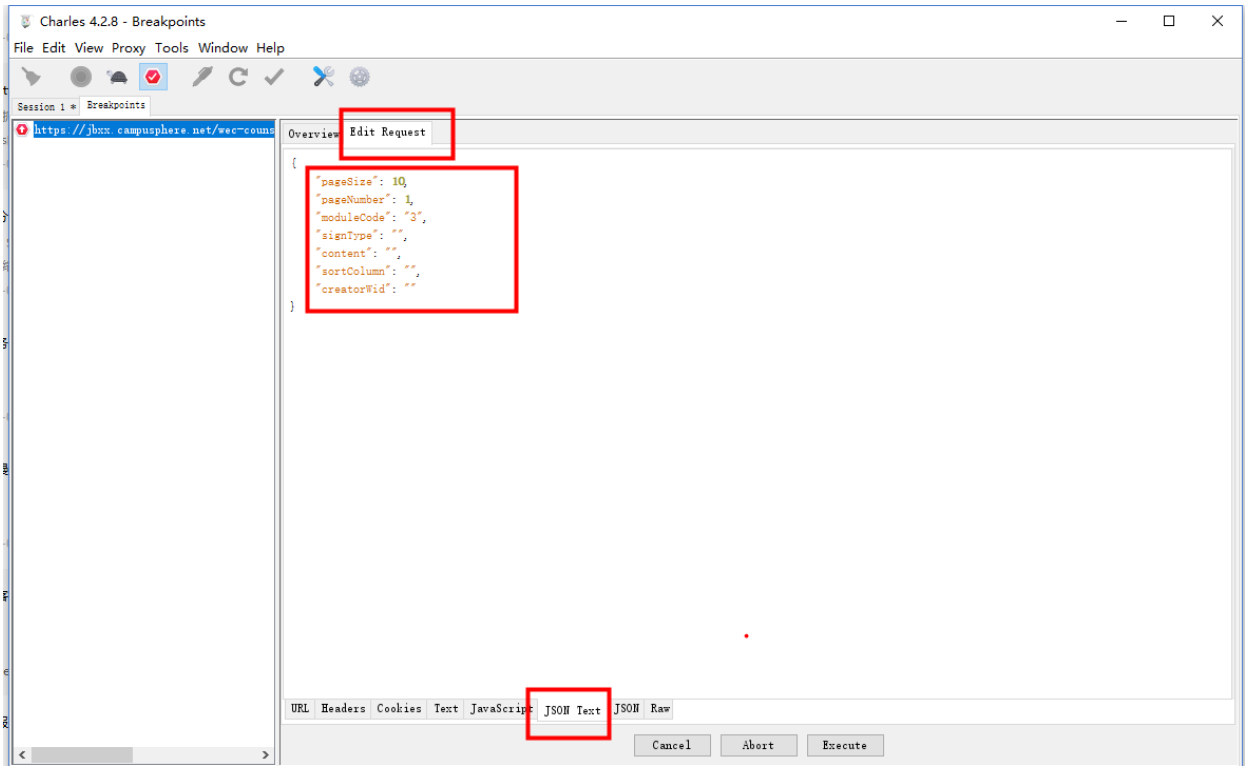
出现如下页面



1.3、修改请求

如下图，断点下，右边出现OverView和Edit Request两个窗口

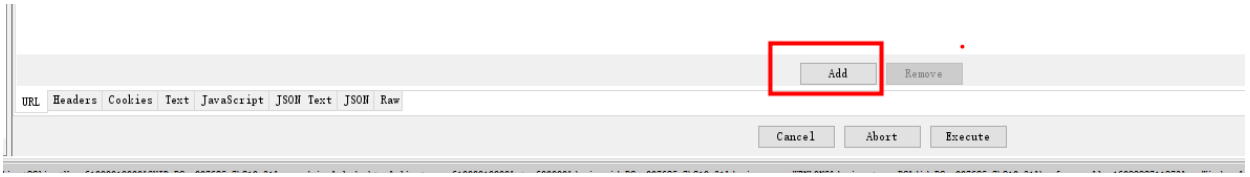




在Edit Request窗口下方有各自选项卡，供大家进行请求的修改

对于Post Json的请求，可以直接修改JSON Text中的参数，

对于Get请求，可以通过Add按钮，新增请求参数



除了参数修改外，下面整理了所有能修改的地方

– URL：

– Method：

– GET

– POST

– PUT

– DELETE

– HEAD

– TRACE

– Content type：

– application/x-www-form-urlencoded

– multipart/form-data; boundary=********

– text/plain

– text/xml

– text/json

– text/javascript

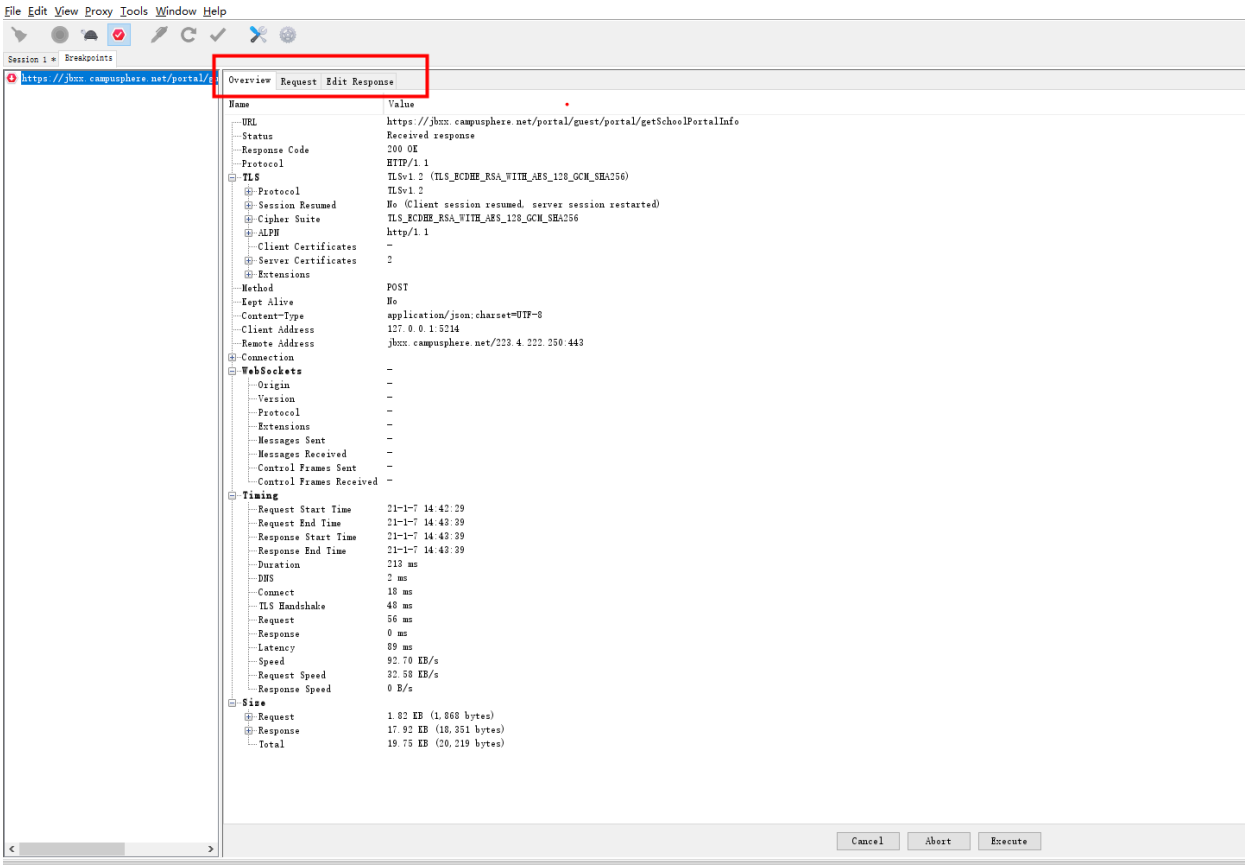
– Protocol version：

– HTTP/1.0

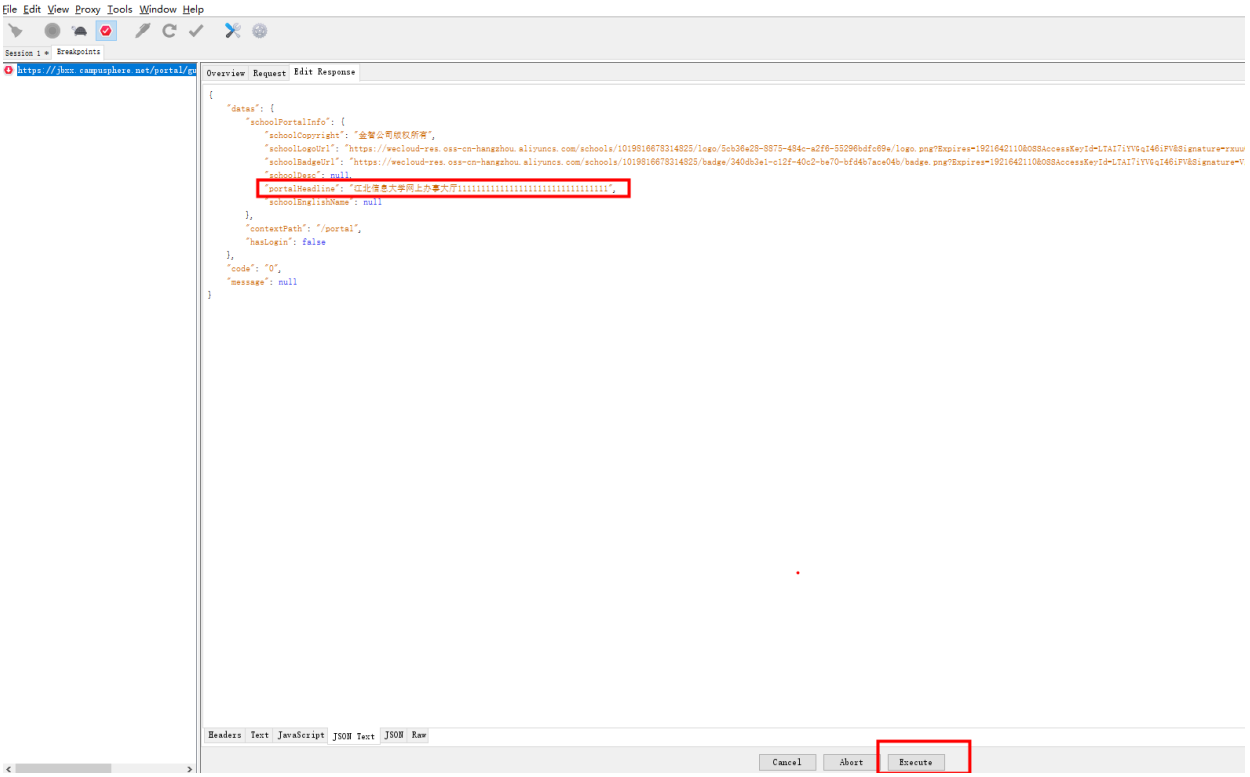
– HTTP/1.1

– HTTP/2.0

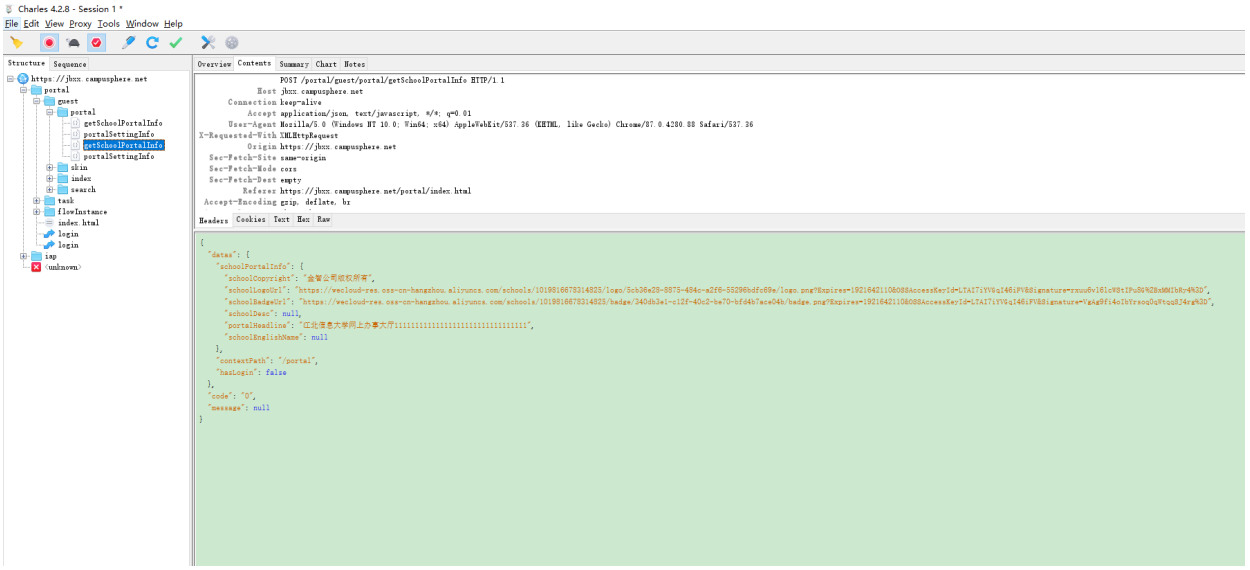
完毕后，点击Execute按钮，将请求发送给服务器，



等服务器响应回来给Charles后，出现了一个新的窗口，即Edit Response窗口，用于修改响应结果；



再次点击Execute按钮，响应结果才会返回给客户端。Charles回到捕获结构/序列视图



二、简单的安全测试

大家学会请求拦截修改操作以后，可以用来做哪些简单的安全测试呢？？举几个例子哈

2.1、前后端参数校验

前端校验：js校验 即页面校验。

后端校验：java等后端服务器校验

大家都知道前端的js页面校验是不可或缺的，但同时也是不可靠的，

为什么？？因为很容易被拦截篡改掉。

所以业界规范里参数校验前后端都必须做，防止前端校验被绕过后，篡改成非法参数发给服务端，如果此时服务端，没有做这个参数校验，而引发一系列问题，那么这个产品/服务就是不安全的。

举例来说，比如请求中参数A不能超过10个字符长度这个需求

页面发起请求A=hello，是5个字符长度，可以通过前端校验

请求被拦截后，修改为A=hellohellohello，是15个字符，超过了10，

将修改后的请求发送到服务器，就可以看一下服务器端有没有对这个参数做校验了

2.2、SQL注入安全测试

在开发网站的时候，出于安全考虑，需要过滤从页面传递过来的字符。通常，用户可以通过以下接口调用数据库的内容：

登陆界面、

URL地址栏、

留言板、

搜索框

这往往给骇客留下了可乘之机。轻则数据遭到泄露，重则服务器被拿下。

就拿用户登陆举例来说，

用户名：admin

密码：meiyoumima

一般判断用户有没有权限登陆该系统，数据库执行的sql如下

```
select * from user where user_name='admin' and
password='meiyoumima';
```

admin这个用户知道自己的密码，所以能登陆成功

对于黑客来说，他们在不知道admin的密码情况下，如何来登陆呢，

那么黑客可以输入用户名admin ' or 1=1# 密码随便输入“管你是啥”

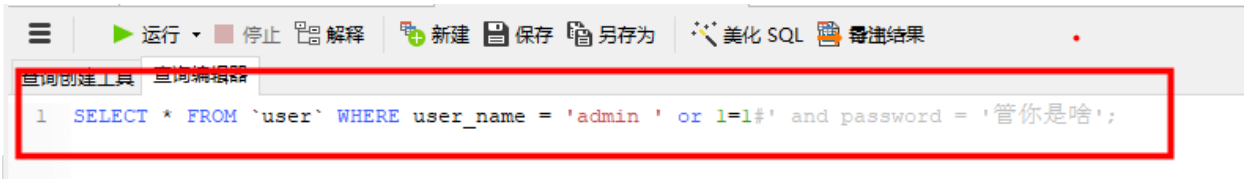
那么校验sql就变成了

```
select * from user where user_name='admin' or 1=1#' and
password='管你是啥';
```

由于#后面的被注释掉了，所以上面的sql等价于

```
select * from user where user_name='admin' or 1=1 ;
```

见下图中 密码被注释，绕过的效果图



这样黑客只需要知道用户名，就可绕过了密码校验，成功登陆。