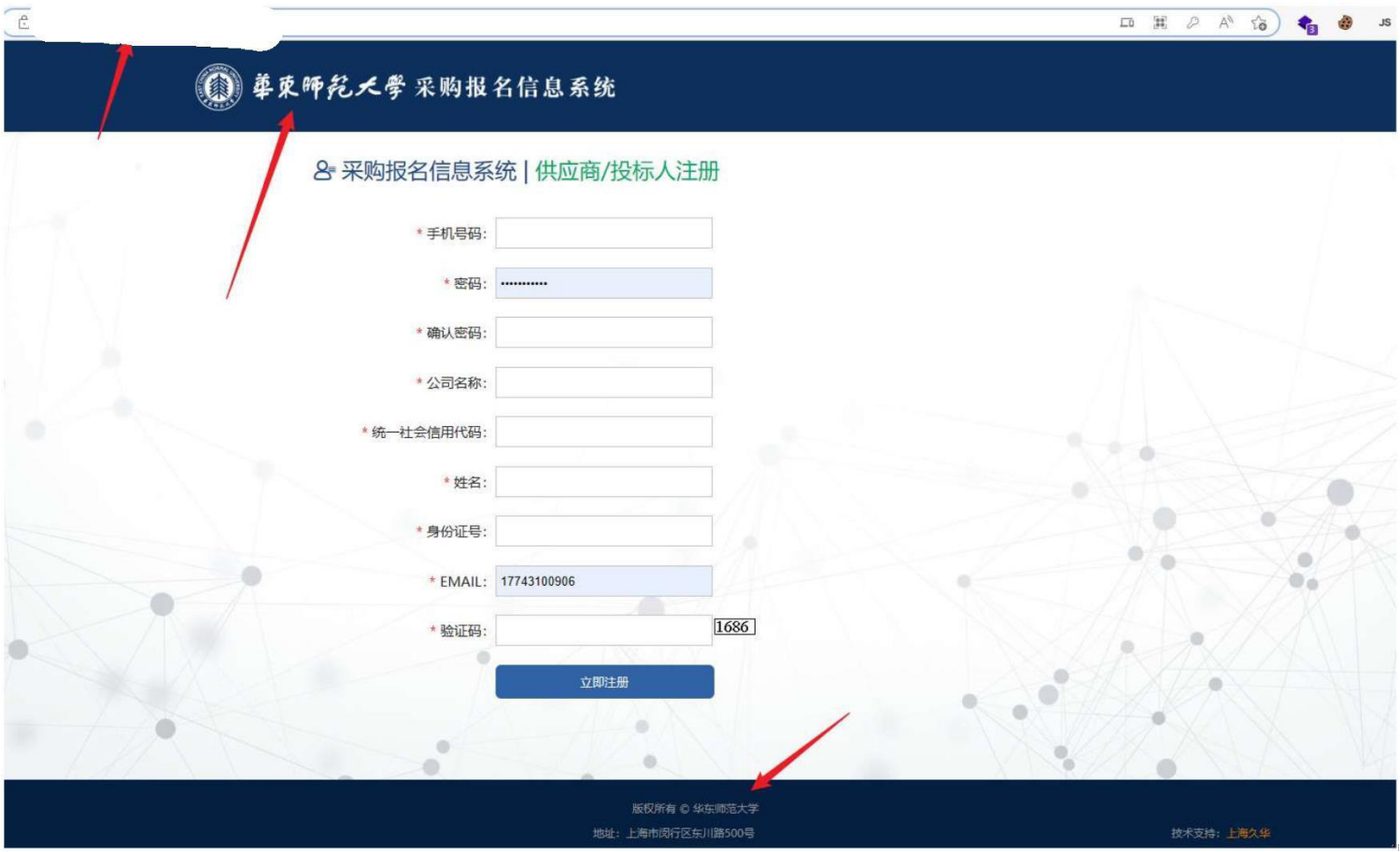
华东师范大学

无描述...

1.漏洞地址：

2.漏洞描述：华东师范大学采购报名管理系统存在接口未鉴权，可获取2764条相关身份证照片，营业执照，授权书照片等敏感信息。

3.资产确认：



4.漏洞详情：

(1) 该系统允许任意用户注册，给审核提供我的注册账号：

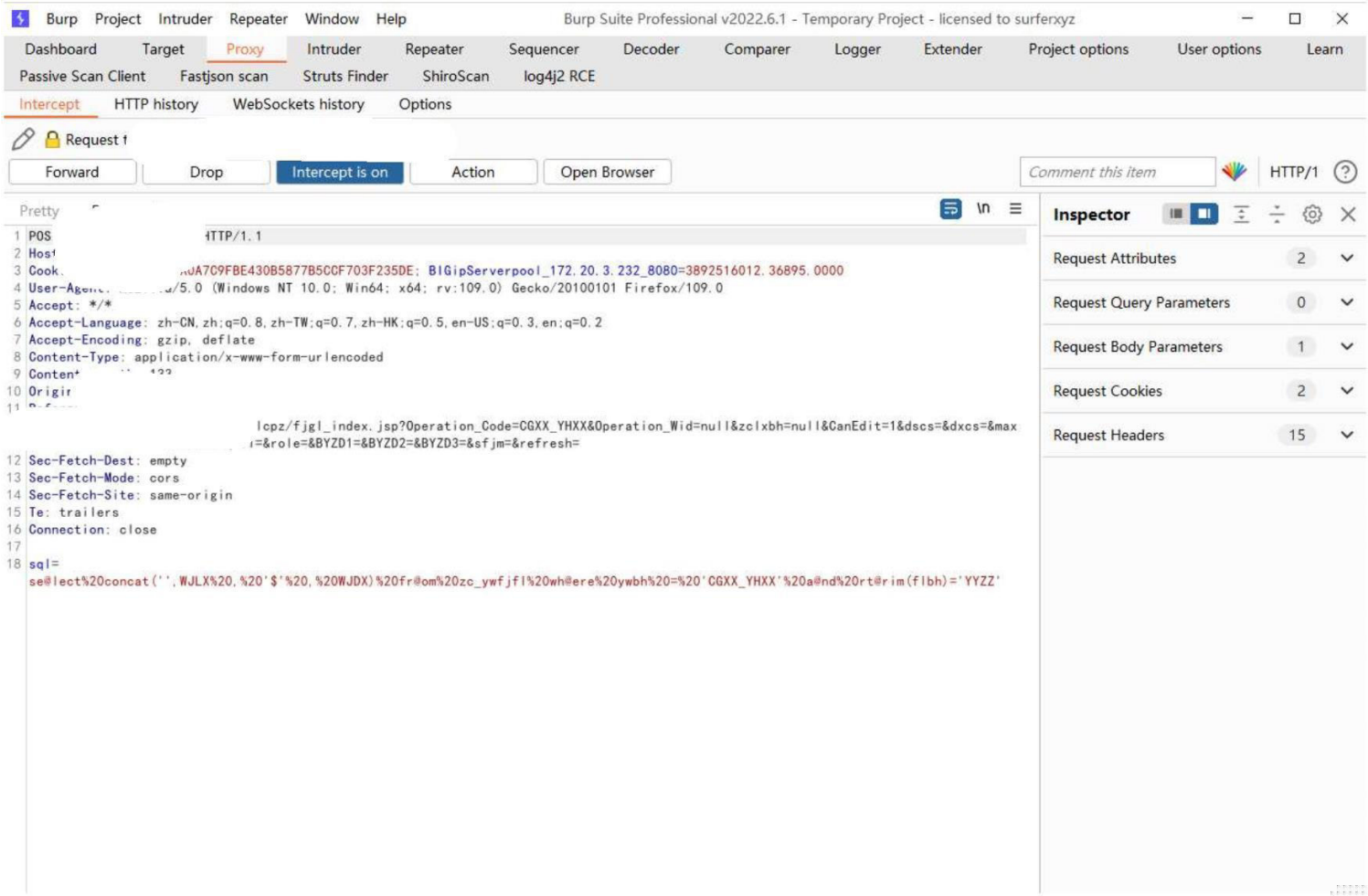
(2)进入系统，通过前端js找到一个接口：

HXX&ywwid=20230125100458177431009O6

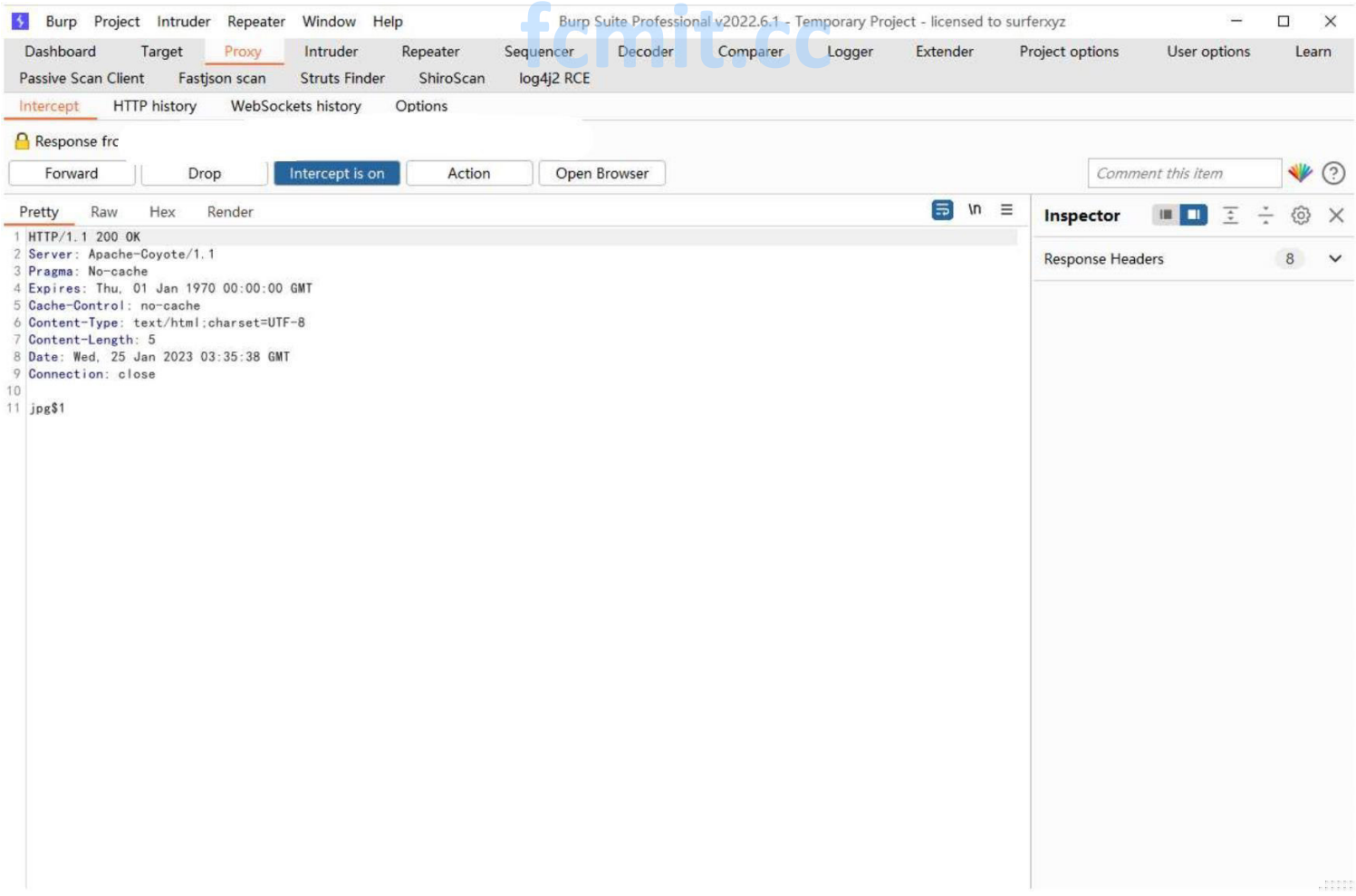
是一个文件管理上传的接口：

点击上传一个任意类型图片，点击上传然后抓包：

第一个包直接放掉，出现下面报文拦截响应：



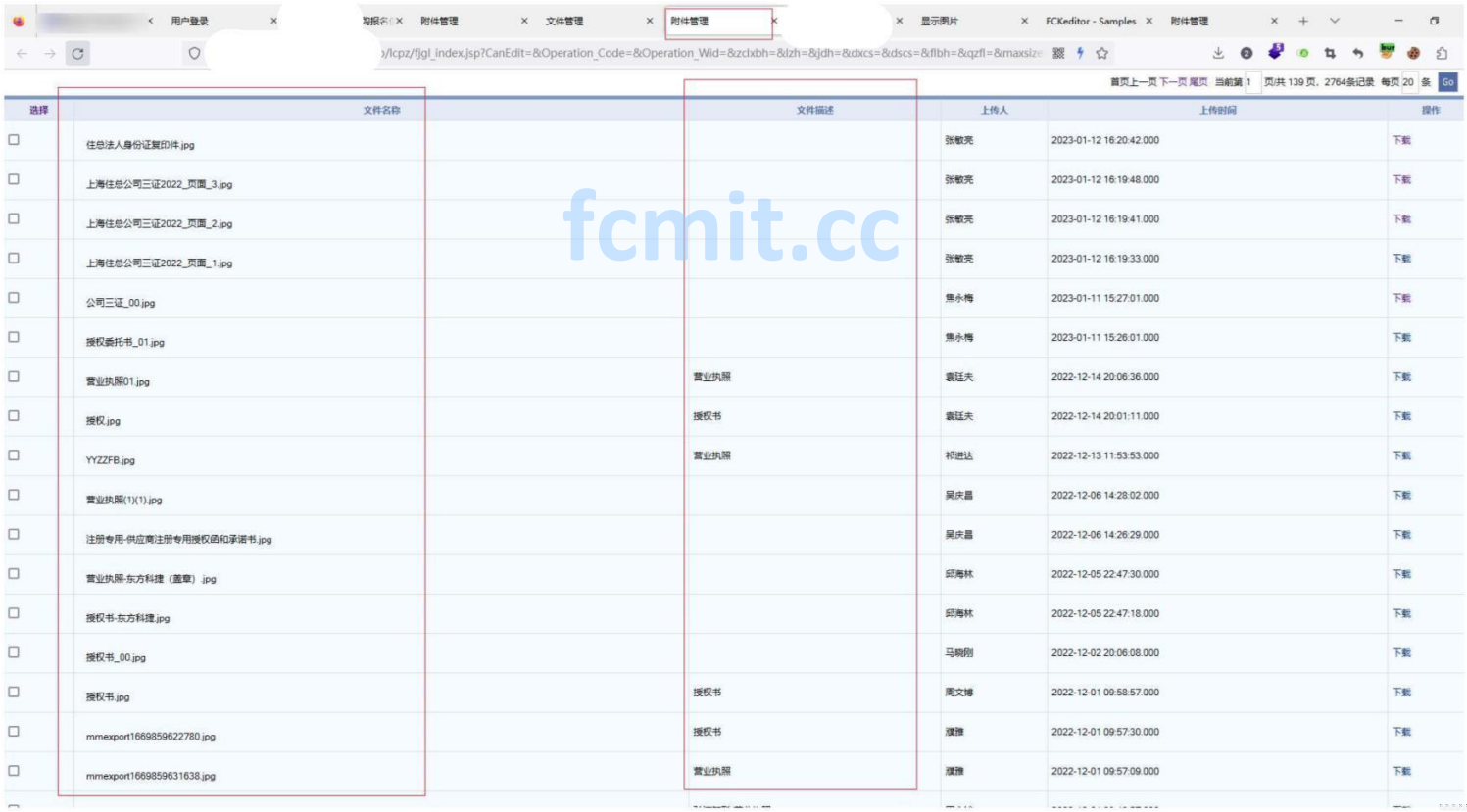
响应报文出现：jpg$1，应该就是检测jpg



把这个jpg$1直接删除，然后后面的报文全放包就可以。浏览器会回显不正常：

点击新窗口打开网站，直接得到了一个附件管理接口：

CanEdit=&Operation_Code=&Operation_Wid=&zclxbh=&lzh=&jdh=&dxcs=&dscs=&flbh=&qzfl=&maxsize=1&returnFileSize=&BYZD1=&BYZD2=&BYZD3=&



此时可以下载任意文件了：部分敏感信息已经打码

单位负责人授权书

本授权书声明：注册于上海市闵行区苏召路 1628 号　　的

公司　　的　　（单位负责人姓名、职务）代表本公司授权（单位）的在下面签字的　　（被授权人的姓名、职务）为本公司的合法代理人，就华东师范大

实验室）项目，项目编　　（项目名称、项目编号）提交响应文件、澄清答复、谈判、签约、执行、完成和保修，并以本公司名义处理一切与之有关的事务。

本授权书

特此声明。

授权代表签字盖章：

代理人（被授权人）签字盖

单位名称：上海

地址：上

法人代表授权书

本授权书声明：注册

技有限公司的在下面签字，代表本公司授权下面签字

，就华东师范

投标及合同的执行、完成和保修，以本公司名义处理一切与之有关的事务。

本授权书 签字生效，特此声明。

（附被授权人代表身份证复印件）

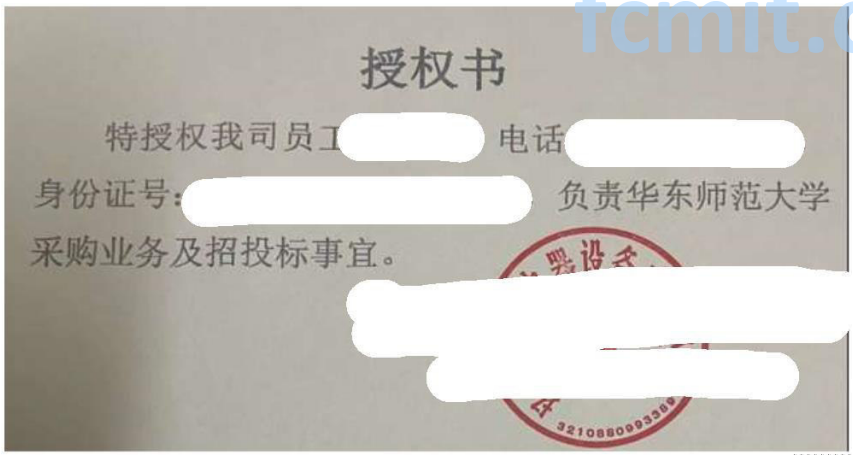
法人代表签字或盖章：

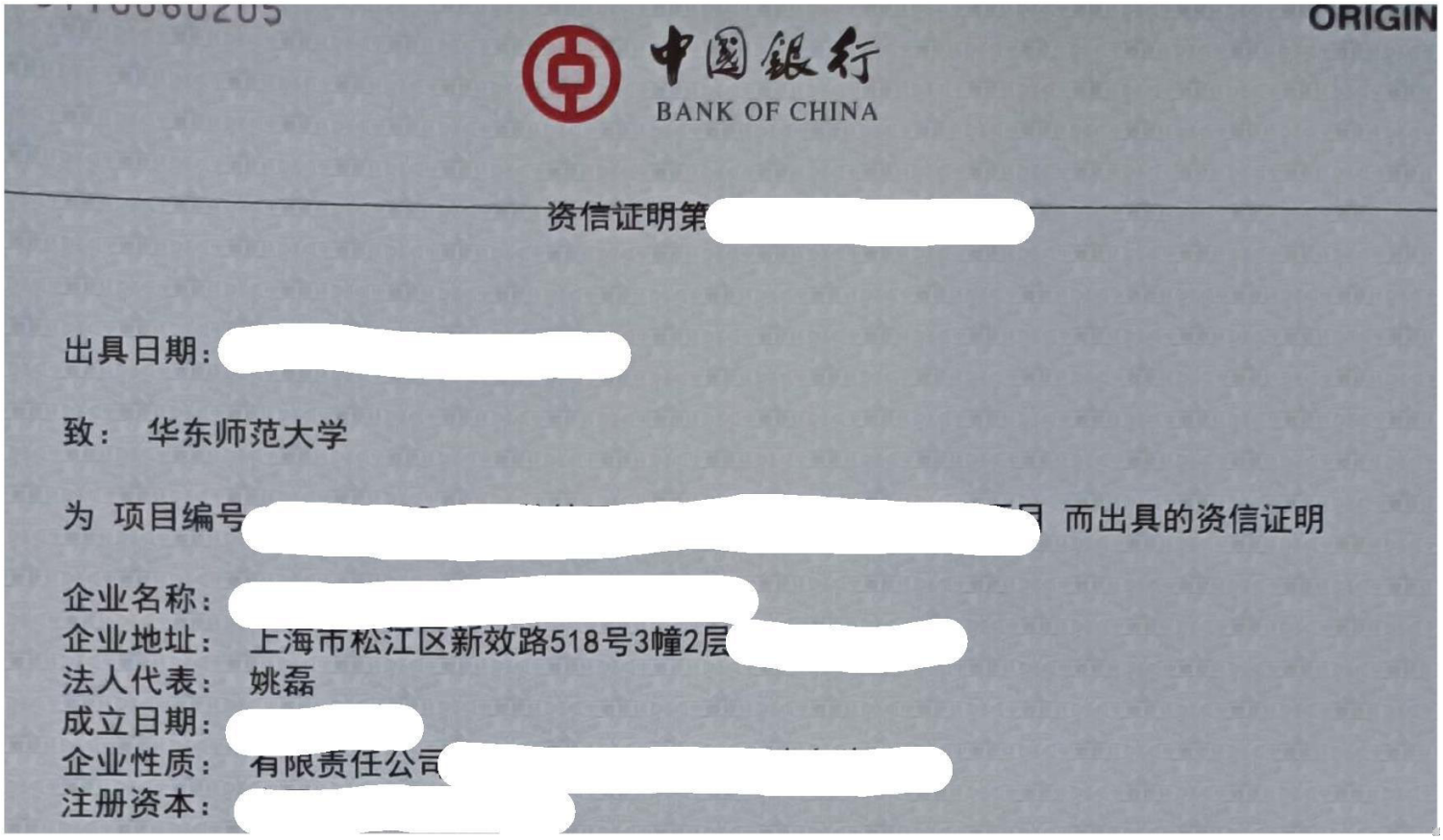
代理人（被授权人）签字或盖章：

投标人名称（盖公章）：上海吉菲电子科技有限公司

地址：

日期：





应商名称）的法定代表人，现授 （姓名、职务）为我方代理人。

代理人根据授权，以我方名义：(1)签署、澄清、补正、修改、撤回、提交

华东师范大学 项目

项目编号）响应文件；(2)签署并重新提交响应文件及最后报价；(3)退出协商；(4)签订合同和处理有关事宜，其法律后果由我方承担。

委托期限：

代理人无转委托权 字生效，特此声明。

附：委托代理人身份证复印件及法定代表人身份证明

供应商名称（盖单位章）：

法定代表人（签字）：

委托代理人（签字）：

日期

首页 上一页 下一页 尾页 当前第 7 页/共 139 页，2764条记录 每页 20 条 Go

上传时间	操作
07 11:11:48.000	下载

共**2764文件可任意下载**，并且可以点击删除功能**删除文件**（本人未尝试删除文件），涉及泄露主要信息有**公民身份证信息**，企业**营业执照**，授权书，委托书，以及**华东师范大学的项目合作合同**等重要敏感信息，通过**接口未鉴权导致的严重信息泄露**，本人已下载的文件已自行删除，请联系开发单位及时修复。

新年快乐，求高rank。

5.修复建议

（1）对该接口进行鉴权，设置非管理员用户不可查看：

CanEdit=&Operation_Code=&Operation_Wid=&zclxbh=&lzh=&jdh=&dxcs=&dscs=&flbh=&qzfl=&maxsize=1&returnFileSize=&BYZD1=&BYZD2=&BYZD3=&

（2）用户注册需要通过审核进入系统，以免攻击者批量恶意注册进入系统；

（3）对网站各个功能做好权限隔离，以免形成越权访问，导致敏感信息泄露。