**阿里云开发者社区某处存在ssrf漏洞**

**漏洞url：**



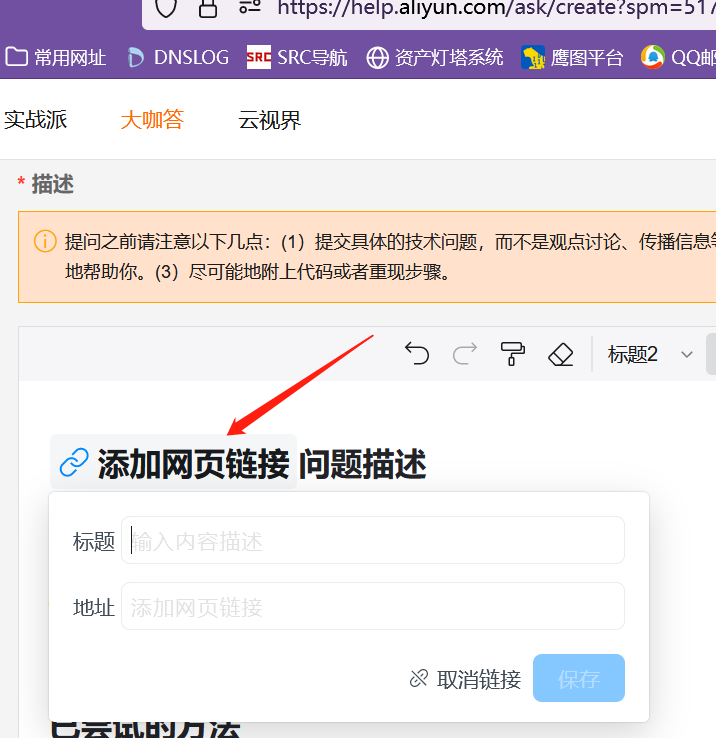
**漏洞描述以及危害：**

SSRF也就是服务端请求伪造，是指攻击者向服务端发送包含恶意URI链接的请求，借由服务端去访问此URI，以获取保护网络资源的安全漏洞，是常见的web安全漏洞的一种

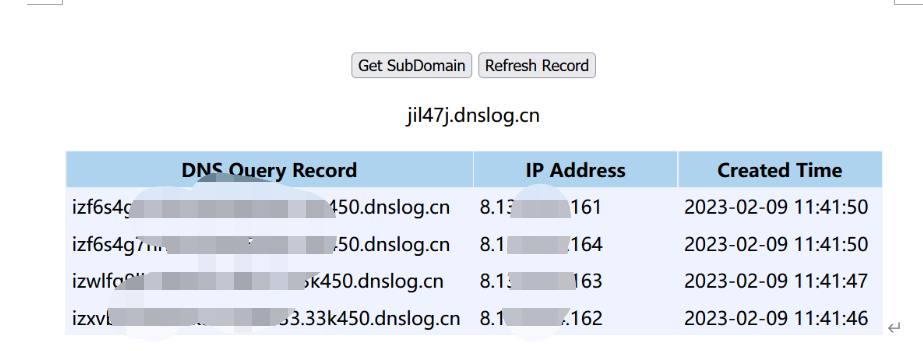
就攻击者发送链接，由服务端去请求。这种方式常常可以用来绕过网络的限制，攻击我们无法直接访问的网络

**漏洞复现：**

1. **访问该web站点帮助中心—个人中心—问题描述功能,发现一尺添加url链接位置：**

****

**2.尝试将dnslog地址插入，查看回显, 发现带MD5的回显以及内网ip**

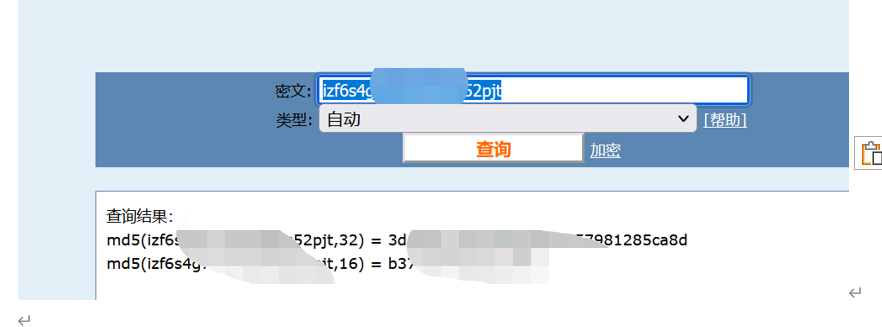


**3.查询ip属地进一步确认该请求是ssrf服务端发起的**

****

****

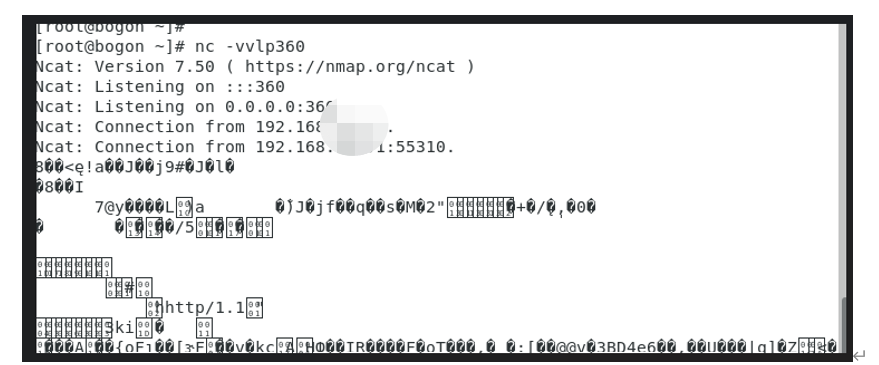
1. **dnslog的回显MD5**



1. **使用一个图片地址，看看nc是否反弹shell**



1. **发现vps反弹了shell说明存在ssrf漏洞**



**修复方案：**

1）禁用不需要的协议，限制协议为HTTP、HTTPS

2）禁止30x跳转

3）设置URL白名单或者限制内网IP