阿里云开发者社区某处存在 ssrf 漏洞

漏洞 url：

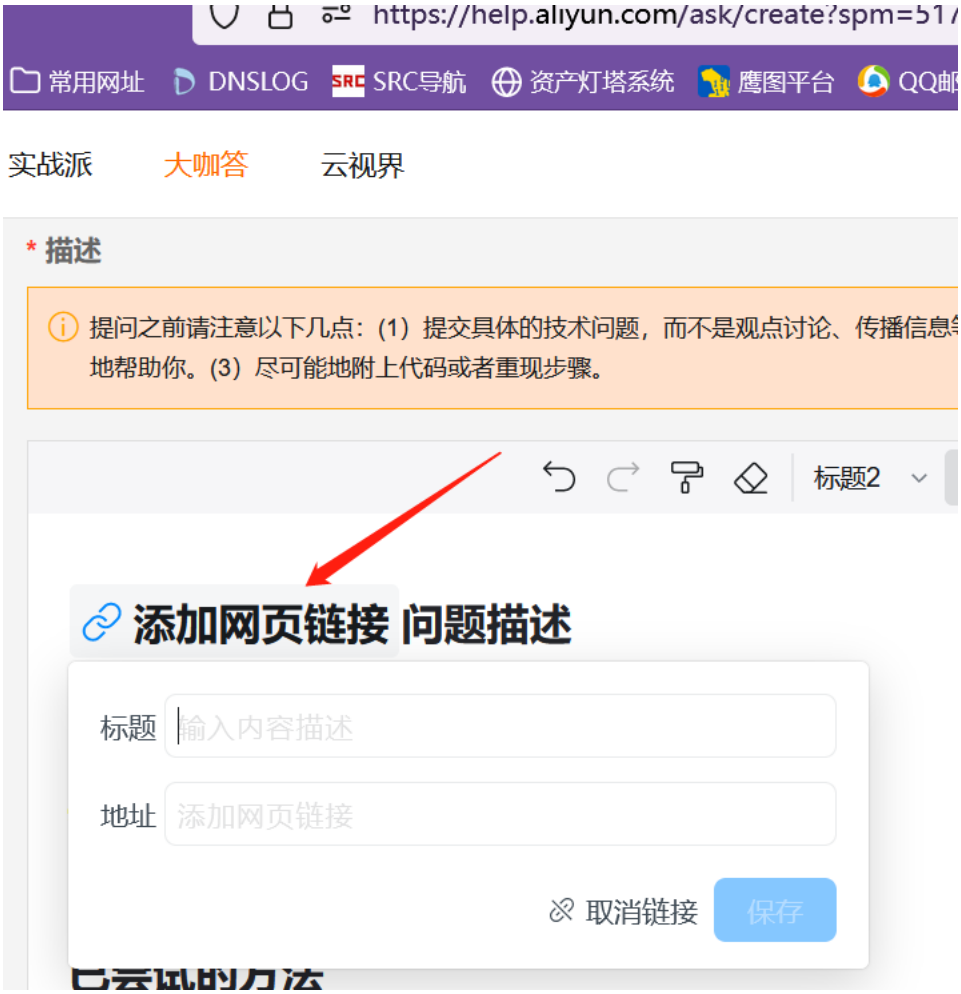
https://help.aliyun.con[redacted]fe36757OKFjE

漏洞描述以及危害：

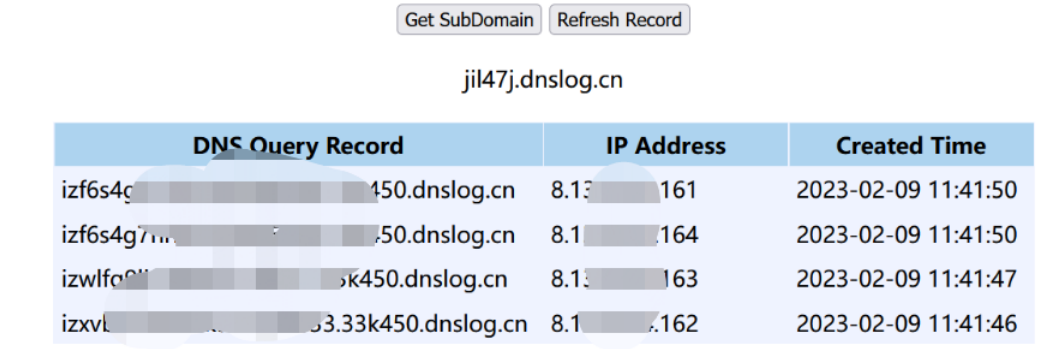
SSRF 也就是服务端请求伪造，是指攻击者向服务端发送包含恶意 URI 链接的请求，借由服务端去访问此 URI，以获取保护网络资源的安全漏洞，是常见的 web 安全漏洞的一种就攻击者发送链接，由服务端去请求。这种方式常常可以用来绕过网络的限制，攻击我们无法直接访问的网络

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

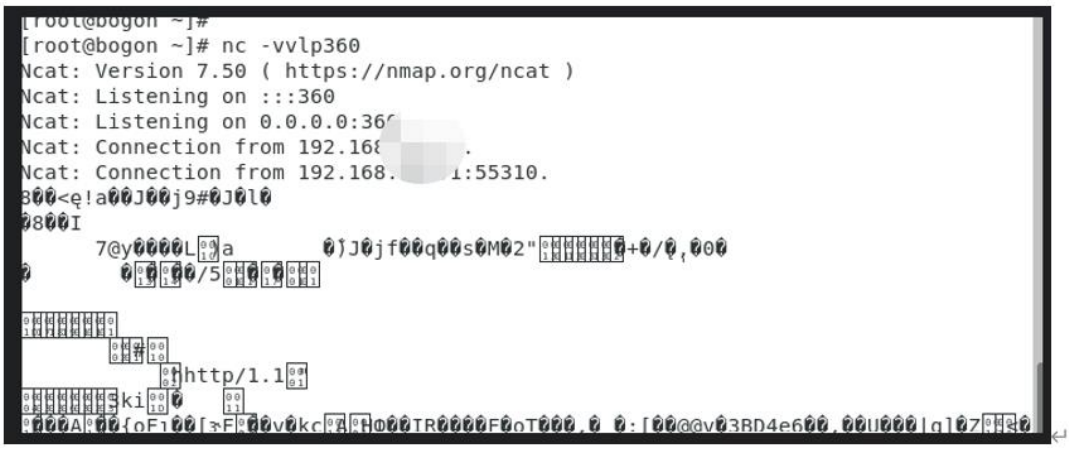


3.查询 ip 属地进一步确认该请求是 ssrf 服务端发起的

2. dnslog 的回显 MD5

3. 使用一个图片地址，看看 nc 是否反弹 shell

4. 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