

T5-1Tomcat-RCE

漏洞描述:

tomcat启用manager（后台管理）功能，且存在弱口令

漏洞复现:

在 conf/tomcat-users.xml 文件中配置用户的权限和一个弱口令 tomcat/tomcat:  
payload:

```
<tomcat-users>
<role rolename="manager-gui"/>
<role rolename="manager-script"/>
<role rolename="manager-jmx"/>
<role rolename="manager-status"/>
<role rolename="admin-gui"/>
<role rolename="admin-script"/>
<user username="tomcat" password="tomcat" roles="manager-gui,manager-script,manager-jmx,manager-status,admin-gui,admin-script"/>
</tomcat-users>
```

效果图:  
访问http://192.168.110.49:8080/manager/html，输入用户名密码可进行后台部署war包getshell

192.168.110.49:8080/manager/html

收集

沙箱

study

MD5

靶场

ZY

php解密加密|php混...

行云管家

	None specified	Serviet and JSP Examples	true
	None specified	Tomcat Host Manager Application	true
	None specified	Tomcat Manager Application	true

ry or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

ploy

Select WAR file to upload

浏览...

未选择文件。

Deploy