# CVE-2023-29922

Powerjob 未授权访问漏洞

目录

[1. 漏洞描述 3](#_Toc27475)

[2. 影响版本 3](#_Toc25949)

[3. 环境部署 3](#_Toc5232)

[4. 漏洞复现 6](#_Toc11219)

# 漏洞描述

PowerJob 的设计目标为企业级的分布式任务调度平台，即成为公司内部的任务调度中间件。整个公司统一部署调度中心 powerjob-server，旗下所有业务线应用只需要依赖 powerjob-worker 即可接入调度中心获取任务调度与分布式计算能力。

PowerJob 受影响版本中由于 JobController#listJobs 方法未对用户身份进行校验，攻击者可通过向 /job/list 接口发送POST请求，指定 appId 参数即可列出对应的正在运行的任务列表以及它们的状态信息。

# 影响版本

PowerJob 4.3.1

# 环境部署

靶机：CentOs7，ip：192.168.88.114

渗透机：Windows 11，ip：192.168.88.2

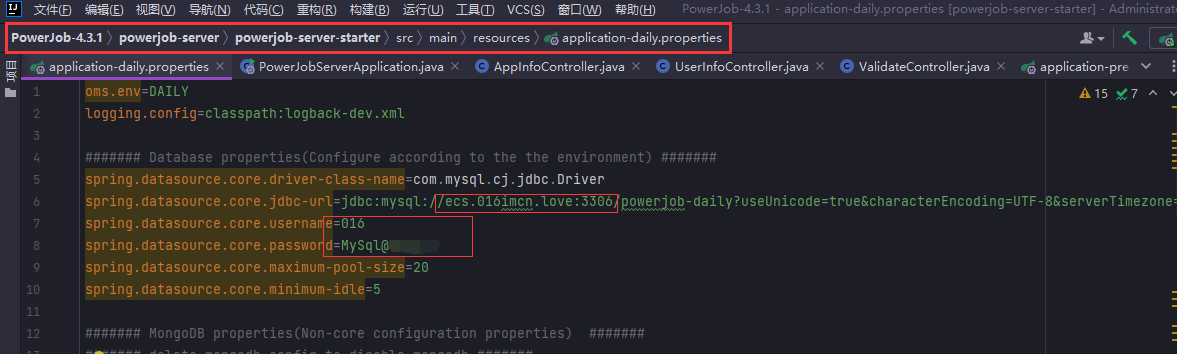
下载含有该漏洞的软件版本

https://github.com/PowerJob/PowerJob/archive/refs/tags/v4.3.1.zip

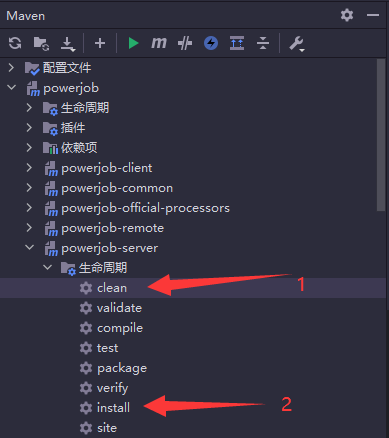
为项目创建数据库

CREATE DATABASE IF NOT EXISTS `powerjob-daily` DEFAULT CHARSET utf8mb4;

修改项目的配置文件，为该项目指定数据库路径



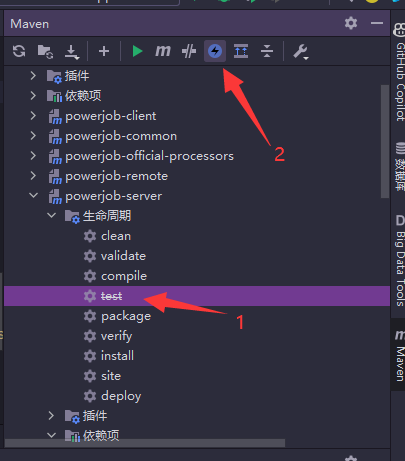
使用maven工具为powerjob服务端打包



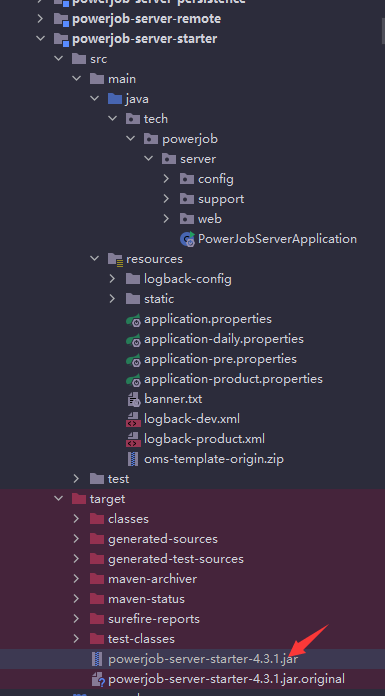
切记：使用jdk1.8来install，否则会出现报错class lombok.javac.apt.LombokProcessor (in unnamed module @0x4f3356c0) cannot access class com.sun.tools.javac.processing.JavacProcessingEnvironment (in module jdk.compiler) because module jdk.compiler does not export com.sun.tools.javac.processing to unnamed module @0x4f3356c0

原因是其使用的lombok框架需要低版本的jdk

随后发现maven的test报错，原因未知，禁用test命令，随后执行package命令代替install

禁用过程

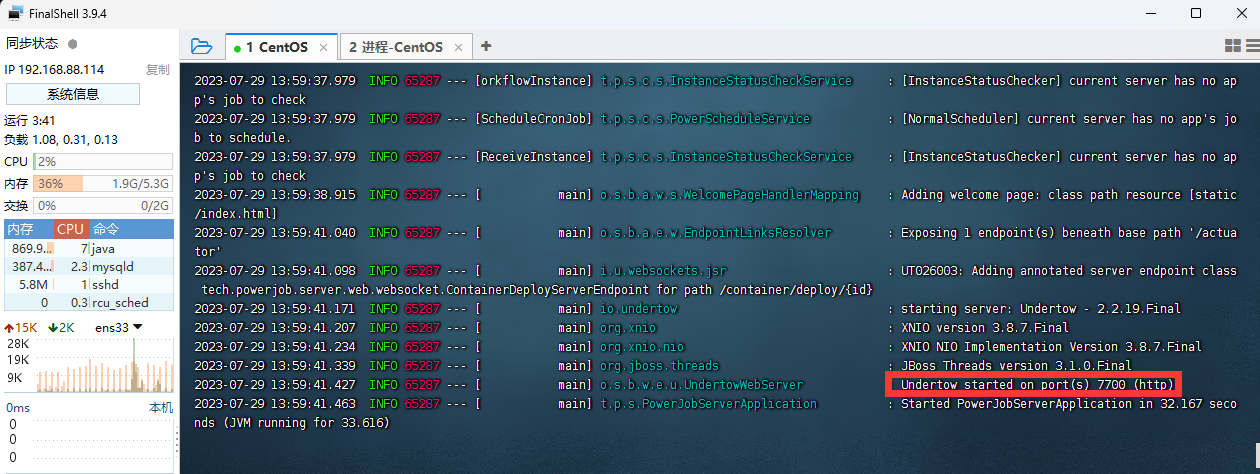
随后使用package命令



执行完成后找到打包好的程序，上传至靶机



运行程序

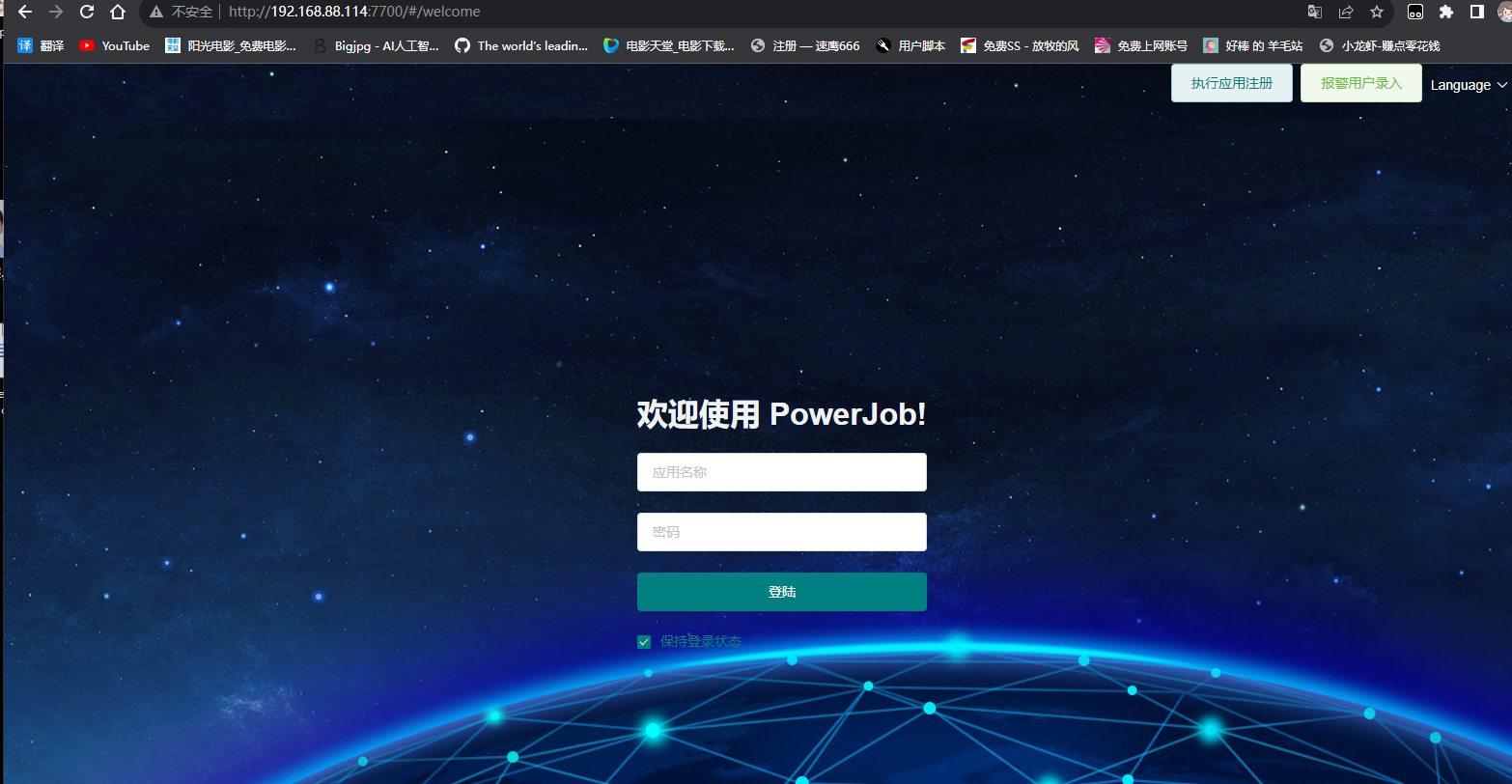


程序运行成功

# 漏洞复现

**【步骤一】**

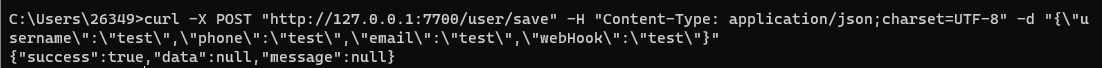
**访问程序主页http://192.168.88.114:7700**



**成功运行**

**【步骤二】**

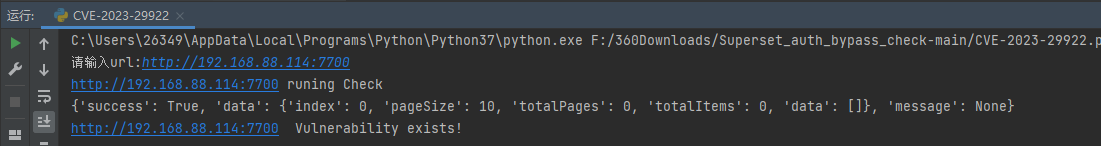
**发送一段注册用户命令（https://github.com/PowerJob/PowerJob/issues/585）**



**执行成功**

**【步骤三】**

执行CVE-2023-29922.py脚本



**发现漏洞存在**