# CVE-2023-27524

Apache Superset 默认SECRET\_KEY 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 5](#_Toc11219)

# 漏洞描述

Apache Superset 是一款现代化的开源大数据工具，也是企业级商业智能 Web 应用，用于数据探索分析和数据可视化。它提供了简单易用的无代码可视化构建器和声称是最先进的 SQL 编辑器，用户可以使用这些工具快速地构建数据仪表盘。CVE-2023-27524 中，未经授权的攻击者可根据默认配置的SECRET\_KEY伪造成管理员用户访问Apache Superset。

# 影响版本

Apache Superset 2.0.1 版本及之前版本

# 环境部署

靶机：CentOs7，ip：192.168.88.114

渗透机：Windows 11，ip：192.168.88.2

部署参考链接：

<https://blog.csdn.net/wangqinyi574110/article/details/130822597>

<https://blog.csdn.net/Jahson/article/details/120802477>

<https://blog.csdn.net/MicalChen/article/details/120240580>

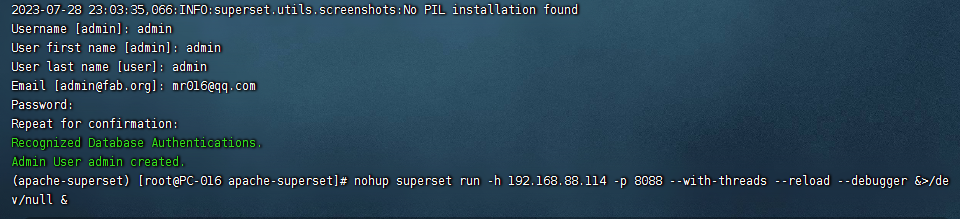
使用的命令

|  |
| --- |
| # 使用python虚拟环境  cd /opt/  python3 -m venv apache-superset  # 激活python虚拟环境  source apache-superset/bin/activate  # 更新pip版本  /opt/apache-superset/bin/python3 -m pip install --upgrade pip  安装apache-superset,安装版本为2.0.0。  pip install apache-superset==2.0.0 -i https://pypi.tuna.tsinghua.edu.cn/simple/  # 因为依赖的关系需要修改这几个依赖的版本  cd /opt/apache-superset/lib/python3.9/site-packages/superset  pip install --force-reinstall cryptography==38.0.4  pip install 'urllib3[secure]==1.26' -i https://pypi.tuna.tsinghua.edu.cn/simple/  pip install --force-reinstall Werkzeug==2.0.3 -i https://pypi.tuna.tsinghua.edu.cn/simple/  pip install --force-reinstall Flask==2.0.3 -i https://pypi.tuna.tsinghua.edu.cn/simple/  pip install --force-reinstall WTForms==2.3.3 -i https://pypi.tuna.tsinghua.edu.cn/simple/  pip install --force-reinstall Werkzeug==2.0.3 -i https://pypi.tuna.tsinghua.edu.cn/simple/ ## 重新安装Werkzeug是因为Flask可能对这个有依赖关系。  # 初始化一些系统权限相关的账号、角色等功能  cd /opt/apache-superset  export FLASK\_APP=superset  cd bin/  python superset db upgrade  superset fab create-admin  # 导入一些示例数据  superset load\_examples  # 初始化默认的角色和权限  superset init  export FLASK\_APP=superset  nohup superset run -h 192.168.88.114 -p 8088 --with-threads --reload --debugger &>/dev/null & |

# 漏洞复现

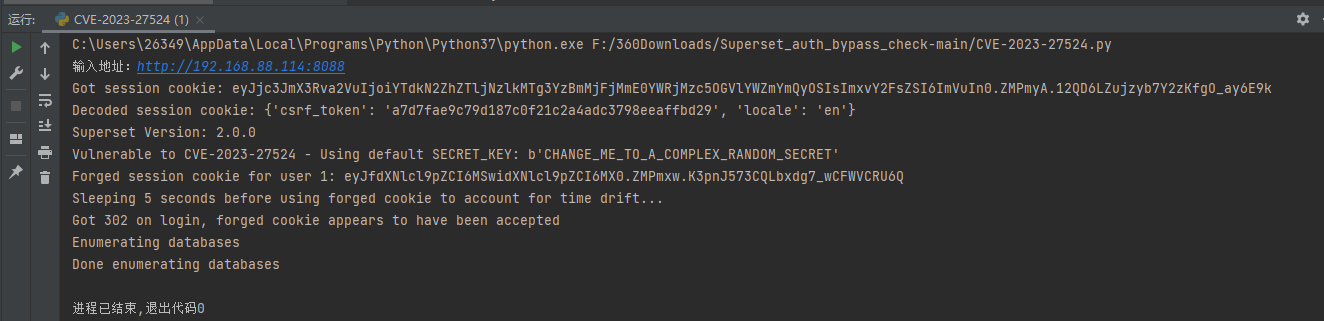
**【步骤一】**

为Apache Superset创建管理员用户：superset fab create-admin



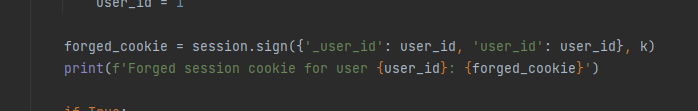
**【步骤二】**

使用CVE-2023-27524.py运行，并输入输入地址：<http://192.168.88.114:8088>，发现，成功执行代码并成功得到权限登陆。

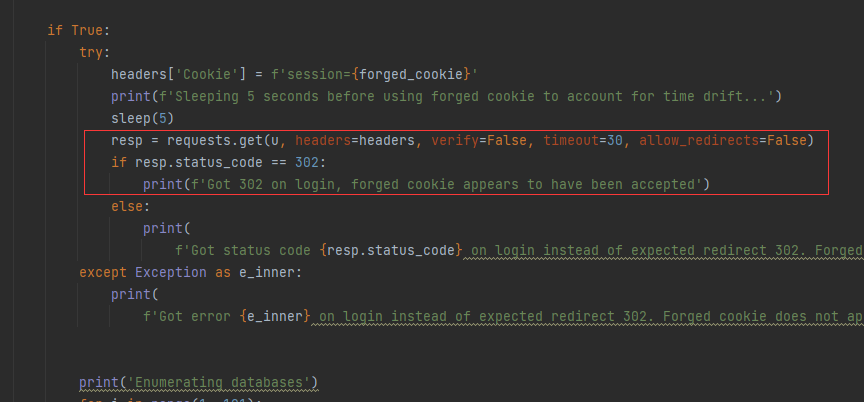


该代码利用了Apache Superset 默认SECRET\_KEY来伪造成管理员用户访问Apache Superset。





伪造管理员设置cookie



当携带着关于管理员的cookie时，访问主页发生了302重定向指管理页面，漏洞利用成功，

并且会扫描该系统下的所有数据库。

此漏洞能够轻易拿到该系统的管理员权限。