

(CVE-2022-43781) 漏洞POC

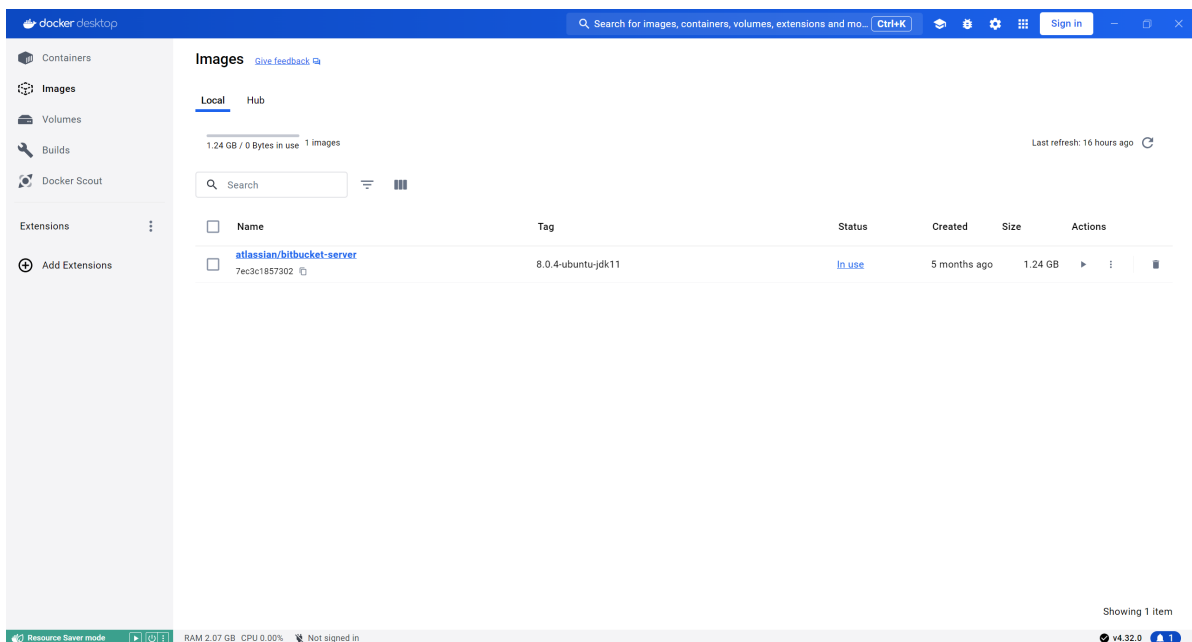
1.环境搭建

1.1 版本

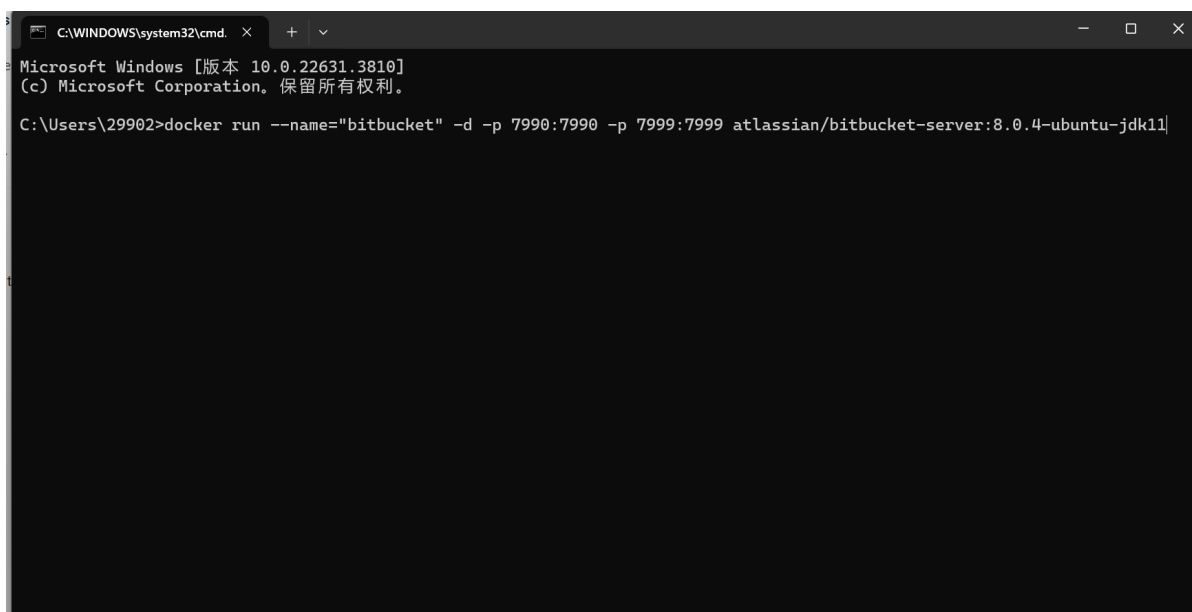
- 主机环境: docker+wsl2
- 漏洞复现版本: atlassian/bitbucket-server:7.0-ubuntu-jdk11
- 虚拟机环境: kali-2024.1

1.2 环境搭建过程

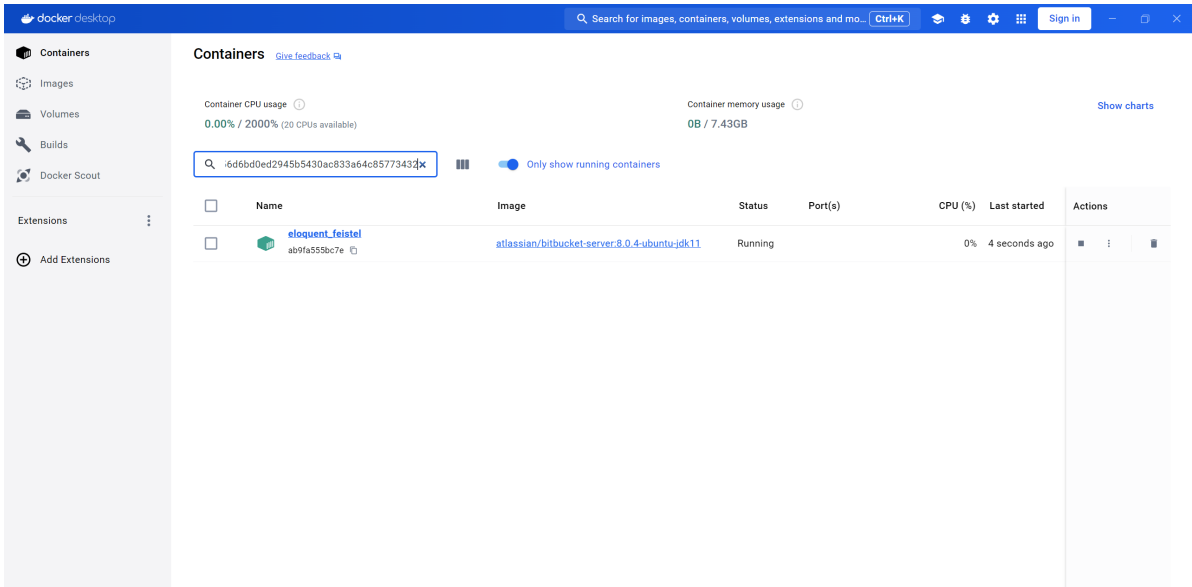
- 利用docker拉取atlassian/bitbucket-server:8.0.4-ubuntu-jdk11镜像到主机（需要会科学上网，国内镜像源并没有所需镜像）



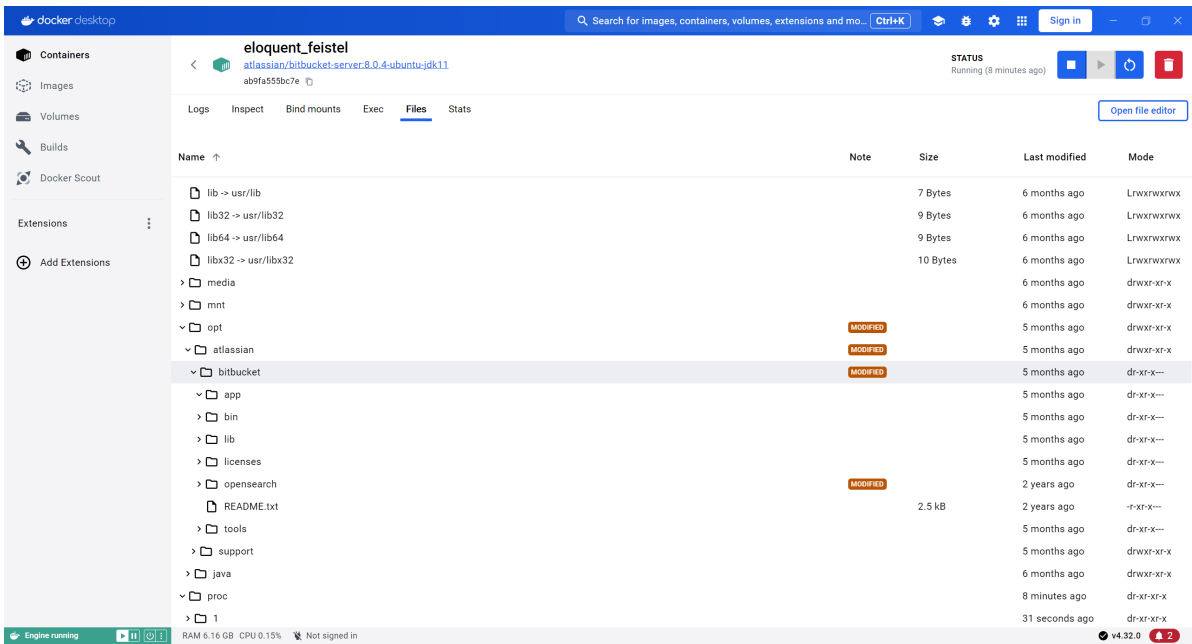
- 利用镜像构建容器



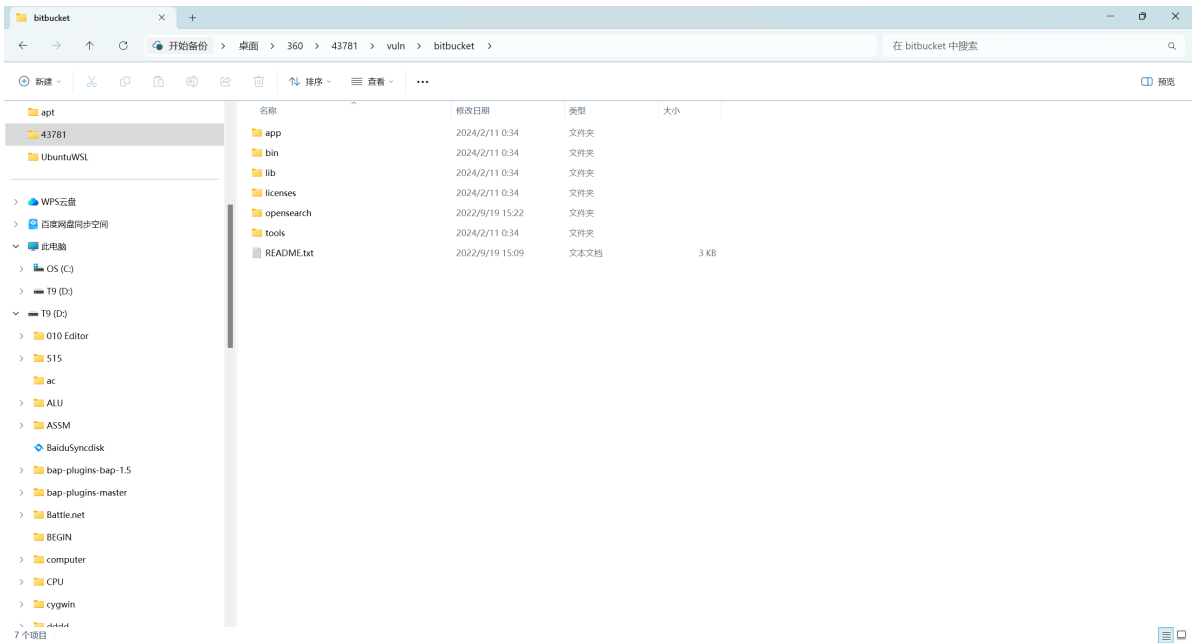
- 成功运行如图所示，端口号映射保持不变



- 找到应用安装处：



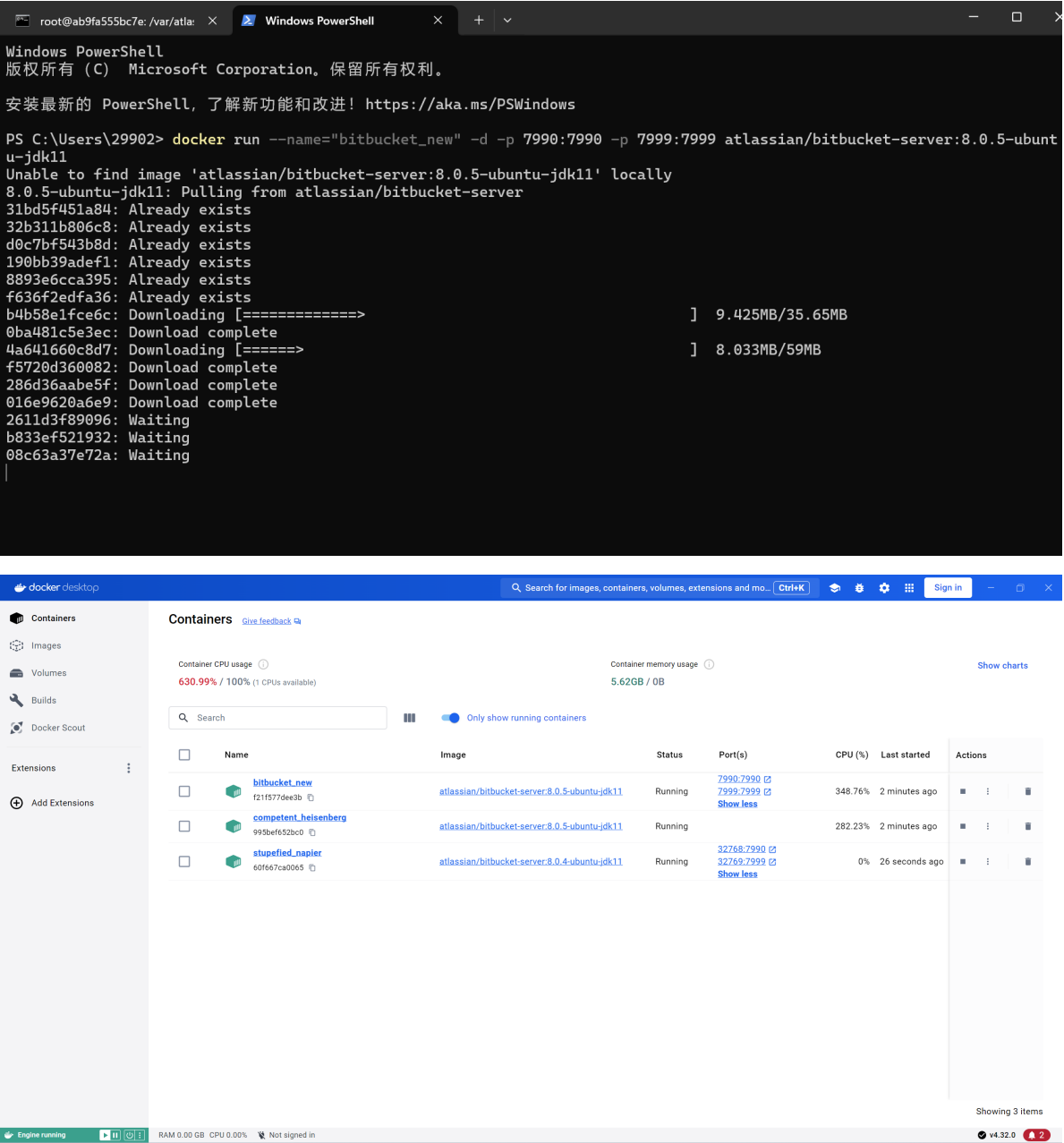
- 最终需要分析代码如图所示：

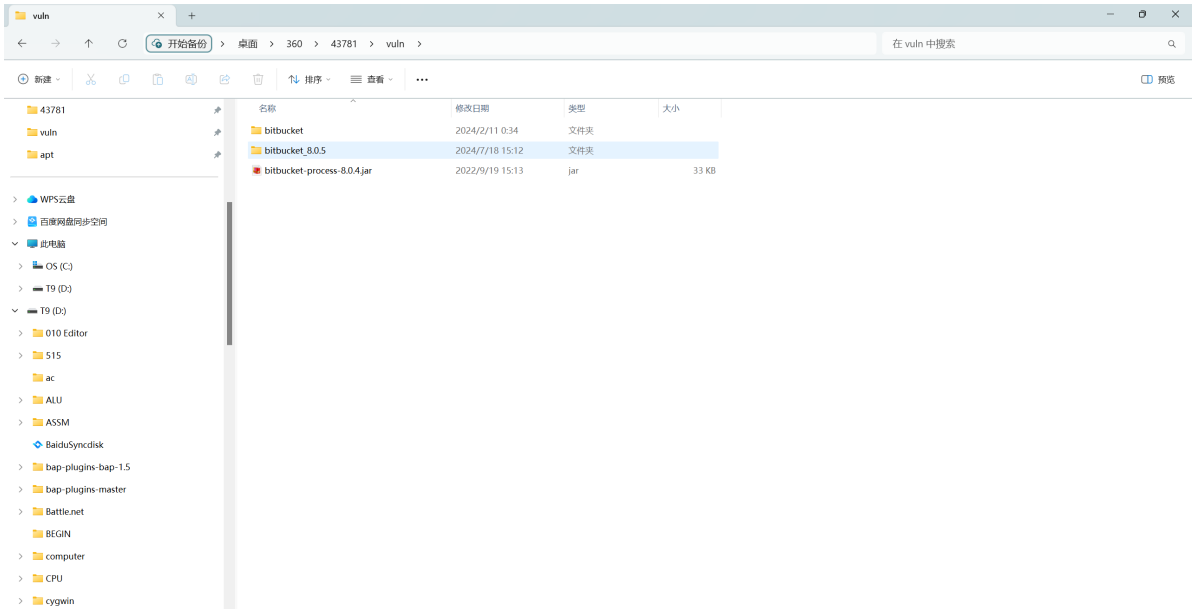


2.代码分析

因代码量庞大，为了便于寻找漏洞可以下载高版本的已修复漏洞版本进行diff对比

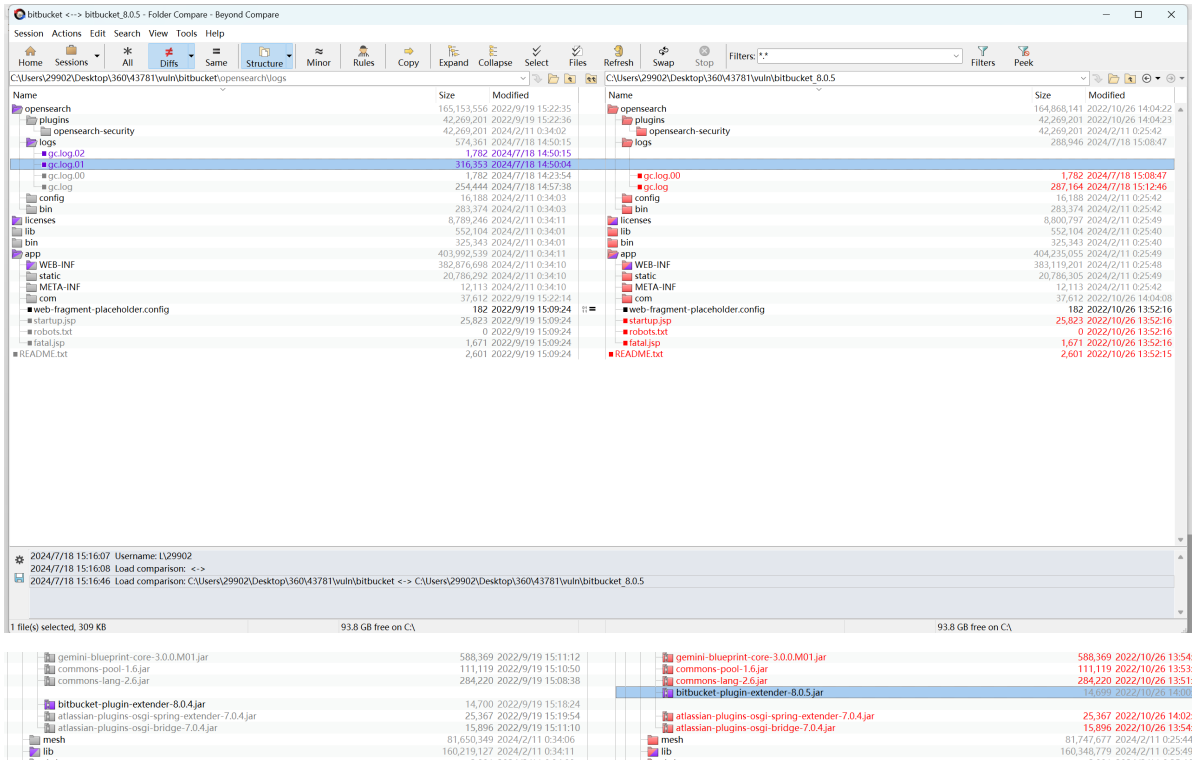
2.1利用第一小节的方法进行8.0.5版本应用的下载，如图所示：



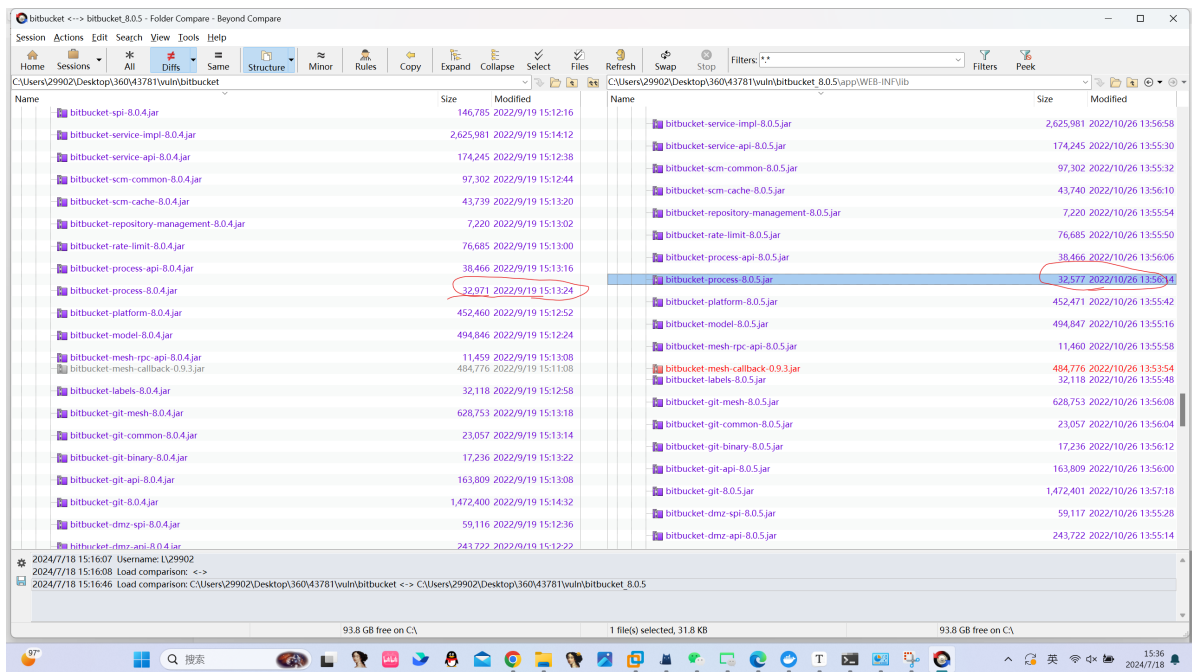


2.2利用diff软件进行文件比对

紫色代表差异部分，其中licenses目录忽略，osgi-framework-bundles目录为osgi的bundle 所在目录，打开可以看到对比结果

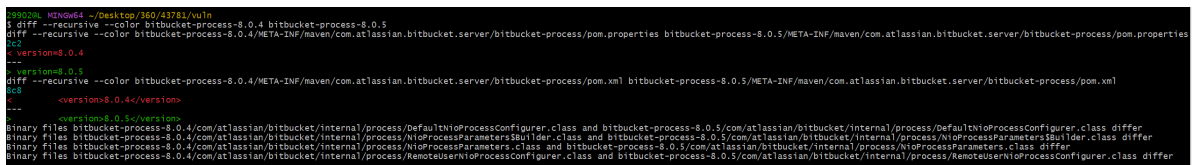


大小相差只有1字节，排除（14700vs14699）。接着是 atlassian-bundled-plugins目录为插件目录（可以不用管），接着看lib根据大小和jar包的名称过一圈，最终锁定为app/WEB-INF/lib/bitbucket-process-8.0.x.jar：



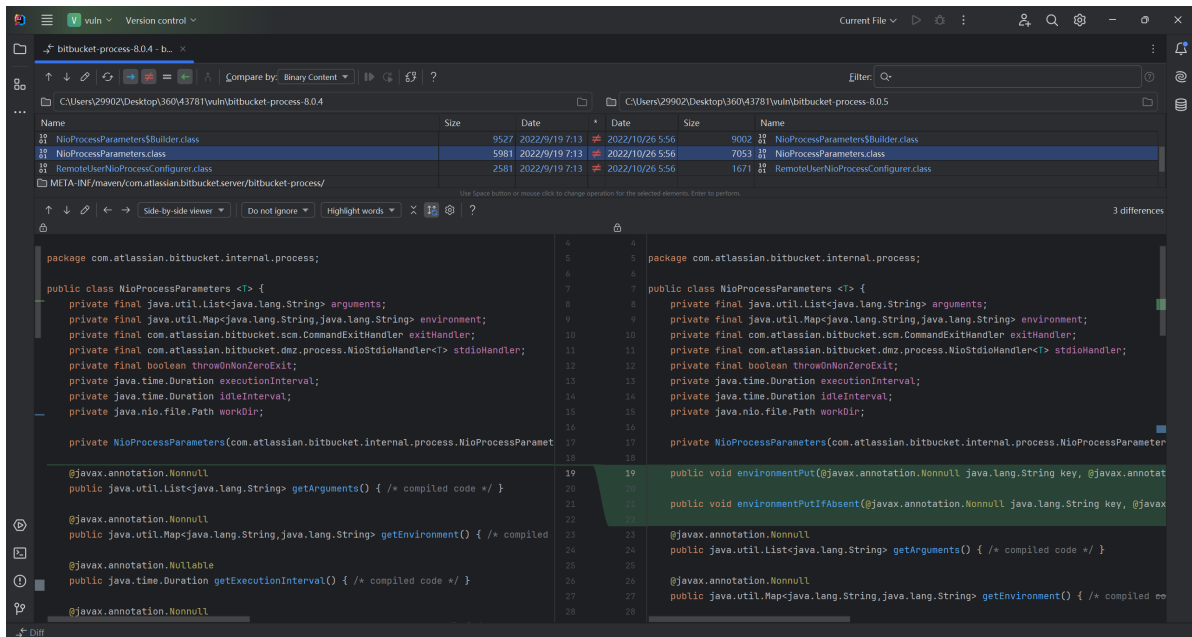
2.3利用diff软件进行代码比对，定位差异位置

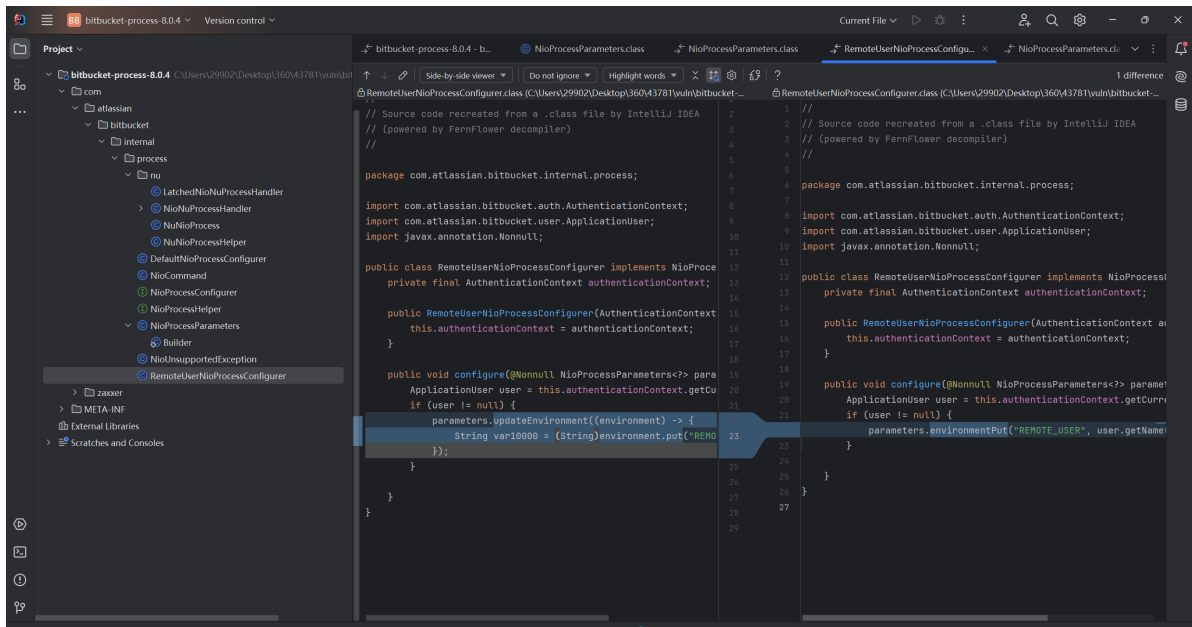
将jar解压后利用git的diff进行代码比对，找到对应不同的class区域，分别为：
DefaultNioProcessConfigurer.class, NioProcessParameters\$Builder.class,
NioProcessParameters.class, RemoteUserNioProcessConfigurer.class



2.4利用ida进行代码比对，定位差异位置

可以看到在8.0.5的版本新增了environmentPut和environmentPutIfAbsent两个函数，其中核心的判断逻辑是对传入值是否为0x00进行了检查，并且在
com.atlassian.bitbucket.internal.process.RemoteUserNioProcessConfigurer 中在将用户名放入环境变量时使用environmentPut代替了原先直接put的操作





而漏洞的描述信息说是由用户控制用户名从而控制环境变量导致命令注入，至此推断基本吻合。


Summary of Vulnerability

This advisory discloses a critical severity security vulnerability introduced in version 7.0.0 of Bitbucket Server and Data Center. The following versions are affected by this vulnerability:

- Bitbucket Data Center and Server 7.0 to 7.21
- Bitbucket Data Center and Server 8.0 to 8.4 if `mesh.enabled` is set to false in `bitbucket.properties`

There is a command injection vulnerability using `environment variables` in Bitbucket Server and Data Center. An attacker with permission to control their username can exploit this issue to gain code execution and execute code on the system.

This issue can be tracked here:

 **BSERV-13522** - Critical severity command injection vulnerability - CVE-2022-43781
PUBLISHED

3.漏洞触发

因为8.0.4版本需要更改一个配置才能出发漏洞，因此漏洞触发用7.0的版本实现，可用此命令获得：`docker run --name="bitbucket" -d -p 7990:7990 -p 7999:7999 atlassian/bitbucket-server:7.0-ubuntu-jdk11`
Unable to find image 'atlassian/bitbucket-server:7.0-ubuntu-jdk11' locally

3.1寻找能够触发命令执行的Git环境变量

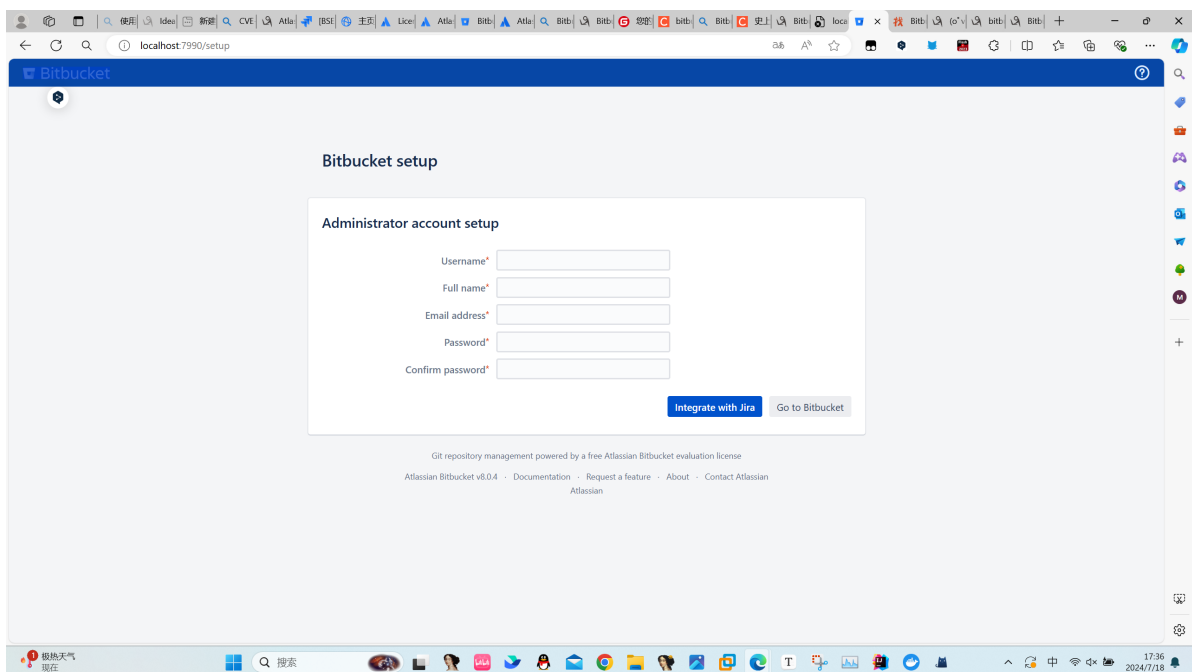
找到GIT_SSH_COMMAND环境变量，Bitbucket调用Git命令，则会同时执行GIT_SSH_COMMAND中的命令。测试如下：

```
# ls
docker-app.pid log shared tmp
# export GIT_SSH_COMMAND='touch /tmp/pwned'
# cat GIT_SSH_COMMAND
cat: GIT_SSH_COMMAND: No such file or directory
# echo GIT_SSH_COMMAND
GIT_SSH_COMMAND
# GIT_SSH_COMMAND
/bin/sh: 5: GIT_SSH_COMMAND: not found
# git clone git@github.com:MagicZero/demo.git
Cloning into 'demo'...
touch: cannot touch "git-upload-pack 'MagicZero/demo.git'": No such file or directory
fatal: Could not read from remote repository.

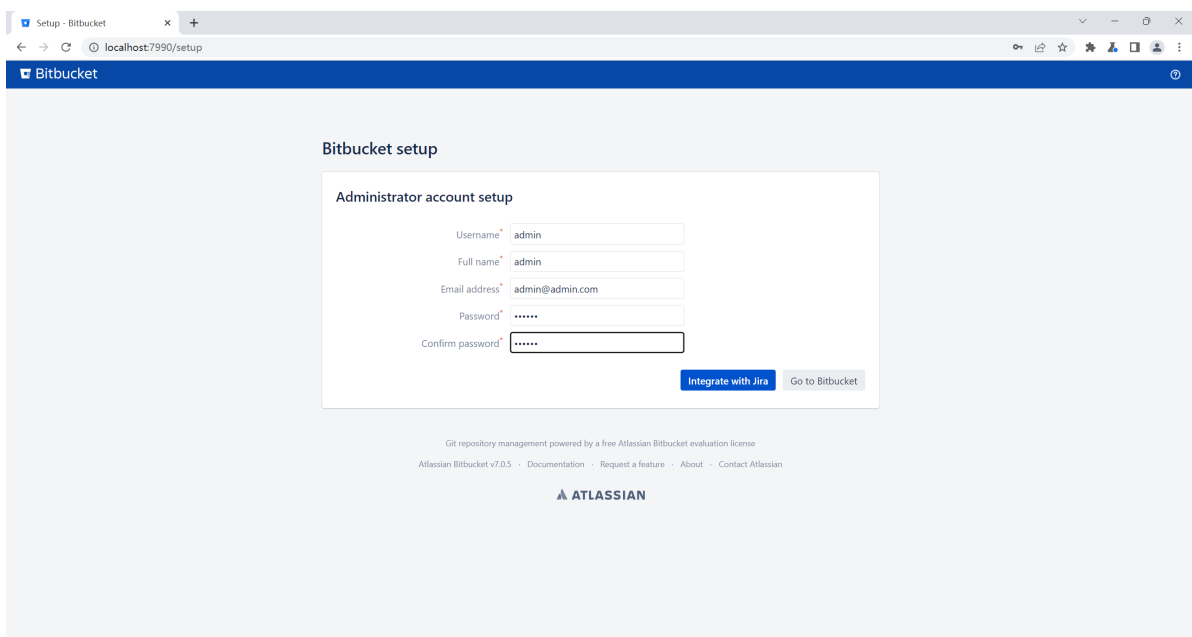
Please make sure you have the correct access rights
and the repository exists.
# ls
analytics-logs bin caches docker-app.pid export git@github.com home.properties lib log mesh plugins shared tmp
# ls /tmp/
hsperfdata_bitbucket hsperfdata_root pwned
#
```

可观察到创建了pwned文件，测试成功

3.2Bitbucket账号注册

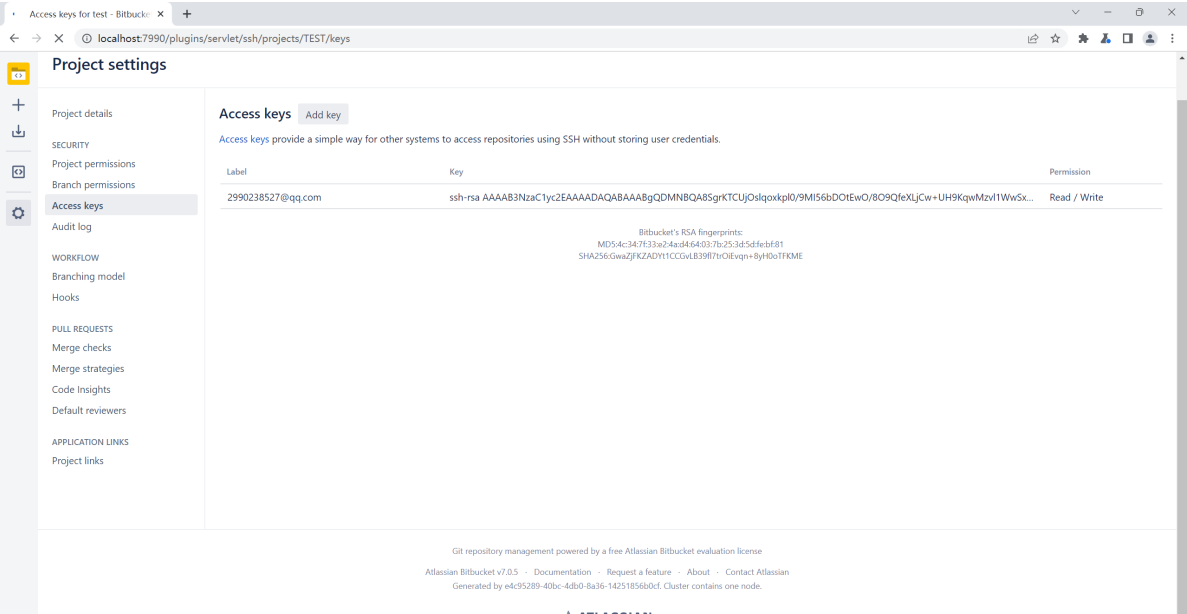


3.3利用bp注册admin账户作为管理员

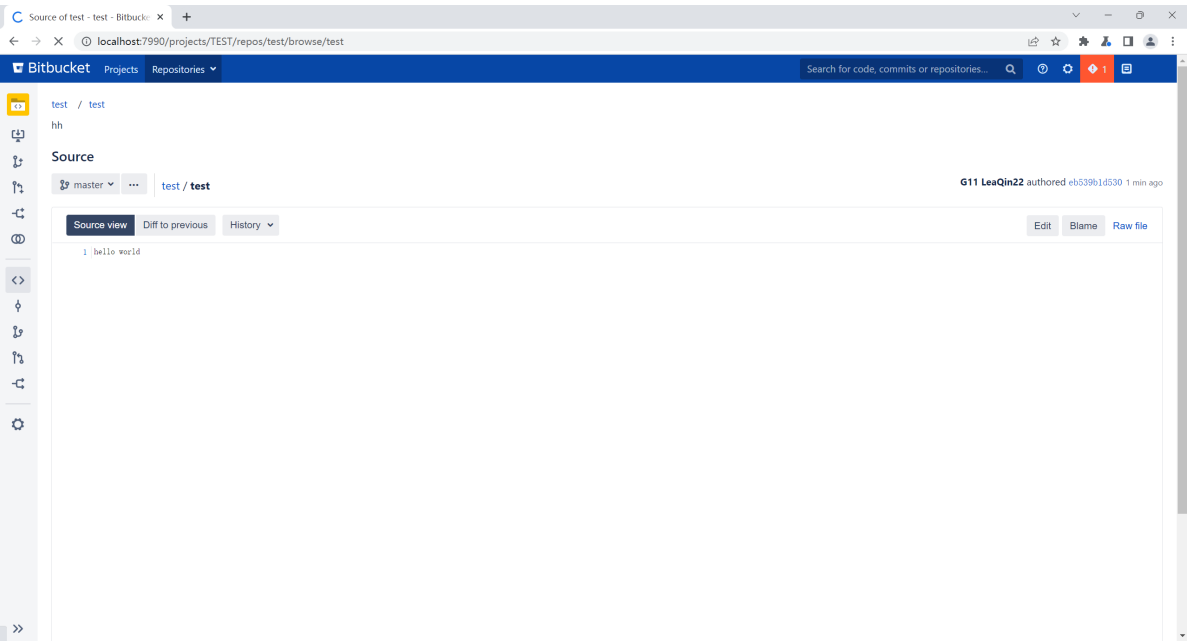


3.4建立public库

需要ssh key 与库建立连接，这点就不多说了



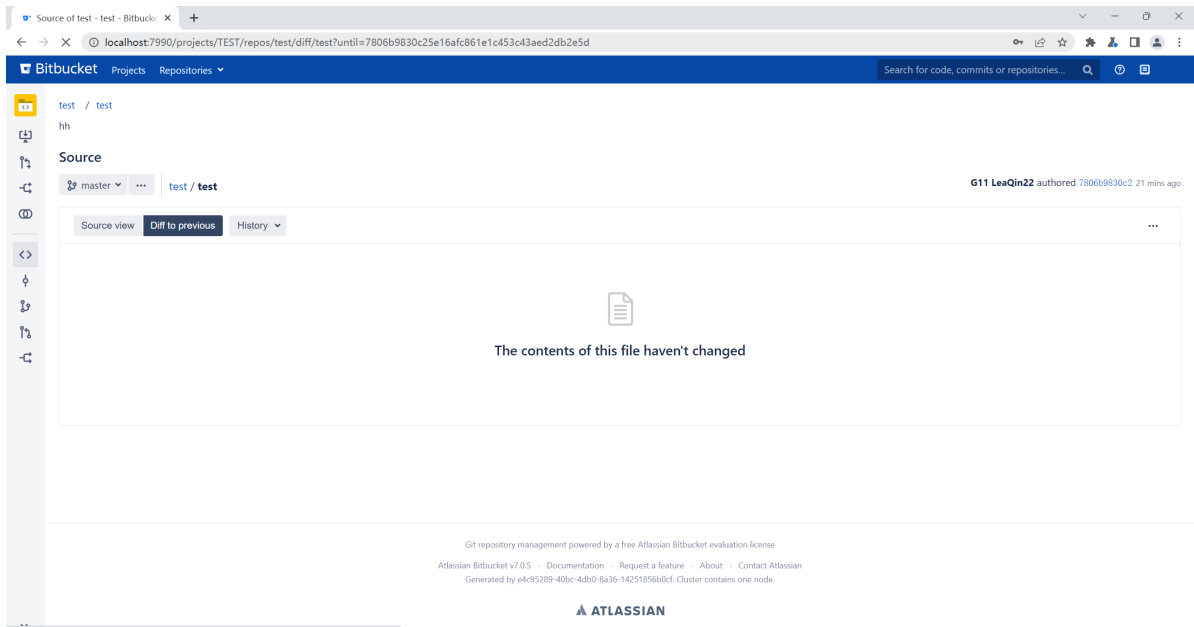
3.4利用git添加内容



3.5创建命令注入用户名



3.6 点击diff触发漏洞



3.6得到结果

