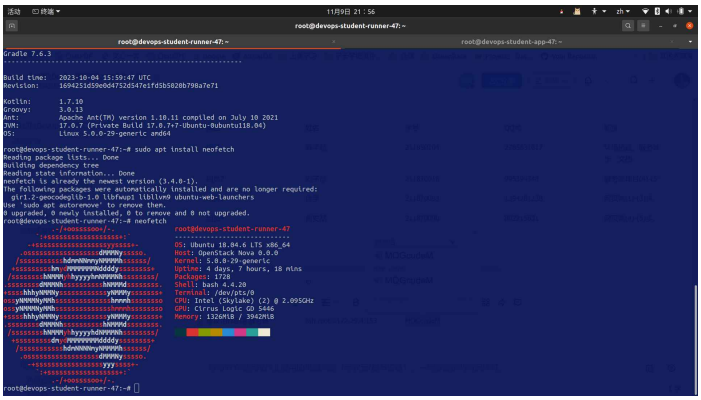
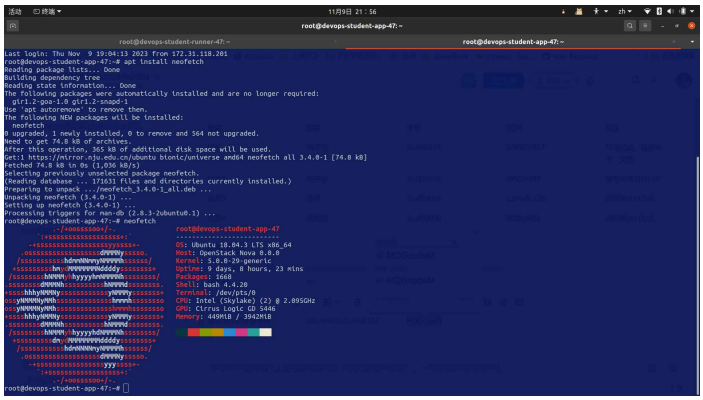
DevSecOps

承载平台：南软云

服务器	ip	密码
runner	ssh root@172.29.4.131	VKVSXmR3
建议用作部署服务器	ssh root@172.29.4.153	MQGcudeM





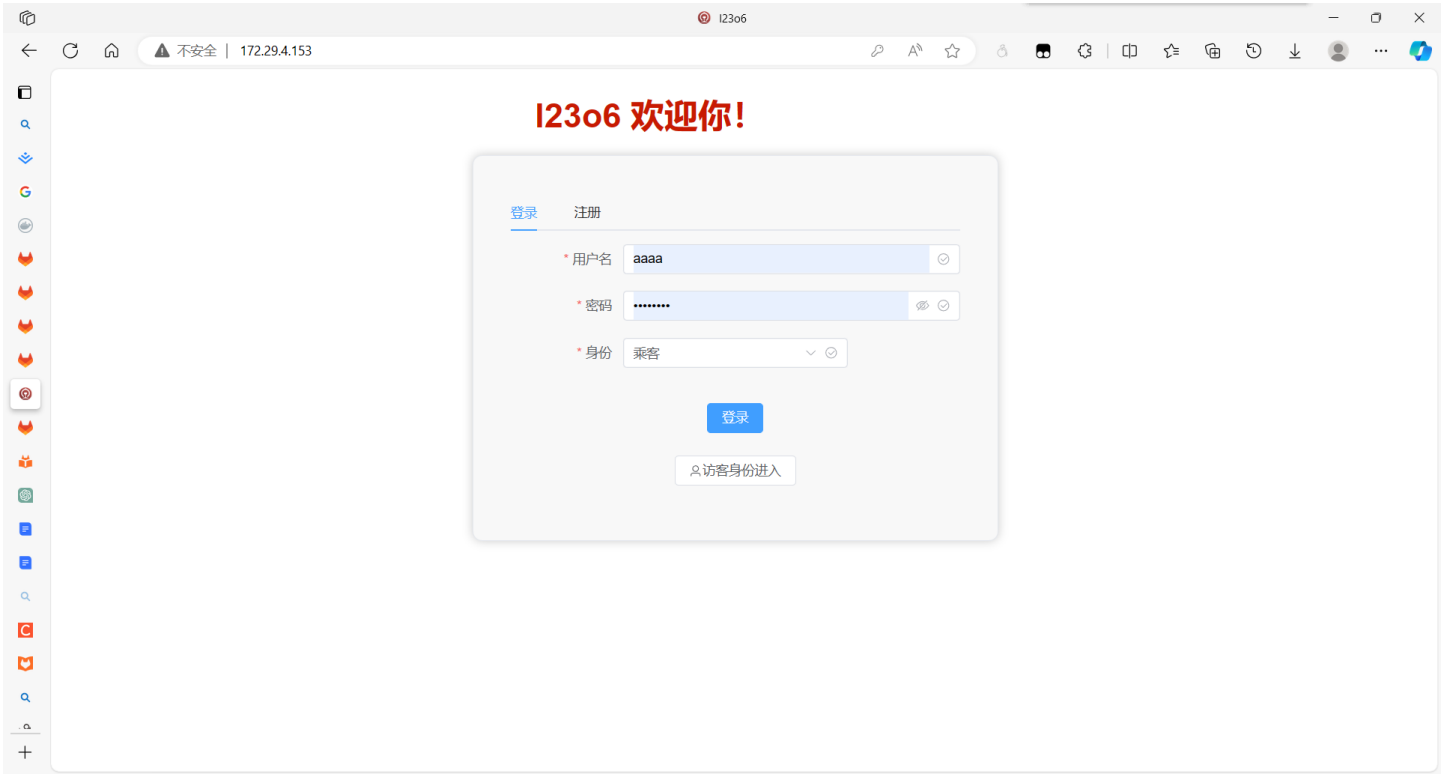
项目功能

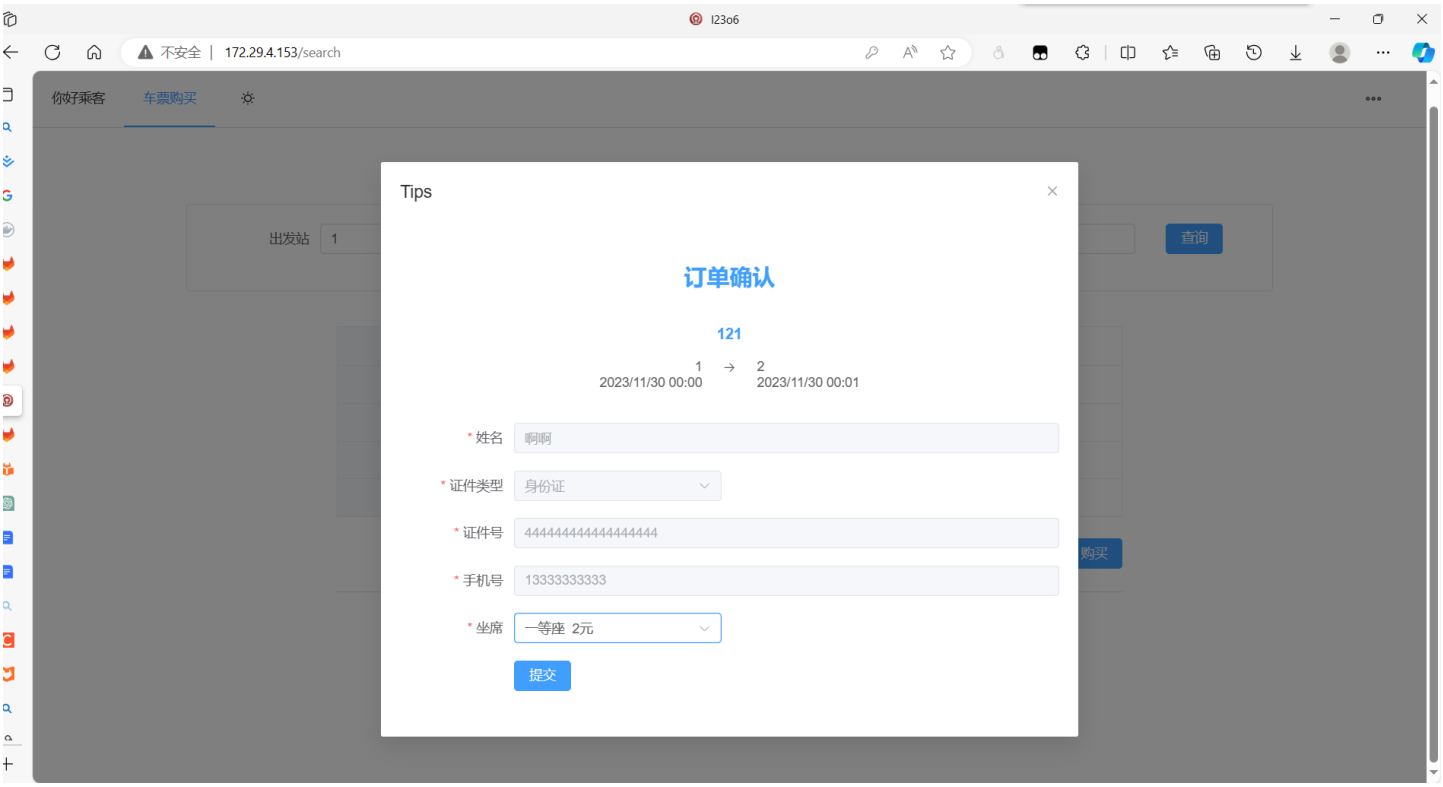
完整流水线：

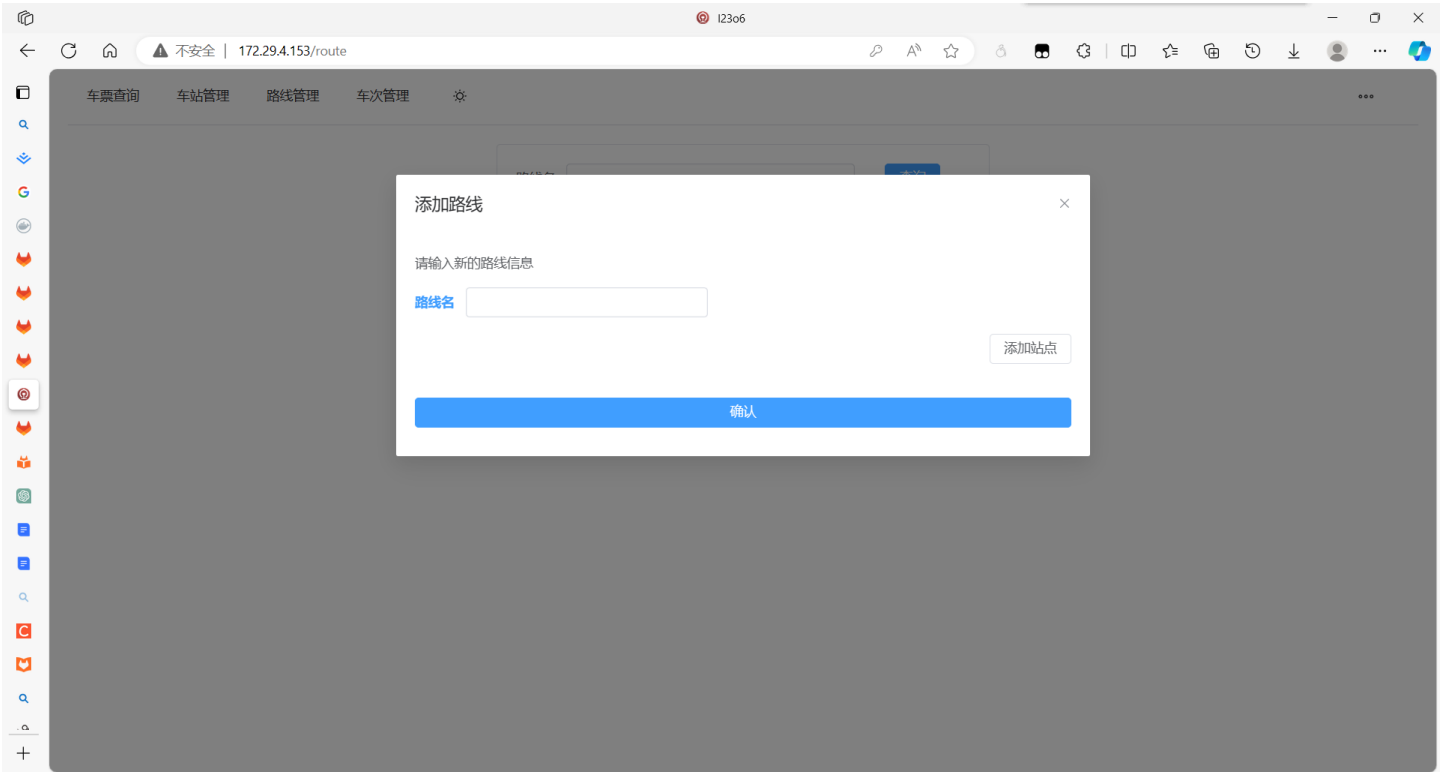
https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_server/-/pipelines

> 简要介绍所部署的项目的功能。只需要一个即可，用于==验收时现场检查==。必须涉及数据的持久化与读取。需要展示网页端截图。

一个用于乘客查询和购买车票以及管理员管理铁路信息的网站。


I23o6
不安全 | 172.29.4.153
I23o6 欢迎你!
登录
注册
* 用户名
aaaa
* 密码
* 身份
乘客
登录
访客身份进入


I23o6
不安全 | 172.29.4.153/search
你好乘客
车票购买
出发站
1
查询
Tips
订单确认
121
1
2023/11/30 00:00
2
2023/11/30 00:01
* 姓名
啊啊
* 证件类型
身份证
* 证件号
444444444444444444
* 手机号
13333333333
* 坐席
一等座 2元
提交
购买



服务端项目

构建与测试（单元测试）

执行记录链接

> 需要提供一次成功的 Pipeline 的页面链接以及其构建阶段对应的 job 的页面链接。

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_server/-/pipelines/85219

构建：https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_server/-/jobs/180780

单元测试：
https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_server/-/jobs/180783

加分项

> 如果有加分项，请说明实现方式并提供截图。如无，直接写“无”即可。每一个加分项占用一个五级标题。

单元测试报告整合到网页端

在unit-test-job中加入：

```yaml
artifacts:
  when: always
  paths:
    - build/test-results/test/*.xml
  reports:
    junit: build/test-results/test/*.xml
```

将单元测试报告上传即可

代码质量检查

执行记录链接

> 需要提供一次成功的 Pipeline 的页面链接以及其构建阶段对应的 job 的页面链接。

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_server/-/pipelines/85219

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_server/-/jobs/180785

加分项

> 如果有加分项，请说明实现方式并提供截图。如无，直接写“无”即可。每一个加分项占用一个五级标题。

无

检测出除了TODO以外的代码质量问题

代码质量门禁

执行记录链接

> 需要提供对应PR，对应 Pipeline 的页面链接以及其构建阶段对应的 job 的页面链接。

加分项

无

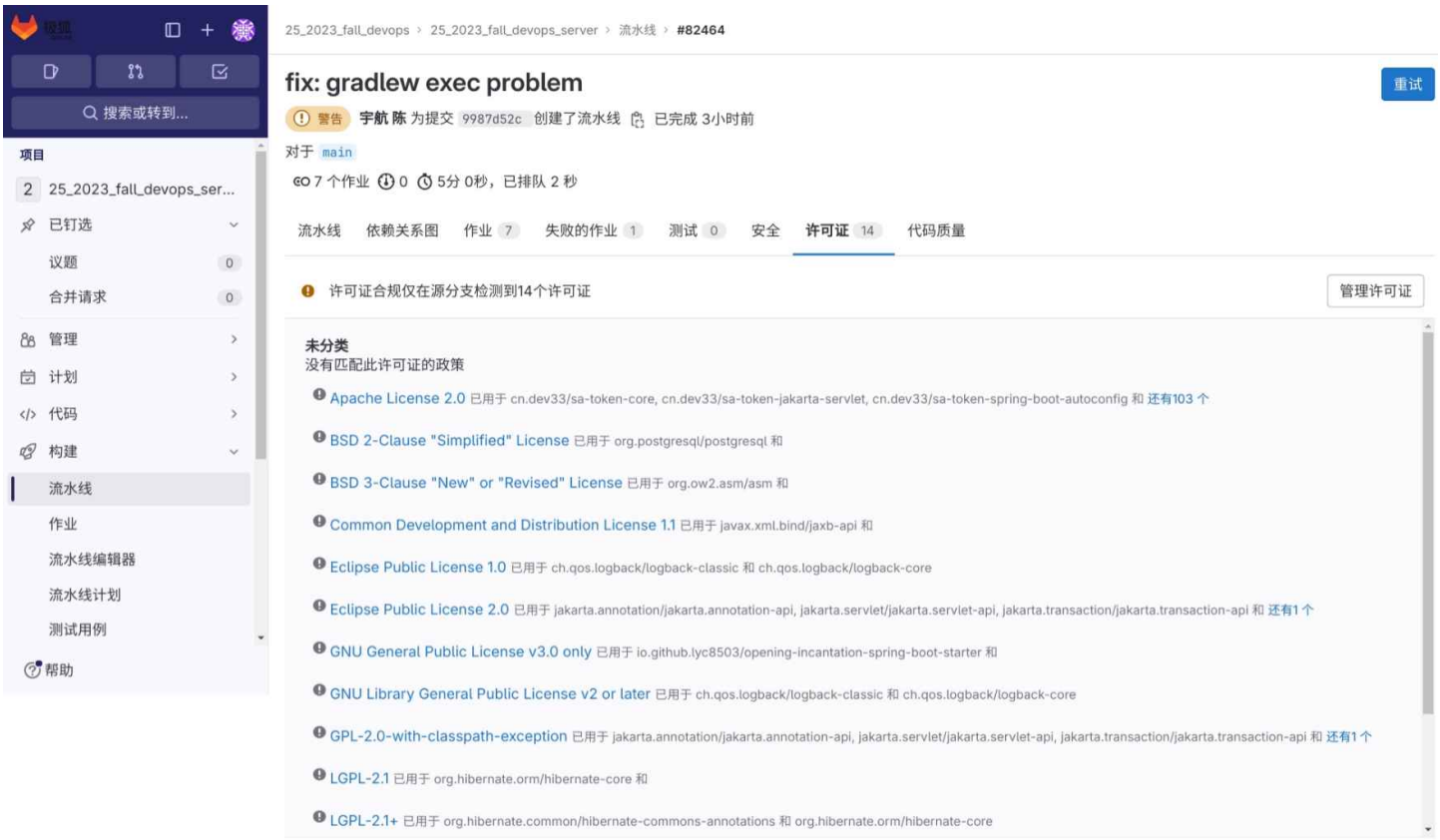
代码依赖检查与静态安全检查

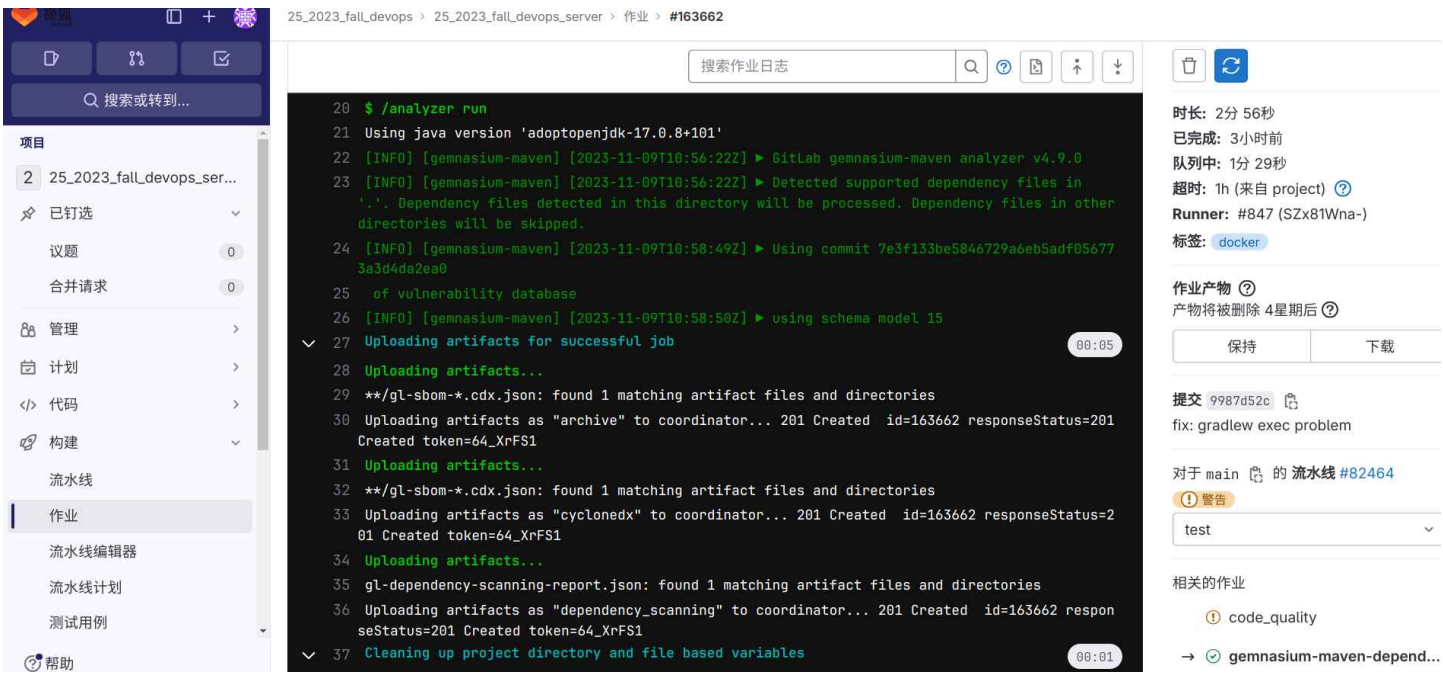
执行记录链接

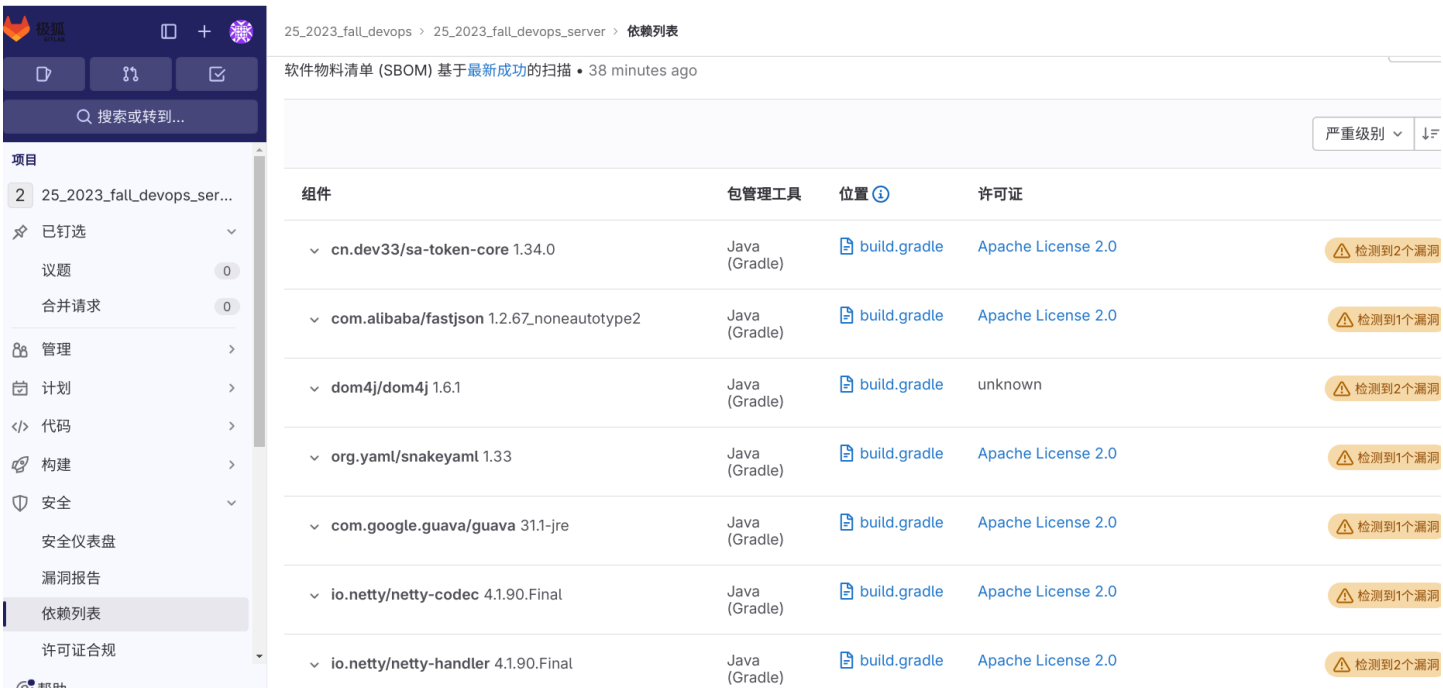
https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_server/-/pipelines/82464

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_server/-/pipelines/82679/builds

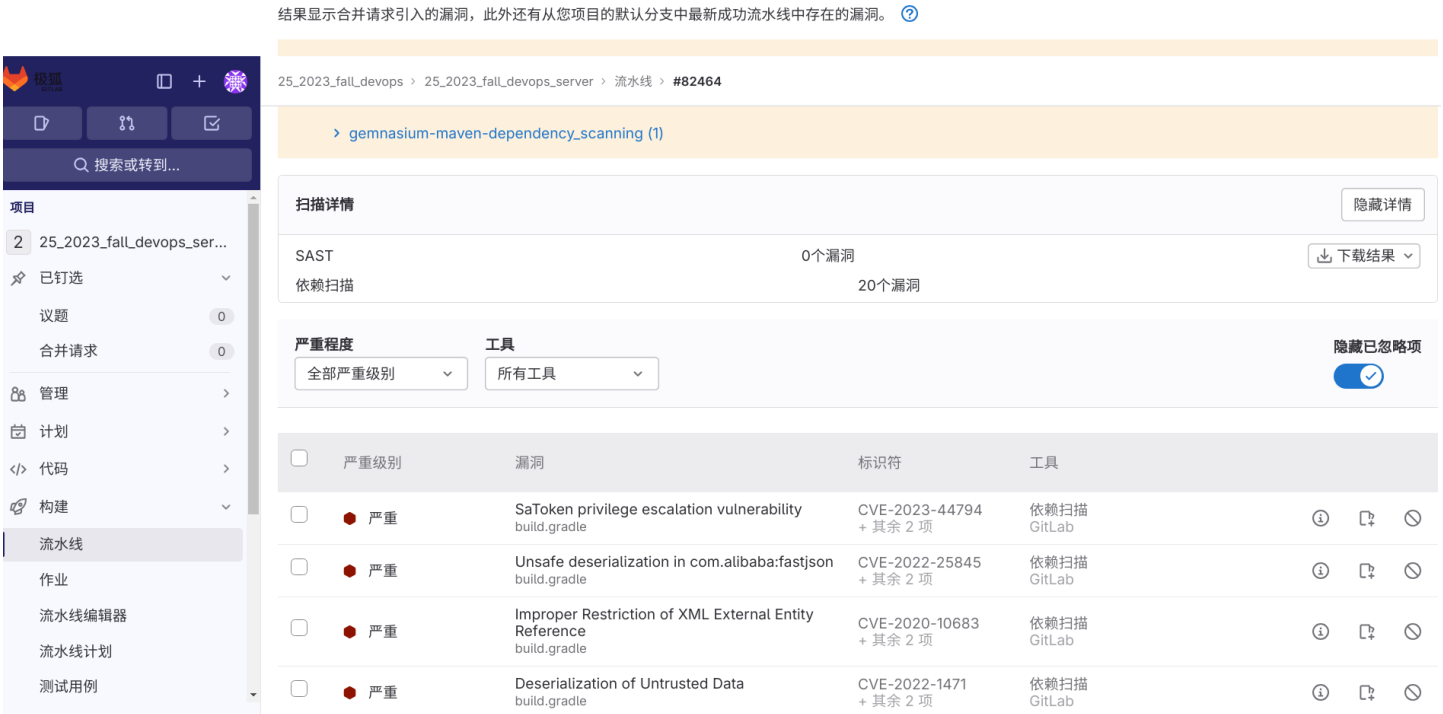
依赖检查：

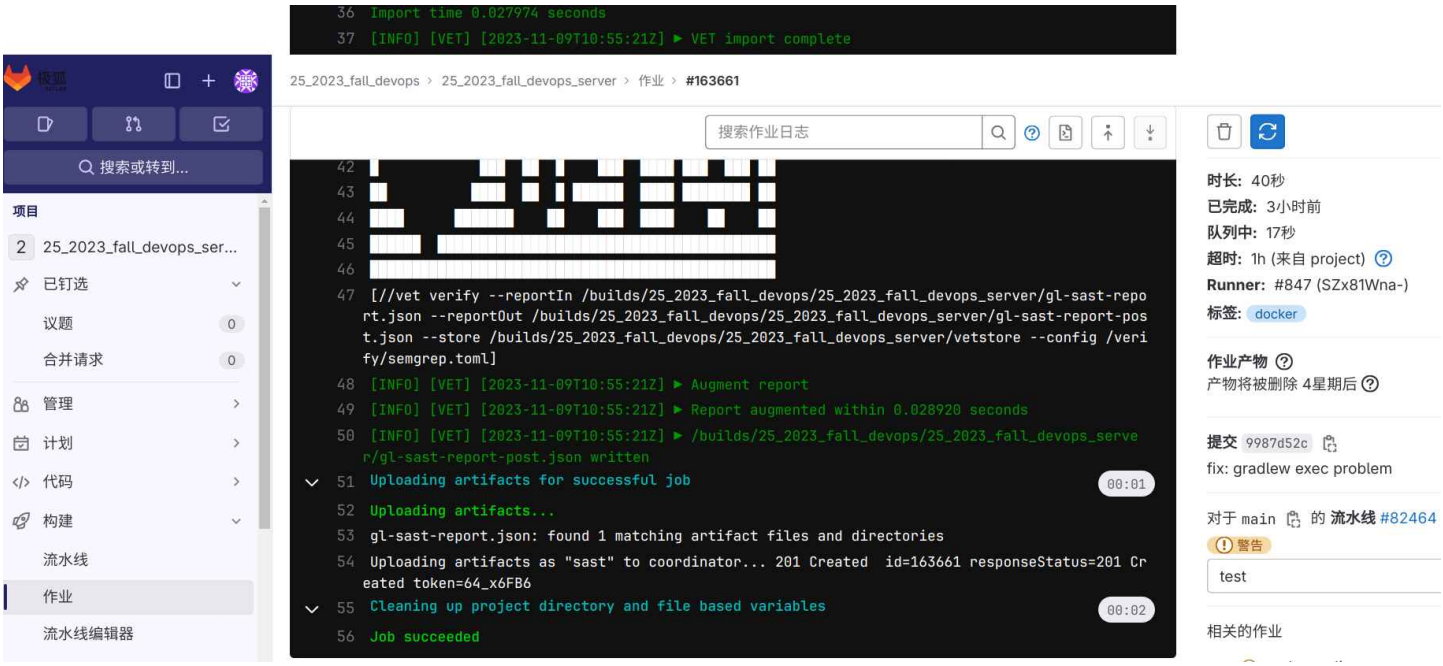

25_2023_fall_devops › 25_2023_fall_devops_server › 流水线 › #82464
fix: gradlew exec problem
重试
警告 宇航 陈 为提交 9987d52c 创建了流水线 已完成 3小时前
对于 main
7 个作业 0 5分 0秒，已排队 2 秒
流水线 依赖关系图 作业 7 失败的作业 1 测试 0 安全 许可证 14 代码质量
许可证合规仅在源分支检测到14个许可证
管理许可证
未分类
没有匹配此许可证的政策
Apache License 2.0 已用于 cn.dev33/sa-token-core, cn.dev33/sa-token-jakarta-servlet, cn.dev33/sa-token-spring-boot-autoconfig 和 还有103 个
BSD 2-Clause "Simplified" License 已用于 org.postgresql/postgresql 和
BSD 3-Clause "New" or "Revised" License 已用于 org.ow2.asm/asm 和
Common Development and Distribution License 1.1 已用于 javax.xml.bind/jaxb-api 和
Eclipse Public License 1.0 已用于 ch.qos.logback/logback-classic 和 ch.qos.logback/logback-core
Eclipse Public License 2.0 已用于 jakarta.annotation/jakarta.annotation-api, jakarta.servlet/jakarta.servlet-api, jakarta.transaction/jakarta.transaction-api 和 还有1 个
GNU General Public License v3.0 only 已用于 io.github.lyc8503/opening-incantation-spring-boot-starter 和
GNU Library General Public License v2 or later 已用于 ch.qos.logback/logback-classic 和 ch.qos.logback/logback-core
GPL-2.0-with-classpath-exception 已用于 jakarta.annotation/jakarta.annotation-api, jakarta.servlet/jakarta.servlet-api, jakarta.transaction/jakarta.transaction-api 和 还有1 个
LGPL-2.1 已用于 org.hibernate.orm/hibernate-core 和
LGPL-2.1+ 已用于 org.hibernate.common/hibernate-commons-annotations 和 org.hibernate.orm/hibernate-core
搜索或转到...
项目
25_2023_fall_devops_ser...
已钉选
议题 0
合并请求 0
管理
计划
代码
构建
流水线
作业
流水线编辑器
流水线计划
测试用例
帮助


25_2023_fall_devops › 25_2023_fall_devops_server › 作业 › #163662
搜索作业日志
20 $ /analyzer run
21 Using java version 'adoptopenjdk-17.0.8+101'
22 [INFO] [gemnasium-maven] [2023-11-09T10:56:22Z] ▶ GitLab gemnasium-maven analyzer v4.9.0
23 [INFO] [gemnasium-maven] [2023-11-09T10:56:22Z] ▶ Detected supported dependency files in '.'. Dependency files detected in this directory will be processed. Dependency files in other directories will be skipped.
24 [INFO] [gemnasium-maven] [2023-11-09T10:58:49Z] ▶ Using commit 7e3f133be5846729a6eb5adf056773a3d4da2ea0
25 of vulnerability database
26 [INFO] [gemnasium-maven] [2023-11-09T10:58:50Z] ▶ using schema model 15
27 Uploading artifacts for successful job 00:05
28 Uploading artifacts...
29 **/gl-sbom-*.cdx.json: found 1 matching artifact files and directories
30 Uploading artifacts as "archive" to coordinator... 201 Created id=163662 responseStatus=201 Created token=64_XrFS1
31 Uploading artifacts...
32 **/gl-sbom-*.cdx.json: found 1 matching artifact files and directories
33 Uploading artifacts as "cyclonedx" to coordinator... 201 Created id=163662 responseStatus=201 Created token=64_XrFS1
34 Uploading artifacts...
35 gl-dependency-scanning-report.json: found 1 matching artifact files and directories
36 Uploading artifacts as "dependency_scanning" to coordinator... 201 Created id=163662 responseStatus=201 Created token=64_XrFS1
37 Cleaning up project directory and file based variables 00:01
时长: 2分 56秒
已完成: 3小时前
队列中: 1分 29秒
超时: 1h (来自 project)
Runner: #847 (SZx81Wna-)
标签: docker
作业产物
产物将被删除 4星期后
保持
下载
提交 9987d52c
fix: gradlew exec problem
对于 main 的 流水线 #82464
警告
test
相关的作业
code_quality
gemnasium-maven-depend...
搜索或转到...
项目
25_2023_fall_devops_ser...
已钉选
议题 0
合并请求 0
管理
计划
代码
构建
流水线
作业
流水线编辑器
流水线计划
测试用例
帮助


25_2023_fall_devops › 25_2023_fall_devops_server › 依赖列表
软件物料清单 (SBOM) 基于最新成功的扫描 • 38 minutes ago
严重级别
组件
包管理工具
位置
许可证
cn.dev33/sa-token-core 1.34.0 Java (Gradle) build.gradle Apache License 2.0 检测到2个漏洞
com.alibaba/fastjson 1.2.67_noneautotype2 Java (Gradle) build.gradle Apache License 2.0 检测到1个漏洞
dom4j/dom4j 1.6.1 Java (Gradle) build.gradle unknown 检测到2个漏洞
org.yaml/snakeyaml 1.33 Java (Gradle) build.gradle Apache License 2.0 检测到1个漏洞
com.google.guava/guava 31.1-jre Java (Gradle) build.gradle Apache License 2.0 检测到1个漏洞
io.netty/netty-codec 4.1.90.Final Java (Gradle) build.gradle Apache License 2.0 检测到1个漏洞
io.netty/netty-handler 4.1.90.Final Java (Gradle) build.gradle Apache License 2.0 检测到2个漏洞
搜索或转到...
项目
25_2023_fall_devops_ser...
已钉选
议题
合并请求
管理
计划
代码
构建
安全
安全仪表盘
漏洞报告
依赖列表
许可证合规

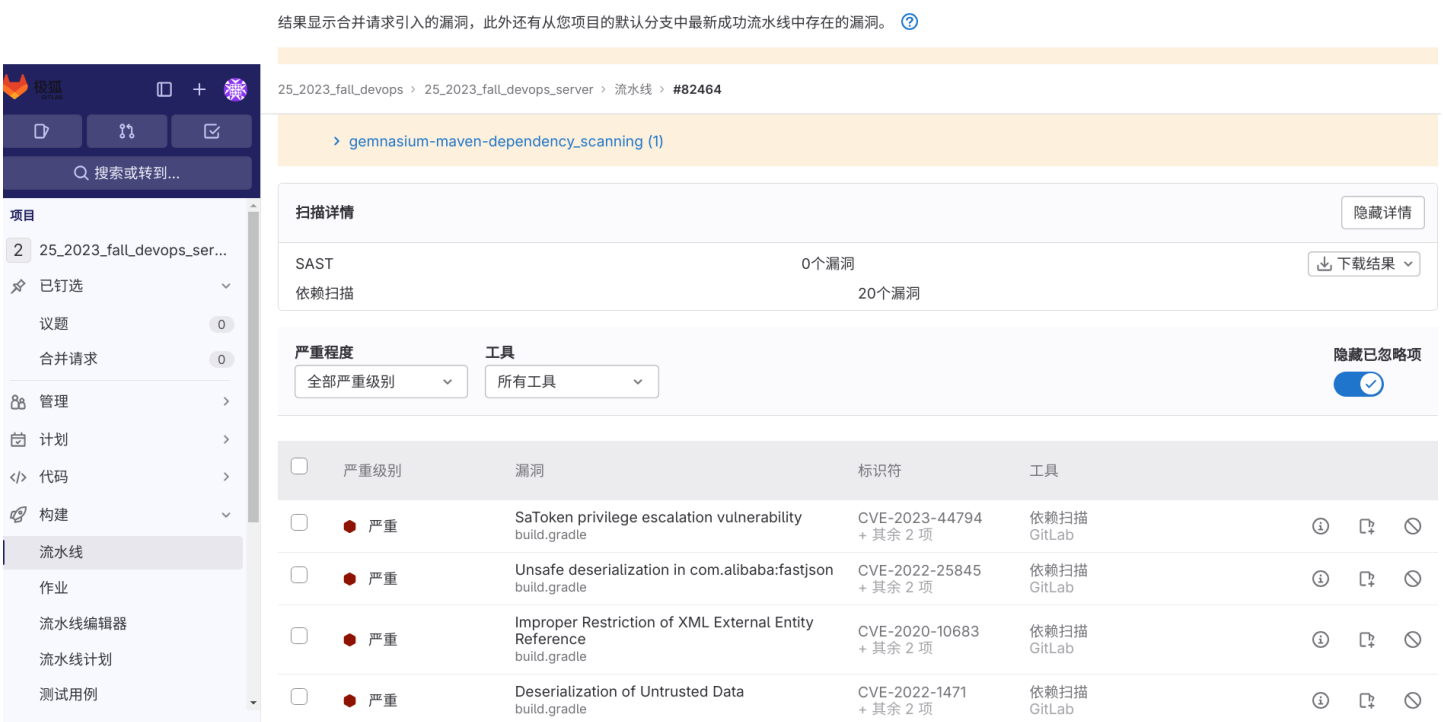
静态安全检查：


结果显示合并请求引入的漏洞，此外还有从您项目的默认分支中最新成功流水线中存在的漏洞。
25_2023_fall_devops › 25_2023_fall_devops_server › 流水线 › #82464
gemnasium-maven-dependency_scanning (1)
扫描详情
隐藏详情
SAST 0个漏洞
依赖扫描 20个漏洞
下载结果
严重程度
全部严重级别
工具
所有工具
隐藏已忽略项
严重级别
漏洞
标识符
工具
严重 SaToken privilege escalation vulnerability build.gradle CVE-2023-44794 + 其余 2 项 依赖扫描 GitLab
严重 Unsafe deserialization in com.alibaba:fastjson build.gradle CVE-2022-25845 + 其余 2 项 依赖扫描 GitLab
严重 Improper Restriction of XML External Entity Reference build.gradle CVE-2020-10683 + 其余 2 项 依赖扫描 GitLab
严重 Deserialization of Untrusted Data build.gradle CVE-2022-1471 + 其余 2 项 依赖扫描 GitLab
搜索或转到...
项目
25_2023_fall_devops_ser...
已钉选
议题
合并请求
管理
计划
代码
构建
流水线
作业
流水线编辑器
流水线计划
测试用例



加分项

检测出



项目部署

执行记录链接

> 需要提供一次成功的 Pipeline 的页面链接以及其构建阶段对应的 job 的页面链接。==验收时要是否可用==。

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_server/-/pipelines/85219/

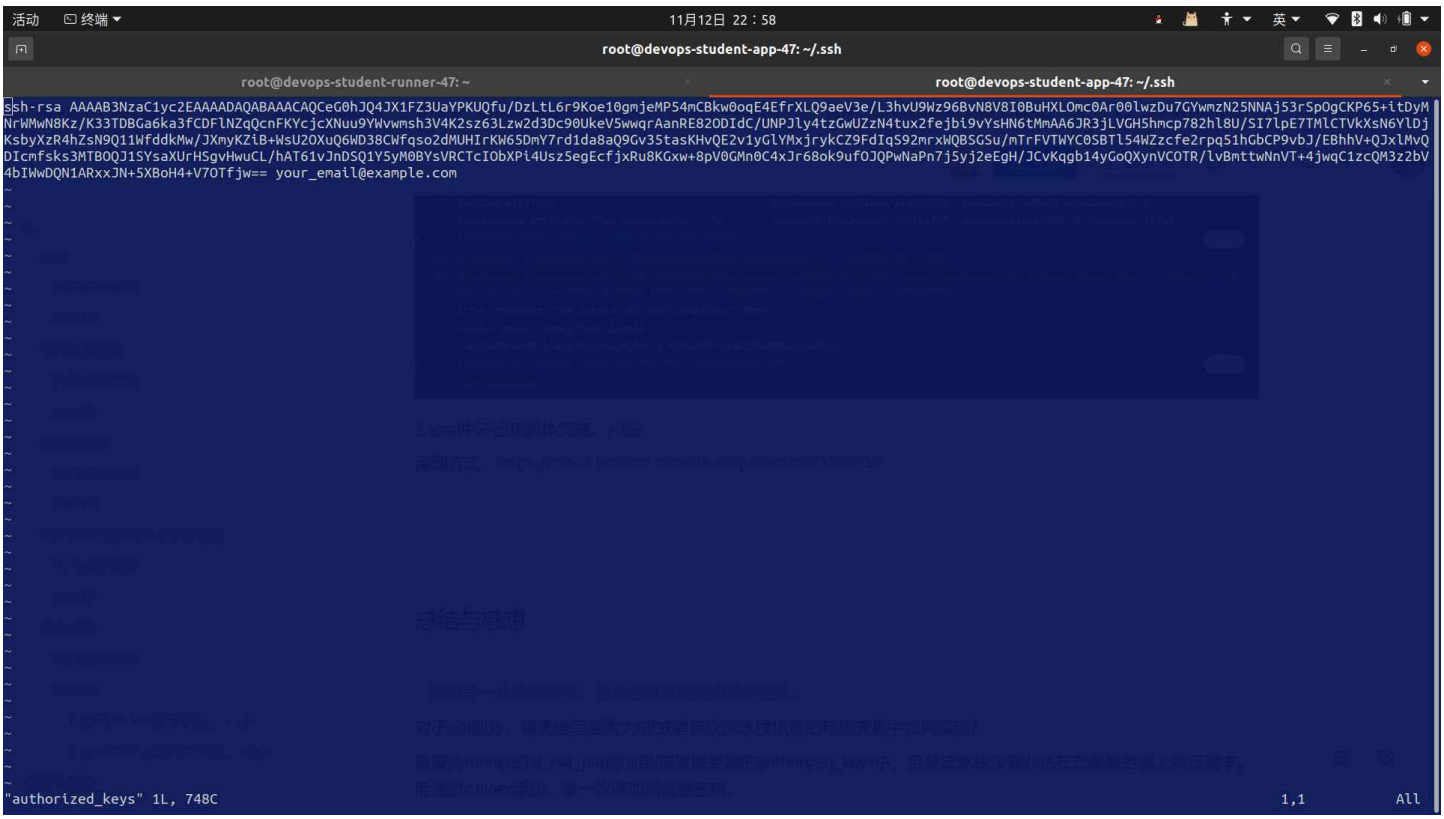
https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_server/-/jobs/180786

加分项

1. yaml中不出现具体凭据。+2分

实现方式：https://cloud.tencent.com/developer/article/1538757

部署服务器的authorized_keys：



实现方法二：

某个文件中

```yaml
deploy-job:
  stage: deploy
  environment: production
  script:
    - chmod +x gradlew
    - ./gradlew build -x test
    - sshpass -f password scp -o StrictHostKeyChecking=no build/libs/l23o6-0.0.1-snapshot.jar root@172.29.4.1
    - sshpass -f password ssh -o StrictHostKeyChecking=no root@172.29.4.153 "killall java;screen -d -m java -
    - echo "test"
```

网页端项目

构建

执行记录链接

npm构建：

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/pipelines/82305

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/jobs/162572

docker构建：

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/pipelines/85215

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/jobs/180761

> 需要提供一次成功的 Pipeline 的页面链接以及其构建阶段对应的 job 的页面链接。

加分项

无

> 如果有加分项，请说明实现方式并提供截图。如无，直接写“无”即可。每一个加分项占用一个五级标题。

代码质量检查

执行记录链接

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/pipelines/82305

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/jobs/162573

> 需要提供一次成功的 Pipeline 的页面链接以及其构建阶段对应的 job 的页面链接。

加分项

（1）检测出除了TODO以外的代码质量问题：

实现方式：非预期的逗号标点符号

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/pipelines/82277/codequality_report

> 如果有加分项，请说明实现方式并提供截图。如无，直接写“无”即可。每一个加分项占用一个五级标题。

自动格式化

执行记录链接

```
PS E:\25_2023_fall_devops_web> git commit -m "25group"
Checking code formatting...
tsconfig.json
warning: LF will be replaced by CRLF in tsconfig.json.
The file will have its original line endings in your working directory
[main 303a733] 25group
 3 files changed, 71 insertions(+), 82 deletions(-)
 rewrite vite.config.js (93%)
PS E:\25_2023_fall_devops_web> git push
Username for 'https://git.nju.edu.cn': 211870063sy
Password for 'https://211870063sy@git.nju.edu.cn':
Enumerating objects: 9, done.
Counting objects: 100% (9/9), done.
Delta compression using up to 12 threads
Compressing objects: 100% (5/5), done.
Writing objects: 100% (5/5), 1.16 KiB | 1.16 MiB/s, done.
Total 5 (delta 2), reused 0 (delta 0), pack-reused 0
To https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web.git
   04aea71..303a733  main -> main
PS E:\25_2023_fall_devops_web>
```

> 需要提供本地运行截图和终端输出。==验收时要现场演示==。

加分项

无

代码依赖检查与静态安全检查

执行记录链接

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/pipelines/82669

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/jobs/164991

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/jobs/164992

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/jobs/164993

> 需要提供一次成功的 Pipeline 的页面链接以及其构建阶段对应的 job 的页面链接。

加分项

无

项目部署

执行记录链接

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/pipelines/82669

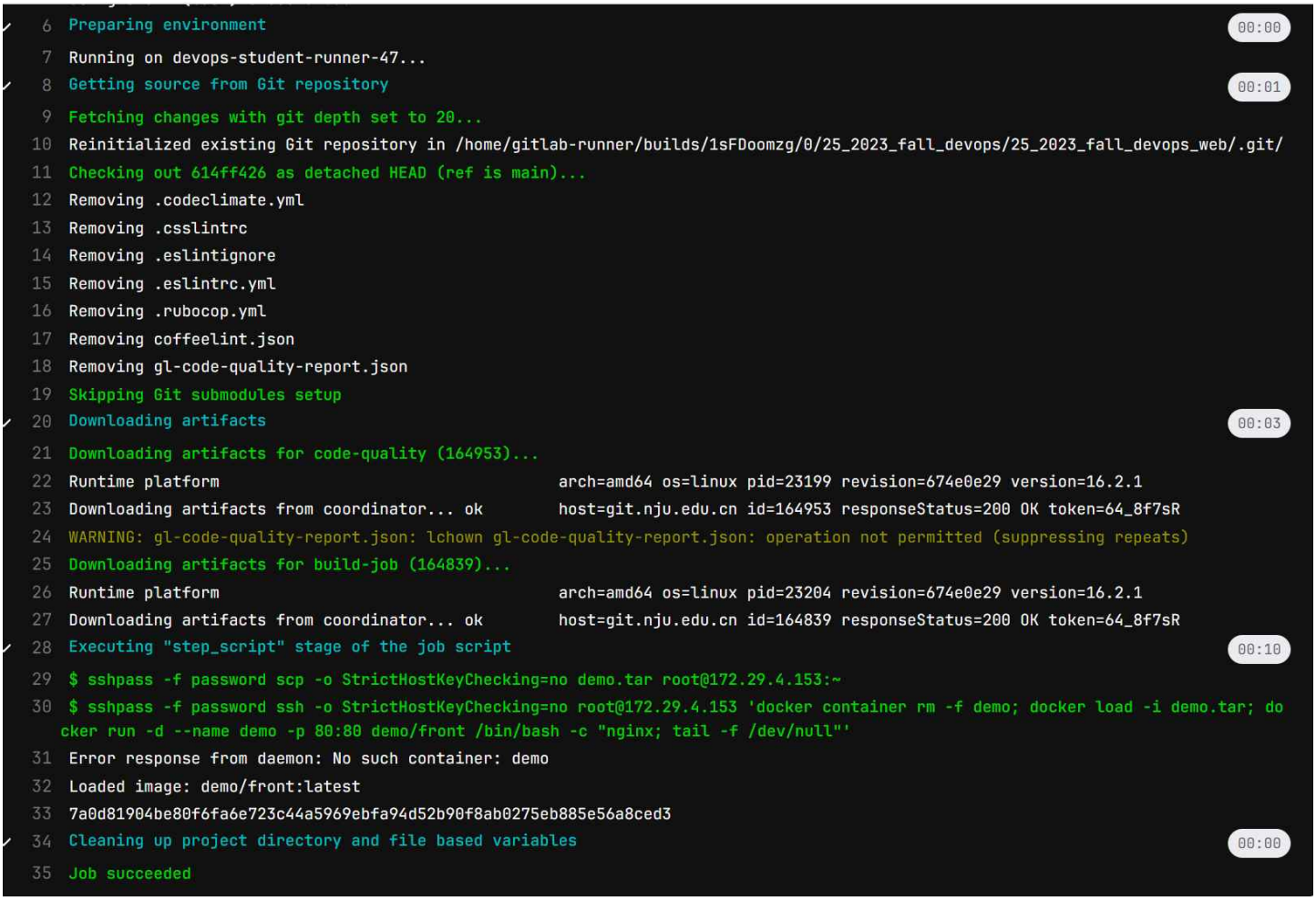
https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/jobs/164844

> 需要提供一次成功的 Pipeline 的页面链接以及其构建阶段对应的 job 的页面链接。==验收时要是否可用==。

加分项

1. 使用docker进行部署。+1分

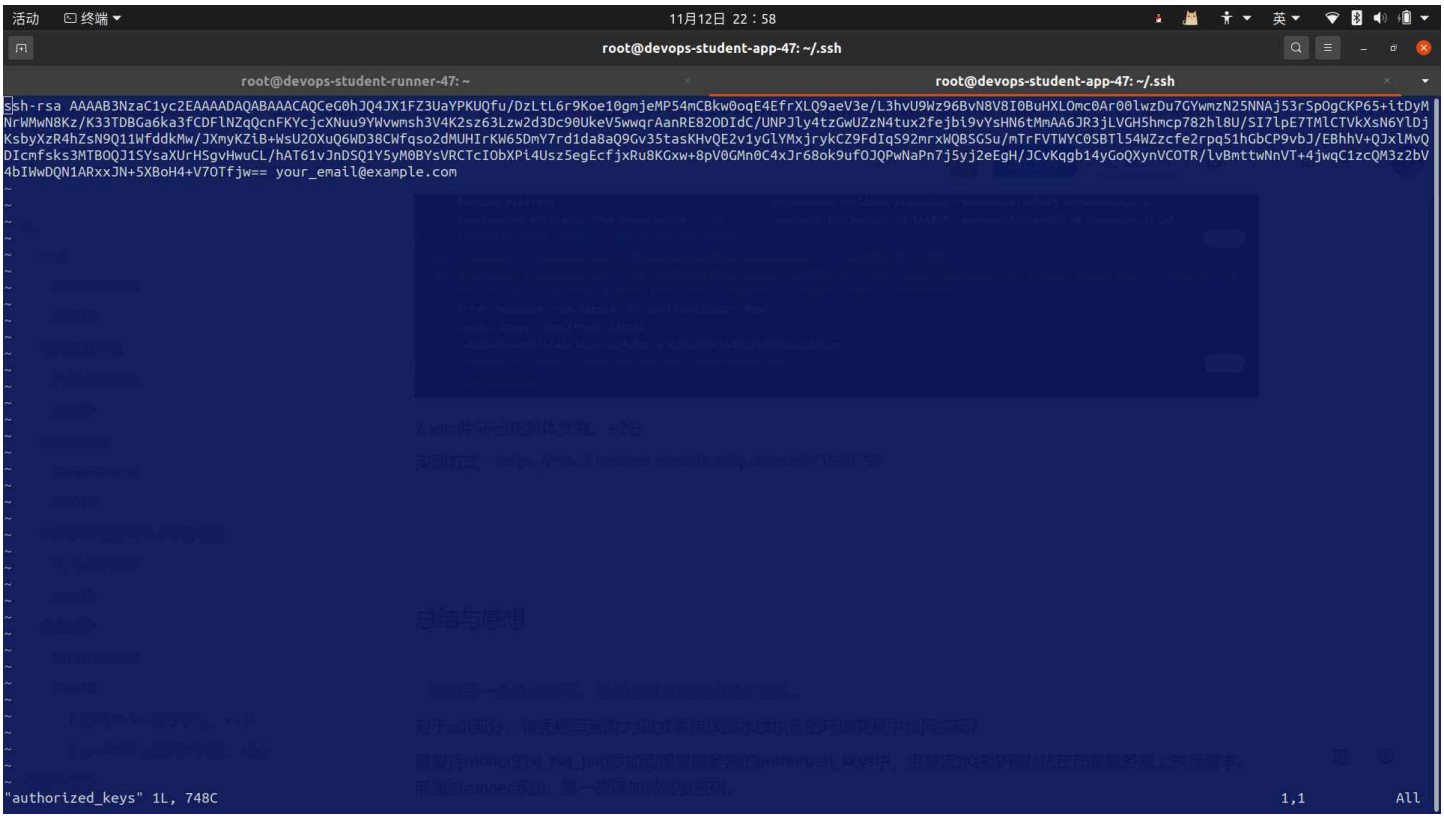
build阶段用docker将代码打包成demo.tar，部署阶段用ssh将demo.tar传入部署服务器，接着加载demo.tar，并进行nginx服务。



2. yaml中不出现具体凭据。+2分

实现方式：https://cloud.tencent.com/developer/article/1538757

部署服务器的authorized_keys：




```yaml
deploy-job: # This job runs in the deploy stage.
 stage: deploy # It only runs when *both* jobs in the test stage complete successfull
 environment: production
 script:
  - scp demo.tar root@172.29.4.153:~
  - ssh root@172.29.4.153 'docker container rm -f demo; docker load -i demo.tar; dock
```

实现方式二：某个文件中

https://git.nju.edu.cn/25_2023_fall_devops/25_2023_fall_devops_web/-/jobs/180479

```
00:05
$ sshpass -f password scp -o StrictHostKeyChecking=no demo.tar root@172.29.4.153:~
$ sshpass -f password ssh -o StrictHostKeyChecking=no root@172.29.4.153 'docker container rm -f demo; docker load -i demo.tar; docker run -d --name demo -p 80:80 demo/front /bin/bash -c "nginx; tail -f /dev/null"'
demo
Loaded image: demo/front:latest
560d011d98089d7eea2b82df3e0da4adfc3f97017bd18bb6e4facc2e93bd5a52
Cleaning up project directory and file based variables
00:00
Job succeeded
```

总结与感想

> 随便写一些总结即可。也欢迎对课程提出更多建议。

对于ssh部分，将凭据写到南大Git或者单次流水线执行的环境变量中如何实现？

需要将runner的id_rsa_pub添加到部署服务器的authorized_keys中，但是流水线没有办法在部署服务器上执行脚本。而通过runner添加，第一次添加仍需要密码。

不会希望我们将明文密码存到环境变量然后引用变量来登录吧，没有搞懂意思。所以直接配置了两台服务器的ssh连接。