环境搭建

引擎安装

https://github.com/github/codeql-cli-binaries/releases
由于是 windows 系统，下载 codeql-win64.zip 即可。下载后解压文件，添加环境变量方便使用。如果命令行运行 codeql 命令，界面如下，即可。

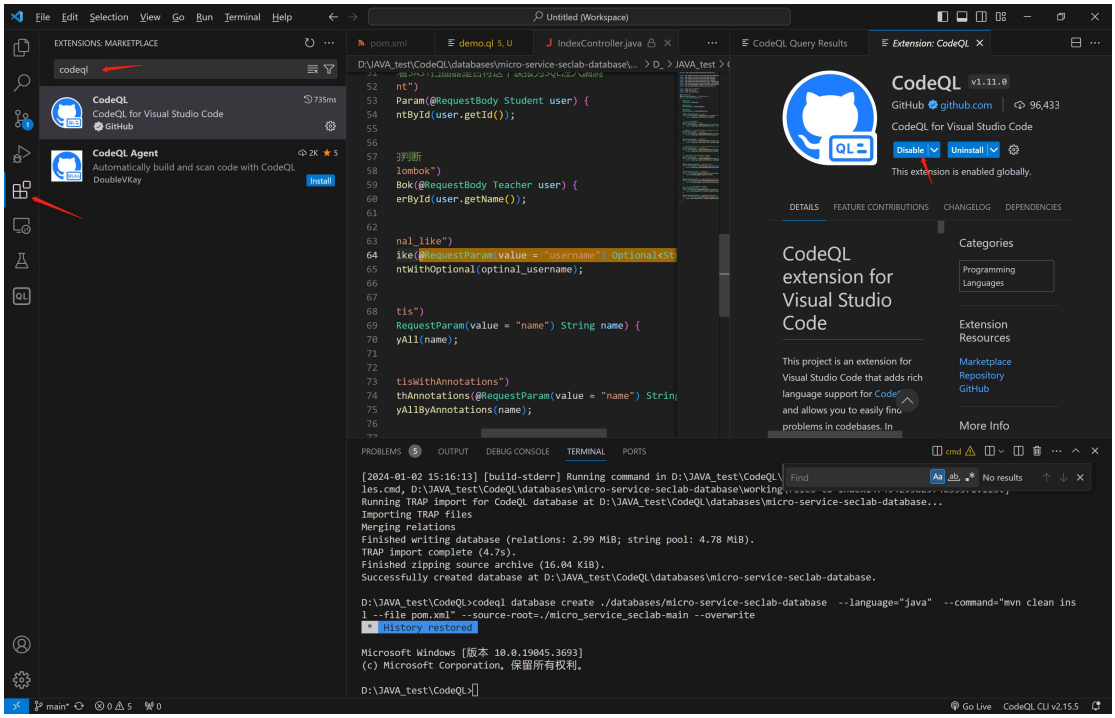
```
C:\Users\MrP01ntSun>codeql
Usage: codeql <command> <argument>...
Create and query CodeQL databases, or work with the QL language.

GitHub makes this program freely available for the analysis of open-source
software and certain other uses, but it is not itself free software. Type
codeql --license to see the license terms.

      --license              Show the license terms for the CodeQL toolchain.
Common options:
  -h, --help                 Show this help text.
  -v, --verbose              Incrementally increase the number of progress
                               messages printed.
  -q, --quiet                Incrementally decrease the number of progress
                               messages printed.
Some advanced options have been hidden; try --help -v for a fuller view.
Commands:
  query       Compile and execute QL code.
  bqrs        Get information from .bqrs files.
  database    Create, analyze and process CodeQL databases.
  dataset     [Plumbing] Work with raw QL datasets.
  test        Execute QL unit tests.
  resolve     [Deep plumbing] Helper commands to resolve disk locations etc.
  execute     [Deep plumbing] Low-level commands that need special JVM options.
  version     Show the version of the CodeQL toolchain.
  generate    Commands that generate useful output.
  github      Commands useful for interacting with the GitHub API through
                CodeQL.
  pack        [Experimental] Commands to manage QL packages.
  diagnostic  [Experimental] Create, process, and export diagnostic information.
```

SDK 安装

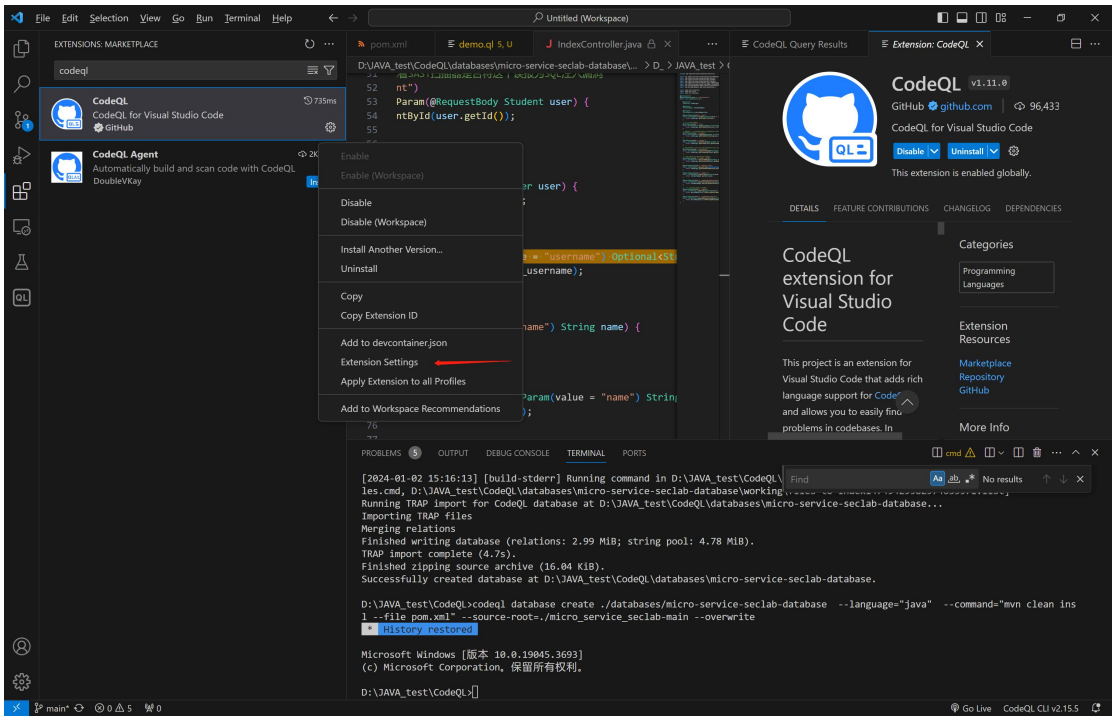
https://github.com/github/codeql
下载后，重命名文件夹为 ql。

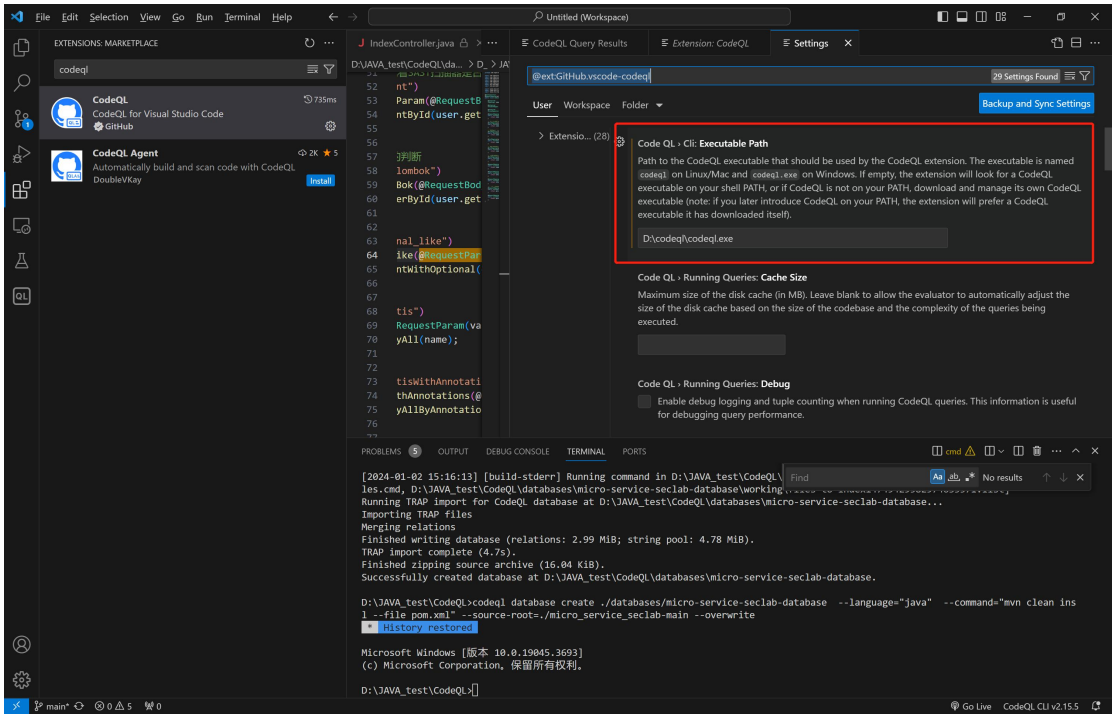
VSCODE 开发插件安装

在插件处搜索 codeql，安装



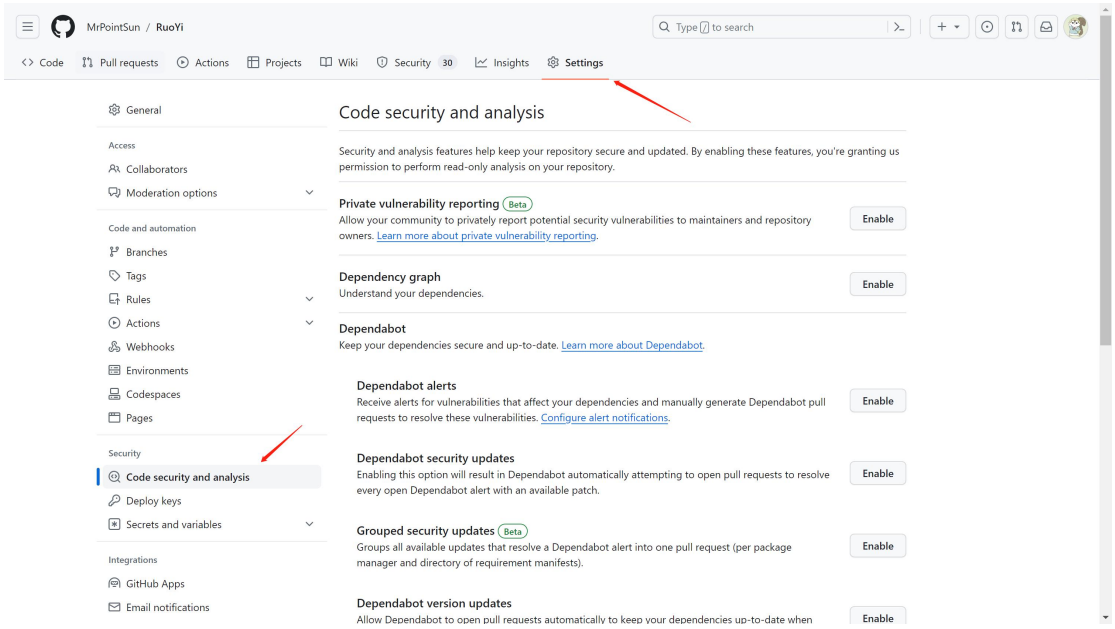
安装后记得配置下引擎路径:

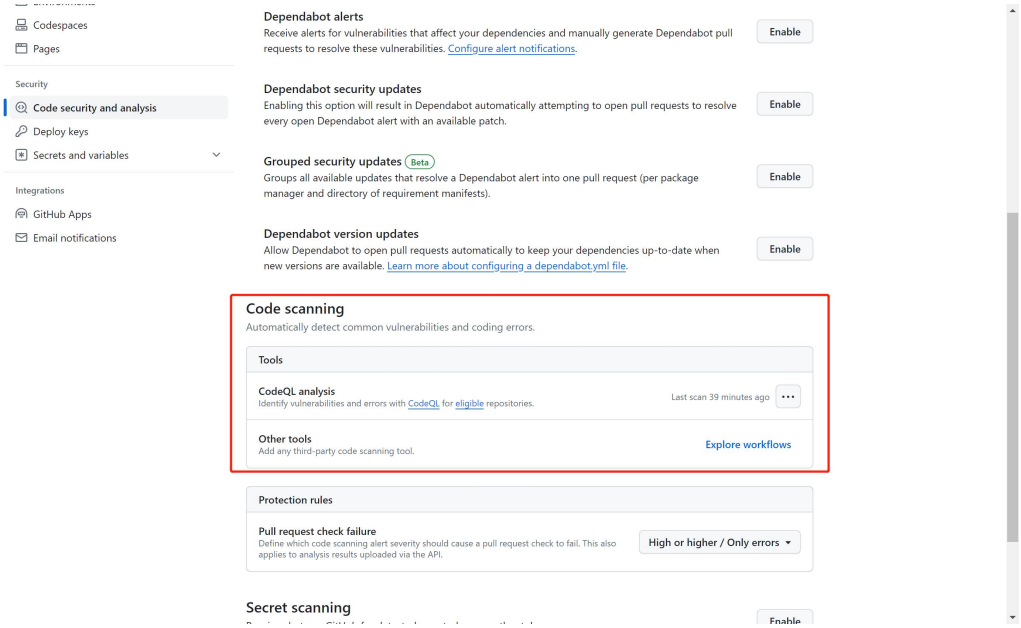




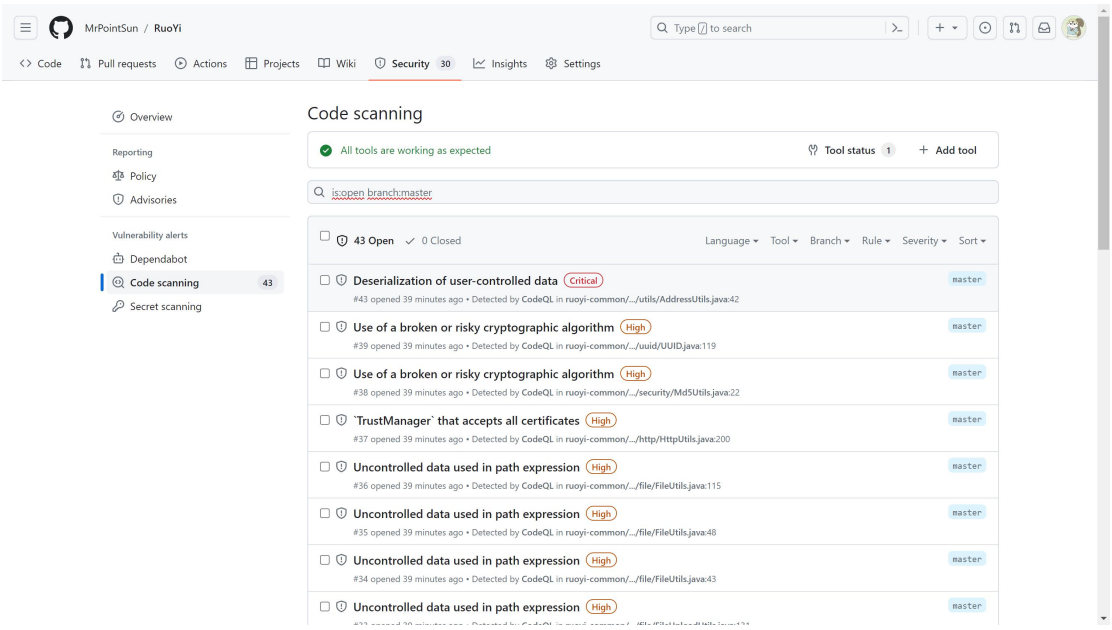
在线扫描

在 github 的 setting 里面可以开始 codeql 的扫描:





扫描结果在 Security 里面：

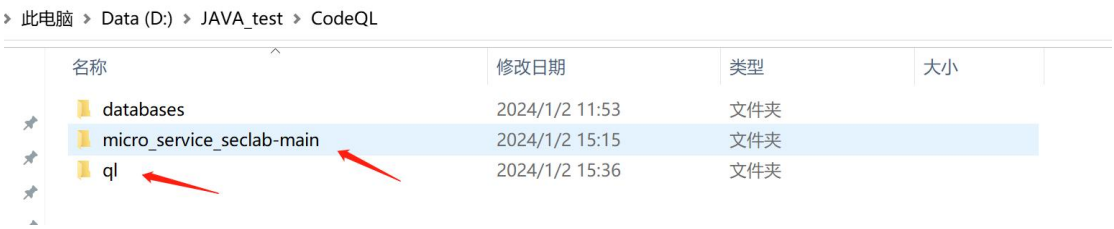


靶场实验

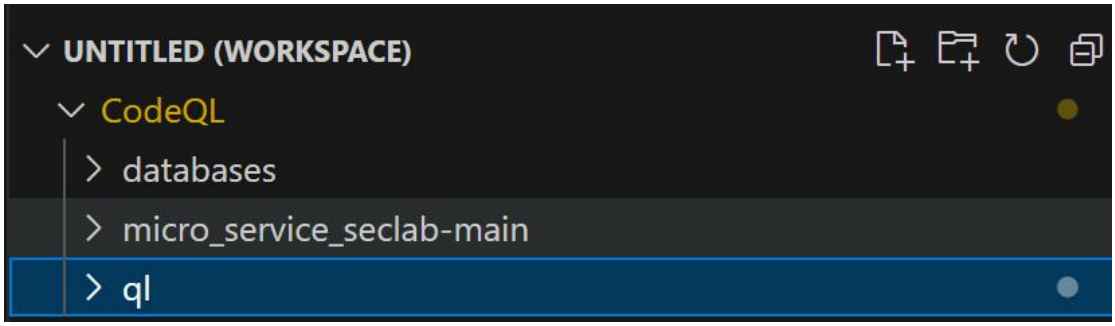
下载靶场环境

https://github.com/l4yn3/micro_service_seclab/

下载后，把 SDK 安装那一步的 ql 文件夹放在同一目录下：



使用 vscode 打开 CodeQL 目录：

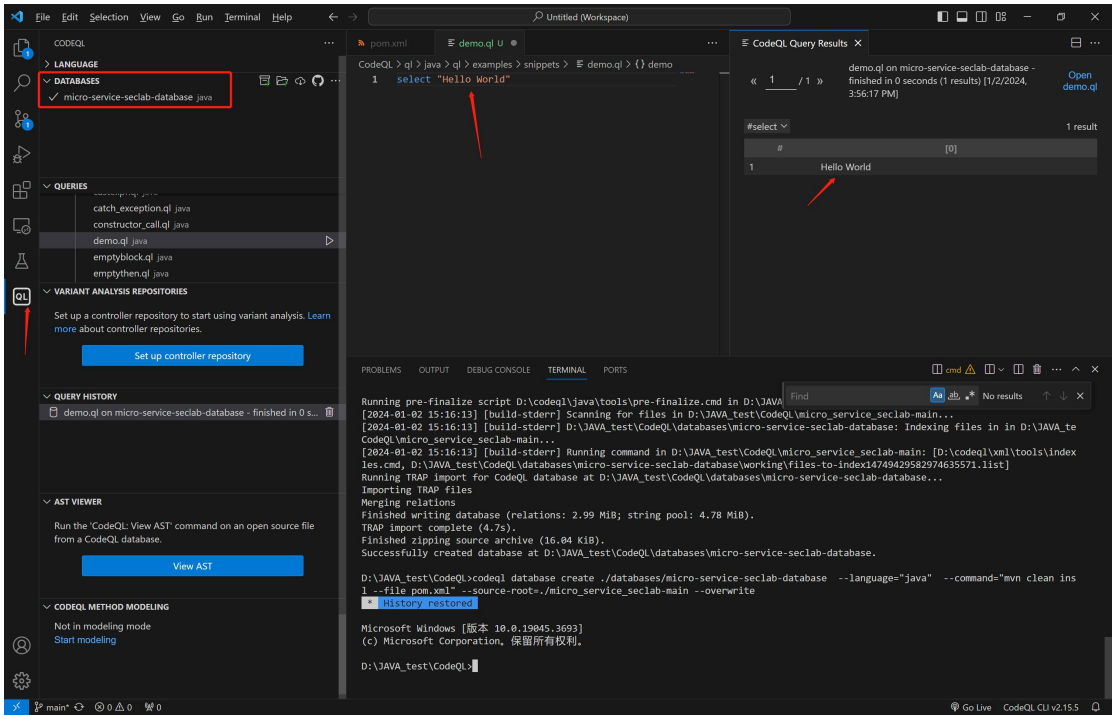


使用 codeql 创建数据库

codeql database create ./databases/micro-service-seclab-database --language="java" --command="mvn clean install --file pom.xml" --source-root=./micro_service_seclab-main –overwrite

这一步可能会报错，排查后是 mvn 报错，可参考 MVN 报错进行更改。

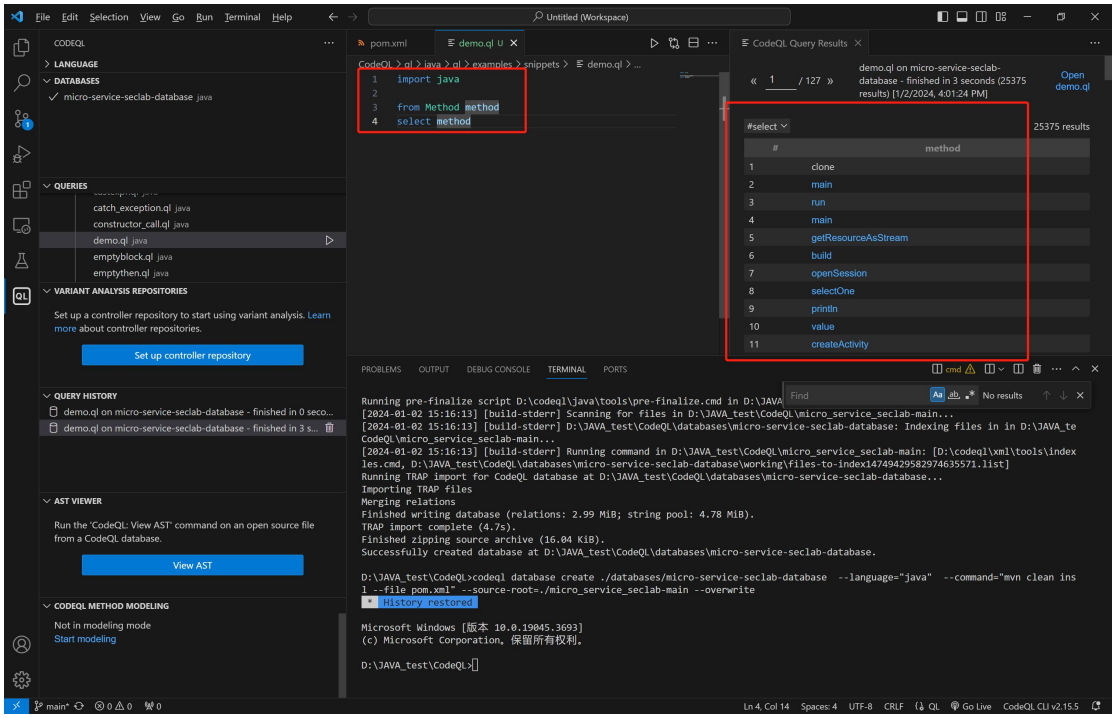
创建成功后添加数据库，这里写了个 demo.ql，证明环境搭建好了：



比如想获取所有的方法：

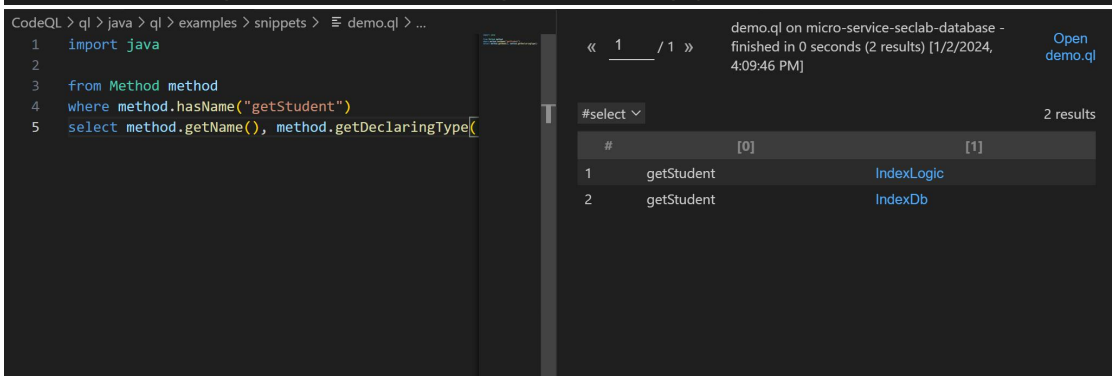
```
import java
```

```
from Method method
select method
```



再通过 Method 类内置的一些方法，过滤一下结果，只获取名字为 getStudent 的方法名称。

```
import java

from Method method
where method.hasName("getStudent")
select method.getName(), method.getDeclaringType()
```



MVN 报错

```
[ERROR] Failed to execute goal org.apache.maven.plugins:maven-compiler-plugin:3.8.1:compile (default-compile) on project micro-servi
ce-seclab: Fatal error compiling: java.lang.IllegalAccessError: class lombok.javac.apt.LombokProcessor (in unnamed module @0x7a60626
0) cannot access class com.sun.tools.javac.processing.JavacProcessingEnvironment (in module jdk.compiler) because module jdk.compile
r does not export com.sun.tools.javac.processing to unnamed module @0x7a606260 -> [Help 1]
[ERROR]
[ERROR] To see the full stack trace of the errors, re-run Maven with the -e switch.
[ERROR] Re-run Maven using the -X switch to enable full debug logging.
[ERROR]
[ERROR] For more information about the errors and possible solutions, please read the following articles:
[ERROR] [Help 1] http://cwiki.apache.org/confluence/display/MAVEN/MojoExecutionException
```

原因 1：
Pom.xml 加上如下内容：

```
<plugin>
                <groupId>org.apache.maven.plugins</groupId>
                <artifactId>maven-surefire-plugin</artifactId>
                <version>2.22.2</version>
                <configuration>
                    <skipTests>true</skipTests>
                </configuration>
            </plugin>
```

原因 2：java 版本不对：

```
<properties>
        <java.version>1.8</java.version>
    </properties>
```

原因 3：lobbok 版本报错，改成 1.18.24 版本：

```
<dependency>
            <groupId>org.projectlombok</groupId>
            <artifactId>lombok</artifactId>
            <version>1.18.24</version>
        </dependency>
```

QI 库

官方库

https://codeql.github.com/codeql-query-help/java/
全是写好的，不仅有 java，还有 C、C++、C#、Go、JavaScript、TypeScript、Python、Ruby、Swift

常用库

对 JAVA 的 CWE 库说明在此链接：https://codeql.github.com/codeql-query-help/java-cwe/
常用 CWE-022、CWE-078(命令注入)、CWE-312、CWE614、CWE-079（XSS）、CWE-1104、CWE-829、CWE-502（反序列化）、CWE-113、CWE-601（url 跳转）、CWE-090（ladp 注入）、CWE-089（sql 注入）、CWE-732（file 权限&目录注入）、CWE-022（file 权限&目录注入）、CWE-611（xml 注入）、CWE-297、CWE-327、CWE-335

执行所有漏洞查询

codeql database analyze source_database_name qllib/java/ql/src/codeql-suites/java-security-extended.qls --format=csv --output=java-results.csv