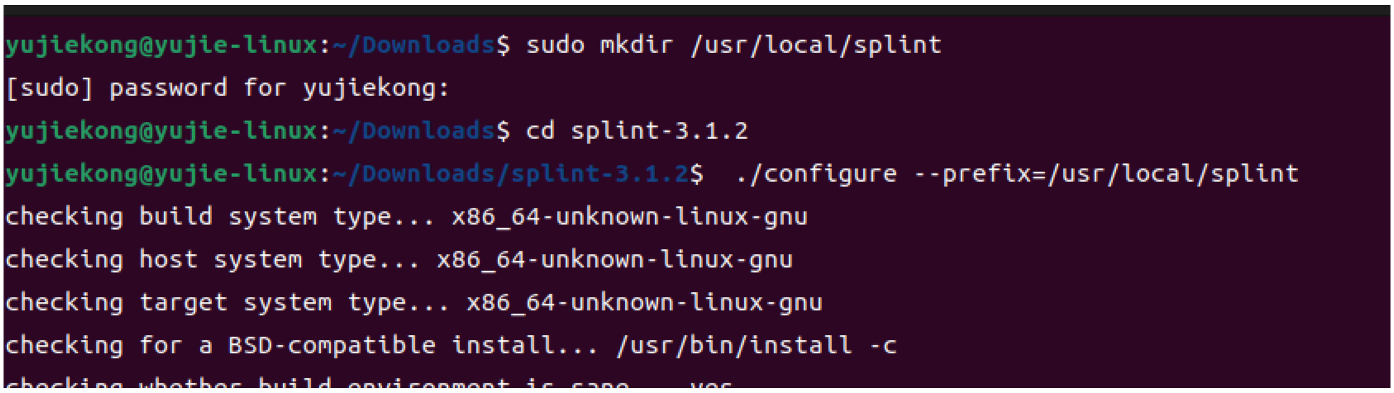
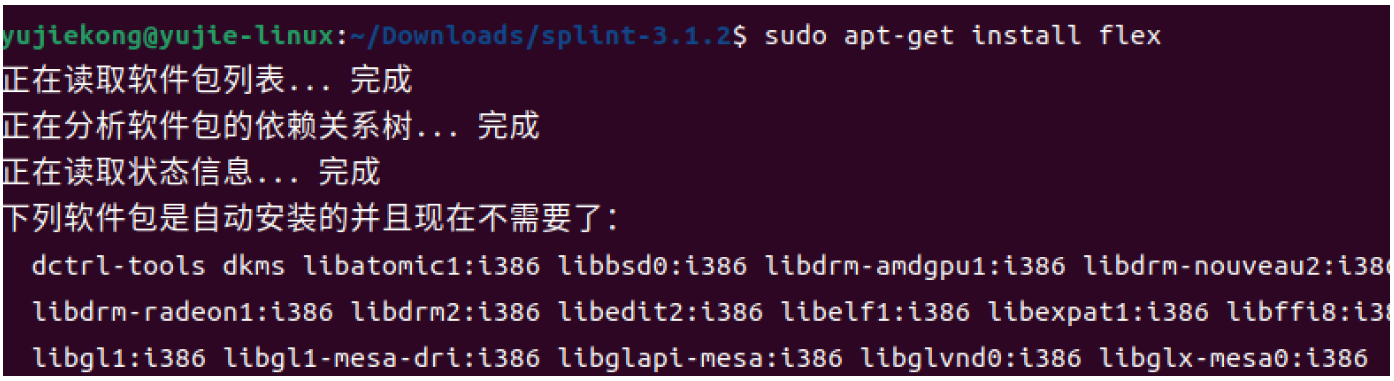
Lab 3.1 Using splint for C static analysis

1 安装并配置splint

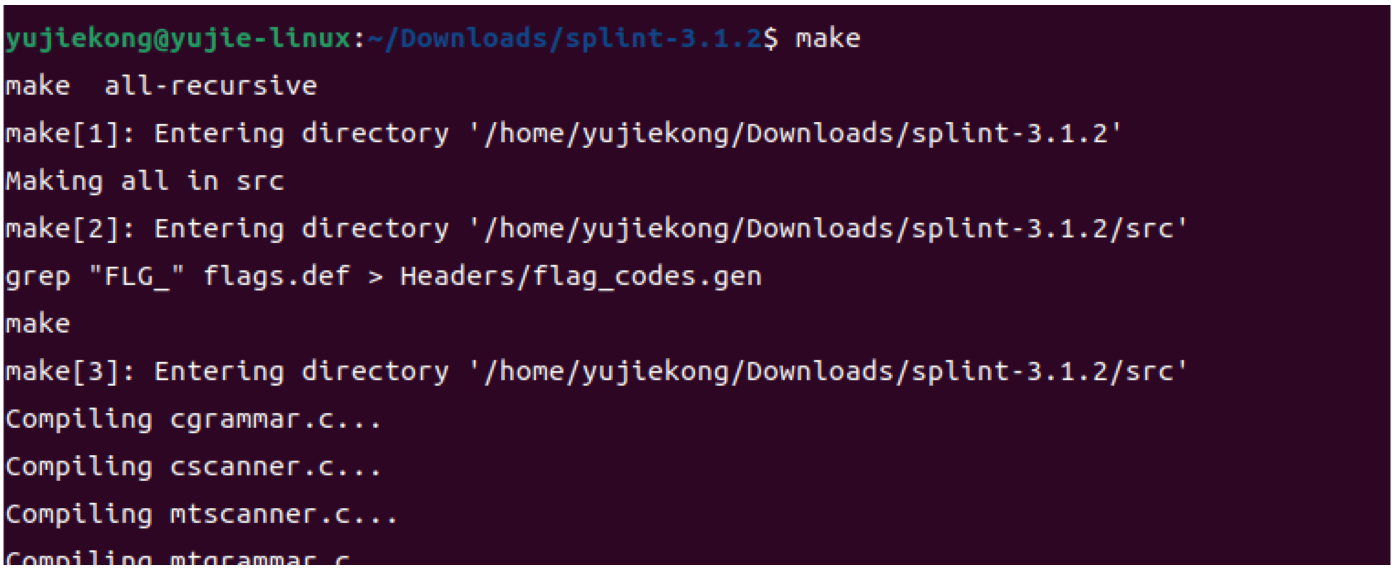
安装



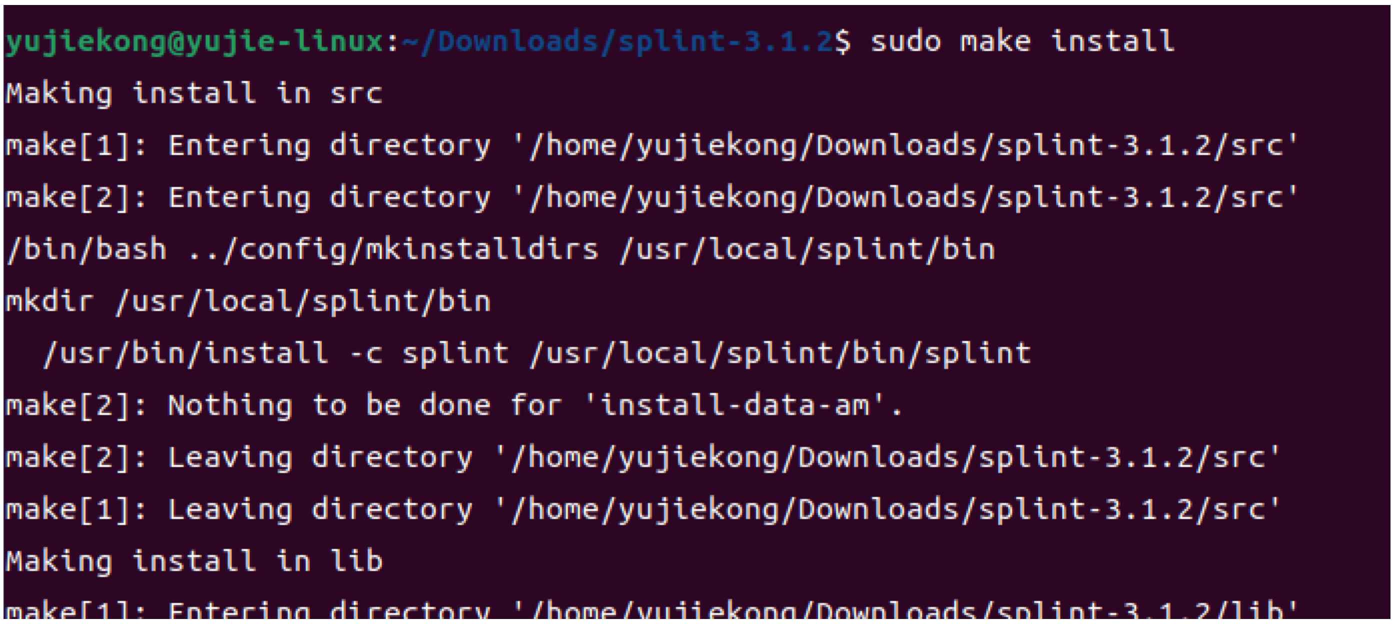
```
yujiekong@yujie-linux:~/Downloads$ sudo mkdir /usr/local/splint
[sudo] password for yujiekong:
yujiekong@yujie-linux:~/Downloads$ cd splint-3.1.2
yujiekong@yujie-linux:~/Downloads/splint-3.1.2$  ./configure --prefix=/usr/local/splint
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking target system type... x86_64-unknown-linux-gnu
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
```



```
yujiekong@yujie-linux:~/Downloads/splint-3.1.2$ sudo apt-get install flex
正在读取软件包列表... 完成
正在分析软件包的依赖关系树... 完成
正在读取状态信息... 完成
下列软件包是自动安装的并且现在不需要了:
  dctrl-tools dkms libatomic1:i386 libbsd0:i386 libdrm-amdgpu1:i386 libdrm-nouveau2:i38
  libdrm-radeon1:i386 libdrm2:i386 libedit2:i386 libelf1:i386 libexpat1:i386 libffi8:i38
  libgl1:i386 libgl1-mesa-dri:i386 libglapi-mesa:i386 libglvnd0:i386 libglx-mesa0:i386
```

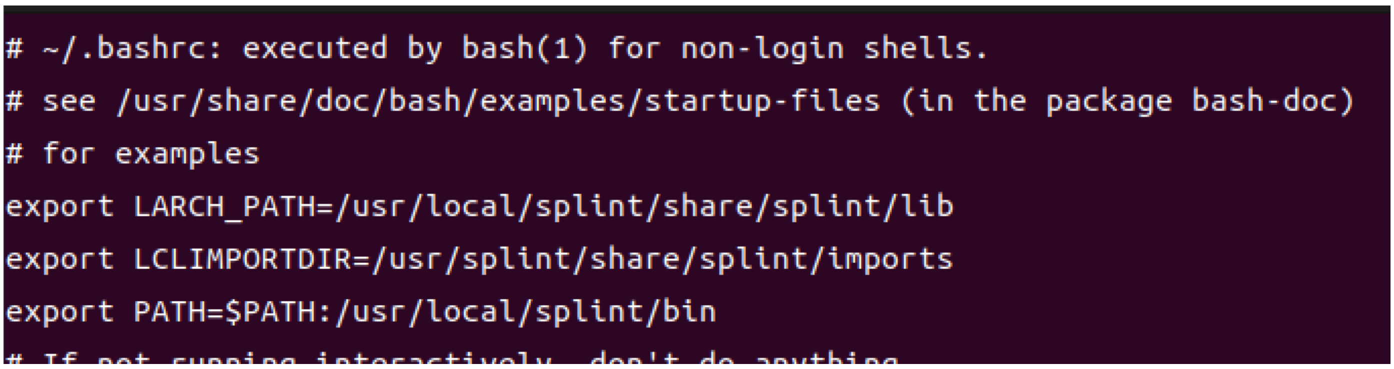


```
yujiekong@yujie-linux:~/Downloads/splint-3.1.2$ make
make  all-recursive
make[1]: Entering directory '/home/yujiekong/Downloads/splint-3.1.2'
Making all in src
make[2]: Entering directory '/home/yujiekong/Downloads/splint-3.1.2/src'
grep "FLG_" flags.def > Headers/flag_codes.gen
make
make[3]: Entering directory '/home/yujiekong/Downloads/splint-3.1.2/src'
Compiling cgrammar.c...
Compiling cscanner.c...
Compiling mtscanner.c...
Compiling mtgrammar.c
```

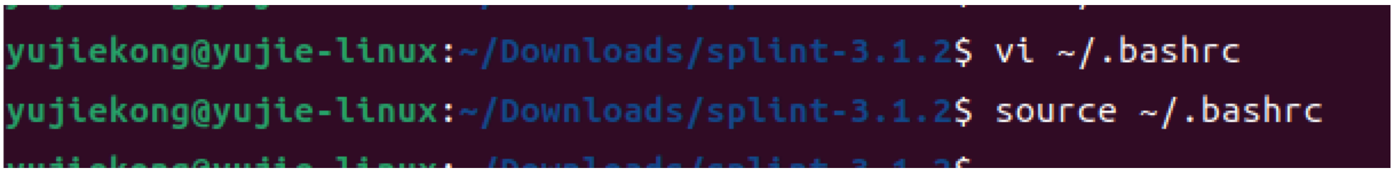


```
yujiekong@yujie-linux:~/Downloads/splint-3.1.2$ sudo make install
Making install in src
make[1]: Entering directory '/home/yujiekong/Downloads/splint-3.1.2/src'
make[2]: Entering directory '/home/yujiekong/Downloads/splint-3.1.2/src'
/bin/bash ../config/mkinstalldirs /usr/local/splint/bin
mkdir /usr/local/splint/bin
  /usr/bin/install -c splint /usr/local/splint/bin/splint
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/yujiekong/Downloads/splint-3.1.2/src'
make[1]: Leaving directory '/home/yujiekong/Downloads/splint-3.1.2/src'
Making install in lib
make[1]: Entering directory '/home/yujiekong/Downloads/splint-3.1.2/lib'
```

配置环境变量



```
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples
export LARCH_PATH=/usr/local/splint/share/splint/lib
export LCLIMPORTDIR=/usr/splint/share/splint/imports
export PATH=$PATH:/usr/local/splint/bin
# If not running interactively, don't do anything
```



```
yujiekong@yujie-linux:~/Downloads/splint-3.1.2$ vi ~/.bashrc
yujiekong@yujie-linux:~/Downloads/splint-3.1.2$ source ~/.bashrc
yujiekong@yujie-linux:~/Downloads/splint-3.1.2$
```

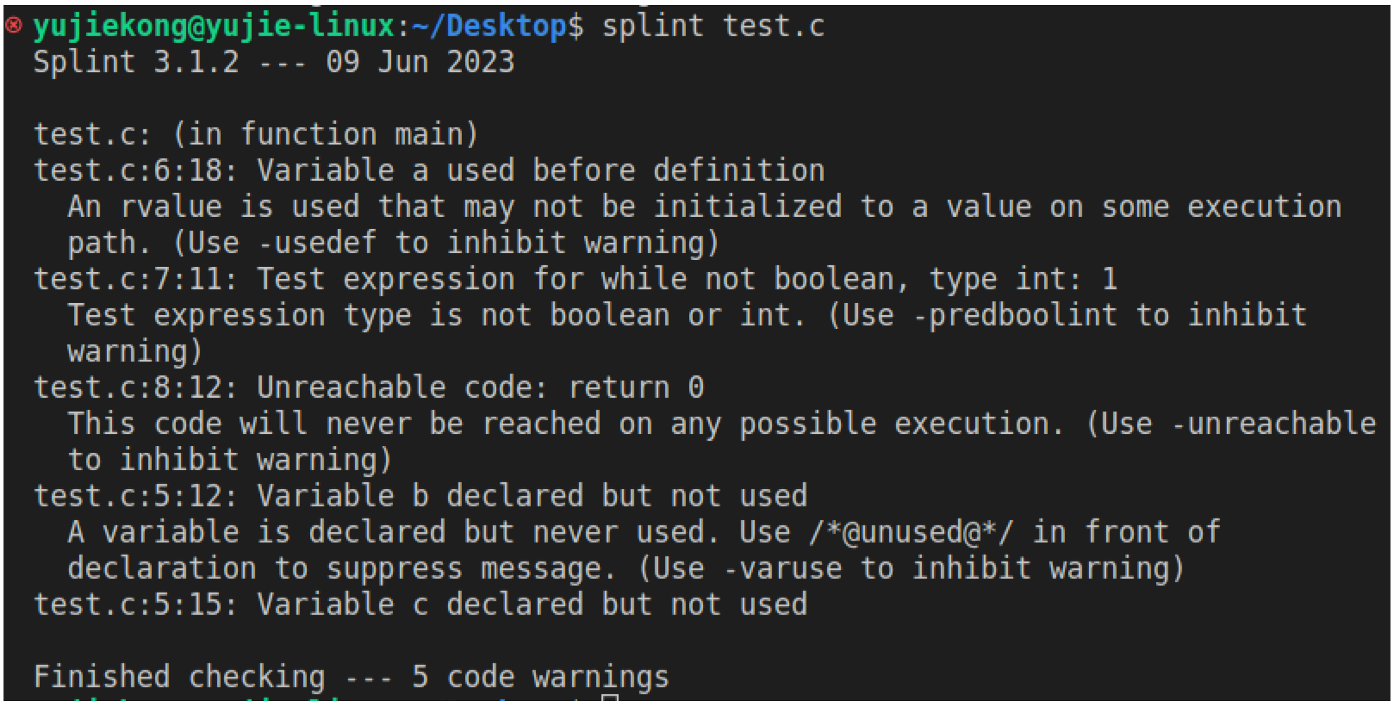
2 使用splint

2.1 编写问题代码

未使用变量、使用未赋值变量、死循环。

```
#include <stdio.h>
#include <string.h>

int main() {
    int a, b, c;
    printf("%d", a);
    while(1){;}
    return 0;
}
```

2.2 静态分析



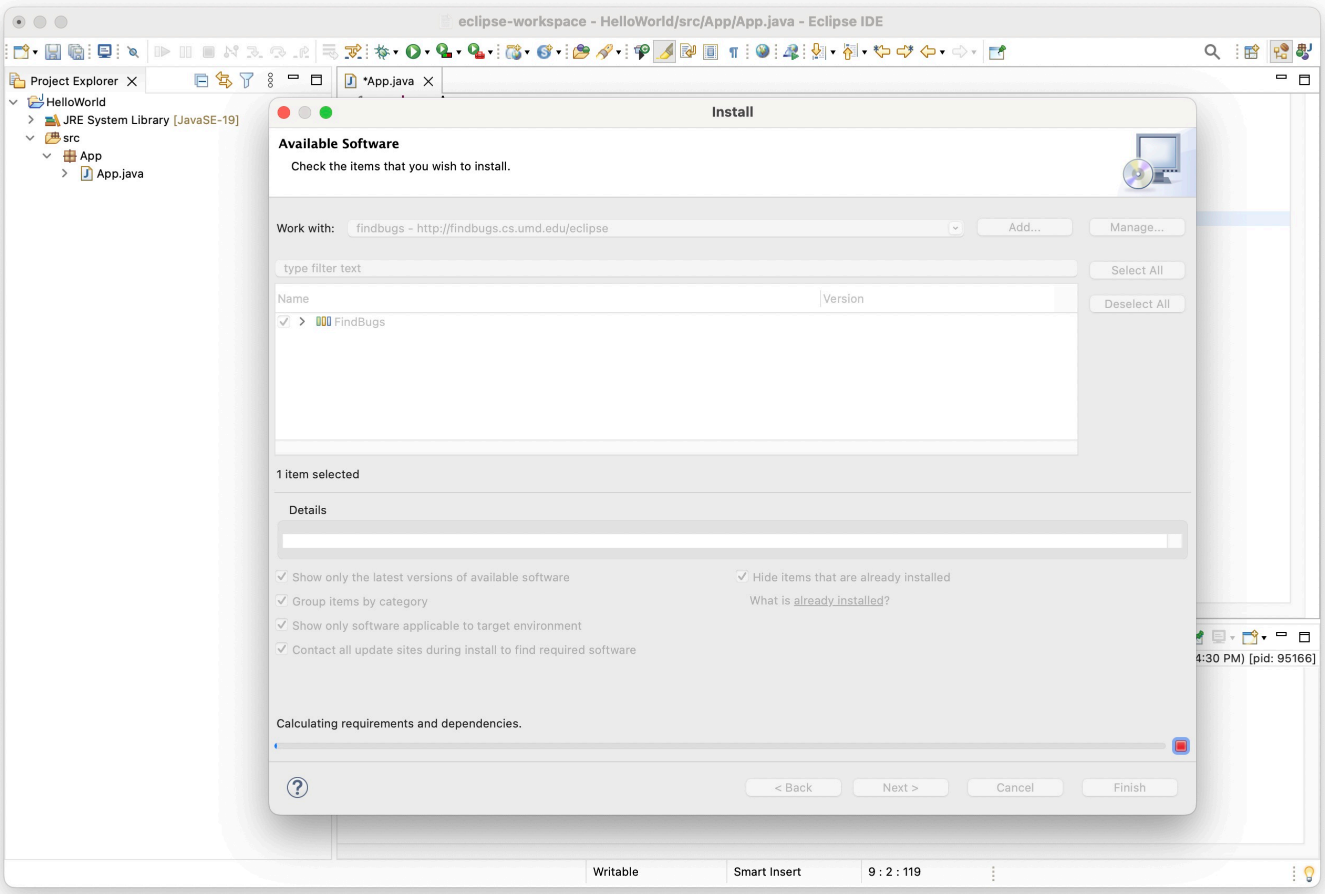
```
yujiekong@yujie-linux:~/Desktop$ splint test.c
Splint 3.1.2 --- 09 Jun 2023

test.c: (in function main)
test.c:6:18: Variable a used before definition
  An rvalue is used that may not be initialized to a value on some execution
  path. (Use -usedef to inhibit warning)
test.c:7:11: Test expression for while not boolean, type int: 1
  Test expression type is not boolean or int. (Use -predboolint to inhibit
  warning)
test.c:8:12: Unreachable code: return 0
  This code will never be reached on any possible execution. (Use -unreachable
  to inhibit warning)
test.c:5:12: Variable b declared but not used
  A variable is declared but never used. Use /*@unused@*/ in front of
  declaration to suppress message. (Use -varuse to inhibit warning)
test.c:5:15: Variable c declared but not used

Finished checking --- 5 code warnings
```

1. 变量 a 在定义之前被使用（第 6 行）
2. while 循环的测试表达式不是布尔类型，而是 int 类型（第 7 行）
3. 死循环（第8行）
4. 变量 b 被声明但未使用（第 5 行）
5. 变量 c 被声明但未使用（第 5 行

Lab 3.2 Using eclipse for java static analysis

本次试验使用findbugs进行静态分析。

1 安装 findbugs


eclipse-workspace - HelloWorld/src/App/App.java - Eclipse IDE

Install

Available Software

Check the items that you wish to install.

Work with: findbugs - http://findbugs.cs.umd.edu/eclipse

☑ FindBugs

1 item selected

Details

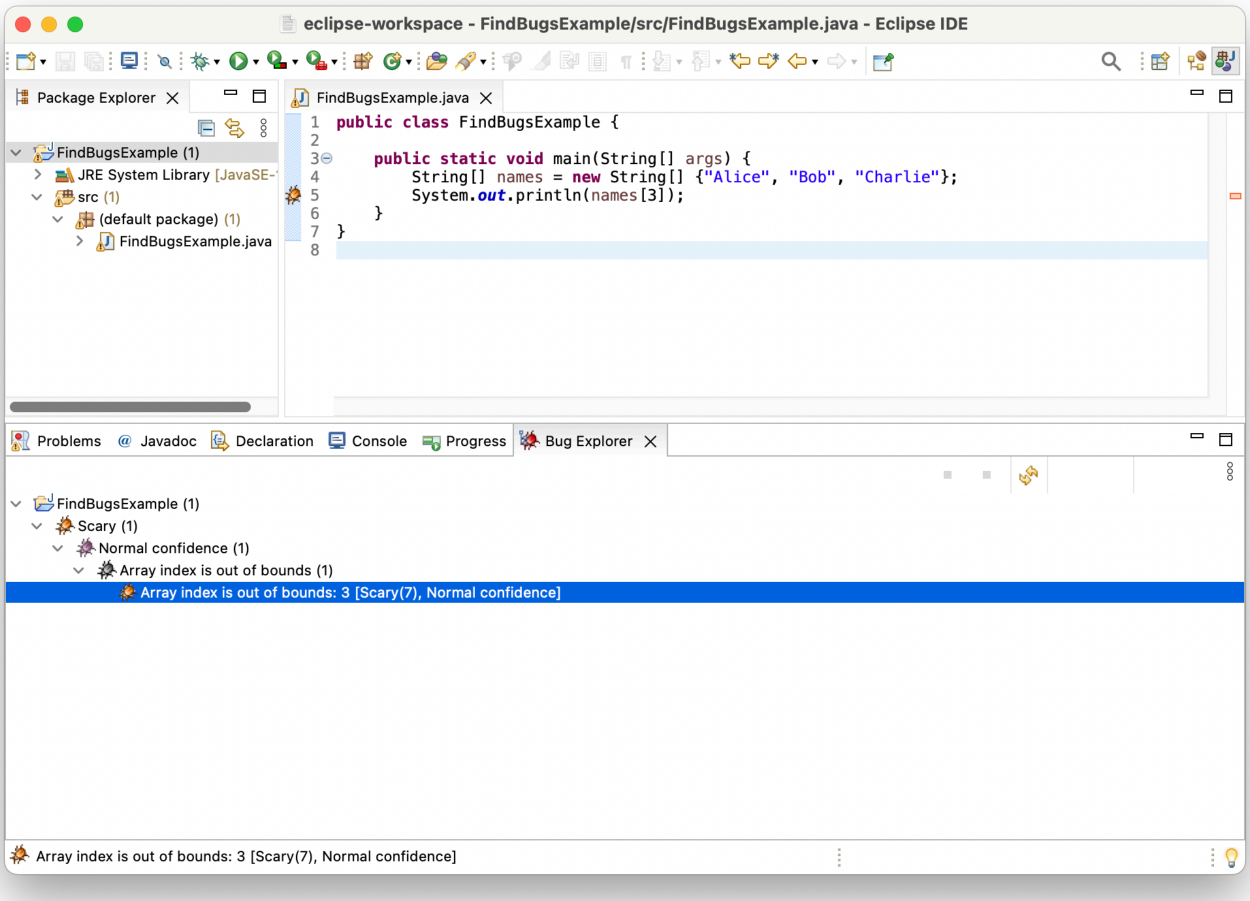
☑ Show only the latest versions of available software
☑ Group items by category
☑ Show only software applicable to target environment
☑ Contact all update sites during install to find required software
☑ Hide items that are already installed
What is already installed?

Calculating requirements and dependencies.

2 使用findbugs

参考实用教程，对以下代码进行静态分析结果如下：

```java
public class FindBugsExample {
    public static void main(String[] args) {
        String[] names = new String[] {"Alice", "Bob", "Charlie"};
        System.out.println(names[3]);
    }
}
```



```java
public class FindBugsExample {

    public static void main(String[] args) {
        String[] names = new String[] {"Alice", "Bob", "Charlie"};
        System.out.println(names[3]);
    }
}
```

```
FindBugsExample (1)
  Scary (1)
    Normal confidence (1)
      Array index is out of bounds (1)
        Array index is out of bounds: 3 [Scary(7), Normal confidence]
```

```
Array index is out of bounds: 3 [Scary(7), Normal confidence]
```

由上图可知，findbugs已经找到了问题。

在代码第五行，使用的index超出了数组的边界。本次试验成功。

试验过程中遇到了findbugs不生效的问题，查阅得知，findbugs不支持jdk1.8以上，调整之后成功。