

# **Find Security Bugs**

## **Ejemplos guiados**

**Realizado por**

Grupo 3 – Corocotta

### **Integrantes**

Hamza Hamda

Iván Sánchez Calderón

Juan David Corrales Gil

Ricardo Armando Blanco López

Jaime Eduardo Baires Escalante

### **Asignatura**

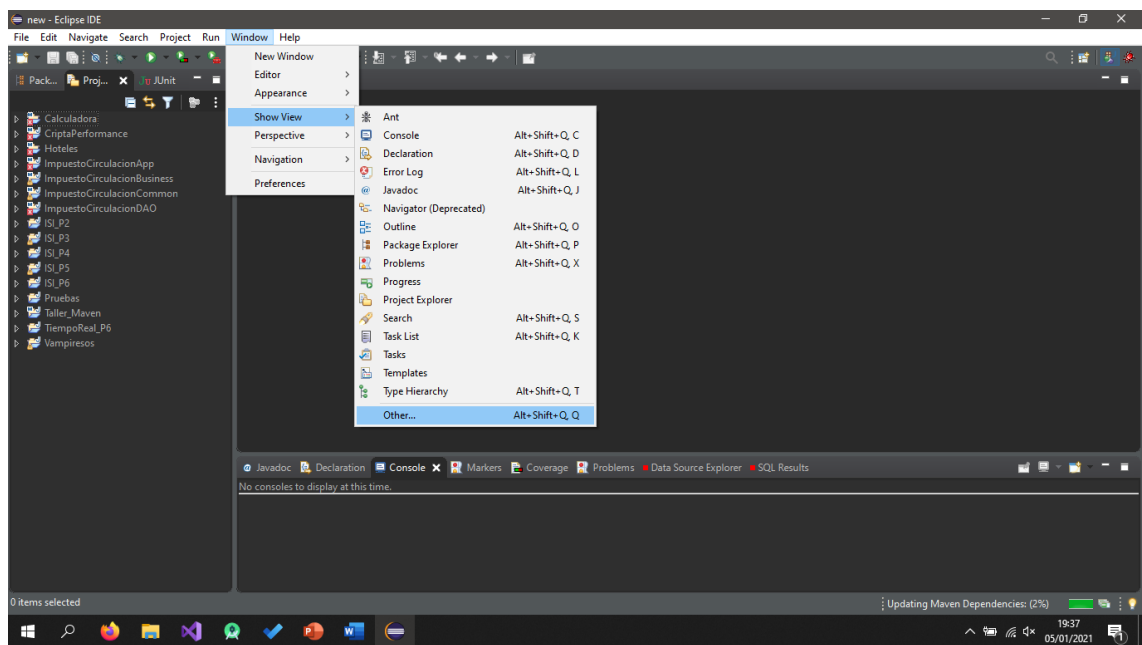
Calidad y Auditoría

## Índice

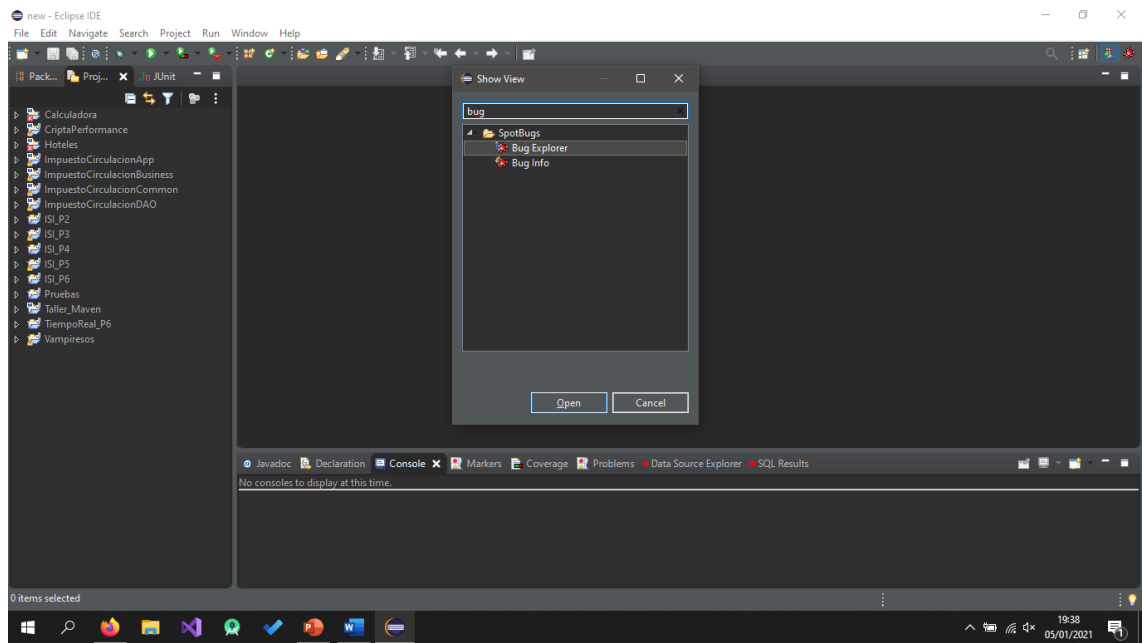
1. Ejemplo guiado con plugin de Eclipse.....	3
2. Ejemplo guiado con plugin de Maven.....	9

# 1. Ejemplo guiado con plugin de Eclipse

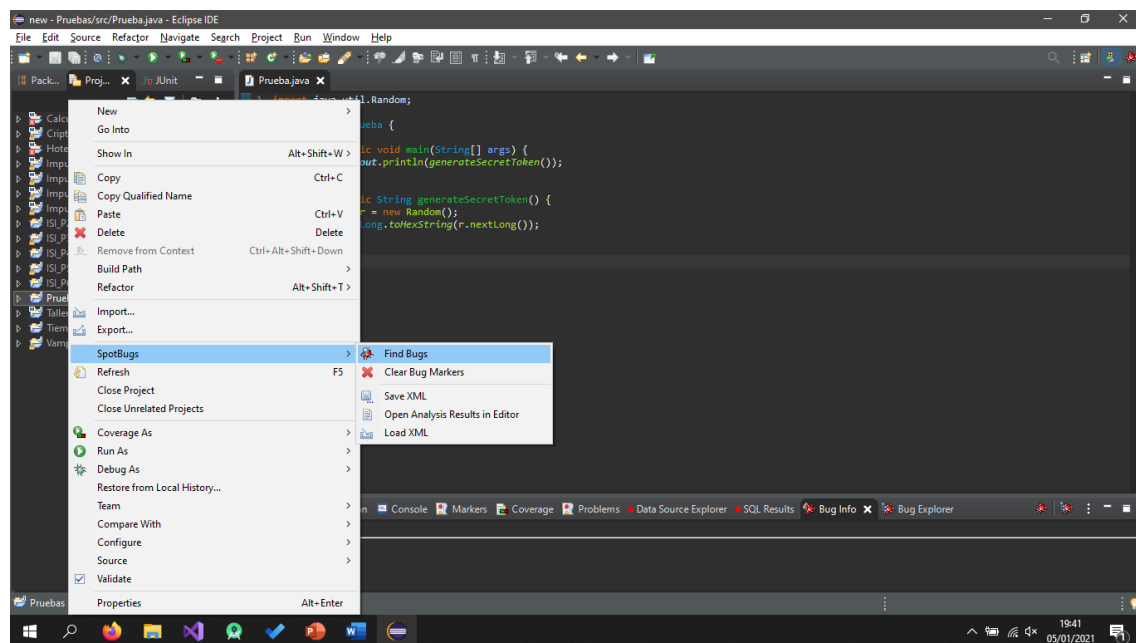
Incluir las vistas relacionadas para poder visualizar los errores. Window -> Show View -> Other...



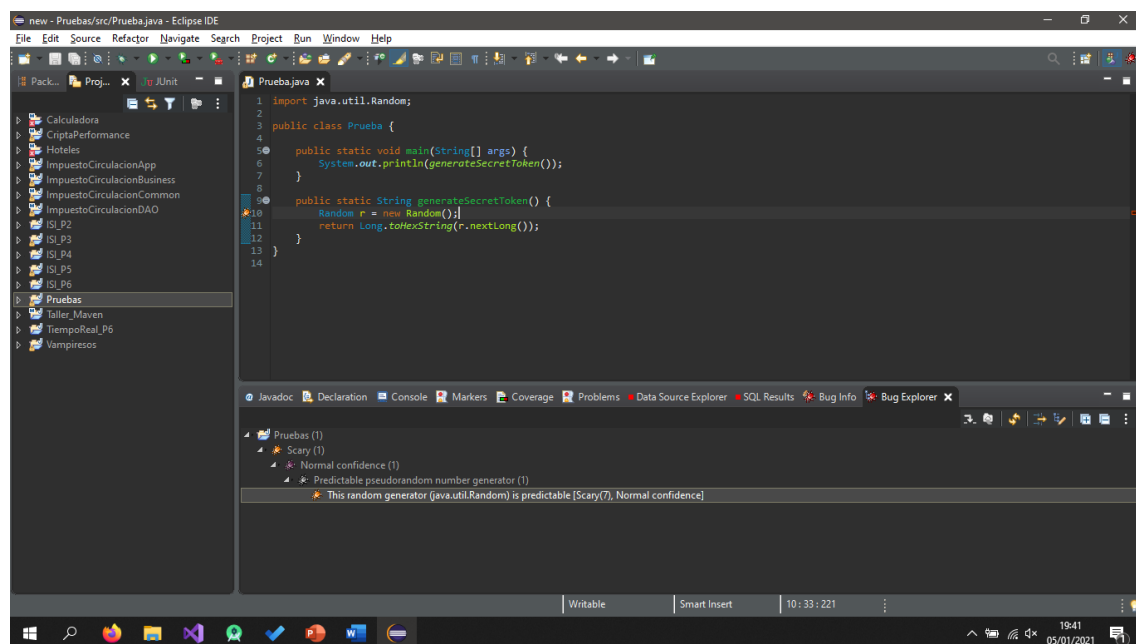
Escribir “bug” y seleccionar las vistas “Bug Explorer” y “Bug Info” -> Open.



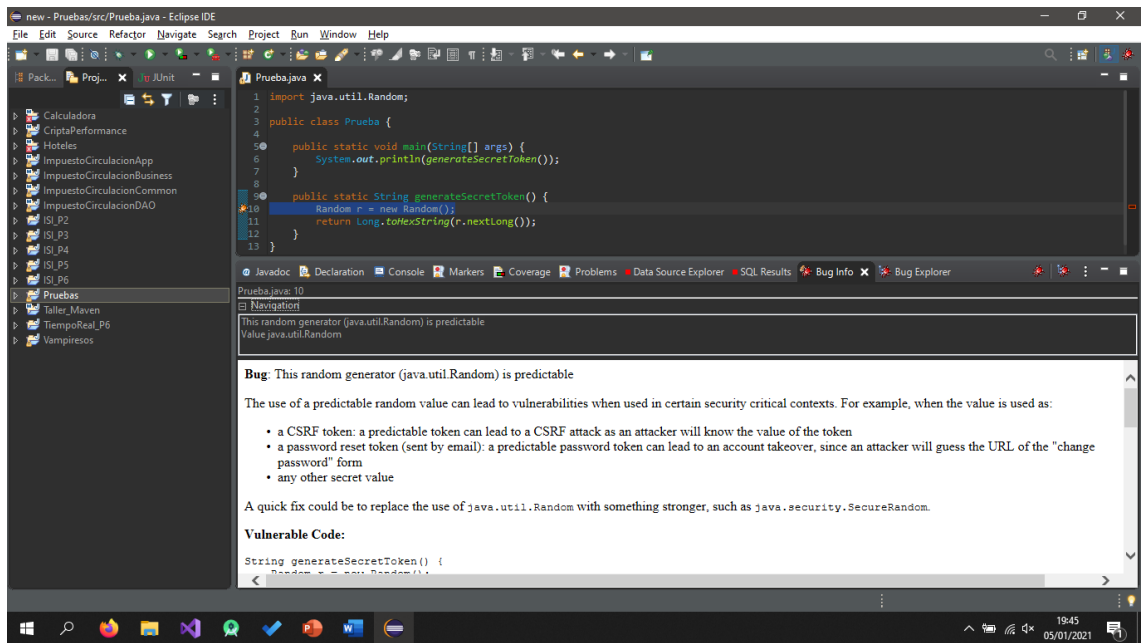
Se da clic derecho al proyecto o clase que se quiera analizar -> SpotBugs -> Find Bugs



Al cabo de unos segundos, aparecerían los resultados, si se tienen bugs de seguridad. En la ventana Bug Explorer se encuentra la lista de todos los errores que se tengan en el código, ordenados por categoría.

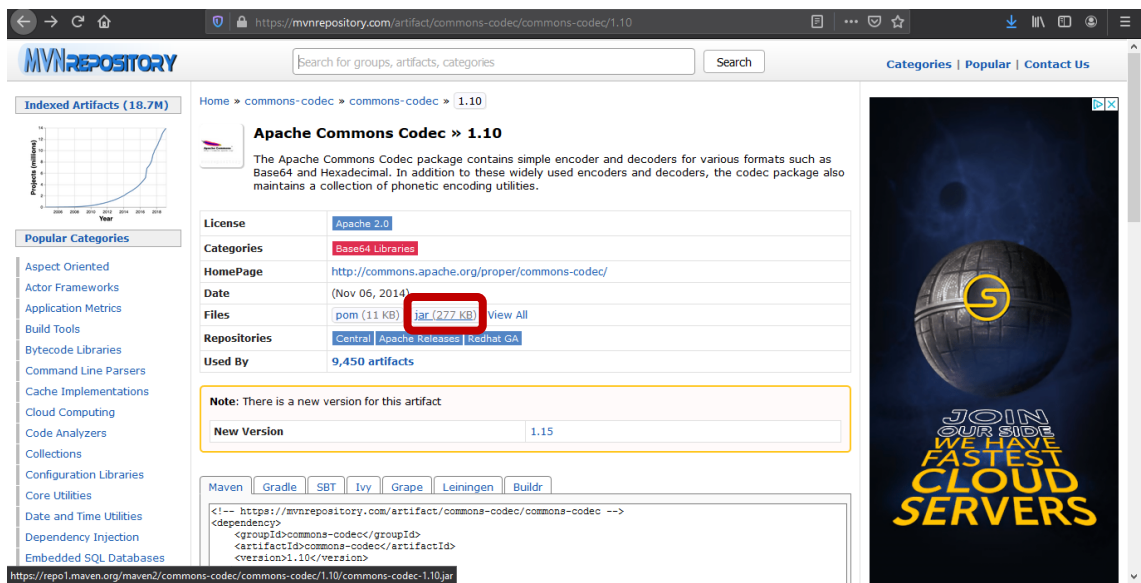


Al darle clic al error, se sombrea en el código la línea en la que se genera el error, la cual se marca con un símbolo especial. A su vez, si se cambia a la vista Bug Info, se tiene diversa información del error, e inclusive, una solución propuesta.

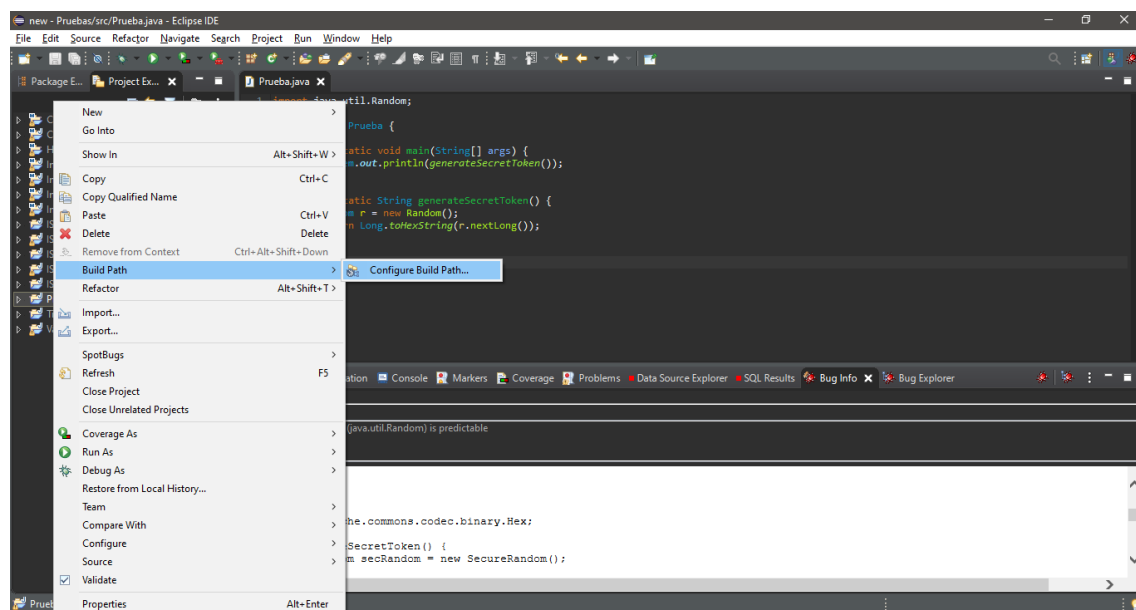


Para solucionar este error, primero se debe descargar un archivo .jar, que servirá como una librería a la solución propuesta.

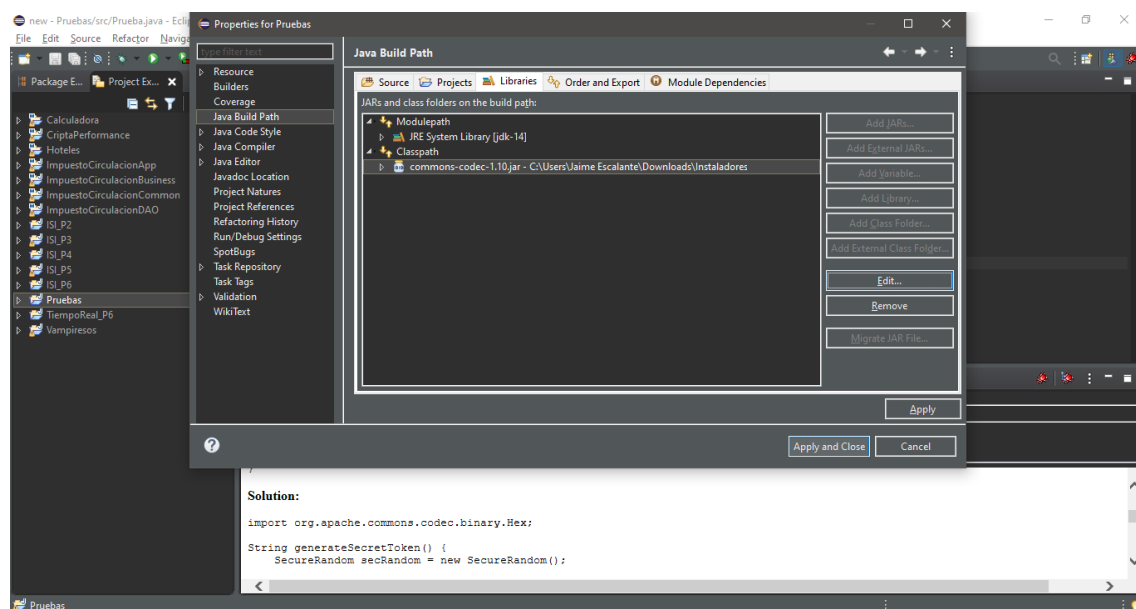
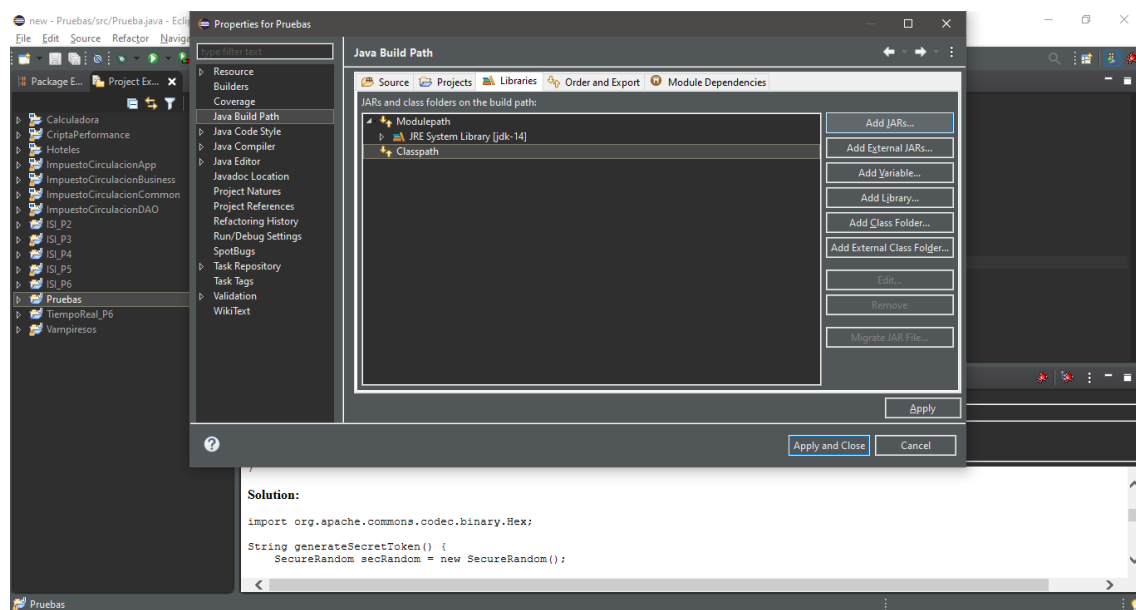
URL: <https://mvnrepository.com/artifact/commons-codec/commons-codec/1.10>



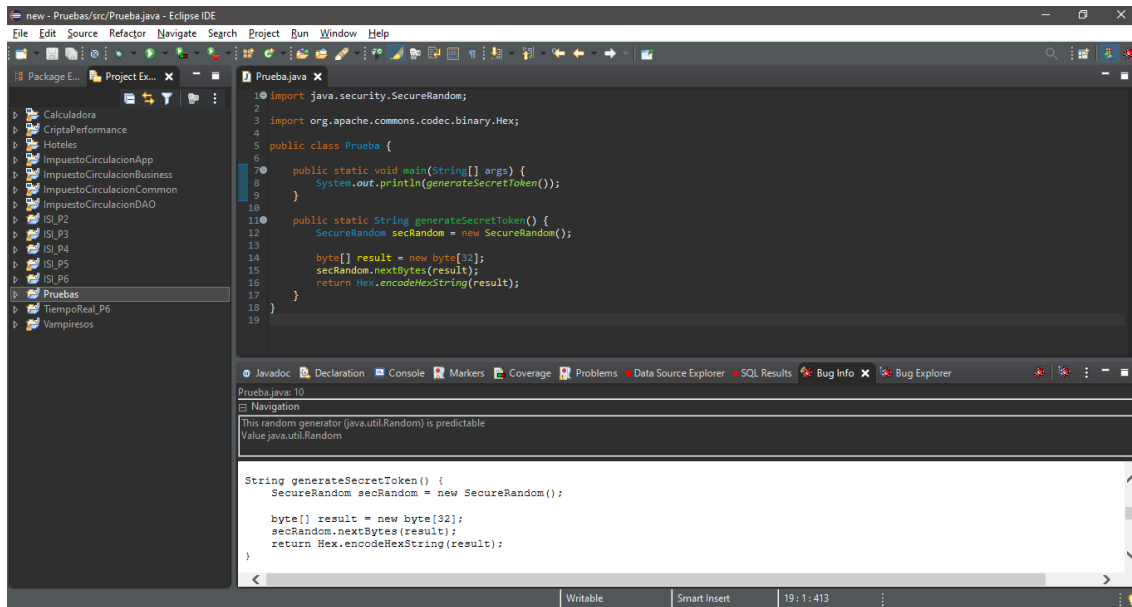
Agregar la librería descargada en el classpath del proyecto. Clic derecho sobre él -> Build Path -> Configure Build Path



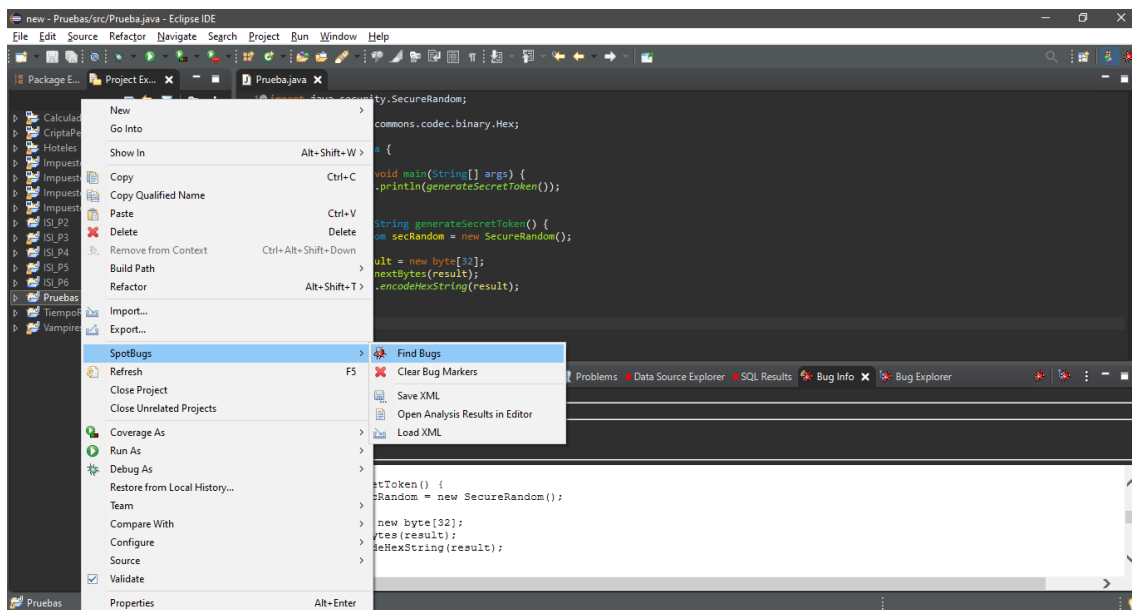
En el Classpath, seleccionar Add JARs y agregarlo.



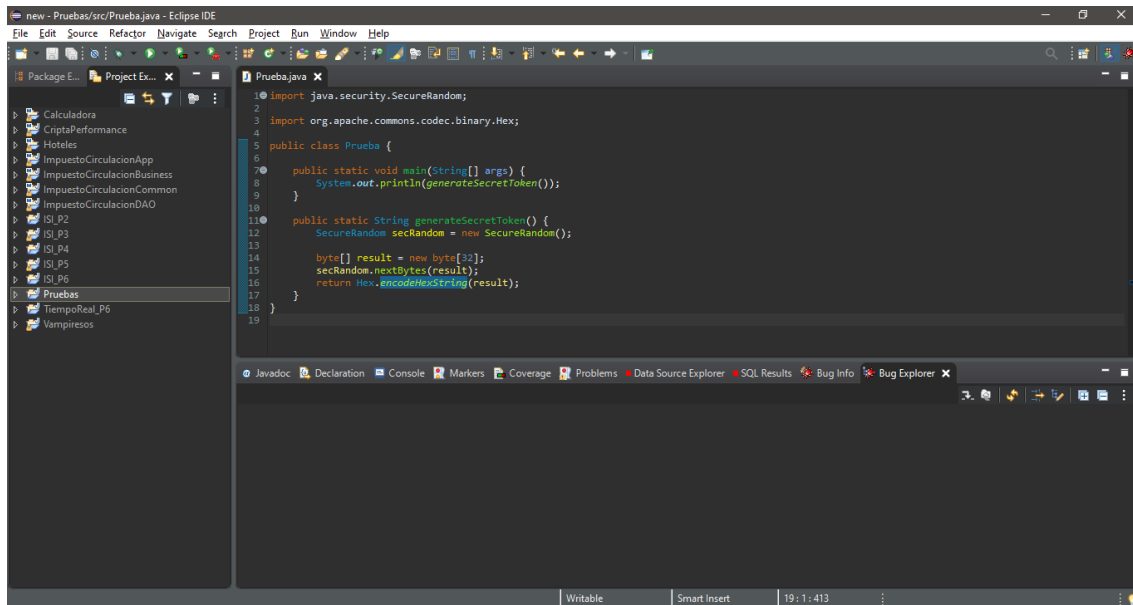
A continuación, se escribe el código seguro o “libre de bugs”.



Dar clic derecho nuevamente sobre el proyecto -> SpotBugs -> Find Bugs



Ahora no se encuentra ningún error de seguridad en el proyecto.



The screenshot shows the Eclipse IDE interface. The top menu bar includes File, Edit, Source, Refactor, Navigate, Search, Project, Run, Window, and Help. The left sidebar displays a project explorer with a tree view containing folders like Calculadora, CriptaPerformance, Hoteles, and a package named Pruebas. The main editor window is titled 'Prueba.java' and contains the following Java code:

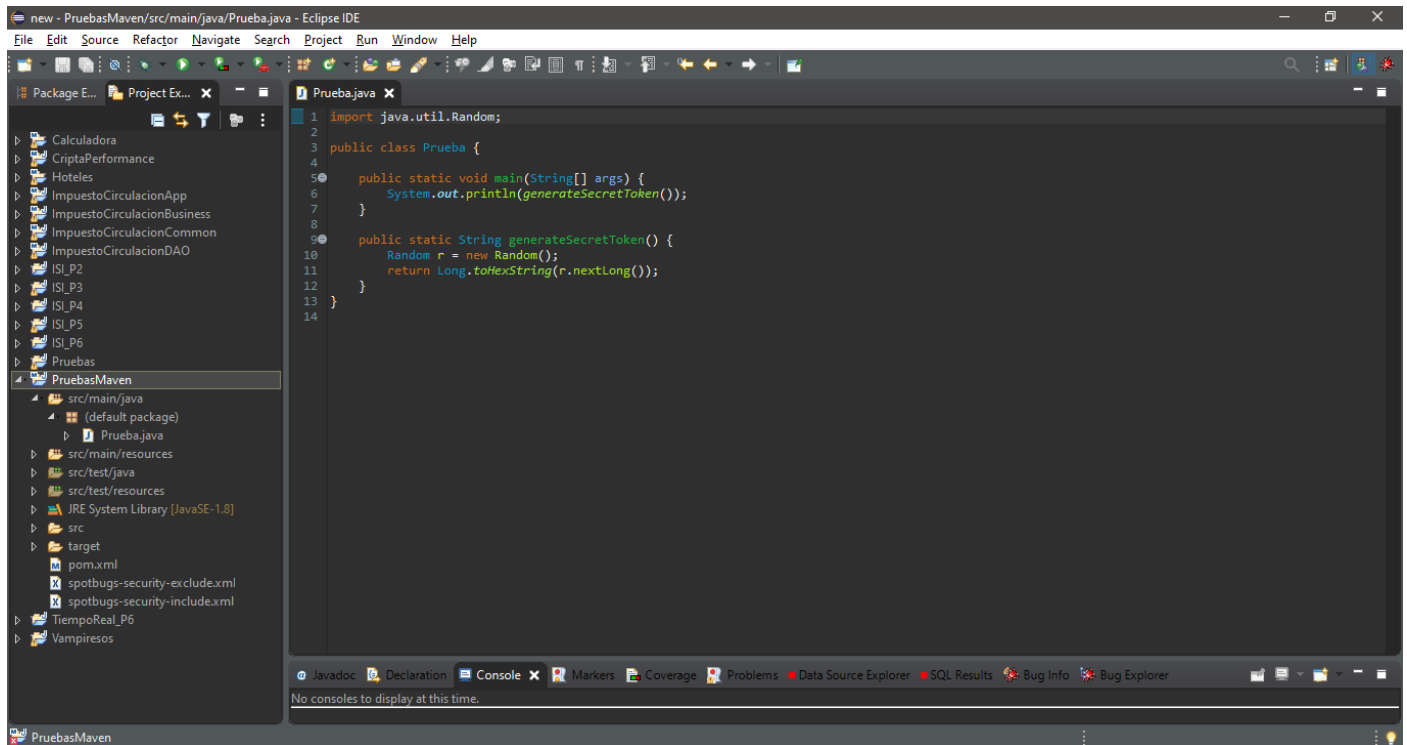
```
1 import java.security.SecureRandom;
2
3 import org.apache.commons.codec.binary.Hex;
4
5 public class Prueba {
6
7     public static void main(String[] args) {
8         System.out.println(generateSecretToken());
9     }
10
11     public static String generateSecretToken() {
12         SecureRandom secRandom = new SecureRandom();
13
14         byte[] result = new byte[32];
15         secRandom.nextBytes(result);
16         return Hex.encodeHexString(result);
17     }
18 }
19
```

Below the editor, a series of tabs are visible: Javadoc, Declaration, Console, Markers, Coverage, Problems, Data Source Explorer, SQL Results, Bug Info, and Bug Explorer. The 'Problems' tab is active, showing a list of issues. The bottom status bar indicates 'Writable', 'Smart Insert', and the cursor position '19: 1: 413'.

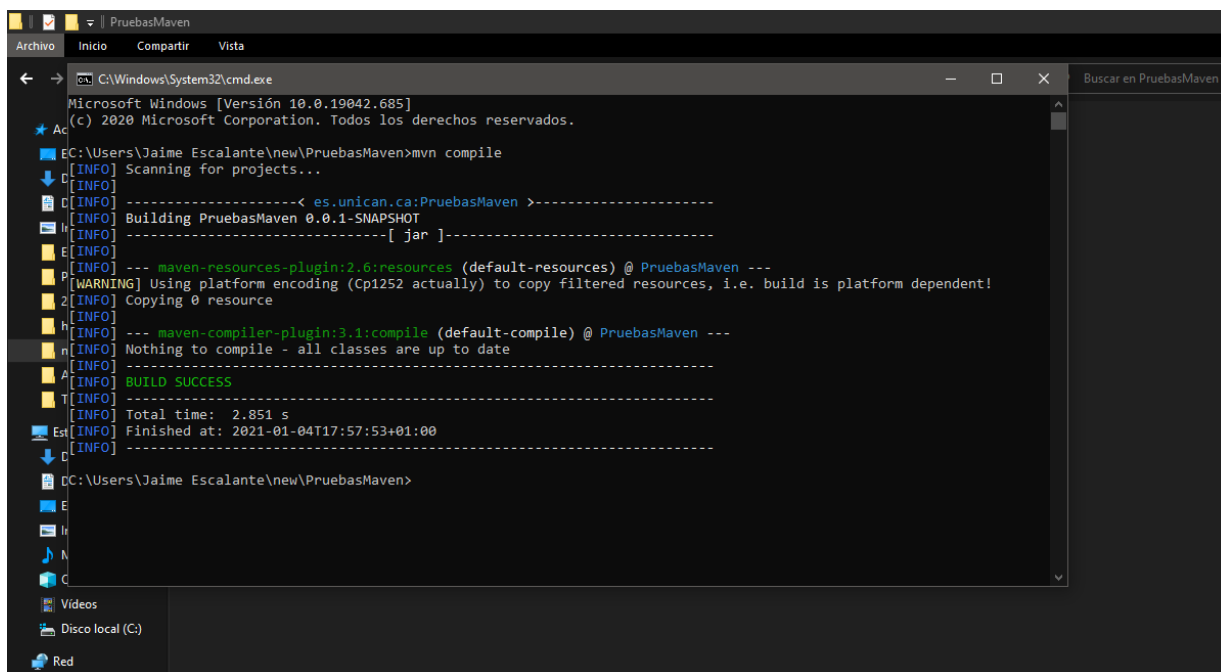


## 2. Ejemplo guiado con plugin de Maven

Se tiene el mismo ejemplo que en caso anterior, solo que ahora se parte de un proyecto Maven, con el fichero pom.xml definido según el manual de instalación.

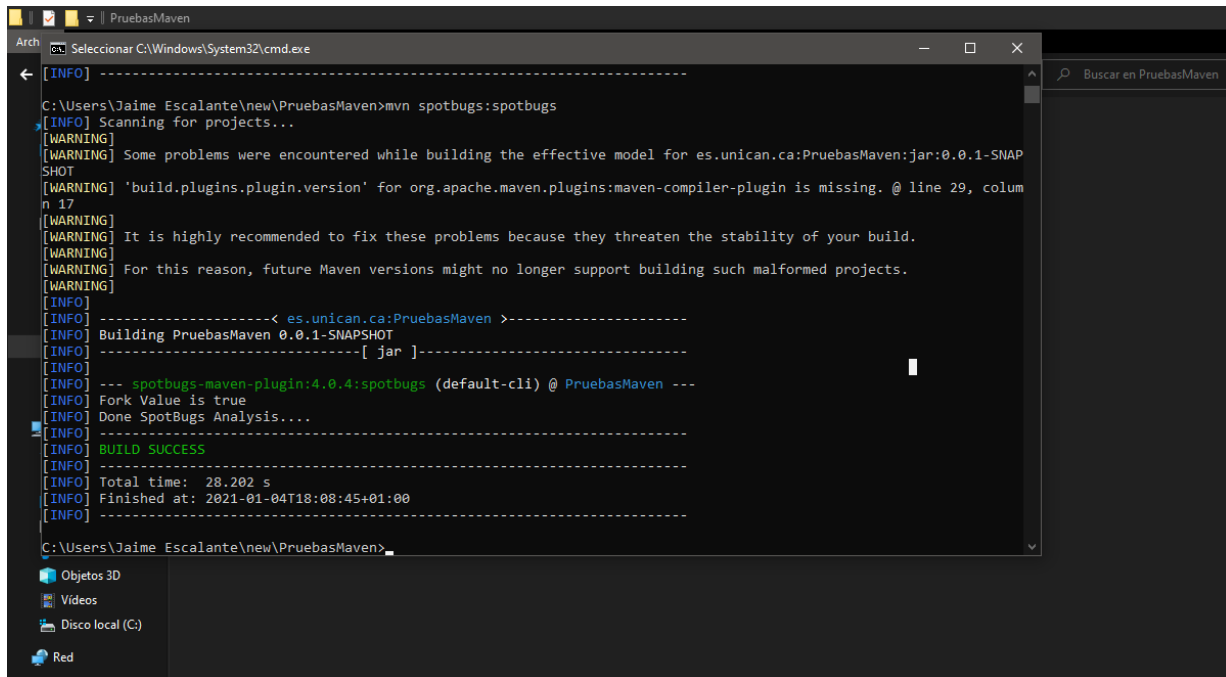


En la ventana de comandos, primero se compila el proyecto, para lo cual se escribe **mvn compile**



A continuación, para ejecutar el análisis escribir **mvn spotbugs:spotbugs**.

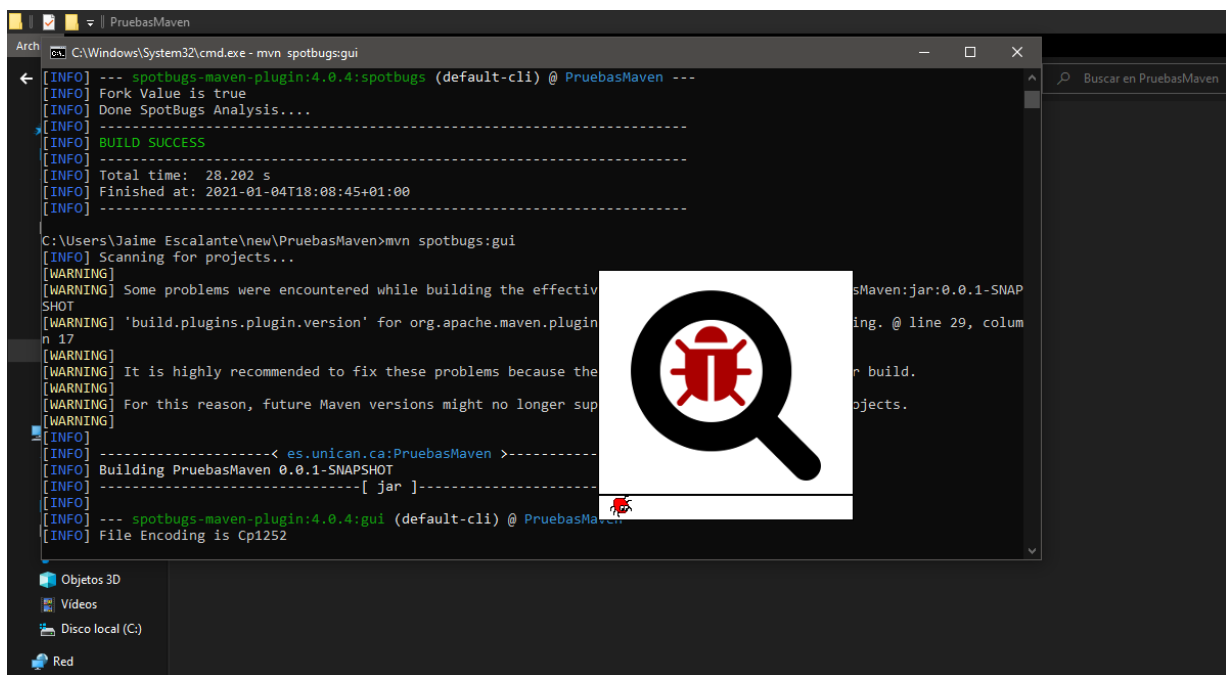
La primera vez que se ejecuta este comando podrán descargarse una serie de librerías.



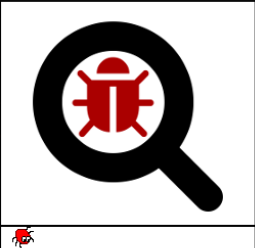
```
Arch C:\Windows\System32\cmd.exe
[INFO] -----
C:\Users\Jaime Escalante\new\PruebasMaven>mvn spotbugs:spotbugs
[INFO] Scanning for projects...
[WARNING] Some problems were encountered while building the effective model for es.unican.ca:PruebasMaven:jar:0.0.1-SNAPSHOT
[WARNING] 'build.plugins.plugin.version' for org.apache.maven.plugins:maven-compiler-plugin is missing. @ line 29, column 17
[WARNING] It is highly recommended to fix these problems because they threaten the stability of your build.
[WARNING] For this reason, future Maven versions might no longer support building such malformed projects.
[WARNING]
[INFO] -----< es.unican.ca:PruebasMaven >-----
[INFO] Building PruebasMaven 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO] --- spotbugs-maven-plugin:4.0.4:spotbugs (default-cli) @ PruebasMaven ---
[INFO] Fork Value is true
[INFO] Done SpotBugs Analysis....
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 28.202 s
[INFO] Finished at: 2021-01-04T18:08:45+01:00
[INFO] -----
C:\Users\Jaime Escalante\new\PruebasMaven>
```

Para poder acceder a los resultados mediante una interfaz de usuario, escribir **mvn spotbugs:gui**.

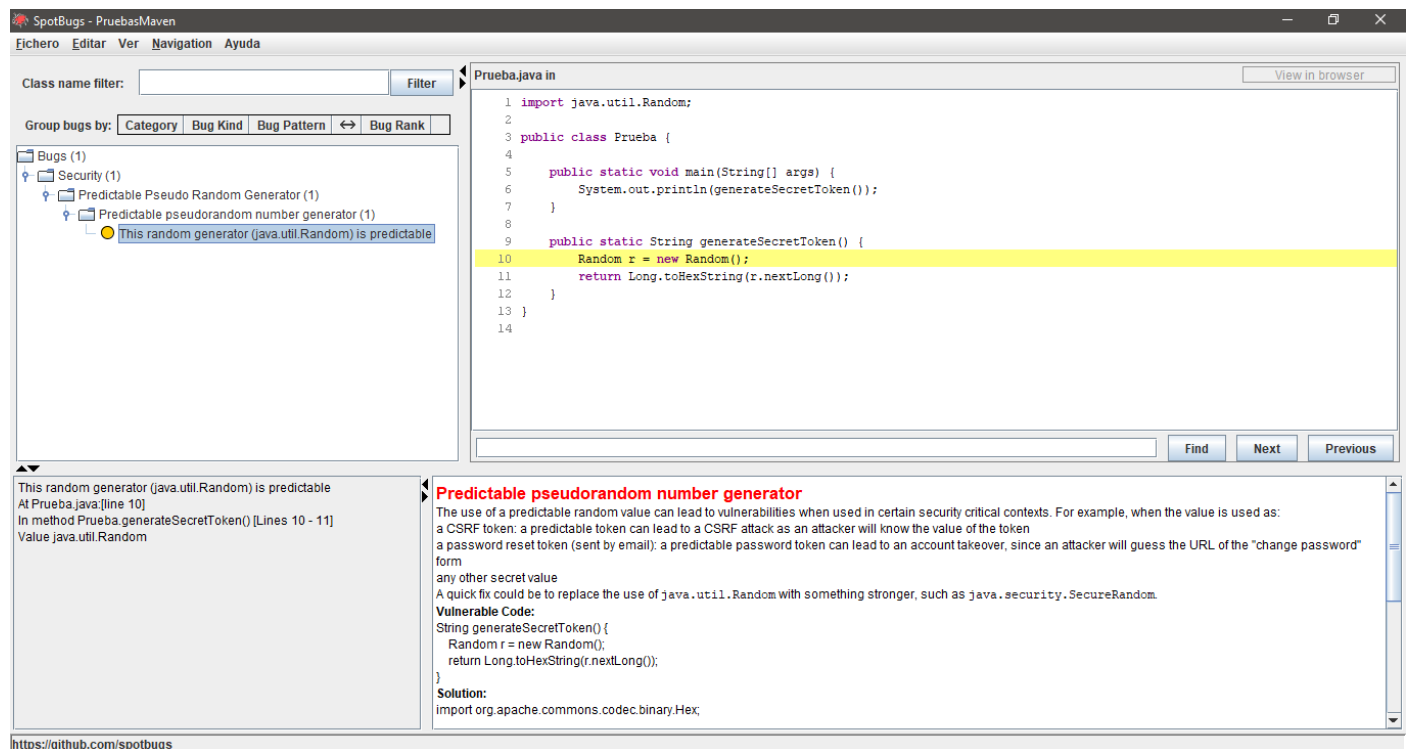
La primera vez que se ejecuta este comando podrán descargarse una serie de librerías.



```
Arch C:\Windows\System32\cmd.exe - mvn spotbugs:gui
[INFO] --- spotbugs-maven-plugin:4.0.4:spotbugs (default-cli) @ PruebasMaven ---
[INFO] Fork Value is true
[INFO] Done SpotBugs Analysis....
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 28.202 s
[INFO] Finished at: 2021-01-04T18:08:45+01:00
[INFO] -----
C:\Users\Jaime Escalante\new\PruebasMaven>mvn spotbugs:gui
[INFO] Scanning for projects...
[WARNING] Some problems were encountered while building the effective model for es.unican.ca:PruebasMaven:jar:0.0.1-SNAPSHOT
[WARNING] 'build.plugins.plugin.version' for org.apache.maven.plugins:maven-compiler-plugin is missing. @ line 29, column 17
[WARNING] It is highly recommended to fix these problems because they threaten the stability of your build.
[WARNING] For this reason, future Maven versions might no longer support building such malformed projects.
[WARNING]
[INFO] -----< es.unican.ca:PruebasMaven >-----
[INFO] Building PruebasMaven 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO] --- spotbugs-maven-plugin:4.0.4:gui (default-cli) @ PruebasMaven ---
[INFO] File Encoding is Cp1252
```



Los resultados se muestran en una ventana como la siguiente, con una estructura y contenido similares al caso anterior.



El proceso para solucionar el bug es equivalente al del apartado previo.