

Visual Code Grepper

Iván Ortiz del Noval, Marcos Fernández Alonso e Irene Zamanillo
Zubizarreta

Índice:

- ▶ ¿Qué es Visual Code Greeper?
- ▶ Características
- ▶ Guía de instalación
- ▶ Ejercicio práctico

Repositorio GitHub con la información: <https://github.com/nDix-OP/talerVCGrepper/>

Qué es Visual Code Grepper

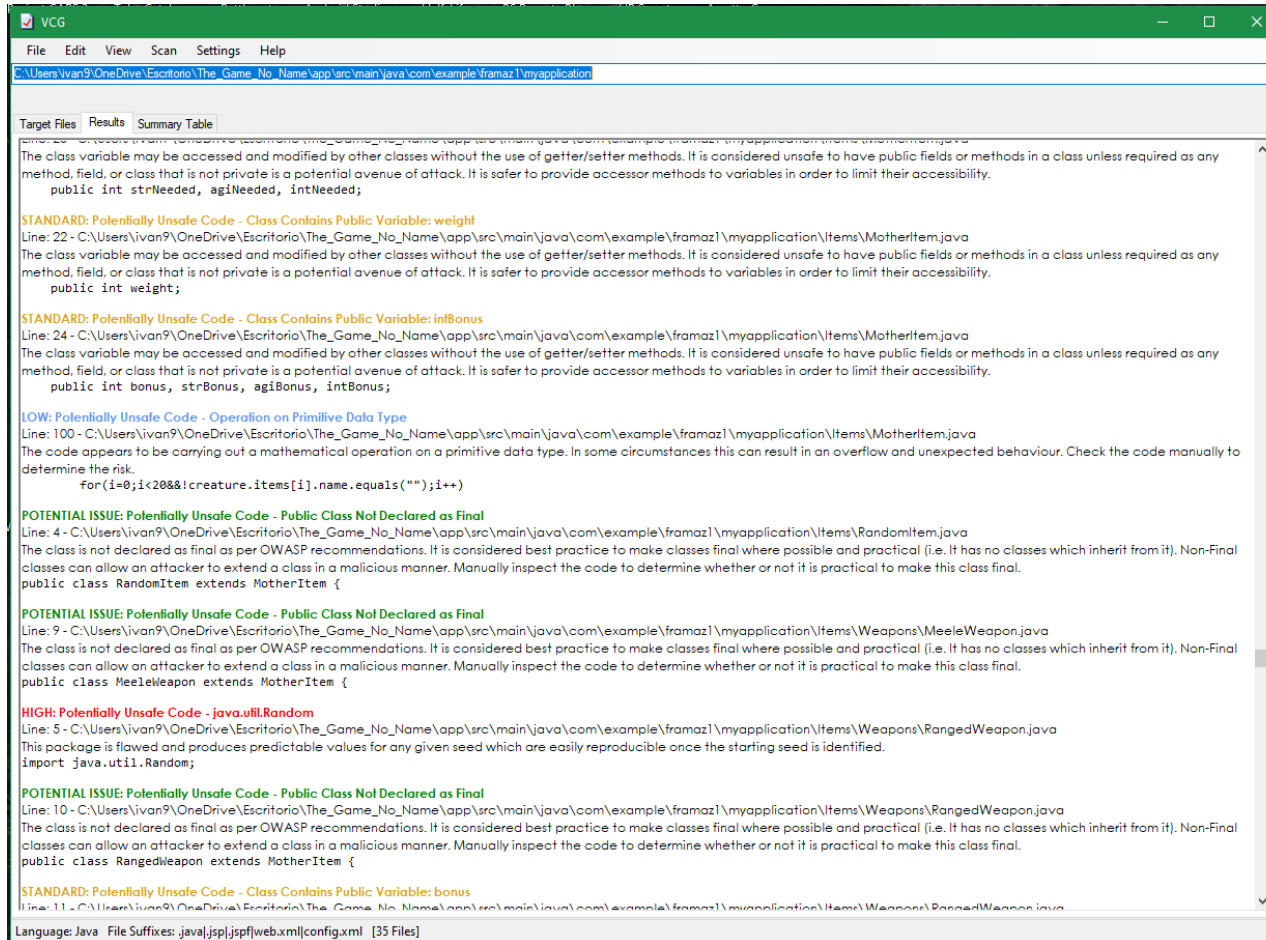
- ▶ Visual Code Grepper es una herramienta de análisis estático de código, centrada en la **seguridad**
- ▶ Permite revisar código rápidamente escaneando código y comentarios en busca de posibles brechas de seguridad
- ▶ Disponible en <https://github.com/nccgroup/VCG>

Características

- ▶ Soporte de múltiples lenguajes: C/C++, Java, C#, VisualBasic y PL/SQL
- ▶ Configurable a través de ficheros (perfiles)
- ▶ Clasificación de errores según su severidad
- ▶ Permite exportar los resultados a un fichero
- ▶ Análisis vía aplicación de escritorio o línea de comandos
- ▶ Gráfico de sectores con proporciones de código, comentarios, etc.

Características

Resultados con la interfaz gráfica



VCG

File Edit View Scan Settings Help

C:\Users\ivan9\OneDrive\Escritorio\The_Game_No_Name\app\src\main\java\com\example\framaz1\myapplication

Target Files Results Summary Table

Line: 22 - C:\Users\ivan9\OneDrive\Escritorio\The_Game_No_Name\app\src\main\java\com\example\framaz1\myapplication\Items\MotherItem.java
The class variable may be accessed and modified by other classes without the use of getter/setter methods. It is considered unsafe to have public fields or methods in a class unless required as any method, field, or class that is not private is a potential avenue of attack. It is safer to provide accessor methods to variables in order to limit their accessibility.
public int strNeeded, agiNeeded, intNeeded;

STANDARD: Potentially Unsafe Code - Class Contains Public Variable: weight
Line: 22 - C:\Users\ivan9\OneDrive\Escritorio\The_Game_No_Name\app\src\main\java\com\example\framaz1\myapplication\Items\MotherItem.java
The class variable may be accessed and modified by other classes without the use of getter/setter methods. It is considered unsafe to have public fields or methods in a class unless required as any method, field, or class that is not private is a potential avenue of attack. It is safer to provide accessor methods to variables in order to limit their accessibility.
public int weight;

STANDARD: Potentially Unsafe Code - Class Contains Public Variable: intBonus
Line: 24 - C:\Users\ivan9\OneDrive\Escritorio\The_Game_No_Name\app\src\main\java\com\example\framaz1\myapplication\Items\MotherItem.java
The class variable may be accessed and modified by other classes without the use of getter/setter methods. It is considered unsafe to have public fields or methods in a class unless required as any method, field, or class that is not private is a potential avenue of attack. It is safer to provide accessor methods to variables in order to limit their accessibility.
public int bonus, strBonus, agiBonus, intBonus;

LOW: Potentially Unsafe Code - Operation on Primitive Data Type
Line: 100 - C:\Users\ivan9\OneDrive\Escritorio\The_Game_No_Name\app\src\main\java\com\example\framaz1\myapplication\Items\MotherItem.java
The code appears to be carrying out a mathematical operation on a primitive data type. In some circumstances this can result in an overflow and unexpected behaviour. Check the code manually to determine the risk.
for(i=0;i<20&&!creature.items[i].name.equals(""));i++)

POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final
Line: 4 - C:\Users\ivan9\OneDrive\Escritorio\The_Game_No_Name\app\src\main\java\com\example\framaz1\myapplication\Items\RandomItem.java
The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.
public class RandomItem extends MotherItem {

POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final
Line: 9 - C:\Users\ivan9\OneDrive\Escritorio\The_Game_No_Name\app\src\main\java\com\example\framaz1\myapplication\Items\Weapons\MeeleWeapon.java
The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.
public class MeeleWeapon extends MotherItem {

HIGH: Potentially Unsafe Code - java.util.Random
Line: 5 - C:\Users\ivan9\OneDrive\Escritorio\The_Game_No_Name\app\src\main\java\com\example\framaz1\myapplication\Items\Weapons\RangedWeapon.java
This package is flawed and produces predictable values for any given seed which are easily reproducible once the starting seed is identified.
import java.util.Random;

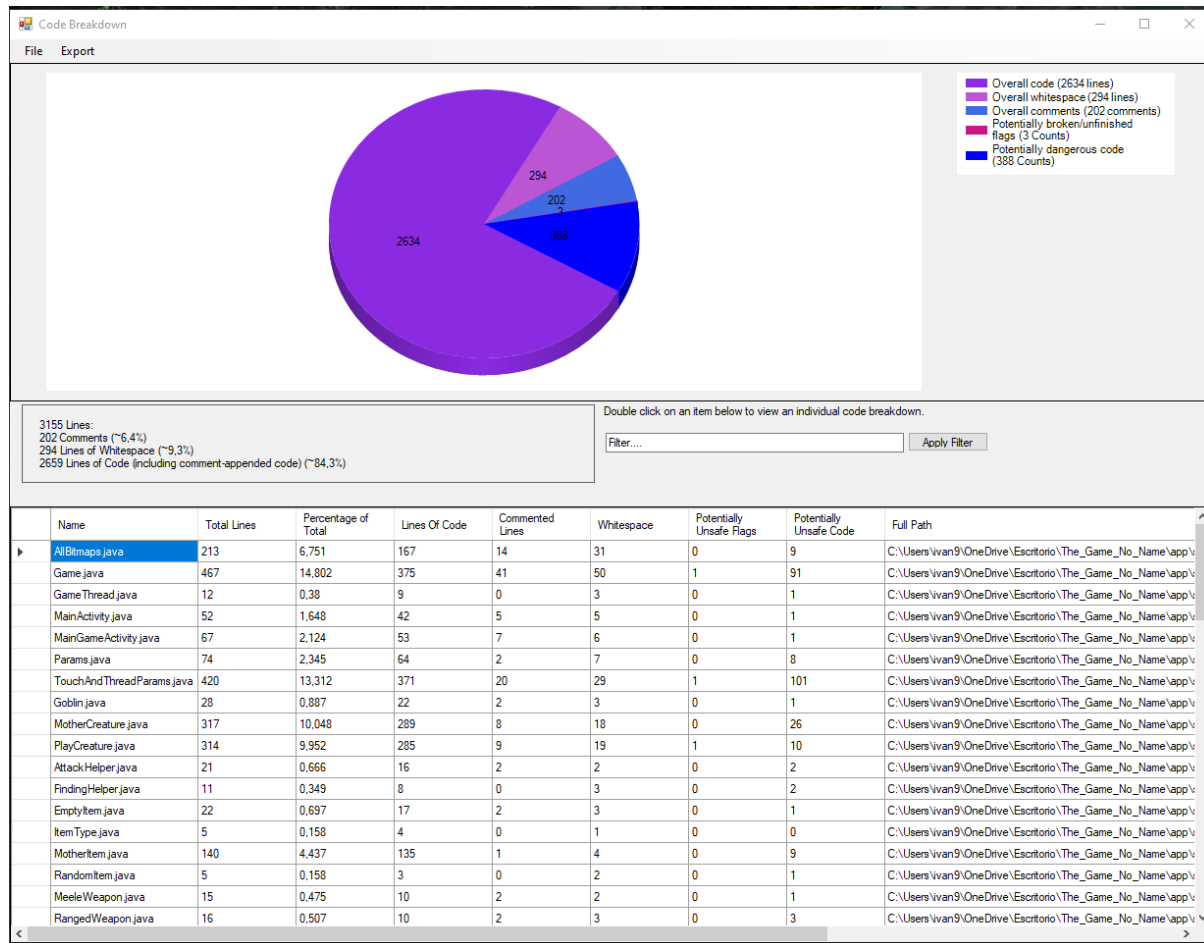
POTENTIAL ISSUE: Potentially Unsafe Code - Public Class Not Declared as Final
Line: 10 - C:\Users\ivan9\OneDrive\Escritorio\The_Game_No_Name\app\src\main\java\com\example\framaz1\myapplication\Items\Weapons\RangedWeapon.java
The class is not declared as final as per OWASP recommendations. It is considered best practice to make classes final where possible and practical (i.e. It has no classes which inherit from it). Non-Final classes can allow an attacker to extend a class in a malicious manner. Manually inspect the code to determine whether or not it is practical to make this class final.
public class RangedWeapon extends MotherItem {

STANDARD: Potentially Unsafe Code - Class Contains Public Variable: bonus
Line: 11 - C:\Users\ivan9\OneDrive\Escritorio\The_Game_No_Name\app\src\main\java\com\example\framaz1\myapplication\Items\Weapons\RangedWeapon.java

Language: Java File Suffixes: java|jsp|jspx|web.xml|config.xml [35 Files]

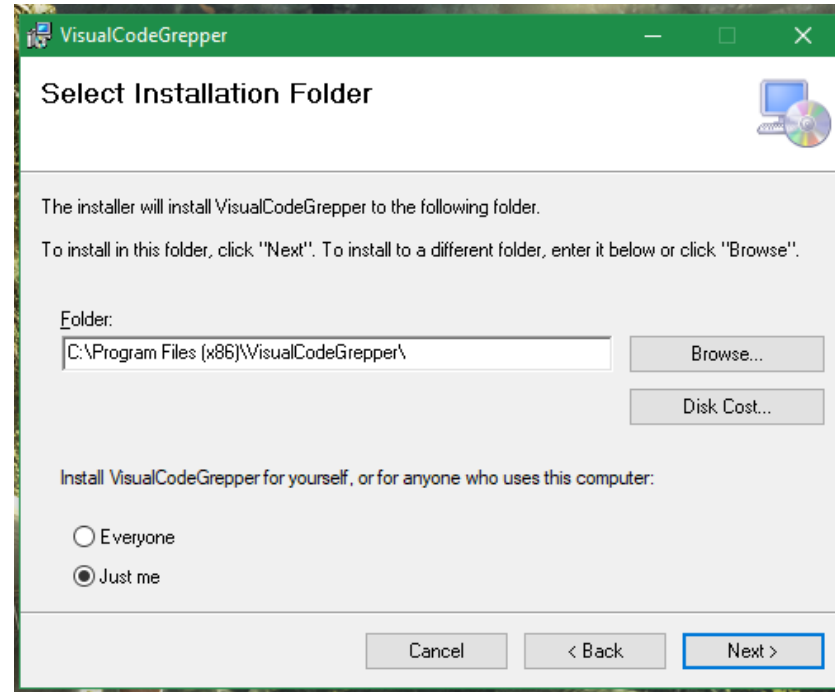
Características

Estadísticas de los resultados



Guía de instalación

- ▶ Descargar el instalador desde el siguiente enlace:
<https://sourceforge.net/projects/visualcodegrepp/>
- ▶ Seguir las instrucciones de instalación
- ▶ Iniciar el programa con el acceso directo en el escritorio



Ejercicio práctico

Comencemos ahora con la realización del ejercicio guiado.