Find Security Bugs

Grupo 3 – Corocotta

Funcionalidades

- Detectar vulnerabilidades de seguridad.
- Analiza patrones de error para comparar código y detectar errores.

Generalidades

- Integración con plataformas de desarrollo y pruebas.

Generalidades

- Compatibilidad con herramientas de integración continua.

sonarqube

Generalidades

- Proyecto open-source bajo la licencia LGPL.
  - https://github.com/find-sec-bugs/find-sec-bugs

Requerimientos

- JRE o JDK >= 1.5.0
- IDE compatible con plugins externos.
- Sistema Operativo GNU/Linux, Windows y MacOS X

Tipos de Bugs que puede detectar

- Generales
  - Referencias a null
- Concurrencia
  - Posibles deadlocks
- Bucles/Condicional
  - Código inalcanzable
- String
  - Igualdades con == o !=

Tipos de Bugs que puede detectar

- Reescritura de objetos
  - Objetos iguales deberían tener hashcodes iguales
- I/O Streams
  - Streams sin cerrar
- Código duplicado
  - Variables, métodos…
- Diseño
  - Clases estáticas

Ejemplo: Patrón de error PREDICTABLE_RANDOM

Problema

```
String generateSecretToken() {
    Random r = new Random();
    return Long.toHexString(r.nextLong());
}
```

Solución

```
import org.apache.commons.codec.binary.Hex;

String generateSecretToken() {
    SecureRandom secRandom = new SecureRandom();

    byte[] result = new byte[32];
    secRandom.nextBytes(result);
    return Hex.encodeHexString(result);
}
```