Reporte análisis estático de código

**Informe detallado de resultados: WebGoat.Net**

Control de cambios

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha** | **Apartado** | **Resumen de cambios** |
| 1.0 | 02/06/2021 | N/A | Versión inicial |
|  |  |  |  |
|  |  |  |  |

Índice

[1. Introducción 5](#_Toc532203416)

[2. Información de la aplicación 6](#_Toc532203417)

[2.1. Datos generales de la aplicación 6](#_Toc532203418)

[2.2. Datos de calidad 6](#_Toc532203419)

[3. Nivel y modelo de calidad 7](#_Toc532203420)

[3.1. Listado de reglas incumplidas 8](#_Toc532203421)

[4. Tendencias e histórico 9](#_Toc532203422)

[5. Análisis de la aplicación 10](#_Toc532203423)

[5.1. Vulnerabilidades 10](#_Toc532203424)

[5.2. Bugs 10](#_Toc532203425)

[5.3. Code Smells 10](#_Toc532203426)

[5.4. Duplicidad 10](#_Toc532203427)

[6. Siguientes pasos 11](#_Toc532203428)

1. Introducción

Los resultados expuestos en este documento tratan de reflejar el estado de la aplicación WebGoat.Net analizada desde el punto de vista de la calidad de su código fuente.

El modelo de calidad aplicado responde a las necesidades planteadas y trata de minimizar el impacto que supone la implantación de un servicio de análisis estático de código en un equipo de desarrollo. La herramienta en la que se apoya el servicio, SonarQube, establece una clasificación en el tipo de problemas detectados atendiendo a la característica de calidad con la que están relacionados y este informe se referirá a ellos en sus mismos términos. De esta forma, surgen los siguientes tipos de problemas:

* ***Vulnerability***. Problemas relacionados con la seguridad de la aplicación y que pueden suponer un riesgo para la integridad de la misma.
* ***Bug***. Problemas relacionados con la fiabilidad de la aplicación, su capacidad para recuperarse de errores inesperados y mantener el servicio.
* ***Code smell.*** Este tipo de problema se relaciona con la mantenibilidad del código fuente, su capacidad para cambiar de una forma eficiente y efectiva.

Así mismo, SonarQube emplea una terminología propia para ciertos aspectos internos que se explica a continuación:

* ***Quality profile.*** Conjunto de reglas de calidad de código que se aplican a un lenguaje en concreto.
* ***Quality gate.*** Métrica o conjunto de métricas asociadas a ciertos valores límite en los cuales se basa SonarQube para valorar el resultado de un escaneo.

De forma adicional a estos conceptos, durante el informe se hará mención a otros aspectos técnicos de la calidad de código que se explican a continuación:

* ***Problema***. Un problema hace referencia a un componente (proyecto, modulo, archivo, bloque de código, etc.) que no cumple con la especificación de una regla de calidad.
* ***Regla cumplida.*** Hace referencia a reglas de calidad de código que pertenecen al modelo de calidad y que no generan ningún problema en el análisis actual.
* ***Regla incumplida.*** Son reglas de calidad de código pertenecientes al modelo de calidad de código aplicado y que generan al menos un problema.
* ***Duplicidad.*** Métrica de calidad de código que recoge el porcentaje de código duplicado que se ha encontrado al analizar la aplicación.
* ***Bloques duplicados.*** Un bloque duplicado es un conjunto de líneas de código que se encuentran al menos dos veces escritos en la aplicación.

1. Información de la aplicación

Esta sección muestra la información de partida para conocer la aplicación que se está valorando, su tamaño y los lenguajes implicados en la misma.

* 1. Datos generales de la aplicación

|  |  |  |
| --- | --- | --- |
| Nombre del proyecto | [WebGoat.Net](http://localhost:9000/dashboard?id=webgoat_net) | |
| Análisis base | 03-06-2021 08:11 | |
| Líneas de código | 30562 LOC | |
| Lenguajes | CSS | 12.842 LOC (42,02 %) |
| JavaScript | 16.575 LOC (54,23 %) |
| HTML | 1.131 LOC (3,7 %) |
| XML | 14 LOC (0,05 %) |
| Nivel reglas SonarQube | Nivel 1 | |
| Quality gates | No se han establecido | |

* 1. Datos de calidad

A continuación, se muestran las métricas de calidad más relevantes.

|  |  |
| --- | --- |
| Vulnerabilities | 49 |
| Hotspots | 49 |
| Bugs | 38 |
| Code smells | 173 |
| Duplicidad | 15,1 % |
| Bloques duplicados | 4 |

1. Nivel y modelo de calidad

WebGoat.Net se encuentra actualmente en el **Nivel 1 del modelo de calidad** acordado entre los equipos de desarrollo y calidad. Dentro de este nivel, se muestran a continuación la relación de reglas cumplidas e incumplidas (reglas que generan al menos un problema):

Además, se muestra a continuación los problemas encontrados categorizados por tipo y lenguaje.

* 1. Listado de reglas incumplidas

Las reglas incumplidas y el número de problemas que ocasiona cada una, separadas por tipo, son las siguientes:

**Security Hotspots**

|  |  |  |
| --- | --- | --- |
| Lenguaje | Regla | Problemas |
| dos | Make sure that using a regular expression is safe here. | 45 |
| weak-cryptography | Make sure that using this pseudorandom number generator is safe here. | 4 |
| Total |  | 49 |

**Vulnerability**

|  |  |  |
| --- | --- | --- |
| Lenguaje | Regla | Problemas |
| Total |  | 0 |

**Bug**

|  |  |  |
| --- | --- | --- |
| Lenguaje | Regla | Problemas |
| CSS | Properties should not be duplicated | 1 |
| JavaScript | Non-empty statements should change control flow or have at least one side-effect | 7 |
| JavaScript | Strict equality operators should not be used with dissimilar types | 1 |
| JavaScript | Variables should not be self-assigned | 1 |
| HTML | "th" tags should have "id" or "scope" attributes | 20 |
| HTML | "table" tags should have a description | 5 |
| HTML | Image, area and button with image tags should have an "alt" attribute | 2 |
| HTML | "fieldset" tags should contain a "legend" | 1 |
| Total |  | 38 |

**Code Smell**

|  |  |  |
| --- | --- | --- |
| Lenguaje | Regla | Problemas |
| CSS | Selectors should not be duplicated | 1 |
| JavaScript | Variables should not be shadowed | 155 |
| JavaScript | Unused assignments should be removed | 6 |
| JavaScript | Assignments should not be redundant | 2 |
| JavaScript | Nested blocks of code should not be left empty | 2 |
| JavaScript | A "while" loop should be used instead of a "for" loop | 2 |
| JavaScript | Functions should not be defined inside loops | 1 |
| JavaScript | Arguments to built-in functions should match documented types | 1 |
| JavaScript | Extra semicolons should be removed | 1 |
| HTML | Attributes deprecated in HTML5 should not be used | 2 |
| Total |  | 173 |

1. Tendencias e histórico

No aplica debido a que es el primer análisis realizado de WebGoat.Net y no existen datos suficientes para realizar la comparativa. En esta sección se realizará un análisis de la evolución de las métricas más destacadas y una valoración de la calidad a nivel histórico, hitos planteados e hitos conseguidos.

1. Análisis de la aplicación

Después de someter la aplicación WebGoat.Net a un análisis más detallado basado en los resultados obtenidos por SonarQube y teniendo en cuenta que este informe, por ser el primero, tiene como objetivo presentar una primera radiografía de la aplicación y establecer un punto de partida sobre el que comenzar a trabajar en la mejora de la calidad del código fuente, se exponen las siguientes conclusiones.

* 1. Vulnerabilidades
  2. Bugs
  3. Code Smells
  4. Duplicidad

1. Siguientes pasos

Se recomiendan las siguientes tareas:

* Centrar las actividades del equipo de desarrollo en los problemas de tipo vulnerability.
* Analizar y confirmar los falsos positivos sugeridos por el equipo de CALIDAD en cuanto a bugs se refiere.
* Comprobar y confirmar que las contraseñas encontradas por el analizador no suponen un riesgo para la integridad de los sistemas.

Así mismo el Equipo de Calidad propone:

* Mantener a la aplicación WebGoat.Net en el Nivel 1 del modelo de calidad hasta que se realicen nuevos informes detallados y se analice la evolución derivada de los mismos.
* Mantener los análisis planificados y desatendidos en SonarQube de forma semanal. Tanto el Equipo de Calidad como el Equipo de Desarrollo podrán acceder a los datos actualizados por cada análisis a través de [SonarQube](http://srv-analiza/sonar).
* Realizar el siguiente análisis detallado y generación de informes durante el mes de \_ o en el momento en que se libere una nueva versión si es anterior a esa fecha.
* La instalación del complemento SonarLint en los equipos de los desarrolladores de la aplicación WebGoat.Net. De esta manera se puedan realizar análisis del código fuente en fases tempranas del desarrollo por parte de los integrantes del equipo.

Sobre ESIIAB

Para más información acceda a: [Escuela Superior de Ingeniería Informática (uclm.es)](https://www.esiiab.uclm.es/)

|  |  |
| --- | --- |
|  |  |

|  |
| --- |
|  |