Reporte análisis estático de código

**Informe detallado de resultados: JuiceShop**

Control de cambios

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

Índice

[1. Introducción 4](#_Toc77068408)

[2. Información de la aplicación 5](#_Toc77068409)

[2.1. Datos generales de la aplicación 5](#_Toc77068410)

[2.2. Datos de calidad 5](#_Toc77068411)

[3. Nivel y modelo de calidad 6](#_Toc77068412)

[3.1. Listado de reglas incumplidas 7](#_Toc77068413)

[3.1.1. Security Hotspots 7](#_Toc77068414)

[3.1.2. Vulnerability 7](#_Toc77068415)

[4. Tendencias e histórico 10](#_Toc77068416)

[5. Análisis de la aplicación 11](#_Toc77068417)

[5.1. Hot Spots 11](#_Toc77068418)

[5.1.1. Credentials should not be hard-coded 11](#_Toc77068419)

[5.1.2. Denial of Service (DOS) 11](#_Toc77068420)

[5.1.3. Remote Code Injection (RCE) 12](#_Toc77068421)

[5.1.4. Weak-cryptography 12](#_Toc77068422)

[5.1.5. Insecure configuration 14](#_Toc77068423)

[5.2. Duplicidad 15](#_Toc77068424)

[6. Siguientes pasos 16](#_Toc77068425)

1. Introducción

Los resultados expuestos en este documento tratan de reflejar el estado de la aplicación JuiceShop 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 | [JuiceShop](http://localhost:9000/dashboard?id=juiceshop) | |
| Análisis base | 03-06-2021 07:20 | |
| Líneas de código | 42956 LOC | |
| Lenguajes | CSS | 1.698 LOC (3,95 %) |
| JavaScript | 26.008 LOC (60,55 %) |
| TypeScript | 11.991 LOC (27,91 %) |
| HTML | 3.259 LOC (7,59 %) |
| 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 | 47 |
| Hotspots | 47 |
| Bugs | 147 |
| Code smells | 688 |
| Duplicidad | 3,7 % |
| Bloques duplicados | 103 |

1. Nivel y modelo de calidad

JuiceShop 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:

* + 1. Security Hotspots

|  |  |  |
| --- | --- | --- |
| Lenguaje | Regla | Problemas |
| auth | Review this potentially hardcoded credential. | 5 |
| dos | Make sure that using a regular expression is safe here. | 17 |
| rce | Make sure that this dynamic injection or execution of code is safe. | 2 |
| weak-cryptography | Make sure that hashing data is safe here. | 21 |
| insecure-conf | Make sure that enabling CORS is safe here. | 2 |
| Total |  | 47 |

* + 1. Vulnerability

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

**Bug**

|  |  |  |
| --- | --- | --- |
| Lenguaje | Regla | Problemas |
| CSS | Properties should not be duplicated | 3 |
| JavaScript | Properties of variables with "null" or "undefined" values should not be accessed | 4 |
| JavaScript | Callbacks of array methods should have return statements | 3 |
| JavaScript | Strict equality operators should not be used with dissimilar types | 2 |
| JavaScript | Non-empty statements should change control flow or have at least one side-effect | 1 |
| JavaScript | Loops should not be infinite | 1 |
| JavaScript | All branches in a conditional structure should not have exactly the same implementation | 1 |
| JavaScript | All code should be reachable | 1 |
| HTML | "strong" and "em" tags should be used | 118 |
| HTML | Image, area and button with image tags should have an "alt" attribute | 6 |
| HTML | "table" tags should have a description | 3 |
| HTML | Tables should have headers | 3 |
| HTML | "html" element should have a language attribute | 1 |
| Total |  | 147 |

**Code Smell**

|  |  |  |
| --- | --- | --- |
| Lenguaje | Regla | Problemas |
| JavaScript | Variables and functions should not be redeclared | 219 |
| JavaScript | Unused local variables and functions should be removed | 154 |
| JavaScript | Variables should not be shadowed | 101 |
| JavaScript | Extra semicolons should be removed | 88 |
| JavaScript | Unused assignments should be removed | 70 |
| JavaScript | Assignments should not be redundant | 4 |
| JavaScript | A conditionally executed single line should be denoted by indentation | 2 |
| JavaScript | Functions should not be defined inside loops | 1 |
| JavaScript | Multiline blocks should be enclosed in curly braces | 1 |
| JavaScript | Comma operator should not be used | 1 |
| TypeScript | Unnecessary imports should be removed | 19 |
| TypeScript | Wrapper objects should not be used for primitive types | 8 |
| TypeScript | Redundant casts and not-null assertions should be avoided | 7 |
| TypeScript | Unused assignments should be removed | 5 |
| TypeScript | Variables should not be shadowed | 4 |
| TypeScript | Two branches in a conditional structure should not have exactly the same implementation | 2 |
| TypeScript | "undefined" should not be passed as the value of optional parameters | 1 |
| HTML | Sections of code should not be commented out | 1 |
| Total |  | 688 |

1. Tendencias e histórico

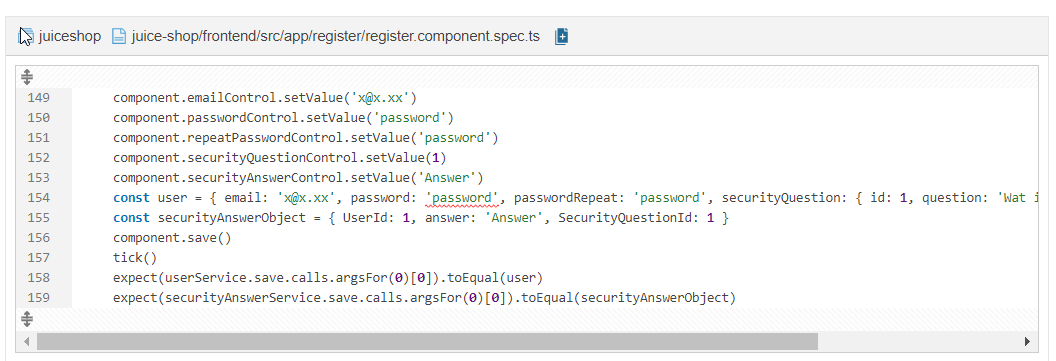
No aplica debido a que es el primer análisis realizado de JuiceShop y no existen datos suficientes para realizar la comparativa. En esta sección se realizará un análisis de la evolución de las métricas más destacadas y una valoración de la calidad a nivel histórico, hitos planteados e hitos conseguidos.

1. Análisis de la aplicación

Después de someter la aplicación JuiceShop 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. Hot Spots
     1. Credentials should not be hard-coded

Debido a que es fácil extraer cadenas del código fuente de una aplicación o binario, las credenciales no deben codificarse en código (hard-coded). Esto es particularmente grave en aplicaciones distribuidas o de código abierto.



En el caso de utilizar usuarios y password de acceso a servicios, dentro del código, estas deben ir cifradas como ***“Secure strings”***, para ello se pueden seguir las siguientes recomendaciones:

* + 1. Denial of Service (DOS)

Se ha detectado una posible fuente que pueden provocar que la aplicación no responda correctamente (DoS):

* Inclusión de expresiones regulares genéricas que hacen uso intensivo de la CPU

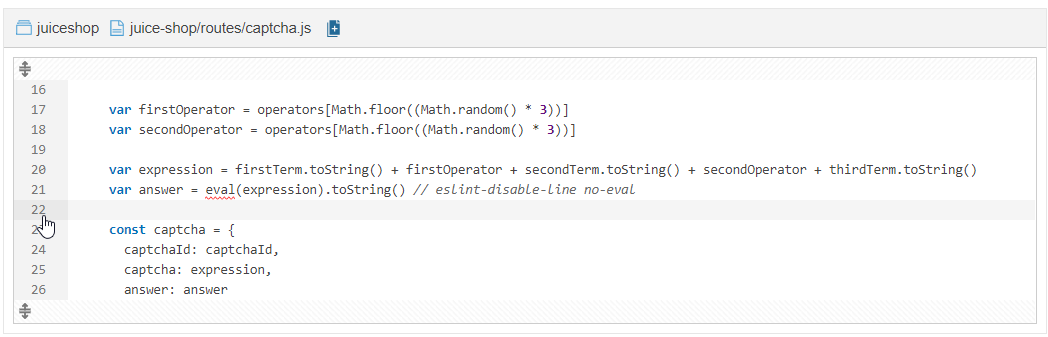
Las expresiones regulares, la evaluación de expresiones regulares es una tarea que consume mucho CPU. Las expresiones regulares especialmente diseñadas como (a+)+s tardarán varios segundos en evaluar la cadena de entrada ‘aaaaaaaaaaaaaaaaaaaaaaaaaaabs’.

El problema es que con cada carácter adicional que se agrega a la entrada, el tiempo requerido para evaluar la expresión regular se duplica. Sin embargo, la expresión regular equivalente, a + s (sin agrupamiento) se evalúa de manera eficiente en milisegundos y se escala linealmente con el tamaño de entrada.

* + 1. Remote Code Injection (RCE)

La falta de verificación de los parámetros de entrada puede provocar la ejecución de comandos de sistema no deseadas.

Sentencias de este estilo deben ser evitadas y cuando se imprescindible su uso deben incluir la verificación de todos los parámetros ante entradas no deseadas:

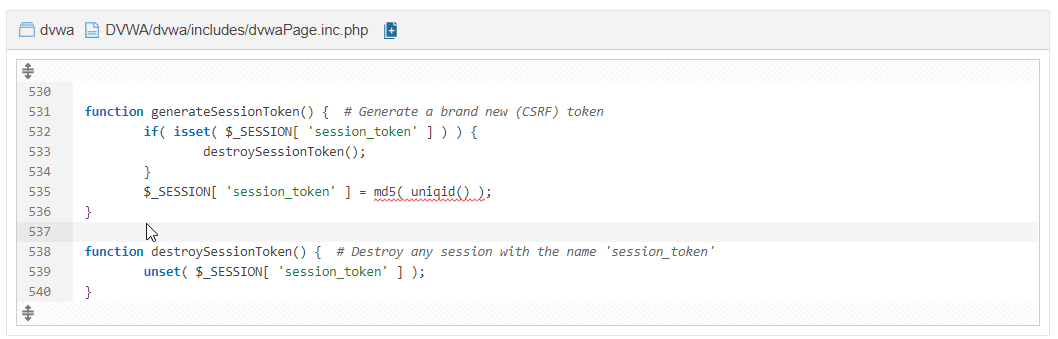


Para más información:

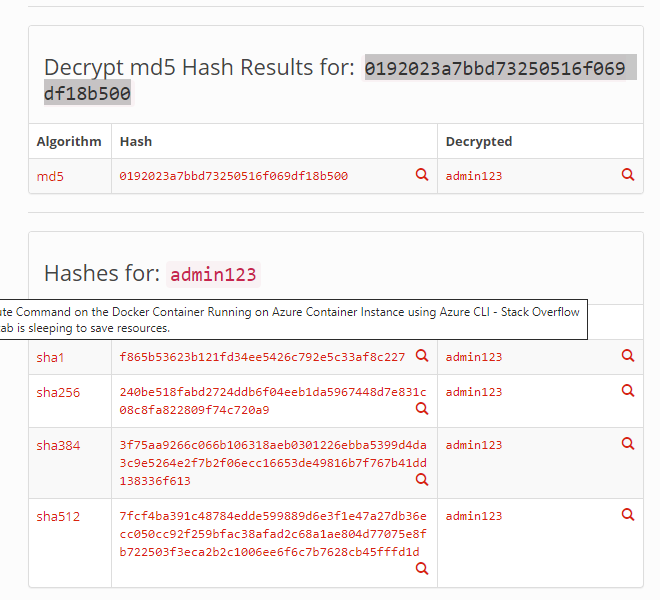
* [OWASP Top 10 2017 Category A1](https://www.owasp.org/index.php/Top_10-2017_A1-Injection) - Injection
* [MITRE, CWE-88](https://cwe.mitre.org/data/definitions/88.html) - Argument Injection or Modification
* [MITRE, CWE-214](https://cwe.mitre.org/data/definitions/214.html) - Information Exposure Through Process Environment
* [SANS Top 25](https://www.sans.org/top25-software-errors/#cat1) - Insecure Interaction Between Components
  + 1. Weak-cryptography

Las funciones de hash criptográficas se utilizan para identificar información de forma única sin almacenar su forma original. Cuando no se hace correctamente, un atacante puede robar la información original adivinándola.

Particularmente la función de hash MD5 lleva ya numerosos años siendo insegura



Un hash generado por MD5 pude ser fácilmente revertido. Por ejemplo, si consiguiéramos el hash de la contraseña del administrador de un sistema como el siguiente hash ‘0192023a7bbd73250516f069df18b500’ puede ser desencriptado fácilmente como muestra la siguiente imagen:



Por tanto, se debe eliminar el uso de librerías de hash inseguras, como es el caso de MD5, en favor de librerías de hash seguras como puede ser el caso de la librería bcrypt

public class BcryptHashingExample

{

    public static void main(String[] args) throws NoSuchAlgorithmException

    {

        String  originalPassword = "password";

        String generatedSecuredPasswordHash = BCrypt.hashpw(originalPassword, BCrypt.gensalt(12));

        System.out.println(generatedSecuredPasswordHash);

        boolean matched = BCrypt.checkpw(originalPassword, generatedSecuredPasswordHash);

        System.out.println(matched);

    }

}

Output:

$2a$12$WXItscQ/FDbLKU4mO58jxu3Tx/mueaS8En3M6QOVZIZLaGdWrS.pK

true

* + 1. Insecure configuration

Una política poco restrictiva Cross-Origin Resource Sharing (CORS) puede permitir la ejecución de scripts de terceros no deseados.



La política de CORS de la siguiente forma:

const http = require('http');

const srv = http.createServer((req, res) => {

res.writeHead(200, { 'Access-Control-Allow-Origin': '\*' }); // Sensitive

res.end('ok');

});

srv.listen(3000);

En el pasado una política CORS poco restrictiva a dado lugar a las siguientes vulnerabilidades:

* [CVE-2018-0269](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0269)
* [CVE-2017-14460](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14460)
  1. Duplicidad

La duplicidad para la parte de código JavaScript/HTML se sitúa en 3,7%, en principio, una cifra nada preocupante de cara al mantenimiento de la aplicación.

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 JuiceShop 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 JuiceShop. 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/)

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

|  |
| --- |
|  |