# Análisis automatizado de vulnerabilidades de código abierto


*Daniel Castellanos*

Pontificia Universidad Javeriana

Arquitectura de Software

Mayo De 2023

# Tabla de contenido

# Introducción

El documento que se está desarrollando no solo proporcionará una definición y una descripción histórica de cada tema, sino también sus aplicaciones en la industria y sus ventajas y desventajas en comparación con otras tecnologías. Además, el documento incluirá casos de estudio que ejemplifiquen cómo se han aplicado estas tecnologías en el mundo real, y también se explorarán las relaciones entre estos temas y cómo se pueden utilizar juntos en una arquitectura de alto nivel. La investigación de estos temas es importante para los ingenieros de sistemas y desarrolladores de software, ya que les permite mantenerse actualizados con las últimas tecnologías y herramientas en su campo y les ayuda a tomar decisiones informadas sobre cómo desarrollar aplicaciones y sistemas.

# Debricked

## Definición

Debricked es una plataforma de seguridad para desarrolladores que ayuda a garantizar la seguridad y la calidad del software en todas las etapas del ciclo de vida del desarrollo de software. Ofrece una amplia gama de herramientas, desde escaneos automatizados de vulnerabilidades hasta análisis de código fuente, lo que permite a los desarrolladores detectar y solucionar problemas de seguridad en sus aplicaciones antes de que lleguen a producción. La plataforma también proporciona informes detallados y recomendaciones para ayudar a los equipos de desarrollo a mejorar continuamente la seguridad de sus productos. En resumen, Debricked ayuda a los equipos de desarrollo a crear software seguro y confiable de manera eficiente y efectiva.

## Ventajas

Estas son algunas ventajas de Debricked:

- **Detección temprana de vulnerabilidades:** Debricked utiliza algoritmos de aprendizaje automático para identificar vulnerabilidades y problemas de seguridad en el código fuente. Al analizar el código en tiempo real, Debricked puede detectar problemas de seguridad temprano en el proceso de desarrollo, lo que ayuda a los desarrolladores a solucionarlos antes de que se conviertan en problemas más grandes.
- **Ahorro de tiempo y recursos:** Al automatizar el análisis de código fuente, Debricked ahorra tiempo y recursos para los desarrolladores. En lugar de revisar manualmente el código para encontrar vulnerabilidades y problemas de seguridad, Debricked realiza el análisis automáticamente y proporciona informes detallados que pueden ayudar a los desarrolladores a solucionar problemas más rápidamente.
- **Mejora de la calidad del código:** Debricked no solo detecta vulnerabilidades y problemas de seguridad, sino que también proporciona sugerencias para mejorar la calidad del código. Al analizar el código fuente en profundidad, Debricked puede identificar áreas donde el código puede mejorarse, lo que puede conducir a un código más limpio y fácil de mantener.

### Desventajas

Estas son algunas desventajas de Debricked:

- **Costo:** Aunque Debricked ofrece una versión gratuita para el análisis de firmware, también tienen planes de pago para empresas que requieren análisis de firmware a gran escala. Dependiendo del plan, el costo de Debricked puede ser significativo y, en algunos casos, puede no ser viable para empresas pequeñas o individuos.
- **Limitaciones en el análisis:** El análisis de vulnerabilidades de firmware es una tarea compleja que requiere experiencia y conocimientos técnicos especializados. Si bien Debricked es una herramienta útil, tiene limitaciones en cuanto a lo que puede identificar. En algunos casos, puede no detectar todas las vulnerabilidades en un firmware y puede ser necesario realizar análisis adicionales por parte de expertos en seguridad.
- **Dependencia de terceros:** Al utilizar una herramienta de análisis de vulnerabilidades de firmware como Debricked, las empresas pueden depender en gran medida de terceros para garantizar la seguridad de sus sistemas. Esto puede ser problemático si hay problemas con la herramienta o si hay retrasos en la identificación y corrección de vulnerabilidades. Además, la dependencia de una sola herramienta para el análisis de firmware puede ser riesgosa, ya que no se puede garantizar que identificará todas las vulnerabilidades.

## Bitbucket

### Definición

Bitbucket es una plataforma de alojamiento de código fuente y gestión de proyectos basada en la nube que permite a los desarrolladores colaborar en equipos y mantener un seguimiento de las versiones del software en un solo lugar. Con Bitbucket, los equipos pueden crear repositorios privados o públicos, realizar revisiones de código, realizar pruebas de integración y despliegue continuo, y automatizar procesos de construcción y lanzamiento de software. Además, Bitbucket ofrece integración con otras herramientas populares de desarrollo, como Jira, Trello, Bamboo, y muchas más. La plataforma también brinda una amplia variedad de opciones de seguridad, control de acceso y autenticación para garantizar la protección del código fuente y la información confidencial del proyecto.

### Ventajas

Estas son algunas ventajas de Bitbucket:

- **Integración con otras herramientas de desarrollo:** Bitbucket tiene integraciones con muchas herramientas populares de desarrollo, como Jira, Bamboo, Trello y Slack. Estas integraciones permiten a los equipos de desarrollo sincronizar sus herramientas y aumentar la eficiencia en el proceso de desarrollo.
- **Control de versiones avanzado:** Bitbucket utiliza Git como su sistema de control de versiones, lo que permite a los desarrolladores trabajar en diferentes ramas del proyecto y fusionar cambios fácilmente. Además, Bitbucket proporciona características avanzadas de

control de versiones, como revisiones de código, etiquetas, ramas y flujos de trabajo personalizados.

- **Colaboración en equipo:** Bitbucket permite a los equipos de desarrollo colaborar en proyectos de forma eficiente. Los desarrolladores pueden trabajar juntos en el mismo código, revisar y comentar el código de los demás y asignar tareas a otros miembros del equipo. Además, Bitbucket proporciona características de seguimiento de problemas y tareas, lo que facilita la colaboración en equipo en torno a un objetivo común.

### Desventajas

Estas son algunas desventajas de Bitbucket:

- **Costo:** Aunque Bitbucket ofrece planes gratuitos para usuarios individuales y pequeñas empresas, también tiene planes de pago para empresas que requieren más características y capacidad de almacenamiento. Dependiendo del tamaño de la empresa y las necesidades de almacenamiento, los costos de Bitbucket pueden ser significativos, lo que puede ser una desventaja para algunas empresas.
- **Personalización limitada:** A diferencia de otras plataformas de alojamiento de repositorios de código fuente, como GitLab, Bitbucket tiene opciones de personalización limitadas. Por ejemplo, los usuarios no pueden personalizar la apariencia del panel de control o agregar funcionalidades adicionales a la plataforma.
- **Limitaciones en la integración de herramientas:** Aunque Bitbucket tiene integraciones con muchas herramientas populares de desarrollo, algunas de las integraciones pueden no ser tan robustas como en otras plataformas. Además, algunas herramientas de desarrollo pueden no ser compatibles con Bitbucket, lo que puede ser una desventaja para los equipos que dependen de herramientas específicas para su trabajo.

## Vulnerabilidades de código abierto

El uso de librerías de código abierto en proyectos de software puede ofrecer muchos beneficios, como la reducción de costos y el aumento de la eficiencia en el desarrollo. Sin embargo, también pueden presentar algunas vulnerabilidades, que incluyen:

- **Vulnerabilidades conocidas:** Las librerías de código abierto se utilizan ampliamente y son muy populares, por lo que los atacantes a menudo buscan vulnerabilidades en ellas. Si una librería tiene una vulnerabilidad conocida, es posible que un atacante pueda explotarla y comprometer la seguridad del software.
- **Dependencia de versiones antiguas:** Muchas veces, los desarrolladores utilizan versiones antiguas de las librerías de código abierto porque son estables y han sido probadas. Sin embargo, esto puede ser problemático si una versión antigua tiene una vulnerabilidad conocida que se ha corregido en versiones posteriores. Si el desarrollador no actualiza la librería, el software puede ser vulnerable a ataques.
- **Dependencia de terceros:** Las librerías de código abierto suelen ser desarrolladas por terceros, lo que significa que los desarrolladores no tienen control directo sobre su calidad

y seguridad. Si una librería tiene una vulnerabilidad que el desarrollador no es consciente, puede ser explotada por los atacantes.

- **Licencias de software:** Al utilizar librerías de código abierto, los desarrolladores deben asegurarse de cumplir con las licencias de software que las rigen. Algunas licencias pueden requerir que los desarrolladores publiquen el código fuente de su software, lo que puede no ser deseable.

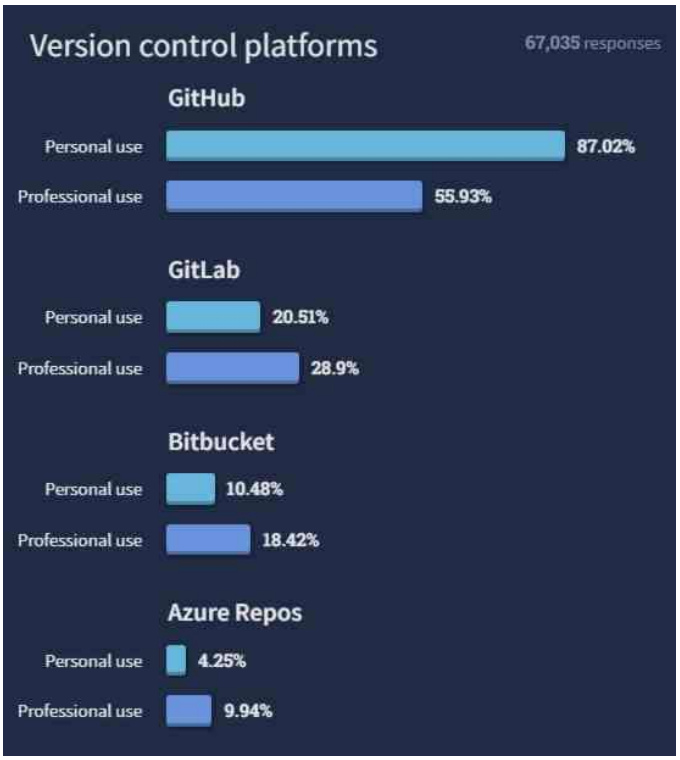
## Estadísticas de uso

A continuación, se presentan las estadísticas de uso de las dos herramientas que utilizamos en esta integración para el análisis de vulnerabilidades de código abierto de forma automatizada.

Figure 1: Magic Quadrant for Application Security Testing


Source: Gartner (April 2022)

Como podemos ver Micro Focus, empresa encragada del manejo de Debricked se encuentra en el cuadrante de lideres para herramientas de testeo de seguridad en aplicaciones, esto nos indica que Debricked como herramienta seguirá innovando y va por buen camino.




Como todos sabemos GitHub es la herramienta mas usada para el control y el manejo de versiones, pero algo sorprendente es que Bitbucket se encuentra en el tercer puesto y que es mas usada para uso profesional que para uso personal, esto nos da una idea de que se usa gracias a sus fáciles integraciones con otras herramientas del mercado.

## Aprendizajes

A lo largo de esta investigación y presentación aprendí sobre las diferentes vulnerabilidades a las que se esta expuesto al usar librerías de código abierto, y como prevenir que estas vulnerabilidades afecten el producto en el que estoy trabajando mediante la configuración de un pipeline al cual se le pueden establecer diferentes reglas para lanzar advertencias o hasta evitar que se realice un commit que presente vulnerabilidades de alto riesgo.

## Referencias

[1] Shifts & Stability In Developer Landscape, Written by Janet Swift [En línea]. Available: https://www.i-programmer.info/news/99-professional/15589-shifts-a-stability-in-developer-landscape.html

[2] 2022 Gartner® Magic Quadrant™ for Application Security Testing [En línea]. Available: https://www.synopsys.com/software-integrity/resources/analyst-reports/gartner-magic-quadrant-appsec.html

[3] Explore the Knowledge Base [En línea]. Available: https://portal.debricked.com/knowledge-base

[4] How to use Bitbucket [En línea], Available: https://bitbucket.org/product/guides