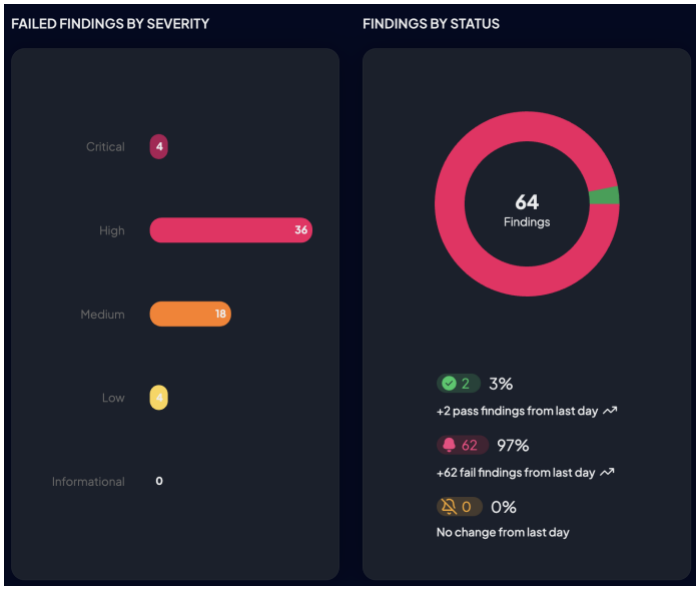
Resolución de Errores Críticos y Altos

En este documento se describe cómo con PROWLER realizamos un escaneo a GitHub para detectar fallos en los repositorios y eventualmente resolverlos según su severidad. Los principales problemas identificados están relacionados con la falta de protección en ramas por defecto (main) y la posibilidad de eliminación de ramas por defecto. En la siguiente imagen podemos visualizar los primeros hallazgos después de realizar el escaneo y a continuación se presentan las recomendaciones para minimizar estos riesgos, enfocándonos en los de severidad **crítica** y **alta**.



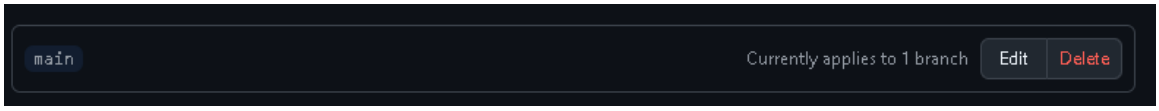
Errores Críticos

Descripción: Falta de protección en la rama por defecto (main).

Riesgo: Permite modificaciones o eliminaciones no controladas en la rama principal del repositorio, lo cual puede comprometer la integridad del código y por ende del proyecto.

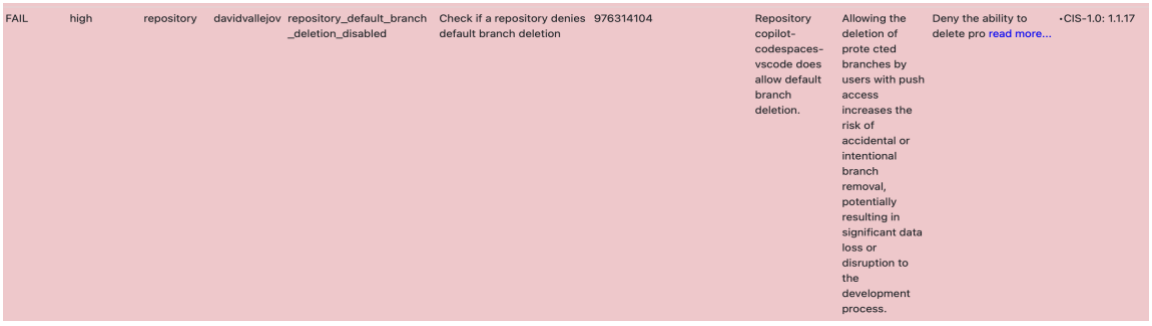
Solución:

- Habilitar la protección de la rama main desde la configuración del repositorio en GitHub.
- Aplicar reglas como: requerir revisiones de pull requests, impedir pushes directos y habilitar validaciones automáticas.
- Configurar notificaciones para cambios en ramas protegidas.



Errores Altos

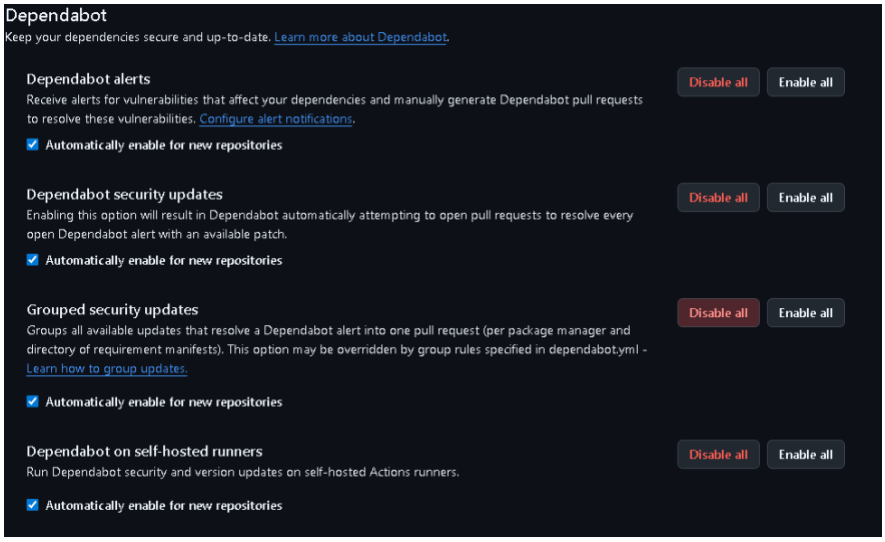
Descripción: Posibilidad de eliminación de la rama por defecto.



Riesgo: Proteger la rama principal es como ponerle una bóveda de seguridad al código más importante del proyecto. Evita que alguien (o incluso uno mismo por accidente) pueda borrarla o hacer cambios sin una revisión adecuada. La eliminación de la rama puede causar pérdida de historial de cambios, afectando así, el flujo de trabajo del equipo.

Solución:

- Deshabilitar la opción de eliminar la rama por defecto desde la configuración del repositorio.
- **Require a pull request before merging**: Obliga a que todos los cambios pasen por una *pull request*. Nadie podrá subir cambios directamente.
- **Require approvals**: Exige que al menos una persona del equipo apruebe los cambios de la *pull request* antes de que se integren. Puedes configurar el número de aprobaciones necesarias.
- **Require status checks to pass before merging**: Si usas pruebas automáticas (integración continua), esta opción impide que se integre código que no pase las pruebas.
- Establecer políticas de revisión para modificaciones en configuraciones críticas.
- Capacitar al equipo sobre la importancia de mantener protegida la rama principal.



Conclusión

La implementación de estas medidas garantiza mayor seguridad en el control de versiones, protege la rama principal contra cambios no autorizados y reduce el riesgo de pérdida de información. Es recomendable revisar periódicamente las configuraciones de seguridad de los repositorios. A pesar de implementar todos estos cambios, al realizar nuevamente un escaneo, obtuve el mismo resultado; Aunque la creación de una regla de protección de rama es el paso fundamental para prevenir la eliminación de la rama principal, la persistencia de una alerta de seguridad indica que la configuración actual podría no estar siendo aplicada como se espera o que la herramienta de escaneo aún no ha registrado el cambio. Es crucial verificar que la regla se aplique **correctamente a la rama por defecto**, que no existan reglas conflictivas y que se incluya a los administradores en esta restricción para asegurar un cierre completo de la vulnerabilidad.