Subject: Security Assessment Findings for BrokenWebAPI – Actions Recommended

---

Dear Development Team Leads,

I hope this message finds you well.

Following the recent security assessment of the **BrokenWebAPI** project, we have completed a thorough analysis using a variety of static (SAST), dynamic (DAST), software composition (SCA), and container security scanning tools. Several high and medium severity issues were observed that require your attention.

Key findings include:

- High-risk code vulnerabilities such as **SQL Injection** and **hardcoded secrets**.
- Use of an **outdated .NET 6.0 runtime**, which reached **End of Life (EOL)** in November 2024, exposing the application to unpatched risks.
- Dependency vulnerabilities and missing essential **security headers** (e.g., Content-Security-Policy, Referrer-Policy).
- Dynamic application flaws including **CORS misconfigurations** and lack of enforced **HTTPS**.

A detailed **Security Assessment Report** has been prepared, outlining all findings, severity ratings, and prioritized recommendations for remediation. I kindly urge the development teams to review the report and take necessary actions promptly, particularly in the areas of:

- Eliminating injection risks,
- Securing sensitive information,
- Upgrading the framework to **.NET 8.0 LTS**, and
- Hardening the application’s security headers and transport layer protections.

If needed, I am available to assist in clarifying any findings, supporting remediation efforts, or integrating additional security controls into your development pipelines.

Thank you for your immediate attention to this important matter.

Best regards,