Documentation: How CodeQL Works in AutoAudit

Overview

CodeQL is GitHub's semantic code analysis engine used to identify vulnerabilities and maintain code quality. Within the AutoAudit project, CodeQL is integrated into the CI/CD pipeline to automatically scan code whenever new commits or pull requests are made.

Workflow Execution

- The repository is structured as a **monorepo** with separate folders for each team (`/engine`, `/frontend`, `/backend-api`, `/security`).
- Each folder has its own YAML workflow file under `.github/workflows`.
- When a commit is pushed:
  - **All workflows trigger initially.**
  - The **path filter** in each workflow checks if files in its corresponding folder were modified.
  - If no relevant changes are found, that workflow exits quickly.
  - Only the workflow linked to the modified folder continues, and that is where CodeQL begins analysis.

This ensures that only relevant parts of the repository are scanned, saving time and resources.

Why CodeQL Analysis Was Added

By default, the workflows were not performing detailed security checks. To address this, a new **`codeql-analysis.yml`** workflow file was added.

- **Purpose:**
  - Integrates CodeQL into the project's CI/CD pipeline.
  - Automates security scans on every commit or pull request.
  - Flags issues directly in **Security → Code scanning alerts** on GitHub.
- **Why it was necessary:**
  - Without this file, only linting and build checks were running.
  - Vulnerabilities introduced during testing were not being flagged.
  - Adding `codeql-analysis.yml` enabled CodeQL's security queries (e.g., SQL injection, ReDoS, XSS) to run automatically.

Scheduling and Manual Runs

- The workflow supports **scheduled scans** (e.g., weekly using CRON jobs).
- Developers can also trigger scans **manually** via the GitHub Actions tab.

Benefits

- Early detection of vulnerabilities before they reach staging or production.
- Clear visibility under GitHub's **Security → Code scanning alerts** tab.
- Seamless integration into the existing CI/CD process with minimal manual setup.