Code Scanning (CodeQL) — One-Page Cheat-Sheet

GitHub Actions + CodeQL quick setup, tips, and ready-to-use YAML

What it is. Code scanning (CodeQL) runs static analysis in CI to detect security issues and code quality problems. It builds or analyzes your code, creates a relational DB, and executes query packs. Supports common languages: C/C++, C#, Go, Java, JavaScript/TypeScript, Python, Ruby.

When to use. Every PR and protected branch; schedule a weekly sweep. Triage alerts in PRs; fix or dismiss with a reason.

Licensing. Public repos: free. Private/internal: requires GHAS.

Drop-in workflow: `.github/workflows/codeql.yml`

```yaml
name: CodeQL

on:
  push:
    branches: [ "main" ]
  pull_request:
    branches: [ "main" ]
  schedule:
    - cron: "0 8 * * 1"    # weekly, Mon 08:00 UTC
  workflow_dispatch: {}

permissions:
  contents: read
  security-events: write
  actions: read

concurrency:
  group: codeql-${{ github.ref }}
  cancel-in-progress: true

jobs:
  analyze:
    name: Analyze (${{ matrix.language }})
    runs-on: ubuntu-latest
    strategy:
      fail-fast: false
      matrix:
        language: [ "cpp", "csharp", "go", "java", "javascript", "python", "ruby" ]

    steps:
      - uses: actions/checkout@v4

      - name: Initialize CodeQL
        uses: github/codeql-action/init@v3
        with:
          languages: ${{ matrix.language }}
          # If not using a config file, you can select a suite here:
          # queries: security-extended

      # For compiled languages, try autobuild first.
      - name: Autobuild
        if: contains('cpp csharp go java', matrix.language)
        uses: github/codeql-action/autobuild@v3

      - name: Perform CodeQL Analysis
        uses: github/codeql-action/analyze@v3
        with:
          category: "/language:${{ matrix.language }}"
```

Optional advanced config: `.github/codeql/codeql-config.yml`

```
name: "CodeQL Advanced Config"

# Choose broader suites for depth:
# - security-extended
# - security-and-quality
queries:
  - uses: security-extended

packs:
  - github/codeql/cpp-queries@latest
  - github/codeql/javascript-queries@latest
  - github/codeql/python-queries@latest

paths:
  - src/
  - services/

paths-ignore:
  - "**/test/**"
  - "docs/**"
  - "**/*.md"
```

10-step setup checklist

1. Confirm GHAS for private/internal or use public repos.

2. Add the workflow file above; commit on a feature branch and open a PR.

3. (Optional) Add the advanced config and set your query suite.

4. Scope triggers to protected branches; keep PR checks required.

5. Ensure runners have resources; consider larger or self-hosted runners for heavy builds.

6. Keep the `autobuild` step for compiled languages, or insert a custom build.

7. Triage PR alerts: fix to auto-close, or dismiss with a reason.

8. Pin actions to maintained major versions (e.g., `@v3`); use Dependabot to update.

9. Control cost with schedules, manual dispatch, and `concurrency`.

10. Monitor results in *Security* → *Code scanning alerts*.

Tips & gotchas

- **Compilation matters.** If your build needs env vars, services, or build tools, add those steps before `init/analyze`.

- **Language matrix.** Remove unused languages to speed up and lower cost.

- **Stable output.** Use consistent `paths` and `paths-ignore` to avoid noisy diffs.

- **Custom queries.** Host your own packs or add `queries:` entries for targeted checks.

- **Minted compile.** Compile with `-shell-escape` and have Python Pygments installed.