

# CodeQL Triage Playbook

## Practical SOP for GitHub Advanced Security

Version v1.0 • January 19, 2026

Build note: This document uses the `minted` package for syntax highlighting. Compile with `pdflatex -shell-escape` (or `xelatex -shell-escape`).

## Contents

<b>1 How to Use This SOP</b>	<b>1</b>
<b>2 Where to Look First</b>	<b>1</b>
2.1 GitHub Security UI . . . . .	1
2.2 Actions Run vs. Query Failure . . . . .	1
2.3 SARIF In/Out . . . . .	2
<b>3 Minimum Triage Flow (10 Minutes)</b>	<b>2</b>
<b>4 Dismissal Reasons (Use Sparingly)</b>	<b>2</b>
<b>5 Known CodeQL Limitations</b>	<b>2</b>
<b>6 Speed and Cost Tips</b>	<b>2</b>
<b>7 Handy Commands and Snippets</b>	<b>3</b>
7.1 <code>gh</code> CLI: List and Inspect Alerts . . . . .	3
7.2 CodeQL CLI: Local Repro and SARIF . . . . .	3
7.3 GitHub Actions: Add Caching Around CodeQL . . . . .	3
<b>8 Done-Done Checklist for Each Alert</b>	<b>3</b>

---

## 1 How to Use This SOP

This playbook distills a lightweight, repeatable triage process for CodeQL findings in GitHub. It is optimized for speed, auditability, and clear decisions. Use it as a runbook during daily triage or while debugging failed code scanning runs.

## 2 Where to Look First

### 2.1 GitHub Security UI

- Navigate to **Repository → Security → Code scanning alerts**.
- Open an alert, review the **rule documentation**, and click **Show paths** to trace the source-to-sink flow.

### 2.2 Actions Run vs. Query Failure

When a scan fails, open the failed **Actions** run and expand the job steps.

- If the failure is in workflow or YAML (checkout, setup, permissions), fix the pipeline first.
- If the failure originates from the CodeQL action or a specific query pack, inspect annotations and logs to isolate the step.

### 2.3 SARIF In/Out

- You can **upload** third-party SARIF to *Code scanning alerts*.
- You can **export** CodeQL SARIF for downstream processing and dashboards.

## 3 Minimum Triage Flow (10 Minutes)

1. **Confirm failure location:** workflow/YAML vs. CodeQL analysis.
2. **Open alert** and use **Show paths** to identify root cause (source, propagators, sink).
3. **Read the rule doc:** impact, examples, and suggested fixes (often links to the query).
4. **Decide:** fix now, file an issue, or dismiss with justification.
5. **Log evidence:** link to path trace, commit, PR, and any compensating controls.

## 4 Dismissal Reasons (Use Sparingly)

If you dismiss, always provide a clear justification and schedule a review.

- **False positive / Not exploitable** in our context (explain why the path is unreachable).
- **Mitigated by design** (e.g., centralized sanitization or enforcement); add references.
- **Test or sample code** (excluded from build/runtime).
- **Legacy with compensating control** (ticket opened, control ID listed, timeline set).

## 5 Known CodeQL Limitations

- **Language coverage varies;** some languages and frameworks have richer modeling than others.
- **AST/DB modeling is not a full compiler:** framework indirection or meta-programming can obscure flows.
- **Signal vs. noise:** narrower queries reduce false positives but may increase scan time; broader queries raise noise.

## 6 Speed and Cost Tips

- **Scope the code:** analyze only relevant directories using workflow `paths`/`paths-ignore`.
- **Cache:** use `actions/cache` for databases and dependencies.
- **Parallelize:** consider matrix builds or larger runners when this meaningfully cuts wall-clock.
- **Prefer built-in suites/packs;** keep custom queries targeted.

## 7 Handy Commands and Snippets

### 7.1 gh CLI: List and Inspect Alerts

---

```
1 # Set a default repo (once per shell)
2 gh repo set-default ORG/REPO
3
4 # List CodeQL alerts (IDs, rule, state)
5 gh api repos/:owner/:repo/code-scanning/alerts \
6   --jq '.[] | "(.number) \(.rule.id) \(.state)"'
7
8 # Get one alert's JSON (replace 123)
9 gh api repos/:owner/:repo/code-scanning/alerts/123
10
11 # Tip: From the Actions UI you can download a run's log archive when debugging.
```

---

### 7.2 CodeQL CLI: Local Repro and SARIF

---

```
1 # Create a CodeQL database (example: Python)
2 codeql database create db-python --language=python --source-root .
3
4 # Analyze with a suite; emit SARIF
5 codeql database analyze db-python \
6   codeql/python-queries:codeql-suites/python-code-scanning.qls \
7   --format=sarifv2 --output=codeql-results.sarif
8
9 # Upgrade the database as code changes
10 codeql database upgrade db-python
```

---

### 7.3 GitHub Actions: Add Caching Around CodeQL

---

```
1 # Excerpt from a CodeQL job
2 - name: Cache CodeQL database
3   uses: actions/cache@v4
4   with:
5     path: |
6       ~/.codeql
7       ./codeql-db
8   key: ${{ runner.os }}-codeql-${{ hashFiles('**/requirements*.txt',
9     '**/package-lock.json', '**/poetry.lock') }}
10
11 # Typical CodeQL init/analyze
12 - uses: github/codeql-action/init@v3
13   with:
14     languages: python, javascript
15 - uses: github/codeql-action/analyze@v3
```

---

## 8 Done-Done Checklist for Each Alert

- Root cause identified via **Show paths**; exploitability assessed.
- Decision recorded (fix/issue/dismiss) with clear justification.

- Evidence captured: rule doc link, query reference if applicable, and commit/PR.
- If dismissed: ticket to re-review later and compensating control noted.
- Any runtime learnings (cache/scope/matrix tweaks) captured in the workflow PR.

## Acknowledgments

This SOP is meant to be adapted to your repository conventions and governance. Keep the document close to the code: propose improvements via pull requests as you learn from real alerts.