GHAS + Dependabot — Quick Cheatsheet

v1.0

Shift-left dependency security • Fast triage • Ready-to-copy snippets

What Dependabot Does

- Scans manifests/lockfiles to flag **outdated/vulnerable dependencies**.
- Auto-opens **PRs with version bumps**, release notes, and CVE context.
- Supports grouping updates and schedules to reduce noise.

Where It Fits in the SDLC

- **Desk/CLI → PR checks → Protected branches → Scheduled scans after deploy**.
- Catch newly disclosed CVEs and open remediation PRs even after release.

Fast Triage Flow (Alerts)

1. **Open alert** → review severity, affected package/version, suggested fix.
2. **Assess blast radius** → repo usage, transitive deps, deployment paths.
3. **Choose remediation**: merge PR, pin/override, or temporarily ignore (with rationale + expiry).
4. **Verify** → CI passes, regression tests, security checks; monitor post-merge.

Suggested SLAs (example)

Severity	Target	Notes
Critical	24–48h	Hotfix, monitor after merge
High	3–5d	Expedite into next release
Medium	Next release	Bundle where possible
Low	Backlog	Review quarterly

If You Ignore Alerts

- ✗ Wider attack surface ✗ Compliance drift ✗ Target for mass exploits.
- Tame noise via **bundling**, **PR limits**, and **ownership rotation**.

Developer Responsibilities

- Read the alert; **learn the vulnerable pattern** and coordinate with security.
- Prefer **patched versions**; avoid pinning to known-vulnerable releases.
- Keep PRs small and monitored; link to tickets if deferred.

Access & Visibility

- Security dashboard is visible to readers; use **RBAC** for least-privilege.
- Protect branches with **required PR checks** and **GHAS status checks**.

SECURITY.md (Starter)

```
# Security Policy

## Supported Versions
We patch the latest minor of the current
     major for active services.

## Reporting a Vulnerability
Email security@yourorg.example or open a
     private security advisory in GitHub.


## Handling
Triage within 1 business day; fix
    targets by severity:
- Critical: 24--48h
- High: 3--5 days
- Medium/Low: next scheduled release

## Dependencies
We use GitHub Dependabot for alerts and
    PRs.
```

.github/dependabot.yml (Copy-Ready)

```yaml
version: 2
updates:
  - package-ecosystem: "pip"
    directory: "/"
    schedule: { interval: "daily" }
    allow: [ { dependency-type: "direct"
         } ]
    ignore:
      - dependency-name: "Django"
        versions: ["<4.2"] # tighten to
            your policy
    open-pull-requests-limit: 5

  - package-ecosystem: "npm"
    directory: "/"
    schedule: { interval: "weekly" }

  - package-ecosystem: "maven"
    directory: "/"
    schedule: { interval: "weekly" }
```

Handy @dependabot PR Commands

- @dependabot rebase recreate merge
- close squash and merge rebase and merge
- check re-run checks

This cheatsheet is a starting point; adapt schedules, SLAs, and policies to your org's risk appetite.