

Homework

Make your patch workflow AI-driven: build a prioritizer, produce a SBOM, and write a CI vulnerability gate.

Task 1 — Prioritizer Prompt

Objective: Create a prompt that takes any vuln scan output and returns the top 10 patches ranked by (exploitability x asset value).

Instructions:

- Must consider KEV list and public PoC presence
- Must output the patch command or upgrade path
- Test on the lab's vuln-scan-results.txt

Deliverable: The prompt and a sample output.

Task 2 — Personal SBOM

Objective: Generate an SBOM for a small project of your own.

Instructions:

- Use CycloneDX or SPDX tooling (or write the JSON by hand)
- Enrich with known CVEs for the top 5 deps
- Decide which to upgrade

Deliverable: An `sbom.json` and a 100-word decision note.

Task 3 — CI Gate

Objective: Write a short CI script that fails the build if any dependency has a CVSS ≥ 8 CVE.

Instructions:

- Uses `pip-audit` / `npm audit` / `osv-scanner`
- Greps for high severity
- Exits non-zero

Deliverable: A `security-gate.sh` you could drop into a CI pipeline.