

Part 1 — Lab Answers

Reference solutions for the lab exercises. Use these only after attempting the exercises yourself.

Exercise 1 — Git History Secret Hunt

Expected findings: at least one AWS access key, one private key header, one `.env` committed and then "removed" (still in history). Rotation order: cloud keys first (minutes), SaaS tokens second (hours), then purge history with `git filter-repo`.

Exercise 2 — Leaked Repo Triage

Typical architectural leaks: internal DNS names, S3 bucket names, queue URLs. Even without secrets, these give an attacker a map. Customer notification decision: YES if PII-related config or customer keys; NO if only internal infra — still rotate and monitor.

Exercise 3 — Crypto Code Review

Common bugs: MD5 for passwords, ECB mode for AES, `random.random()` for tokens, hard-coded key, string compare for MACs. Rewrite uses `argon2` for passwords, `AES-GCM` for encryption, `secrets.token_bytes` for nonces, `hmac.compare_digest` for comparisons.

Exercise 4 — TLS Config Audit

```
ssl_protocols TLSv1.2 TLSv1.3;  
ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECI  
ssl_prefer_server_ciphers off;
```

```
add_header Strict-Transport-Security "max-age=63072000; includeSubDomains  
ssl_stapling on; ssl_stapling_verify on;
```

Final Exercise — Secret-handling Policy

One page: vault path scheme, rotation cadence, pre-commit hooks, incident playbook, approved primitives, TLS baseline.

Part 2 — Homework Answers

Model answers for the homework tasks. Your solution may differ and still be correct.

Task 1 — Secret Scanner Prompt

JSON output with: type, match, confidence, rotation_command. Include regex for AWS AKIA, GitHub `ghp_`, JWT `eyJ`.

Task 2 — Rotate Your Own Token

Rotation log should cover: revoke old, generate new, update storage, verify, scrub bash history. Never include the actual token.

Task 3 — Crypto Replacement

Diff should show MD5 → SHA-256 or bcrypt; verify backwards-compat via a migration path (double-hash or "upgrade on next login").