The 10x Developer's Security Checklist

Security isn't an afterthought; it's a habit. Use this checklist before every commit and deployment to keep your secrets safe.

Phase 1: Local Environment

Gitignore Check

Verify .env added to .gitignore

Prevents sensitive environment variables from being accidentally committed

Global Ignore

Configure global .gitignore for system files

System-specific files like .DS_Store shouldn't be tracked in any project

No Hardcoding

Scan for "sk_live", "api_key", "password"

Hardcoded secrets in code are easily exposed through reviews or breaches

Local Variables

Use .env.local for personal overrides

Allows personal API keys without affecting shared configuration

</> Phase 2: Git & Version Control

☐ **Pre-commit Hooks**

trufflehog • git-secrets • Block secrets from commits

Automatically scan code for secrets before each commit, preventing accidental exposure

☐ **History Scan**

Old repos • History audit • Past commits

Old repositories may contain secrets committed years ago that still pose security risks

☐ **Repo Visibility**

Public vs. Private • Repository settings • Access control

Public repositories are accessible to anyone, while private ones restrict access

🚀 Phase 3: Deployment & Docker

☐ **Docker Cleanliness**

COPY . . • Secrets in images • .dockerignore

Using COPY . . in Dockerfiles can inadvertently include sensitive files like .env

☐ **Runtime Injection**

AWS Secrets Manager • Environment variables • Build vs Runtime

Injecting secrets at runtime prevents them from being stored in container images

☐ **Container User**

Non-root • USER directive • Principle of least privilege

Running containers as root increases security risks; non-root users limit potential damage

🛡️ Phase 4: Maintenance

☐ **Rotation Schedule**

90 days • Calendar reminder • API keys

Regular key rotation limits the damage potential of compromised keys

☐ **Least Privilege**

Database users • Permissions audit • Minimal access

Granting only necessary permissions reduces the impact of potential breaches

---

Made with Love for the Web Dev Community. Stay Secure.

Made by bou~codes from 10xdev.blog: Your source for bite-sized podcasts, roadmaps for 2025+, and posts on programming, career growth, productivity, deveneurship, indie hacking, technical writing, and personal branding for devs.

✳️ Free Certifications Hub   >_ AI CLI Tools Hub   📖 Our Story By Pythonista Naima