**Phase 0 Summary – Setup & Automation**

1. **Created complete project structure** with organized folders for:
   * GitHub workflows and templates (.github/)
   * Docker environment (docker/)
   * Scripts (scripts/)
   * Output and logs (artifacts/)
2. **Configured a Docker-based penetration testing lab** including:
   * **Kali Linux** (for tools like nmap, sqlmap)
   * **DVWA / Juice Shop** (vulnerable web apps)
   * **MinIO**, **Neo4j**, and **Milvus** (for data storage and analysis)
3. **Set up automation and security controls:**
   * Added **allowlist mechanism** (allowlist.json) and **run script** (run\_allowed.sh) to control which tools can run.
   * Configured **CI workflow (ci.yml)** for automated testing and build checks.
   * Created **branch protection and PR templates** for teamwork discipline.
4. **Connected LLM integration layer (stub):**
   * Added llm\_client.py (for future AI integration).
   * Created .env.example (for API keys, not committed to Git).
5. **Saved and organized scan results:**
   * sqlmap\_output.txt and related data stored in artifacts/ and MinIO for record-keeping.