Orange Sage – Project Scope

Project Title: Orange Sage — AI-Powered Cybersecurity Assessment Platform

1. Objective

Orange Sage is an autonomous AI agent platform that mimics ethical hackers: it dynamically executes testing code, discovers vulnerabilities, and validates them through controlled exploitation. The system is built to reduce manual pentesting overhead and false positives from static tools, providing accurate, actionable findings to developers and security teams.

2. Project Overview

Orange Sage combines a FastAPI backend, autonomous agent framework, and React frontend to manage and run security assessments. Agents perform reconnaissance, scanning, exploitation attempts (where authorised), and post-exploitation analysis. Results are stored in a relational database (SQLite for local testing, configurable to PostgreSQL in production) and artifacts are stored in MinIO (S3-compatible) when deployed.

3. In-Scope

- Autonomous vulnerability discovery and validation via AI agents

- Web-based dashboard for creating projects, targets, and managing scans

- Real-time scan logs and agent orchestration

- Report generation (PDF / DOCX / HTML) and findings management

- Local and Dockerized deployment using docker-compose

4. Out of Scope

- Offering manual pentesting services to clients

- Mobile application (planned for future roadmap)

- On-prem hardware appliance delivery

5. Deliverables

- Fully functional web application (frontend + backend)

- Autonomous agent framework (pentesting_agent.py and orchestration)

- Documentation: Scope, SRS, SDS

- Test reports and sample vulnerability findings

6. Constraints

- Requires API keys for LLMs (OpenAI/Gemini) for advanced agent reasoning

- Local development uses SQLite; production recommended to use PostgreSQL

- Docker and Docker-Compose required for full local stack

7. Assumptions

- Users will only scan systems they own or have explicit permission to test

- Network connectivity available for LLM integration and dependency fetching

8. Stakeholders

- Developers and Security Engineers

- Project Supervisors and Academic Examiners (if used as a final-year submission)

- DevOps and IT administrators