1. Master Orchestrator Agent

- The top-level LangGraph workflow
- Manages state flow and phase transitions

2. Validation & Initialization Agents

- Request Validator - Verifies project permissions and scan prerequisites
- State Initializer - Creates scan records
- GitHub Auth - Handles authentication for GitHub projects

3. Setup & Acquisition Agents

- Volume Creator - Sets up Docker volumes for code and outputs
- GitHub Cloner / Local Copier - Acquires codebase based on project type
- Codebase Stats - Analyzes project metadata and characteristics
- Memory Loader - Retrieves context from long-term storage
- Size Checker - Evaluates if human-in-the-loop approval is needed

4. Analysis Agents

- Analysis Planner - Determines which scanners to run
- AST Scanner - Parses code into AST
- Regex Scanner - Applies pattern matching for vulnerabilities
- Dependency Scanner - Checks dependencies against CVE databases
- Config Scanner - Examines configuration files
- Signal Aggregator - Collects and maps findings to OWASP categories
- Reflector - Performs self-critique and identifies coverage gaps
- Targeted Rescan - Fills identified gaps
- OWASP Mapper - Finalizes category assignments

5. Correlation & Decision Agents

- Base Scorer - Calculates initial OWASP category scores
- Correlation Applier - Adjusts scores based on vulnerability relationships
- Spawn Decider - Determines which OWASP subagents to create
- Tech Stack Filter - Applies architecture-based filtering
- Execution Planner - Determines optimal execution order

6. OWASP Category Subagents

Specialized subgraph agents for each OWASP category (e.g., Cryptographic Failure, Injection, Authentication Failure, etc.).

Each contains:

- Subgraph Init - Sets subagent status
- Tool Selector - Chooses appropriate security tools
- Tool Prioritizer - Orders tools by expected value
- Docker Executor - Manages container lifecycle for tools
- Execution Recorder - Tracks tool execution metrics
- Result Aggregator - Collects tool outputs
- Conditional Evaluator - Reassesses whether to create more agents

7. Smart Dedup Agents

- Artifact Collector - Catalogs all tool outputs
- Format Detector - Identifies output formats (SARIF, JSON, XML, etc.)
- Known Format Parsers - Handle standard formats
- LLM Extractor - Fallback parser for unknown formats
- Schema Mapper - Transforms to unified schema
- OWASP Tagger - Confirms/adjusts category assignments
- Signature Dedup - Handles exact/near-exact matches
- Semantic Dedup - Uses embeddings for similar descriptions
- Context Dedup - Identifies shared root causes
- Merge Executor - Finalizes duplicate clusters
- Severity Adjuster - Makes final severity assessments

9. Reporting & Cleanup Agents

- Result Persister - Writes to database
- Volume Cleanup - Removes temporary resources
- Final results - Sends completion events

10. Error Handling Agent

- Global Error Handler - Manages failures and cleanup

11. Human-in-the-Loop (HITL) Agent

- Manages user interactions at decision points with timeouts and defaults