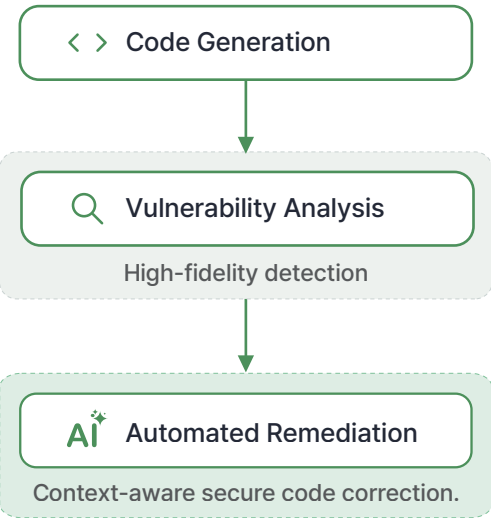


From Intelligent Prioritization to Frictionless Remediation

Sparrow Enterprise AI Package represents a paradigm shift in Application Security Testing (AST), transitioning from mere vulnerability identification to automated, AI-driven remediation. Comprising the AI Prioritization and the AI Remediation Guide, this enterprise-grade package seamlessly integrates the discovery and patching phases.

By drastically minimizing security noise and providing prescriptive, actionable guidelines on exactly what to fix first and how to execute the fix, we empower developers—regardless of their deep cybersecurity expertise—to remediate critical vulnerabilities instantaneously. This ensures frictionless DevSecOps pipeline execution, safeguarding software integrity without compromising release velocity or time-to-market.



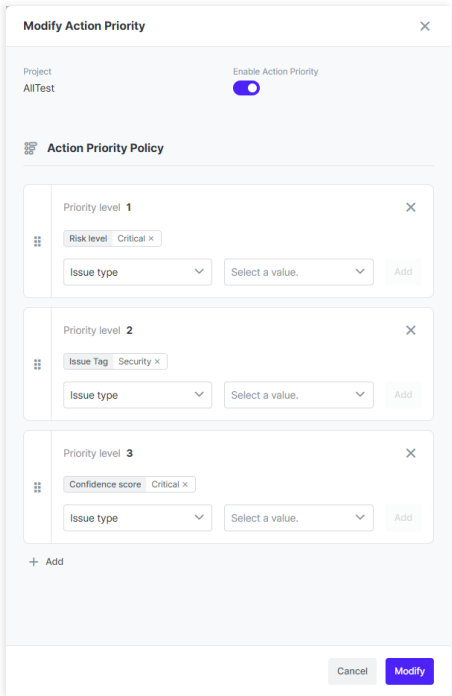
Deterministic Analysis Meets Generative Remediation

Leverages highly precise, rule-based data flow engines for accurate vulnerability detection. We apply deterministic rules for strict validation and Generative AI for intelligent code synthesis, creating a secure and agile development ecosystem.

Deterministic Reproducibility	Guarantees identical, consistent results across source code iterations, providing a reliable CI/CD baseline.
Auditability & Compliance Mapping	Provides comprehensive audit trails and policy mapping to CWE, OWASP, and CERT for compliance.
Governance & Policy Enforcement	Delivers clear detection of open-source license violations and security policy breaches for proactive risk management.

Key Feature ① AI Remediation Prioritization

AI automatically prioritizes detected issues by analyzing vulnerability risk together with asset criticality and contextual impact.



Why It Matters

- Finding overload slows remediation.
- Single-factor prioritization misses actual risk.
- Priorities depend on policy, asset criticality, and risk appetite.

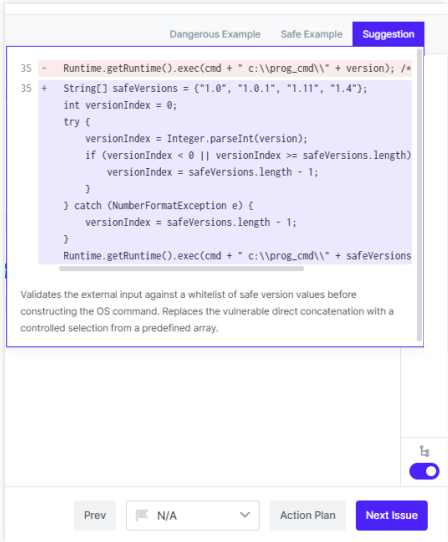
Key Capabilities

- ✔ Smart Asset Classification
Automatically classifies asset types using embedding models and classifiers.
- ✔ Up to 10 Custom Priority Levels
Align prioritization with organizational security policies and risk criteria.
- ✔ Five-Level Severity Display
Clearly highlights what to address first, from Critical to Low.
- ✔ Context-Aware Prioritization
Uses risk, confidence, language, file, asset type, keywords, and other available context.

Key Feature ②

Key Feature 2 — AI Remediation Guide

AI recommends remediation approaches and example code to reduce the security remediation workload for developers.



Why It Matters

- Maintaining remediation guidance for every security rule manually does not scale.
- Developers without deep security expertise may struggle to remediate findings directly.
- Custom security rules often lack standardized remediation guidance.

Key Capabilities

- ✓ **General-Purpose Remediation Model**
Provides tailored remediation suggestions across source-code findings.
- ✓ **Context Optimization**
Performs method-level semantic analysis to preserve context and explores related variables, classes, and functions.
- ✓ **Syntax Validation & Correction**
Validates merged code, detects syntax errors, and supports regeneration and correction.

Business Value

Improve Developer Productivity	Shorten the time from vulnerability discovery to remediation, reducing unnecessary work while strengthening application security.
Streamline Developer – Security Collaboration	Help developers understand and resolve findings with less security expertise, reducing review and communication overhead.
Scale with Organizational Security Policies	Adapt to organizational security policies, asset criticality, coding practices, and custom rules without extensive manual guidance management.

Product & Licensing

Package	Sparrow Enterprise AI Package	Deployment	On-Premise (Integration with a Private LLM)
Core Features	AI Remediation Prioritization + AI Remediation Guide	License	Separate Add-on License

Security For AI & Security By AI

Sparrow Enterprise AI Package combines AI-based remediation prioritization and AI remediation guidance to connect security findings with practical developer action.