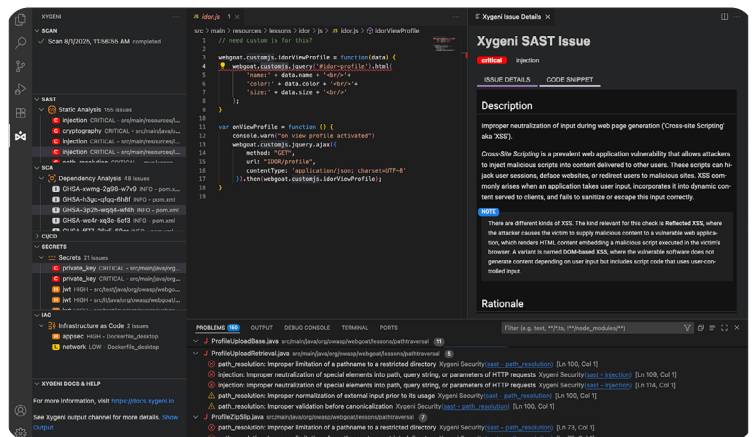


Xygeni SAST with AI Secure Code, Delivered Fast

Xygeni AI SAST identifies vulnerabilities as soon as they appear, filters them through a smart prioritization engine, and applies **AI-powered remediation** to fix what truly matters. Stay ahead of threats without slowing down development.



About Xygeni

Xygeni is an **All-in-One Application Security Platform** built to protect every stage of the software development lifecycle. We offer complete control over application risks, a unified security view from code to cloud, and eliminate noise to prioritize risks effectively. Our advanced malware detection and early warning system makes Xygeni a leader in protecting applications from emerging threats, ensuring rapid and secure software delivery.

Modern applications are under constant pressure from tight release cycles to growing security debt. According to Security Today, **60% of applications contain vulnerabilities in first-party code**, increasing the risk of breaches, compliance failures, and production outages.

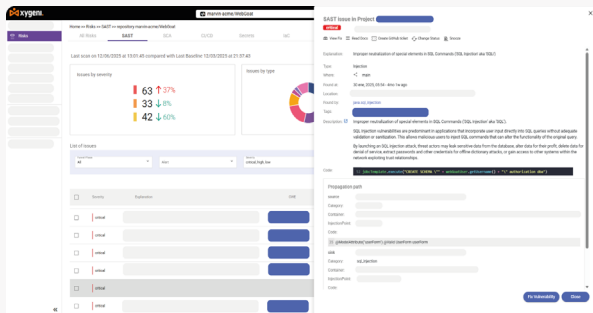
Xygeni AI SAST empowers your team to **stop threats before they start**. Our solution performs **deep static analysis** to uncover injection flaws, memory mismanagement, XSS, and even malicious code like backdoors or ransomware. But detection is just the beginning.

With Xygeni, findings are filtered through a **smart exploitability prioritization funnel** so teams focus on what's exploitable, not just what exists. Finally, AI AutoFix accelerates resolution by generating context-aware code fixes developers can trust.

60%
of Codebases
Contain Known
Vulnerabilities
in First-Party
Code

Detect Vulnerabilities from the First Line of Code

Xygeni's Static Application Security Testing (SAST) empowers organizations to identify vulnerabilities early and prevent malicious code infiltration. Our advanced scanning capabilities provide a comprehensive view of your code's security posture, enabling faster remediation and secure software delivery without compromising development speed.



Uncover Vulnerabilities Across Your Application Code

Xygeni SAST uses deep static analysis to find and fix critical vulnerabilities, ensuring your code meets the highest reliability and compliance standards.

Key Vulnerability Detection Features:

- **Injection Flaws:** SQL injection, code injections, and command injections.
- **Cross-Site Scripting (XSS):** Prevent attackers from injecting malicious scripts into your applications.
- **Misconfigurations and Information Leakage:** Identify improper configurations and prevent unintentional exposure of sensitive data.
- **Buffer Overflows:** Detect memory management issues that can compromise application integrity.
- **Insufficient Authentication or Authorization Mechanisms:** Ensure robust user authentication and secure access control.

IDE Integration

Scan code directly from your IDE to catch vulnerabilities as you write them. With Xygeni's IDE integration, you can view issue details, check severity and metadata, and get remediation guidance instantly.

Unmatched Detection Accuracy

100% True Positive Rates - OWASP Benchmark Proven

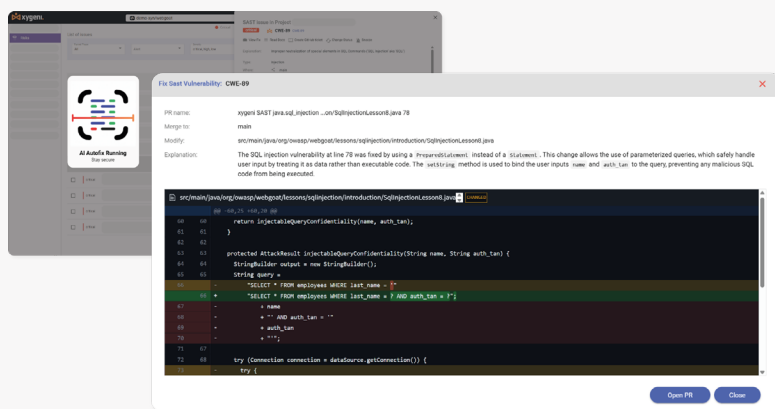
Xygeni-SAST scores among the lowest in false positives on the OWASP Benchmark, catching critical flaws like SQL Injection and XSS with zero misses and minimal noise.

AI Auto-Fix and Advanced Threat Detection

Xygeni goes beyond traditional SAST by not only identifying vulnerabilities but also helping teams fix them automatically and detect malicious code threats early in the SDLC.

With AI AutoFix, developers get secure, context-aware fixes delivered directly to their pull requests eliminating the need for manual patching. Combined with deep malware detection capabilities, Xygeni helps you secure both your code and your supply chain.

Remediate Vulnerabilities Instantly with **AI AutoFix**

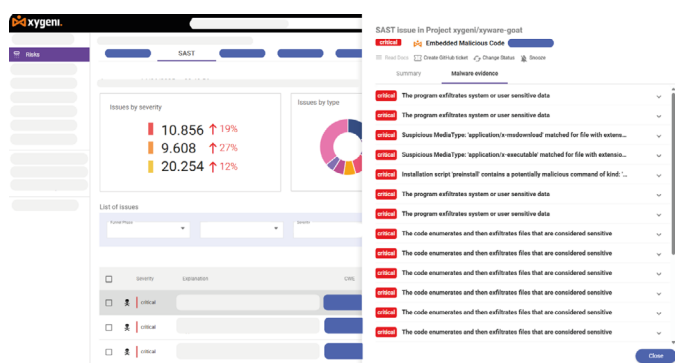


- **Instantly remediates issues** like XSS and SQL Injection with developer-ready fixes ansomware and Spyware.
- **Replaces risky patterns** with secure alternatives using context from the codebase.
- **Generates pull requests** with safe code suggestions aligned with language best practices.

Detect Malicious Code Attacks

While traditional SAST tools focus primarily on vulnerabilities, Xygeni goes a step further by detecting malicious code behaviors that could indicate a software supply chain attack.

Malware Detection Capabilities:



- **Backdoors, Trojans, and Worms:** Detect code designed to open unauthorized access points.
- **Ransomware and Spyware:** Identify potential threats that could encrypt sensitive data or exfiltrate confidential information.
- **Obfuscated Code Execution:** Uncover attempts to hide malicious behaviors through advanced obfuscation techniques.
- **System Registry Tampering:** Flag unauthorized modifications that could compromise system security.

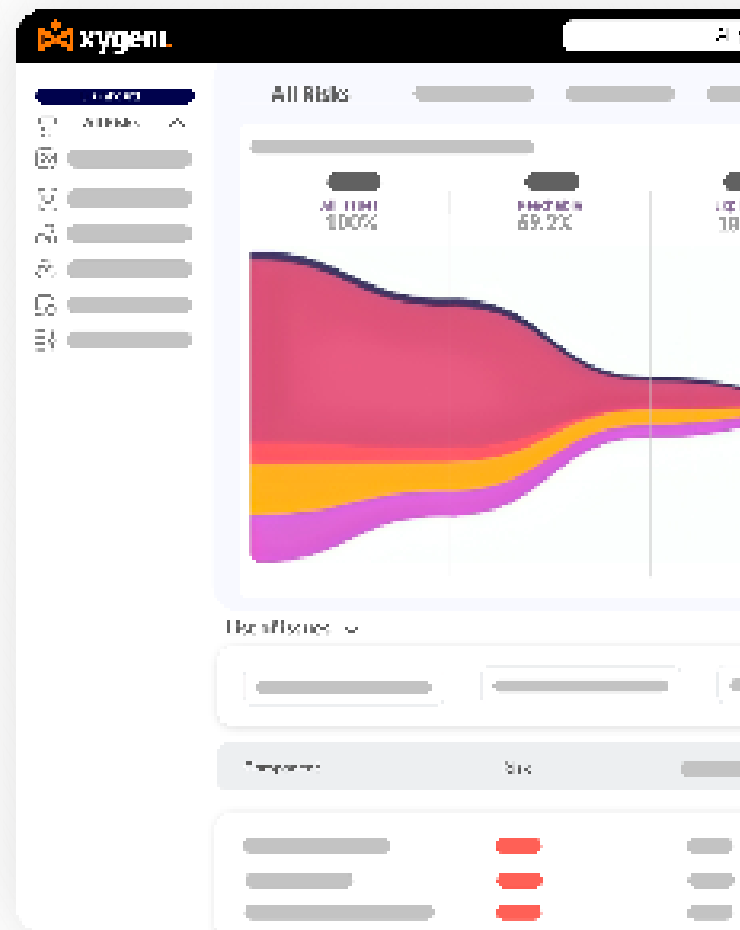


Secure Your Code with Xygeni-SAST

Detect vulnerabilities, block malicious code, and protect your applications—all in one powerful solution.

- No credit card needed
- Quick setup, instant results

[Start your free trial](#)



Get in touch today!

www.xygeni.io

[in https://www.linkedin.com/company/xygeni](https://www.linkedin.com/company/xygeni)

[X https://twitter.com/xygeni](https://twitter.com/xygeni)