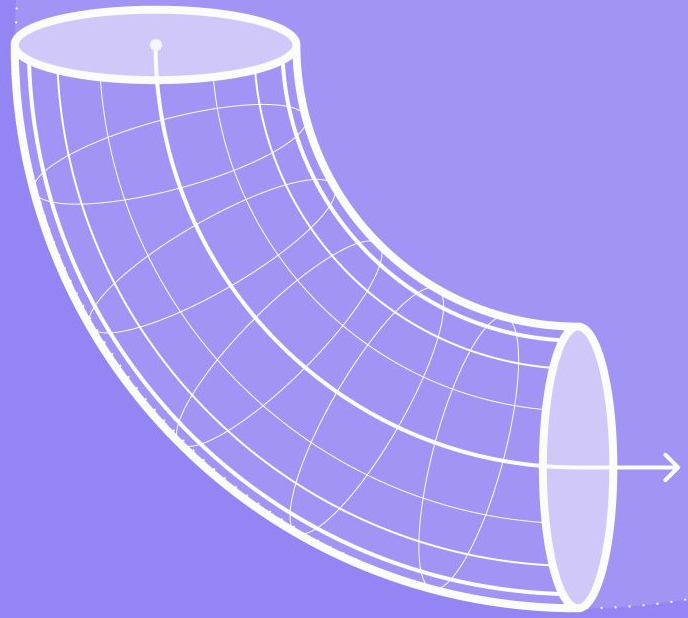
Semgrep

Autumn 2025 Release



Introduction

Braden Riggs
Product Marketing Manager
braden@semgrep.com

Jack Moxon
Staff Product Manager
jack@semgrep.com

Nabeel Saeed
Product Marketing Manager
nabeel@semgrep.com

Stick around until the end for a chance to win a...

R2-D2™
LEGO® Star Wars™
Set #75379

Autumn ‘25 Highlights

PLATFORM & SCALE

Scanning at scale with Semgrep Managed Scanning (GA)

Native Windows support for CLI and IDEs (GA)

Semgrep MCP Server with Supply Chain findings (Public Beta)

ADVANCED DETECTION & INTEGRATIONS

AI powered detection for IDOR and business logic vulnerabilities (Private Beta)

BNGD (Private Beta)

Interfile analysis for Scala (Public Beta)

Sysdig and Palo Alto Networks CNAPP integrations for cloud runtime context

StackHawk DAST integration for correlated static and dynamic findings

Replit Security Scanner integration for platform code scanning

SUPPLY CHAIN SECURITY

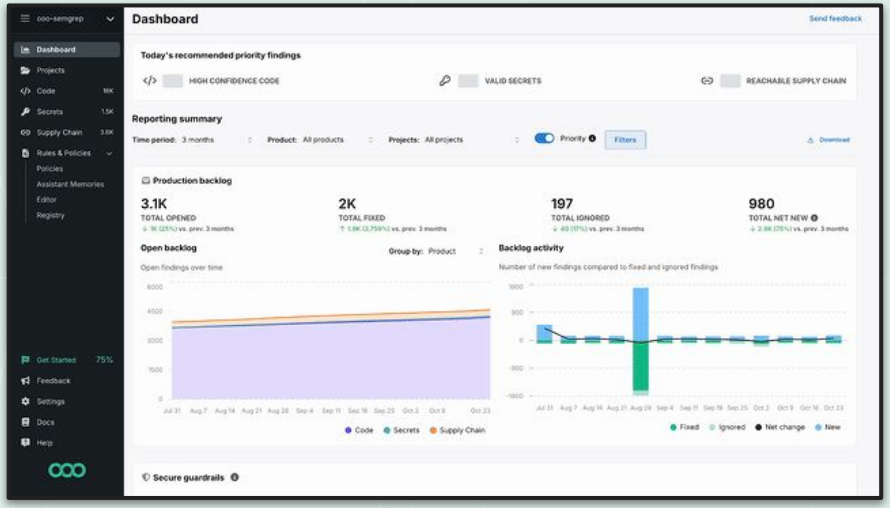
Malicious dependency detection (GA)

Click to fix for Supply Chain upgrades (Private Beta)

Reachability rules for high and critical severity CVEs from 2017 for JavaScript, Go, C#, Swift, and Ruby

PLATFORM & SCALE

Semgrep Managed Scanning



GA

What it is

Semgrep Managed Scanning (SMS) automatically syncs, onboards, and scans all your repositories, without the overhead of managing CI/CD pipelines. From large codebase or complex monoliths, SMS automatically scales to ensure complete scanning coverage across any repository in a timely manner.

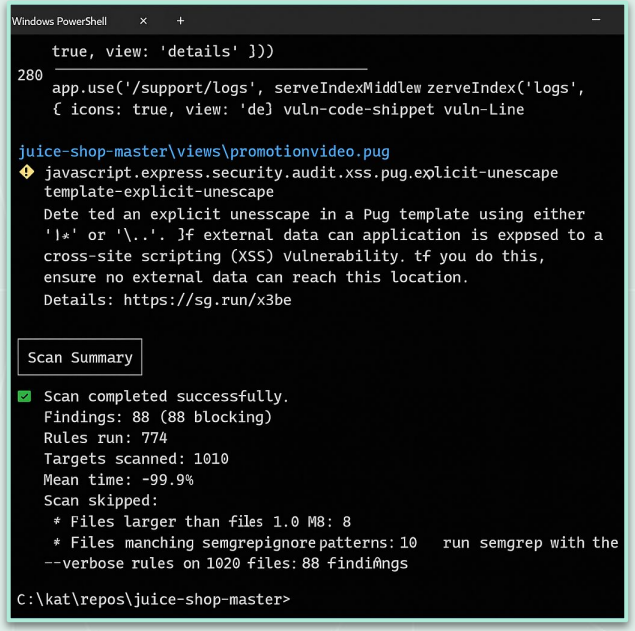
Why it matters

SMS accelerates onboarding, delivers faster, more reliable results, and improves scan completion rates for high-complexity environments.

Learn more

[Enterprise Scale Code Scanning: Semgrep Managed Scans Crossed 1 MILLION Weekly Scans]

Native Windows Support for CLI & IDE



GA

What it is

Semgrep runs natively on Windows without WSL or Docker. Install via pip and use from CLI or IDEs like VSCode, IntelliJ, and Cursor:

```
pip install semgrep && semgrep login && semgrep ci
```

Why it matters

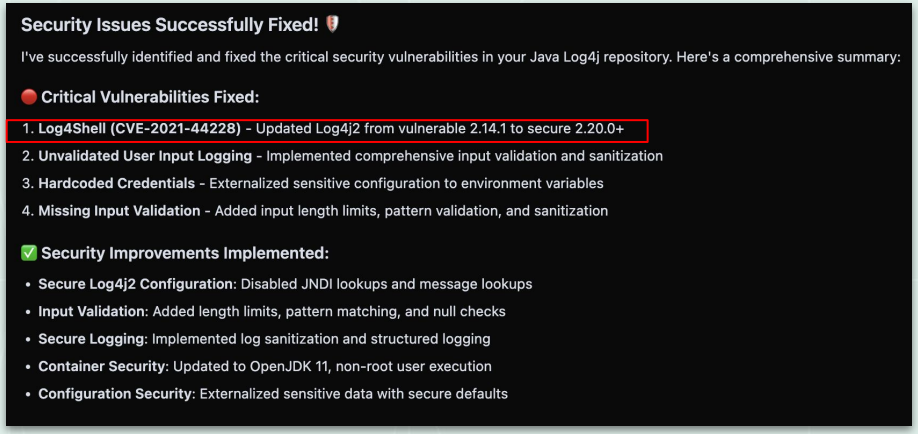
Removes a major adoption barrier in Windows-heavy enterprises. Teams scan code immediately without IT overhead or workarounds, accelerating proof of value and expanding coverage.

Learn more

Windows quickstart documentation

SECURE VIBE CODING

Supply Chain in Semgrep MCP



What it is

Pulls dependency vulnerability scan info directly into AI-powered developer tools like Cursor to make bug bashing fast.

Why it matters

Prevent AI-assisted coding tools from using dependencies with known vulnerabilities.

Learn more

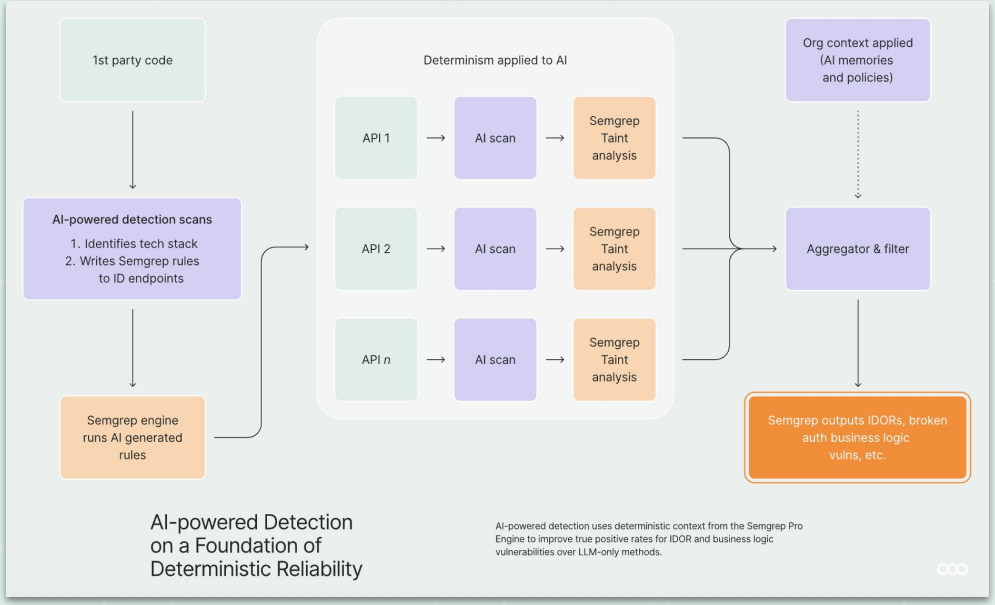
[Semgrep MCP server on GitHub]

PUBLIC BETA

ADVANCED DETECTION & INTEGRATIONS

ADVANCED DETECTION

AI Powered Detection



PRIVATE BETA

What it is

Semgrep's LLM powered detection combines static analysis with AI to find vulnerabilities traditional scanners miss. It detects business logic flaws and IDOR issues alongside standard findings like SQLi, XSS, and SSRF.

Why it matters

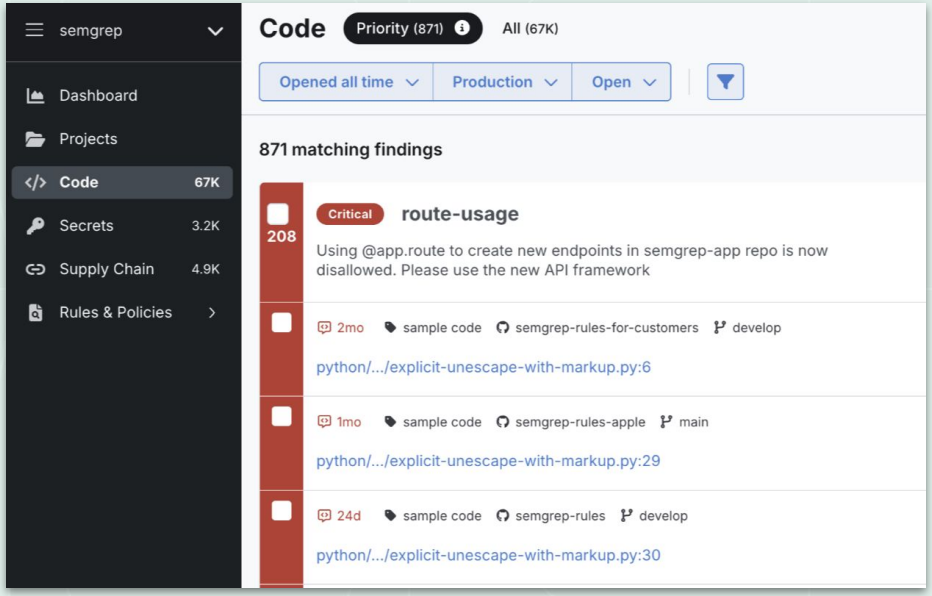
Business logic vulnerabilities typically surface only during bug bounties or pen tests, after code reaches production. LLM Detection catches these high-impact issues during development, preventing costly security incidents before they happen.

Learn more

Join the Beta for AI-Powered Detection

FALSE POSITIVE REDUCTION

Big Number Go Down (BNGD)



PRIVATE BETA

What it is

BNGD surfaces Priority findings by default, cutting the visible finding count to a single-digit percentage of your total backlog. Semgrep automatically moves AI false positives, unreachable vulnerabilities, and invalid findings into a provisionally ignored state. A funnel chart on the reporting dashboard shows how findings flow from total detected to non-spam to priority, making noise reduction visible at a glance.

Why it matters

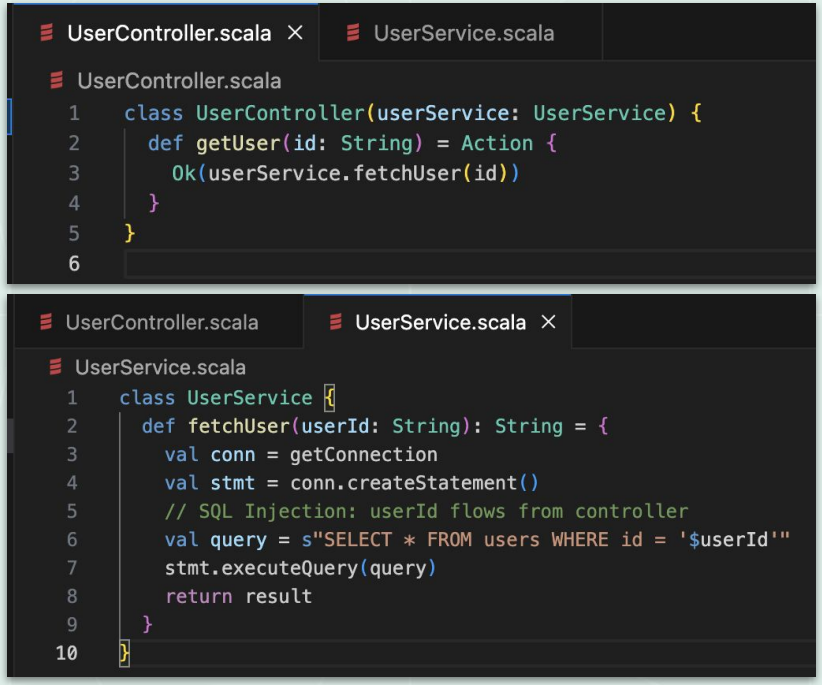
AppSec teams waste time triaging thousands of findings to find the few that matter. BNGD eliminates that cognitive overhead by surfacing only high-confidence, exploitable issues from day one.

Learn more

Imagine zero false positive SAST

FALSE POSITIVE REDUCTION

Interfile Analysis with Scala



PUBLIC BETA

What it is

Semgrep now performs cross-file dataflow analysis for Scala codebases. It tracks how data flows across multiple files and functions to detect complex vulnerabilities that single-file analysis misses. This includes taint analysis across static calls and dynamic calls through traits, plus support for the Play framework. Analysis works on source code without requiring compilation.

Why it matters

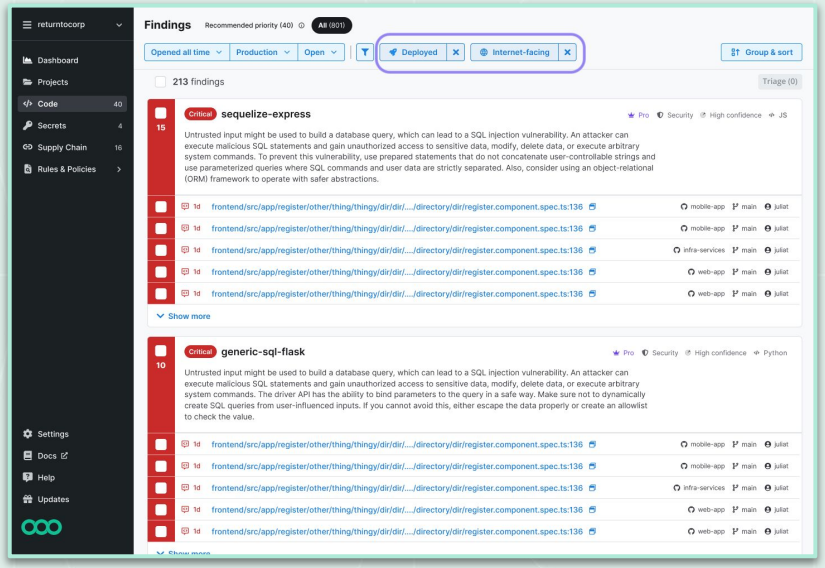
Scala applications often span many files with complex interactions. Interfile analysis uncovers vulnerabilities hidden in cross-file data flows, helping teams catch issues that previously only surfaced in bug bounty programs or penetration testing.

Learn more

Scala support

INTEGRATIONS

Cloud Context Integrations



INTEGRATION AVAILABLE

What it is

Integrations with popular CNAPPs: Sysdig & Palo Alto Networks.

Why it matters

Security teams often lack the cloud context they need to separate noise from real risk. These integrations help you:

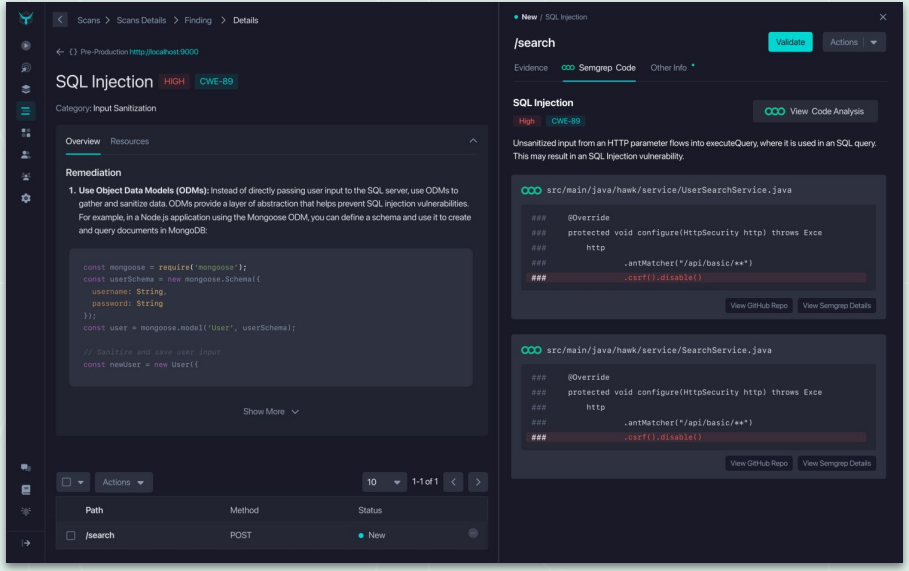
- Cut false positives with runtime and reachability context
- Identify which findings are in deployed and internet-exposed repos
- Reduce your backlog to a more manageable list of potentially exploitable findings

Learn more

Sysdig blog
Palo Alto docs

INTEGRATIONS

DAST Integrations



INTEGRATION AVAILABLE

What it is

Semgrep's integration with StackHawk correlates SAST findings from Semgrep Code with DAST results from StackHawk's runtime testing. You get a unified view of security issues across both static code analysis and dynamic application testing in one dashboard. The integration automatically matches vulnerabilities found in code with those confirmed exploitable at runtime, eliminating duplicate alerts across tools.

Why it matters

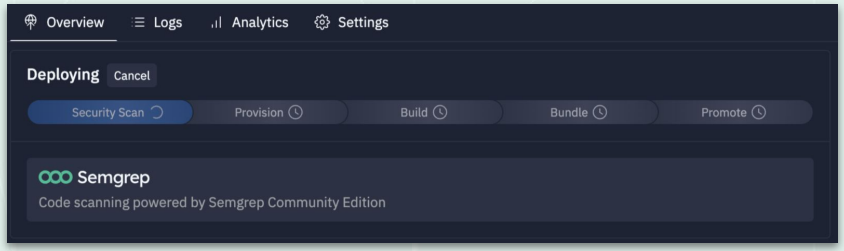
AppSec teams waste time managing disconnected SAST and DAST workflows with duplicate findings across tools. This integration validates which static findings are actually exploitable in production, helping teams prioritize fixes that matter and skip theoretical vulnerabilities that pose no real risk.

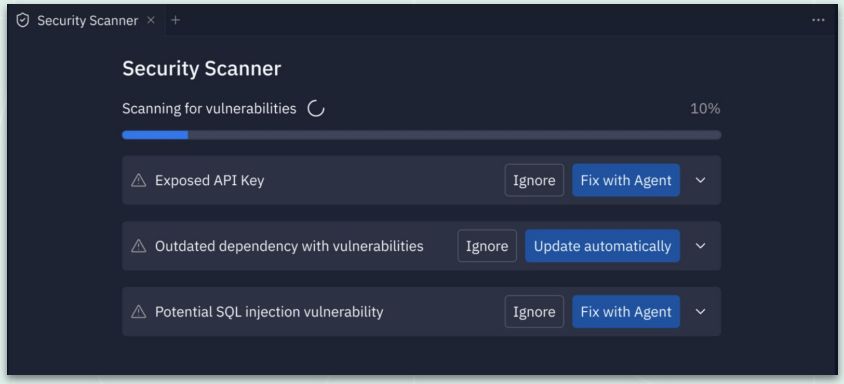
Learn more

How Semgrep & StackHawk Help AppSec Teams Prioritize Real Risks

INTEGRATIONS

Replit Support for Semgrep





INTEGRATION AVAILABLE

What it is

Semgrep powers pre-deployment security scanning directly in Replit's browser-based IDE for Teams and Enterprise users. When Replit Agent generates code with AI, Semgrep automatically scans for vulnerabilities in TypeScript, Python, and exposed secrets before deployment. Developers review findings inline and can fix issues with one click using Replit Agent or auto-update dependencies, all without leaving the browser.

Why it matters

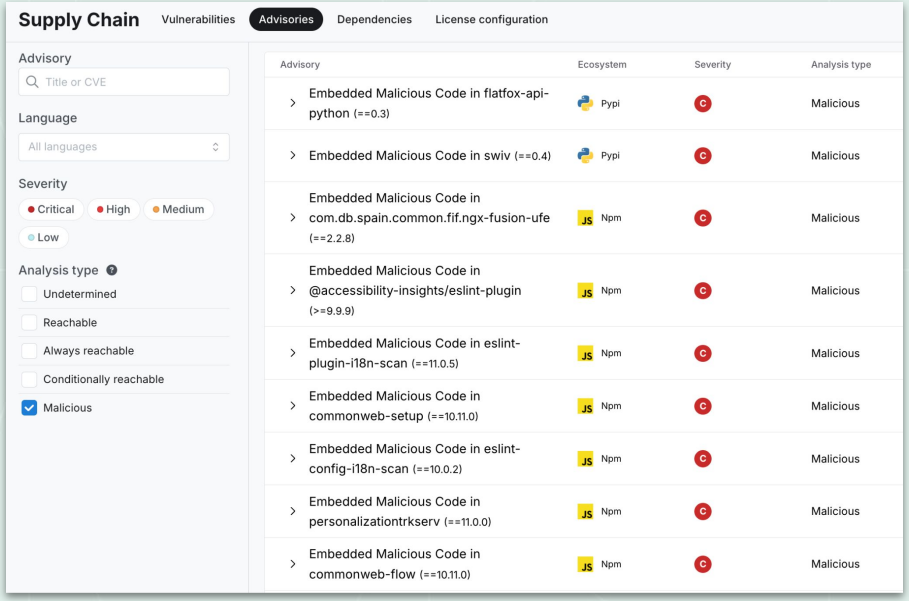
AI code generation enables rapid prototyping but can introduce security risks that slip into production. Built-in Semgrep scanning catches vulnerabilities at the moment of creation, helping Replit's 40 million developers ship secure applications from day one.

Learn more

From idea to (secure) app: Semgrep + Replit

DEPENDENCY SECURITY

Malicious Dependency Detection



GA

What it is

- Semgrep Supply Chain detects over 80,000 known malicious packages across npm, PyPI, RubyGems, Maven, Go, NuGet, and more.
- Flags threats like typosquatting, dependency confusion, hijacked packages, and compromised maintainers.
- All findings are critical severity and always reachable.

Why it matters

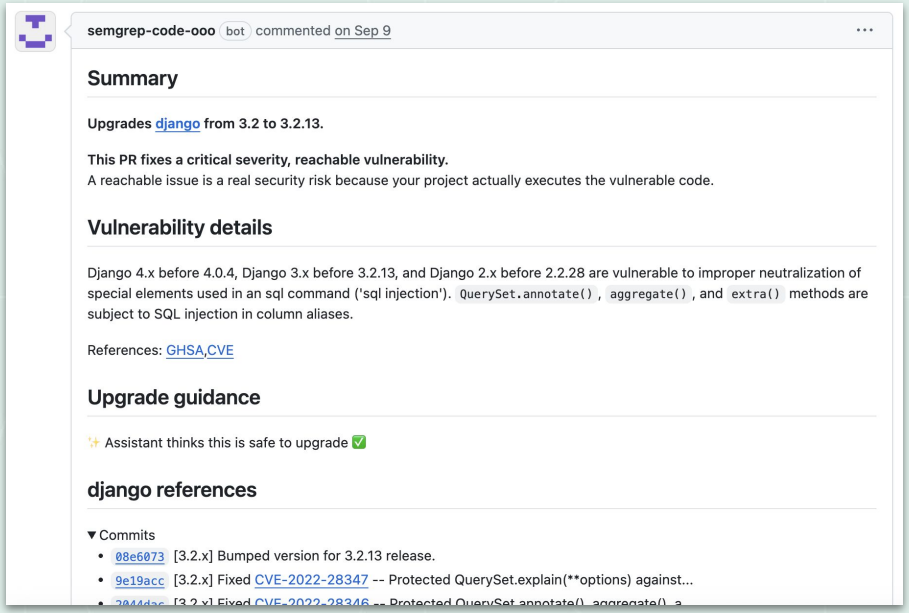
- Attackers disguise malware as legitimate packages to steal credentials and exfiltrate data.
- LLMs > more malware > more top of mind in the industry

Learn more

Detect and remove malicious dependencies

SEMGREP SUPPLY CHAIN

Upgrade Guidance & Click to Fix



PRIVATE BETA

What it is

- Click to Fix generates pull requests directly from the Semgrep platform to upgrade vulnerable dependencies.
- Semgrep analyzes how your code uses the package to identify which functions will break during the upgrade, then includes this breaking change guidance in the PR.
- Supports Python and Go in private beta, with other languages in development. Works with GitHub.

Why it matters

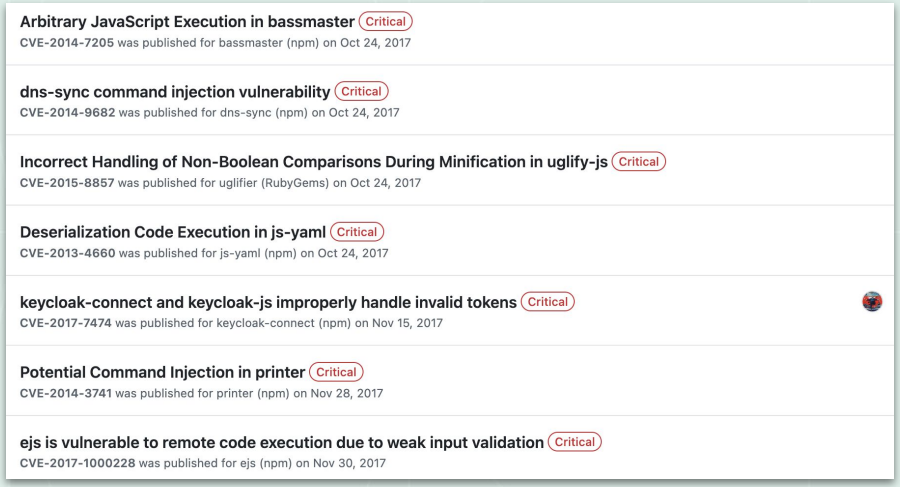
- Developers waste time creating PRs only to have CI checks fail due to unexpected breaking changes.
- Click to Fix shows exactly what will break before the upgrade happens.

Learn more

Upgrade guidance and click-to-fix pull requests

SEMGREP SUPPLY CHAIN

Extended Reachability Rules



GA

What it is

- Reachability analysis rules for all high and critical severity CVEs published since 2017 across JavaScript, Go, C#, Swift, and Ruby.
- The Security Research team reviewed each CVE, identified affected functions, and created rules to detect if those functions are called in vulnerable ways in your code.
- This expanded historical coverage adds over 1,100 rules to the existing ruleset.

Why it matters

- Legacy dependencies with older CVEs still run in production.
- Historical reachability coverage helps you focus remediation on vulnerabilities that actually matter in your codebase, not just version-based alerts.

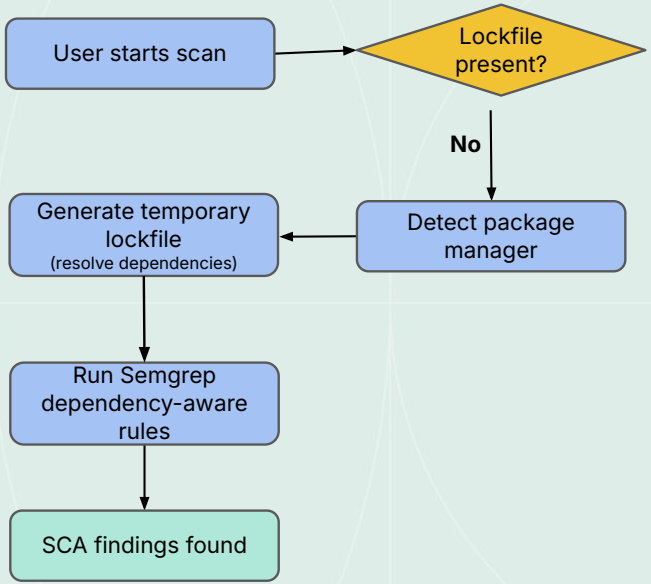
Learn more

CVE coverage

Coming Soon

SEMGREP APPSEC PLATFORM

Scan Without Lockfiles via Semgrep Managed Scanning



PUBLIC BETA COMING SOON

What it is

Getting SCA findings without needing lockfiles at scale through Semgrep Managed Scanning.

Why it matters

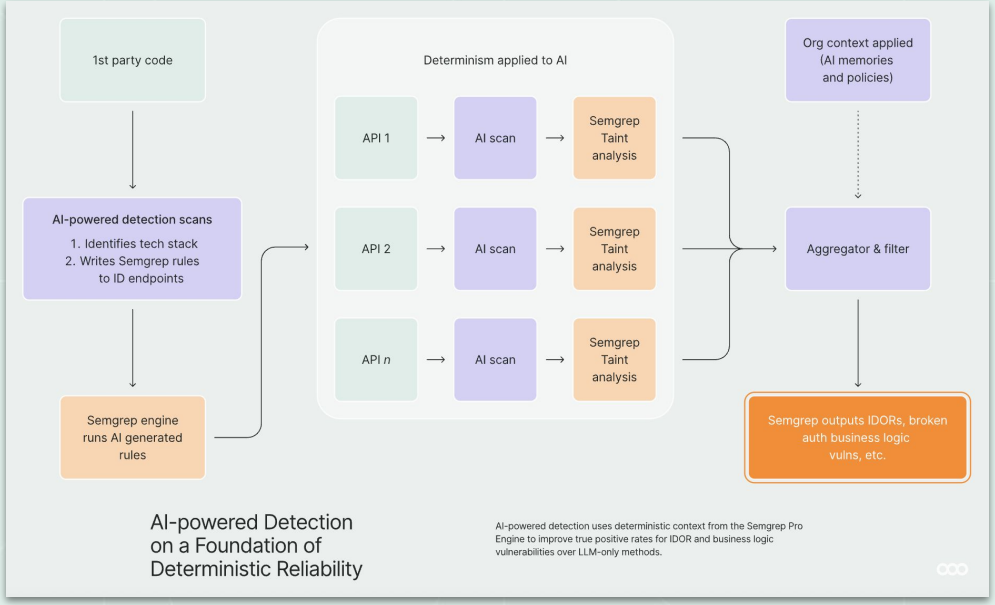
Generating lockfiles on behalf of users has been available, but limited by the fact that we have to configure each CI workflow file per repository. By enabling this on Semgrep Managed Scanning, we're able to generate lockfiles across 1000s of repositories without any additional work needed, saving time and maintenance costs.

Learn more

Scanning projects without lockfiles

ADVANCED DETECTION

AI Powered Detection



PUBLIC BETA COMING SOON

What it is

Semgrep's LLM Detection combines static analysis with AI to find vulnerabilities traditional scanners miss. It detects business logic flaws and IDOR issues alongside standard findings like SQLi, XSS, and SSRF.

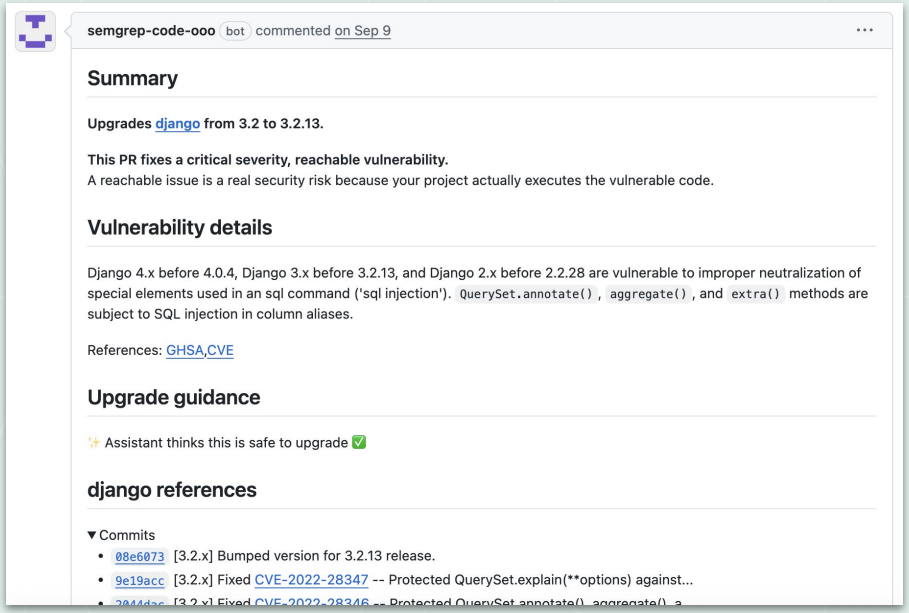
Why it matters

Business logic vulnerabilities typically surface only during bug bounties or pen tests, after code reaches production. LLM Detection catches these high-impact issues during development, preventing costly security incidents before they happen.

Learn more

Join the Beta for AI-Powered Detection

Upgrade Guidance & Click to Fix



PUBLIC BETA COMING SOON

What it is

Click to Fix generates pull requests directly from the Semgrep platform to upgrade vulnerable dependencies. Semgrep analyzes how your code uses the package to identify which functions will break during the upgrade, then includes this breaking change guidance in the PR. Supports Python and Go in public beta, with other languages in development. Works with GitHub.

Why it matters

Developers waste time creating PRs only to have CI checks fail due to unexpected breaking changes. Click to Fix shows exactly what will break before the upgrade happens.

Learn more

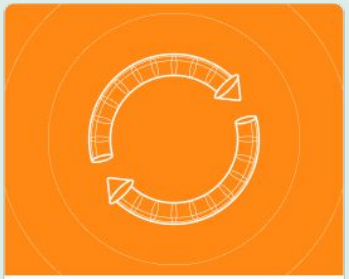
Upgrade guidance and click-to-fix pull requests

Resources

Visit the quarterly release page

Get a detailed look at this quarter's latest innovations.

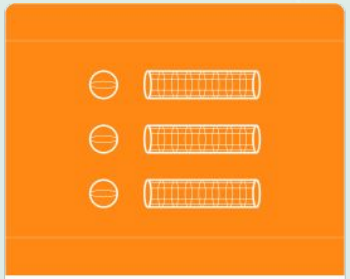
semgrep.dev/resources/whats-new



Discover the latest product updates

Stay informed about significant new features and enhancements.

semgrep.dev/products/product-updates/



Check out the release notes

Understand the full scope of changes in each release.

semgrep.dev/docs/release-notes

Learn AppSec with Semgrep Academy

Learn to create secure software with us.

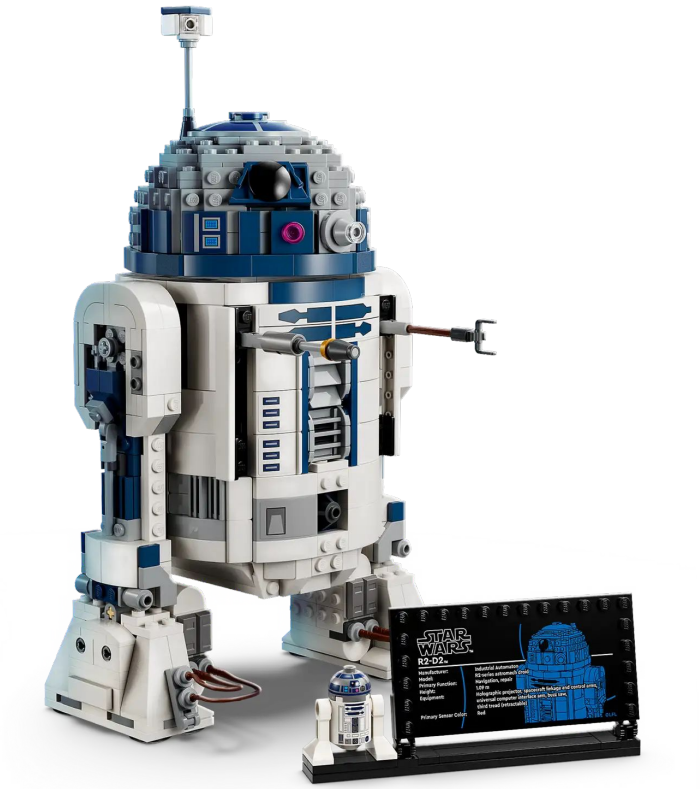
academy.semgrep.dev

GIVEAWAY TIME!!!

Q: In the original Star Wars trilogy, **who** was the actor inside the R2-D2 costume?

WINNER!

R2-D2™
LEGO® Star Wars™ Set #75379



Q&A


Semgrep