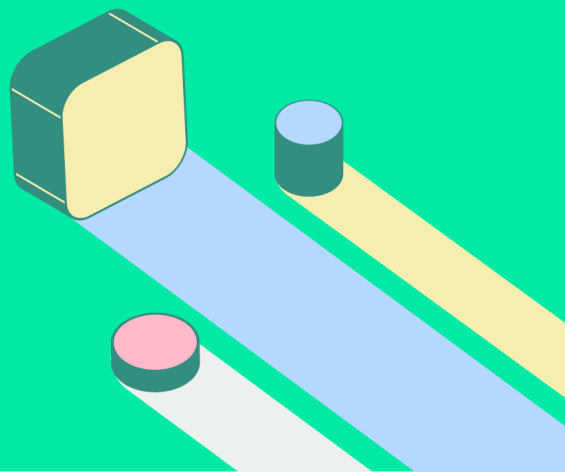
VULCAN.

GitLab



Solution brief

Vulcan Cyber and GitLab

The challenge

In the modern enterprise landscape, the adoption of Continuous Integration/Continuous Deployment (CI/CD) methodologies is paramount for business growth. However, a significant challenge emerges as engineering teams are tasked with not only writing code but also securing it, which often falls lower on their list of priorities. Naturally, engineers typically prefer working within their native tools, focusing solely on coding rather than integrating security measures. To overcome this, security teams need to maintain comprehensive asset inventories and ensure all assets are surfaced and continually monitored for potential software risks.

- Over 75% of applications have at least one flaw
- About 20% of cyber attacks target vulnerabilities in web applications

Vulcan Cyber and GitLab – better together

The Vulcan Cyber and GitLab integration enables the ingestion of code project inventories that correlate with other third-party security findings, ensuring comprehensive monitoring for potential risks related to their software assets. This integration empowers organizations to enhance their application security posture by proactively identifying vulnerabilities in their codebases and dependencies, and communicating remediation guidelines to developers and engineers effectively. For GitLab Ultimate users, this integration goes a step beyond by injecting both static and dynamic application security testing capabilities, along with dependency scanning functionalities.

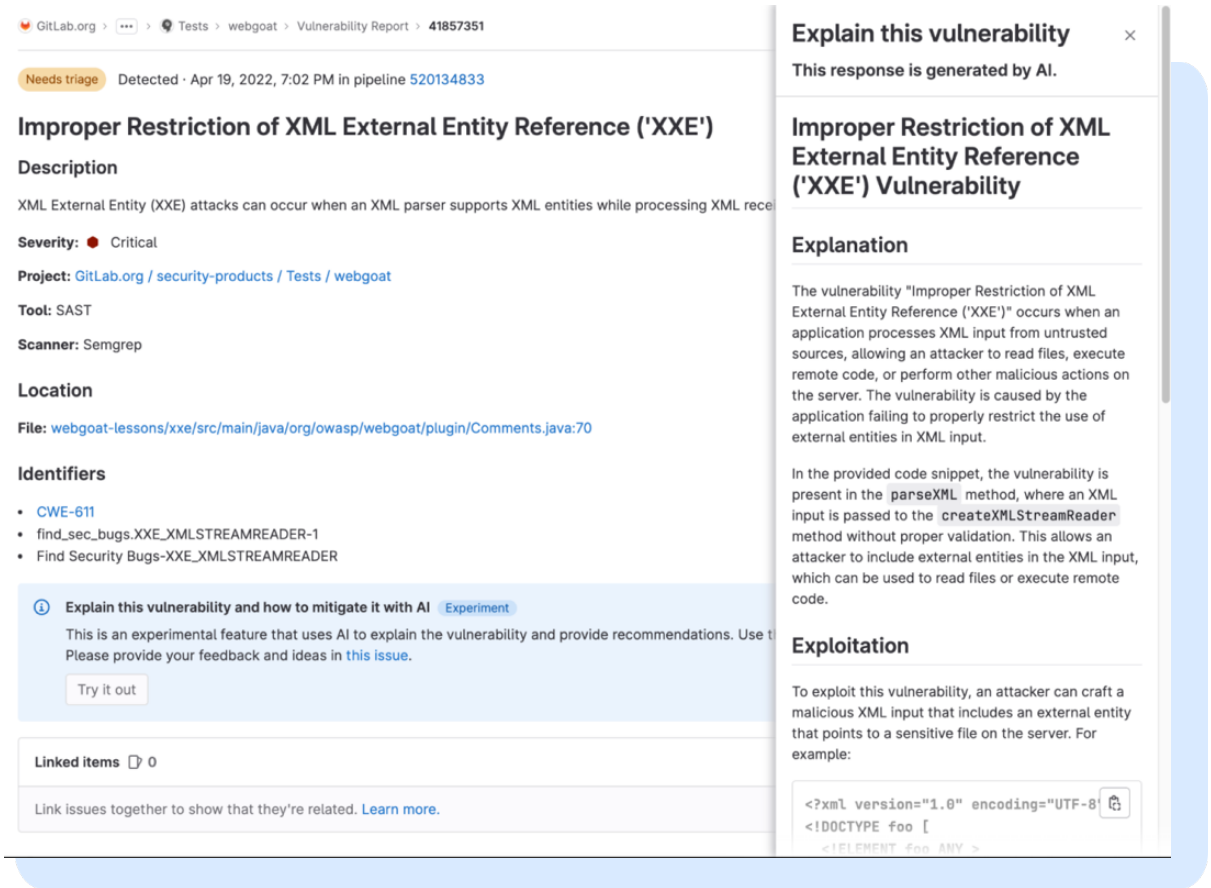
Joint solution key features

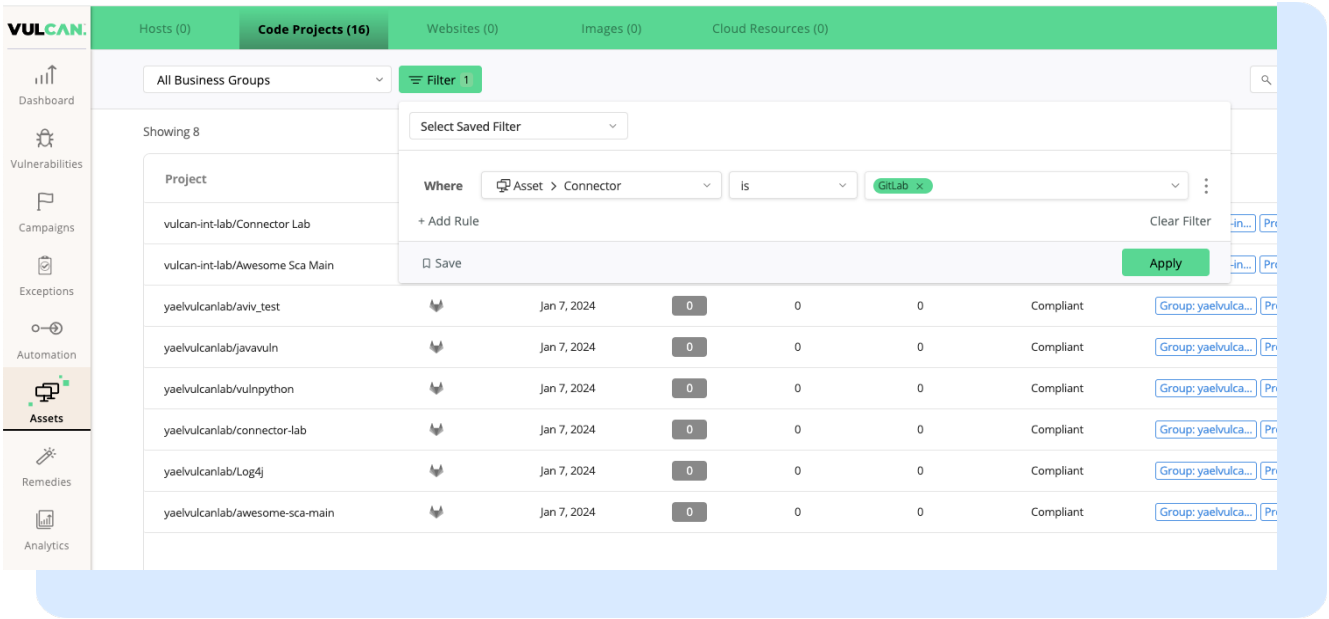
- Risk exception: Streamline exception handling by communicating it directly to engineers, ultimately reducing operational burdens and shortening remediation cycles.
- Reporting: Access advanced reporting capabilities including historical trends, policy compliance tracking, and Root Cause Analysis (RCA) insights.

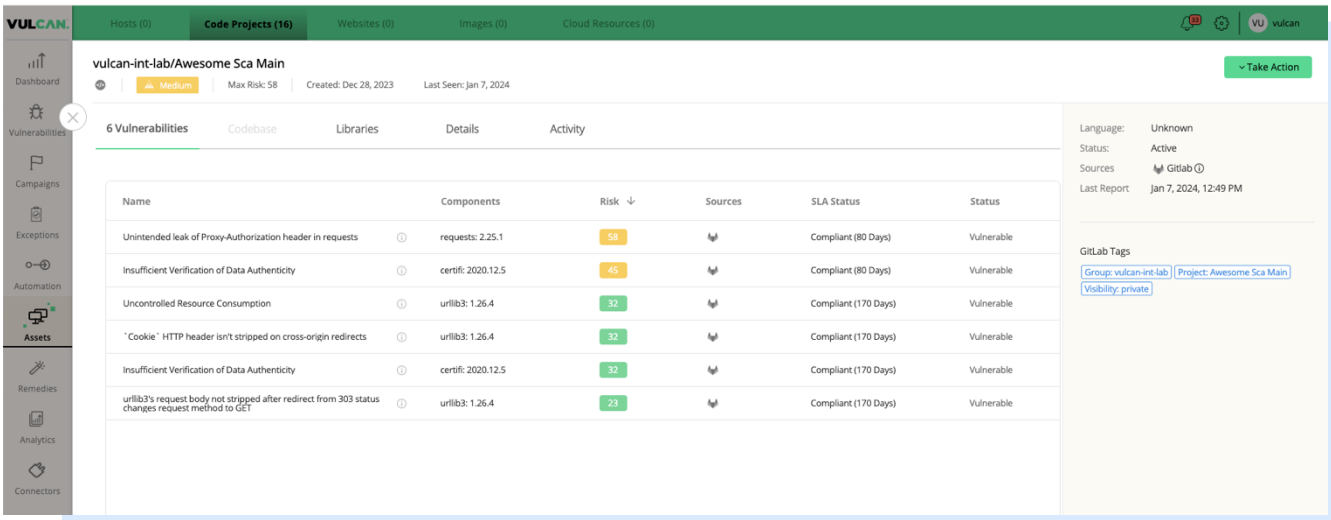
- **Incorporate code projects into your organization's holistic view:** Enable structured organization hierarchy for business units, departments, GEOs, and applications.

Use cases

- **Effective Software Bill of Materials (SBOM) management:** Identify vulnerabilities within code libraries and mitigate associated risks
- **Dev security collaboration:** Accelerate software risk remediation by fostering collaboration between engineering and security teams, allowing each to work within their native tools.
- **Comprehensive visibility of application risks:** Get a centralized view of all code and application assets and their associated risks (alongside other types of risks).
- **SLA compliance:** Ensure stakeholder alignment within the organization to adhere to company software risk policies.







About Vulcan Cyber

Vulcan Cyber has developed the market-leading Exposure operating system (ExposureOS) to provide information security teams with one platform to prioritize, orchestrate, and mitigate exposure risk at scale throughout the entire attack surface.

About GitLab

GitLab, The DevOps Platform, empowers organizations to maximize the overall return on software development by delivering software faster and more efficiently while strengthening security and compliance.