FOSSID

Reinventing Vulnerability Detection

The FossID vulnerability snippet finder takes open source vulnerability detection to new levels. It detects and identifies the actual lines of code that introduce vulnerabilities in open source and proprietary code!

- Detects the lines of code (snippets) that introduce the vulnerabilities
- Removes false positives and common human errors
- Finds matches inside open source components and proprietary code

At its best, software scanners identify open source components and adhering versions in the scanned code and correlate them to known vulnerability lists from public repositories (most commonly the “National Vulnerability Database”, NVD).

Oftentimes, though, the vulnerabilities only relate to a few files or even a couple of lines of code within a whole component, and with traditional tools you stand the risk of being overwhelmed by unprecise vulnerability lists and false positives.

This is where FossID’s vulnerability snippet finder, or “VulnSnippet Finder”, comes in.

The VulnSnippet Finder is a market first, and a revolutionary new tool that detects the actual lines of code (snippets) that introduce the vulnerabilities. And it does so regardless of if it scans known or unknown open source components, or even proprietary code.

Designed for Continuous Integration

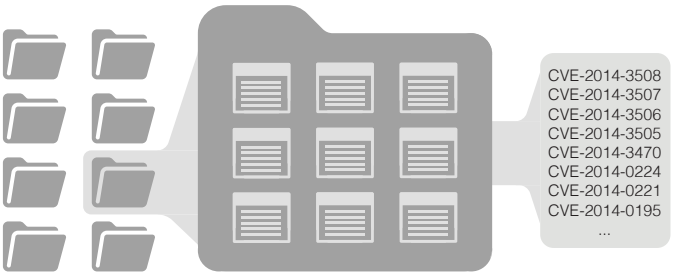
The VulnSnippet Finder is an add-on to the patented FossID scan engine and open source knowledge base and can be used via FossID’s Command Line Interface (CLI).

It only requires one single command to find matches to vulnerable snippets, and the matches are reported in JSON format together with information of the vulnerability.

www.fossid.com
@fossid_ab
linkedin.com/company/fossid-ab

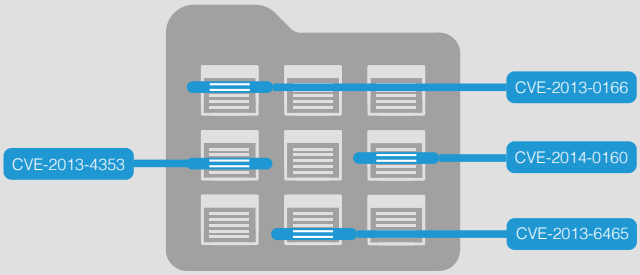
Traditional Security Scanning

- Assumes vulnerabilities based on component/ version
- Assumes the identified version for a component is correct. This is not always true and it can result in an incorrect set of vulnerabilities being reported.
- Assumes entire components are used. Though sometimes only some parts (files or even snippets) of open source components are used.
- Flags any file that matches a known vulnerable component (false positives)



FOSSID VulnSnippet Finder

- Detects the actual lines of code (snippets) that introduce the vulnerabilities
- Removes common human errors such as selecting the incorrect component or version for an open source match
- Finds matches inside known or unknown open source components as well as proprietary code.
- Reduces the amount of false positives
- Detects known vulnerabilities in derivatives and forks



Built for Easy Integration

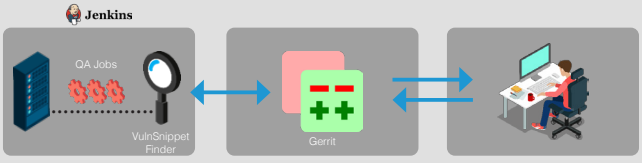
Example 1 Nightly Build Scan Trigger

Compares specific branch against vulnerable code from FossID's knowledge base and detects if a vulnerability is being introduced over night.

Security engineer reads daily security vulnerability reports.

Example 2 Commit Upload Scan Trigger

Compares introduced code against vulnerable code from FossID's knowledge base and detects vulnerabilities before the code is merged.



Triggers VulnSnippet Finder via Jenkins plugin and reports matches. Stops commit from merging if necessary.

Developer uploads code to review tool.

Developer and code reviewers get notified of any introduced vulnerability.

FossID offers a state-of-the-art open source scanner that integrates in your development process seamlessly and detects pieces of Free and Open Source Software (FOSS) in your code base, from entire components to code snippets. FossID's software uncovers license obligations and compliance issues so that you can focus on creating great products.

www.fossid.com
@fossid_ab
linkedin.com/company/fossid-ab

GET IN TOUCH!

Discover all FossID products and services at **www.fossid.com**

FossID AB
Gåsgränd 3
111 27 Stockholm
Sweden

FossID K.K.
1-10-3-200 Roppongi, Minato-ku
Tokyo 106-0032
Japan