<https://owasp.org/www-community/Source_Code_Analysis_Tools>

# Source Code Analysis Tools

**Contributor(s):** Dave Wichers, itamarlavender, will-obrien, Eitan Worcel, Prabhu Subramanian, kingthorin, coadaflorin, hblankenship, GovorovViva64, pfhorman, GouveaHeitor, Clint Gibler, DSotnikov, Ajin Abraham, Noam Rathaus

[Source code analysis](https://owasp.org/www-community/Static_Code_Analysis) tools, also referred to as Static Application Security Testing (SAST) Tools, are designed to analyze source code or compiled versions of code to help find security flaws.

Some tools are starting to move into the IDE. For the types of problems that can be detected during the software development phase itself, this is a powerful phase within the development life cycle to employ such tools, as it provides immediate feedback to the developer on issues they might be introducing into the code during code development itself. This immediate feedback is very useful, especially when compared to finding vulnerabilities much later in the development cycle.

## Strengths and Weaknesses

### Strengths

* Scales well – can be run on lots of software, and can be run repeatedly (as with nightly builds or continuous integration).
* Useful for things that such tools can automatically find with high confidence, such as buffer overflows, SQL Injection Flaws, and so forth.
* Output is good for developers – highlights the precise source files, line numbers, and even subsections of lines that are affected.

### Weaknesses

* Many types of security vulnerabilities are difficult to find automatically, such as authentication problems, access control issues, insecure use of cryptography, etc. The current state of the art only allows such tools to automatically find a relatively small percentage of application security flaws. However, tools of this type are getting better.
* High numbers of false positives.
* Frequently can’t find configuration issues, since they are not represented in the code.
* Difficult to ‘prove’ that an identified security issue is an actual vulnerability.
* Many of these tools have difficulty analyzing code that can’t be compiled. Analysts frequently can’t compile code because they don’t have the right libraries, all the compilation instructions, all the code, etc.

## Important Selection Criteria

* Requirement: Must support your programming language, but not usually a key factor once it does.
* Types of vulnerabilities it can detect (out of the [OWASP Top Ten](https://owasp.org/www-project-top-ten/) (plus more?))
* How accurate is it? False Positive/False Negative rates? - Does the tool have an OWASP [Benchmark](https://owasp.org/www-project-benchmark/) score?
* Does it understand the libraries/frameworks you use?
* Does it require a fully buildable set of source?
* Can it run against binaries instead of source?
* Can it be integrated into the developer’s IDE?
* How hard is it to setup/use?
* Can it be run continuously and automatically?
* License cost for the tool. (Some are sold per user, per organization, per application, per line of code analyzed. Consulting licenses are frequently different than end user licenses.)

## Disclaimer

**The tools listed in the tables below are presented in alphabetical order. OWASP does not endorse any of the vendors or tools by listing them in the table below. We have made every effort to provide this information as accurately as possible. If you are the vendor of a tool below and think that this information is incomplete or incorrect, please send an e-mail to our mailing list and we will make every effort to correct this information.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name/Link** | **Owner** | **License** | **Platforms** | **Note** |
| [.NET Security Guard](https://security-code-scan.github.io/) |  | Open Source or Free |  | .NET, C\#, VB.net |
| [42Crunch](https://42crunch.com/) |  | Commercial |  | REST API security platform that includes Security Audit (SAST), dynamic conformance scan, runtime protection, and monitoring. |
| [APIsecurity.io Security Audit](https://apisecurity.io/tools/audit/) |  | Open Source or Free |  | online tool for OpenAPI / Swagger file static security analysis |
| [Agnitio](https://sourceforge.net/projects/agnitiotool/) |  | Open Source or Free | Windows | ASP, ASP.NET, C\#, Java, Javascript, Perl, PHP, Python, Ruby, VB.NET, XML |
| [AppScan Source](https://www.hcltechsw.com/wps/portal/products/appscan/offerings/source) | HCL Software | Commercial |  | Static application security testing solution that helps identify vulnerabilities early in the development lifecycle, understand their origin and potential impact and remediate the problem. |
| [AppScan on Cloud](https://cloud.appscan.com/) | HCL Software | Commercial |  | Cloud-based application security testing suite to perform SAST, DAST, IAST & SCA on web and mobile application. |
| [Application Inspector](https://www.ptsecurity.com/ww-en/products/ai/) | Positive Technologies | Commercial |  | combines SAST, DAST, IAST, SCA, configuration analysis and other technologies, incl. unique abstract interpretation; has capability to generate test queries (exploits) to verify detected vulnerabilities during SAST analysis; Supported languages include: Java, C\#, PHP, JavaScript, Objective C, VB.Net, PL/SQL, T-SQL, and others. |
| [Bandit](https://github.com/PyCQA/bandit) |  | Open Source or Free |  | Bandit is a comprehensive source vulnerability scanner for Python |
| [Beyond Security beSOURCE](https://beyondsecurity.com/solutions/besource.html) | Beyond Security | Commercial |  | Static application security testing (SAST) used to be divorced from Code quality reviews, resulting in limited impact and value. beSOURCE addresses the code security quality of applications and thus integrates SecOps into DevOps. |
| [BlueClosure BC Detect](https://www.blueclosure.com/) | BlueClosure | Commercial |  | Analyzes client-side JavaScript. |
| [Brakeman](https://brakemanscanner.org/) |  | Open Source or Free |  | Brakeman is an open source vulnerability scanner specifically designed for Ruby on Rails applications |
| [CAST AIP](https://www.castsoftware.com/products/application-intelligence-platform) |  | Commercial |  | Performs static and architectural analysis to identify numerous types of security issues. Supports over 30 languages. [AIP's security specific coverage is here](https://www.castsoftware.com/solutions/application-security/cwe#SupportedSecurityStandards). |
| [Checkmarx Static Code Analysis](https://www.checkmarx.com/) |  | Open Source or Free |  | Android, Apex, ASP.NET, C\#, C++, Go, Groovy, HTML5, Java, JavaScript, JSP, .NET, Objective-C, Perl, PHP, PL/SQL, Python, Ruby, Scala, Swift, TypeScript, VB.NET, Visual Basic 6, Windows Phone |
| [Codacy](https://www.codacy.com/) |  | Commercial |  | Offers security patterns for languages such as Python, Ruby, Scala, Java, JavaScript and more. Integrates with tools such as Brakeman, Bandit, FindBugs, and others. (free for open source projects) |
| [CodeScan Cloud](https://www.codescan.io/) |  | Commercial |  | A Salesforce focused, SaaS code quality tool leveraging SonarQube's OWASP security hotspots to give security visibility on Apex, Visualforce, and Lightning proprietary languages. |
| [CodeSec](http://www.seczone.cn/2018/06/27/codesec%E6%BA%90%E4%BB%A3%E7%A0%81%E5%AE%89%E5%85%A8%E6%A3%80%E6%B5%8B%E5%B9%B3%E5%8F%B0/) |  | Open Source or Free |  | C, C++, C\#, Java, JavaScript, PHP, Kotlin, Lua, Scala, TypeScript, Android |
| [CodeSonar](https://www.grammatech.com/products/codesonar) |  | Commercial |  | tool that supports C, C++, Java and C\# and maps against the OWASP top 10 vulnerabilities. |
| [CodeSonar](https://www.grammatech.com/) |  | Open Source or Free |  | C, C++, Java |
| [Contrast Assess](https://www.contrastsecurity.com/interactive-application-security-testing-iast) |  | Commercial |  | Contrast performs code security without actually doing static analysis. Contrast does Interactive Application Security Testing (IAST), correlating runtime code & data analysis. It provides code level results without actually relying on static analysis. |
| [Coverity](https://www.synopsys.com/software-integrity/security-testing/static-analysis-sast.html) |  | Open Source or Free |  | Android, C\#, C, C++, Java, JavaScript, Node.js, Objective-C, PHP, Python, Ruby, Scala, Swift, VB.NET |
| [Coverity Static Analysis](https://www.synopsys.com/content/dam/synopsys/sig-assets/datasheets/SAST-Coverity-datasheet.pdf) | Synopsys | Commercial |  |  |
| [CxSAST](https://www.checkmarx.com/technology/static-code-analysis-sca/) | Checkmarx | Commercial |  |  |
| [Dawnscanner](https://rubygems.org/gems/dawnscanner) |  | Open Source or Free |  | Dawnscanner is an open source security source code analyzer for Ruby, supporting major MVC frameworks like Ruby on Rails, Padrino, and Sinatra. It also works on non-web applications written in Ruby. |
| [Deep Dive](https://discotek.ca/deepdive.xhtml) |  | Open Source or Free |  | Byte code analysis tool for discovering vulnerabilities in Java deployments (EAR, WAR, JAR). |
| [DeepSource](https://deepsource.io/) | DeepSource Corp. | Commercial | SaaS or On-Premises | DeepSource helps you automatically find and fix issues in your code during code reviews, such as bug risks, anti-patterns, performance issues, and security flaws. It takes less than 5 minutes to set up with your Bitbucket, GitHub, or GitLab account. It works for Python, Go, Ruby, and JavaScript. |
| [DerScanner](https://derscanner.com/) | DerScanner Ltd. | Commercial |  | Capable of identifying vulnerabilities and backdoors (undocumented features) in over 30 programming languages by analyzing source code or executables, without requiring debug info. |
| [DevBug](http://www.devbug.co.uk/) |  | Open Source or Free | Web Based | PHP |
| [ECG](https://ecg.voidsec.com/) | VoidSec | Commercial |  | SaaS TCL Static Source Code Analysis Tool able to detect real and complex security vulnerabilities in TCL/ADP source-code. Discovered vulnerabilities will be mapped against the OWASP top 10 vulnerabilities. |
| [Enlightn](https://www.laravel-enlightn.com/) | Enlightn Software | Open Source |  | Enlightn is a vulnerability scanner specifically designed for Laravel PHP applications that combines SAST, DAST, IAST and configuration analysis techniques to detect vulnerabilities. |
| [Find Security Bugs](https://find-sec-bugs.github.io/) |  | Open Source or Free |  | Java, Scala, Groovy |
| [FindBugs](https://github.com/findbugsproject/findbugs) |  | Open Source or Free |  | Find bugs (including a few security flaws) in Java programs [Legacy - NOT Maintained - Use SpotBugs (see other entry) instead] |
| [FindSecBugs](https://find-sec-bugs.github.io/) |  | Open Source or Free |  | A security specific plugin for SpotBugs that significantly improves SpotBugs's ability to find security vulnerabilities in Java programs. Works with the old FindBugs too. |
| [Flawfinder](http://www.dwheeler.com/flawfinder/) |  | Open Source or Free |  | Scans C and C++. |
| [Fortify](https://www.microfocus.com/en-us/products/static-code-analysis-sast/overview) | Micro Focus | Commercial | Windows, Linux, and MacOSX | Free trial scan available. Supported languages include: ABAP/BSP, ActionScript/MXML (Flex), APEX, ASP.NET, VB.NET, C\# (.NET), C/C++, Classic ASP (w/VBScript), COBOL, ColdFusion CFML, Go, HTML, Java (including Android), JavaScript/AJAX, JSP, Kotlin, Objective-C, PHP, PL/SQL, Python, Typescript, T-SQL, Ruby, Scala, Swift, Visual Basic (VB.NET), Visual Basic 6, VBScript, XML |
| [GitLab](https://docs.gitlab.com/ee/user/application_security/sast/index.html) | GitLab | Commercial | SaaS, Linux, Windows |  |
| [GolangCI-Lint](https://golangci-lint.run/) |  | Open Source or Free |  | A Go Linters aggregator - One of the Linters is [gosec (Go Security)](https://github.com/securego/gosec), which is off by default but can easily be enabled. |
| [Google CodeSearchDiggity](https://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/) |  | Open Source or Free |  | Uses Google Code Search to identify vulnerabilities in open source code projects hosted by Google Code, MS CodePlex, SourceForge, Github, and more. The tool comes with over 130 default searches that identify SQL injection, cross-site scripting (XSS), insecure remote and local file includes, hard-coded passwords, and much more. \*Essentially, Google CodeSearchDiggity provides a source code security analysis of nearly every single open source code project in existence – simultaneously.\* |
| [Graudit](https://github.com/wireghoul/graudit/) |  | Open Source or Free | Linux | Scans multiple languages for various security flaws. Basically security enhanced code Grep. |
| [HCL AppScan CodeSweep](https://hclsw.co/codesweep) |  | Open Source or Free |  | This is the first Community edition version of AppScan. It is delivered as a VS Code plugin and scans files upon saving them. The results show the location of a finding, type and remediation advice. The tool currently supports Python, Ruby, JS (Node, Angular, JQuery, etc) , PHP, Perl, COBOL, APEX & a few more. |
| [HCL AppScan Source](https://www.hcltechsw.com/wps/portal/products/appscan/offerings/source) |  | Open Source or Free |  | Android, Apex, ASP, C, C++, COBOL, ColdFusion, Go, Java, JavaScript(Client-side JavaScript, NodeJS, and AngularJS), .NET (C#, ASP.NET, VB.NET), .NET Core, Perl, PHP, PL/SQL, Python, Ruby, T-SQL, Visual Basic 6 |
| [HCL AppScan on Cloud](https://cloud.appscan.com/) |  | Open Source or Free |  | Apex, ASP, C, C++, COBOL, ColdFusion, Go, Java, JavaScript(Client-side JavaScript, Kotlin, NodeJS, and AngularJS), .NET (C#, ASP.NET, VB.NET), .NET Core, Perl, PHP, PL/SQL, Python, Ruby, T-SQL, Swift, Visual Basic 6 |
| [Hdiv Detection](https://hdivsecurity.com/interactive-application-security-testing-iast) | Hdiv Security | Commercial |  | Hdiv performs code security without actually doing static analysis. Hdiv does Interactive Application Security Testing (IAST), correlating runtime code & data analysis. It provides code-level results without actually relying on static analysis. |
| [Horusec](https://github.com/ZupIT/horusec) |  | Open Source or Free |  | Python(3.x), Ruby, Javascript, GoLang, .NetCore(3.x), Java, Kotlin, Terraform |
| [HuskyCI](https://huskyci.opensource.globo.com/) |  | Open Source or Free |  | HuskyCI is an open-source tool that orchestrates security tests inside CI pipelines of multiple projects and centralizes all results into a database for further analysis and metrics. HuskyCI can perform static security analysis in Python (Bandit and Safety), Ruby (Brakeman), JavaScript (Npm Audit and Yarn Audit), Golang (Gosec), and Java(SpotBugs plus Find Sec Bugs) |
| [Insider CLI](https://github.com/insidersec/insider) | InsiderSec | Open Source or Free |  | A open source Static Application Security Testing tool (SAST) written in GoLang for Java Maven and Android), Kotlin (Android), Swift (iOS), .NET Full Framework, C#, and Javascript (Node.js). |
| [Kiuwan](https://www.kiuwan.com/) | a division of Idera, Inc. | Commercial |  | provides an application security testing and analytics platform – including SAST and SCA solutions – that reduces risk and improves change management and DevOps processes |
| [Klocwork](https://www.perforce.com/products/klocwork) | Perforce | Commercial |  | Static Code Analysis for C, C++, C#, and Java |
| [Klocwork](https://www.roguewave.com/products-services/klocwork/static-code-analysis) |  | Open Source or Free |  | C, C++, C\#, Java |
| [Kroogal](http://www.kroogal.com/) |  | Commercial |  | C, C++ |
| [LGTM](https://lgtm.com/help/lgtm/about-lgtm) |  | Open Source or Free |  | A free for open source static analysis service that automatically monitors commits to publicly accessible code in Bitbucket Cloud, GitHub, or GitLab. Supports C/C++, C\#, Go, Java, JavaScript/TypeScript, Python. |
| [Microsoft FxCop](https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-3.0/bb429476%28v=vs.80%29) |  | Open Source or Free |  | .NET |
| [Microsoft PREFast](https://docs.microsoft.com/en-us/previous-versions/windows/embedded/ms933794%28v=msdn.10%29) |  | Open Source or Free |  | C, C++ |
| [MobSF](https://mobsf.github.io/Mobile-Security-Framework-MobSF/) |  | Open Source or Free |  | Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis. |
| [MobSF](https://github.com/MobSF/Mobile-Security-Framework-MobSF) |  | Open Source or Free | Windows, Unix | Android Java, Objective C, Swift |
| [NextGen Static Analysis](https://www.shiftleft.io/nextgen-static-analysis/) |  | Open Source or Free |  | C\#, Go, Java, JavaScript, Python, Scala |
| [OWASP ASST (Automated Software Security Toolkit)](https://github.com/OWASP/ASST) | Tarik Seyceri & OWASP | Open Source or Free | Ubuntu, MacOSX and Windows | An Open Source, Source Code Scanning Tool, developed with JavaScript (Node.js framework), Scans for PHP & MySQL Security Vulnerabilities According to OWASP Top 10 and Some other OWASP's famous vulnerabilities, and it teaches developers of how to secure their codes after scan. |
| [OWASP Code Crawler](https://wiki.owasp.org/index.php/Category:OWASP_Code_Crawler) | OWASP | Open Source |  | .NET, Java |
| [OWASP LAPSE Project](https://wiki.owasp.org/index.php/OWASP_LAPSE_Project) | OWASP | Open Source |  | Java |
| [OWASP Orizon Project](https://wiki.owasp.org/index.php/Category:OWASP_Orizon_Project) | OWASP | Open Source |  | Java |
| [OWASP WAP (Web Application Protection)](https://wiki.owasp.org/index.php/OWASP_WAP-Web_Application_Protection) | OWASP | Open Source |  | PHP |
| [Oversecured](https://oversecured.com/) | Oversecured Inc | Commercial | Android | A static SaaS-based vulnerability scanner for Android apps (APK files), supports apps written on Java and Kotlin. Also allows integrations into DevOps processes. |
| [PITSS.CON](https://pitss.com/products/pitss-con/) | PITTS | Commercial |  | Scans Oracle Forms and Reports Applications |
| [PMD](https://pmd.github.io/) |  | Open Source or Free |  | PMD scans Java source code and looks for potential code problems (this is a code quality tool that does not focus on security issues). |
| [PT Application Inspector](https://www.ptsecurity.com/ww-en/products/ai/) | Positive Technologies | Commercial |  | Combines SAST, DAST, IAST, SCA, configuration analysis and other technologies for high accuracy. Can generate special test queries (exploits) to verify detected vulnerabilities during SAST analysis. Supports Java, C\#, PHP, JavaScript, Objective C, VB.Net, PL/SQL, T-SQL, and others. |
| [PVS-Studio](https://www.viva64.com/en/pvs-studio/) |  | Open Source or Free |  | C, C++, C\# |
| [PVS-Studio Analyzer](https://www.viva64.com/en/pvs-studio/) | PVS-Studio | Commercial |  | Static code security analysis for C, C++, C#, and Java. A commercial B2B solution, but provides several free [licensing options](https://www.viva64.com/en/b/0614/). |
| [ParaSoft](https://www.parasoft.com/) |  | Open Source or Free |  | C, C++, Java, .NET |
| [Parasoft Test](https://www.parasoft.com/products) | Parasoft | Commercial |  | Test tools for C/C++, .NET, Java |
| [Polyspace Static Analysis](https://www.mathworks.com/products/polyspace.html) |  | Open Source or Free |  | C, C++, Ada |
| [PreFast](https://docs.microsoft.com/en-us/previous-versions/windows/embedded/ms933794(v=msdn.10)?redirectedfrom=MSDN) | Microsoft | Open Source or Free |  | PREfast is a static analysis tool that identifies defects in C/C++ programs. Last update 2006. |
| [Progpilot](https://github.com/designsecurity/progpilot) |  | Open Source or Free |  | Progpilot is a static analyzer tool for PHP that detects security vulnerabilities such as XSS and SQL Injection. |
| [Puma Scan](https://pumascanpro.com/) | Puma Security | Commercial |  | A .NET C\# static source code analyzer that runs as a Visual Studio IDE extension, Azure DevOps extension, and Command Line (CLI) executable. |
| [Puma Scan Professional](https://pumascan.com/pricing/) |  | Open Source or Free |  | .NET, C\# |
| [Pyre](https://pyre-check.org/) |  | Open Source or Free |  | A performant type-checker for Python 3, that also has [limited security/data flow analysis](https://pyre-check.org/docs/pysa-basics.html) capabilities. |
| [RIPS Code Analysis](https://www.ripstech.com/) | RIPS Technologies - Acquired by SonarSource | Commercial |  | Static security analyzer for Java and PHP. |
| [SecureAssist](https://community.synopsys.com/s/article/SecureAssist-Overview) | Synopsys | Commercial |  | Scans code for insecure coding and configurations automatically as an IDE plugin for Eclipse, IntelliJ, and Visual Studio, etc. Supports Java, .NET, PHP, and JavaScript. |
| [Security Code Scan](https://security-code-scan.github.io/) |  | Open Source or Free |  | Static code analyzer for .NET. It will find SQL injections, LDAP injections, XXE, cryptography weakness, XSS and more. |
| [Seeker](https://www.synopsys.com/software-integrity/security-testing/interactive-application-security-testing.html) | Synopsys | Commercial |  | Seeker performs code security without actually doing static analysis. Seeker does Interactive Application Security Testing (IAST), correlating runtime code & data analysis with simulated attacks. It provides code level results without actually relying on static analysis. |
| [Semgrep](https://github.com/returntocorp/semgrep) |  | Open Source or Free |  | Like Grep, for code. A lightweight static analysis tool with intuitive rule syntax for searching code. Scans source code. No compilation required. Supports Python, JavaScript, Go, Java, C. |
| [Sentinel Source](https://www.whitehatsec.com/products/static-application-security-testing/) | Whitehat | Commercial |  | Static security analysis for 10+ languages. |
| [ShiftLeft Scan](https://github.com/ShiftLeftSecurity/sast-scan) |  | Open Source or Free |  | A free open-source DevSecOps platform for detecting security issues in source ode and dependencies. It supports a broad range of languages and CI/CD pipelines by bundling various open source scanners into the pipeline. |
| [Sink Tank](https://discotek.ca/sinktank.xhtml) |  | Open Source or Free |  | Java byte code static code analyzer for performing source/sink (taint) analysis. |
| [SonarCloud](https://sonarcloud.io/about) |  | Open Source or Free |  | ABAP, C, C++, Objective-C, COBOL, C\#, CSS, Flex, Go, HTML, Java, Javascript, Kotlin, PHP, PL/I, PL/SQL, Python, RPG, Ruby, Swift, T-SQL, TypeScript, VB6, VB, XML |
| [SonarQube](https://www.sonarqube.org/downloads/) |  | Open Source or Free |  | Scans source code for 15 languages for Bugs, Vulnerabilities, and Code Smells. SonarQube IDE plugins for Eclipse, Visual Studio, and IntelliJ provided by [SonarLint](https://www.sonarlint.org/). |
| [Splint](https://www.splint.org/) |  | Open Source or Free |  | C |
| [SpotBugs](https://spotbugs.github.io/) |  | Open Source or Free |  | Java. This is the active fork replacement for FindBugs, which is not maintained anymore. Very little security. FindSecBugs plugin provides security rules. |
| [Thunderscan SAST](https://www.defensecode.com/thunderscan-sast/) | DefenseCode | Commercial |  | Static security analysis for 27+ languages. |
| [VS Code OpenAPI (Swagger) Editor extension](https://marketplace.visualstudio.com/items?itemName=42Crunch.vscode-openapi) |  | Open Source or Free |  | Plugin to Microsoft Visual Studio Code that enables rich editing capabilities for REST API contracts and also includes linting and Security Audit (static security analysis). |
| [Veracode](https://www.veracode.com/) |  | Open Source or Free |  | Android, ASP.NET, C\#, C, C++, Classic ASP, COBOL, ColdFusion/Java, Go, Groovy, iOS, Java, JavaScript, Perl, PhoneGap/Cordova, PHP, Python, React Native, RPG, Ruby on Rails, Scala, Titanium, TypeScript, VB.NET, Visual Basic 6, Xamarin |
| [Veracode Static Analysis](https://www.veracode.com/products/binary-static-analysis-sast) | Veracode | Commercial |  |  |
| [VisualCodeGrepper](https://sourceforge.net/projects/visualcodegrepp/) |  | Open Source or Free | Windows | C/C++, C\#, VB, PHP, Java, PL/SQL |
| [VisualCodeGrepper (VCG)](https://sourceforge.net/projects/visualcodegrepp/) |  | Open Source or Free |  | Scans C/C++, C\#, VB, PHP, Java, PL/SQL, and COBOL for security issues and for comments which may indicate defective code. The config files can be used to carry out additional checks for banned functions or functions which commonly cause security issues. |
| [Xanitizer](https://www.xanitizer.com/xanitizer/) |  | Commercial |  | Scans Java, Scala, and JavaScript/TypeScript for security vulnerabilities, mainly via taint analysis. (http://www.xanitizer.net) |
| [bugScout](https://bugscout.io/en/) | Nalbatech, Formerly Buguroo | Commercial |  |  |
| [nodejsscan](https://github.com/ajinabraham/nodejsscan) |  | Open Source or Free | Unix | Node.js |
| [phpcs-security-audit](https://github.com/FloeDesignTechnologies/phpcs-security-audit) |  | Open Source or Free |  | A set of PHP\_CodeSniffer rules to finds flaws or weaknesses related to security in PHP and its popular CMS or frameworks. It currently has core PHP rules as well as Drupal 7 specific rules. |
| [reshift](https://www.reshiftsecurity.com/) |  | Commercial |  | A CI/CD static code security analysis tool for Java that uses machine learning to give a prediction on false positives. |