Secure coding supports in IDEs

Raviteja Srigiriraju, Srivathsava Nelaturi and Aniqua Z. Baset
School of Computing, University of Utah

Table 1: List of available IDE plugins for security check

Plugin	IDE	Language	Type	Installation stat
ASIDE	Eclipse	Java, PHP	Free	N/A
CodeAssure	Eclipse	Java, C	Commercial ($48,000/year)	N/A
CodeDX	Eclipse, Visual Studio	Java, C/C++, C#, Python, JavaScript, .NET, Ruby, XML/XSL	Commercial ($2500/year)	N/A
CodeSonar	Eclipse	C/C++, Java	Commercial ($18000/Year)	N/A
Codepro AnalytiX	Eclipse	Java	Free	T:69, R:935
Codescan	Eclipse, IntelliJ, Netbeans	Java	Free	N/A
Contrast	Eclipse	Java, .Net	Commercial	T:1647, R:456
Cppeclipse	Eclipse	C++	Free	
Crypto-assistant	Eclipse	Java	Commercial	N/A
CxSuite	Eclipse, Visual Studio	Java	Commercial	N/A
ESVD	Eclipse	Java	Free	T:732,R:588
Findbugs	Eclipse, Maven, Netbeans, Hudson, IntelliJ/Android Studio	Java		N/A
JSLint	Notepad++	JavaScript	Free	N/A
Klocwork Solo	Eclipse	Java(Android)	Commercial	N/A
Klocwork	Eclipse, IntelliJ, Visual Studio	Java, C/C++, C#	Commercial	N/A
LAPSE+	Eclipse	Java	Free	N/A
PVS-studio	Visual Studio	C/C++	Commercial ($250)	N/A
Parasoft dotTEST	Visual Studio	.NET	Commercial	N/A
SecureAssist	Eclipse, Visual Studio, Springsource	Java, PHP, .NET	Commercial	N/A
SonarLint	Eclipse, Visual Studio	XML, .NET	N/A	T:6039, R:255
SSV checker	Eclipse	C/C++, Python, PHP	N/A	T:679, R:610
Tern	Eclipse, Visual Studio, Sublime, Emacs, Vim	JavaScript	Free	N/A

T = Total installation, R = Rank in Eclipse marketplace based on number of installation

Table 2: Plugins and supported vulnerability checks

	Vulnerability checks	CWE#	ASIDE	CodeDX	CodeSonar	Codepro AnalytiX	Codescan	Contrast	Cppeclipse	Crypto-assistant	CxSuite	ESVD	Findbugs	JSLint	Klocwork	Klocwork Solo	LAPSE+	PVS-studio	Parasoft dotTEST	SecureAssist	SonarLint	SSVchecker	Tern
CWE/SANS Top Most Dangerous Software Errors	SQL Injection*	89	✓	-	-	-	✓	✓	-	-	-	✓	✓	-	✓	-	✓	-	-	-	-	✓	-
	Buffer Overflow	120	-	-	✓	-	✓	✓	✓	-	-	-	✓	-	✓	✓	-	✓	-	-	-	✓	-
	Cross-site Scripting*	79	✓	-	-	-	✓	✓	-	-	-	✓	-	-	✓	-	-	-	-	-	-	✓	-
	Missing Authentication for Critical Function	306	✓	✓	-	-	✓	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-	✓	-
	Missing Authorization	86	✓	✓	-	-	-	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-	✓	-
	Use of Hard-coded Credentials	798	-	-	-	✓	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-	✓	-	-
	Missing Encryption of Sensitive Data	311	-	-	-	-	✓	-	-	-	-	✓	-	-	-	-	✓	-	-	-	-	✓	-
	Cross-Site Request Forgery*	352	-	-	✓	-	-	-	-	-	-	-	-	✓	-	-	-	-	-	-	✓	-	-
	Path Traversal	22	-	-	-	-	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-
	Incorrect Authorization	863	✓	✓	✓	-	✓	-	-	-	-	✓	-	-	-	✓	✓	-	-	-	-	✓	-
	Use of a Broken or Risky Cryptographic Algorithm	327	-	-	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Other errors	Cookie poisoning	N/A	-	-	-	-	-	-	-	-	-	-	✓	-	✓	-	✓	✓	-	-	✓	-	✓
	Parameter tampering	N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	-	-	-	-	-	-
	Memory/resource leaks		-	✓	-	-	-	-	✓	-	-	-	✓	✓	✓	-	-	-	-	-	-	-	-
	Improper input validation	20	-	-	✓	-	✓	-	-	-	✓	-	-	-	-	-	-	-	-	✓	-	✓	-
	Broken authentication	N/A	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

*Also in OWASP Top 10

Table 3: More info about some of the plugins

Plugin	Feedback-style	Ease of install/use	Known issues	Additional Features	Analysis(local or server)
ASIDE	Like regular compile errors with a description of possible attack	Easy	Not a good choice for visual studio	Has another version called ESIDE to help educating students secure programming knowledge and practices	Local
CodeDX	Need to upload code from Jenkins jobs to CodeDx application, it then shows a detailed report	Easy		Detailed report with information about code efficiency	Server
Codescan	Lists evaluation and performance info both as a report and index	Difficult, need to install salseforce IDE		Detailed report with information about performance	Both
CodeSonar	Possible vulnerabilities with historical data about CodeSonar warning counts and code size is presented in the job dashboard	Need to install some Dependencies	No run-time feedback. Need to run it as job.	Job based detailed reports.Can be configured to change the build result if the CodeSonar analysis results meet specified conditions.	Server
Codepro AnalytiX		Easy		Detects, reports and repairs deviations or non-compliance with predefined coding standards, popular frameworks, security and style conventions. Also identifies the similar code	Both
Findbugs	Problem markers like regular compiler errors	Easy	Not on run time	Supports contribution of custom FindBugs detectors	Local
Klocwork	Problem markers like regular compiler errors	Easy		Many false-positive	Local