

IDE PLUGINS FOR DETECTING INPUT-VALIDATION VULNERABILITIES

Aniqua Z. Baset, Tamara Denning
School of Computing, University of Utah

Researcher hacks city's WiFi service using buffer-overflow exploit

SC Magazine-Nov 15, 2016

Researcher hacks city's WiFi service using buffer-overflow exploit ... Routers are increasingly used to launch DDoS attacks, although many ...

SQL Injection flaw found in Ninja Forms WordPress plugin

SC Magazine-Aug 17, 2016

A dangerous SQL Injection vulnerability has been disclosed and ... impacting the 600,000 sites using that website construction software.

IBM: Financial services industry bombarded by malware, security threats

IBM X Force says financial services are targeted 65% more by cyber-attacks than the average organization



Unpatched Vulnerability on Wix.com Puts Millions of Sites at Risk

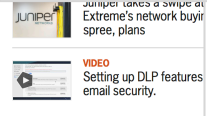
Threatpost-Nov 2, 2016

Update Cloud-based web host Wix.com is vulnerable to a DOM-based cross-site scripting vulnerability that can give attackers control over any ...

New Joomla SQL Injection Flaw Is Ridiculously Simple to Exploit

BleepingComputer-May 17, 2017

The Joomla CMS project released today Joomla 3.7.1 to fix an SQL injection flaw that allows attackers to execute custom SQL code on affected ...



Spotify Hacked? Thousands Of Accounts' Login Credentials ...

International Business Times-1 hour ago

If true, and your account details are in that list, it is all the more reason ... Late Monday night, a ... led the login credentials

Exploit kits, Slammer worm top April's most wanted malware list ...

SC Magazine-May 18, 2017

The worm- which exploits a buffer overflow bug in Microsoft's SQL ... Lotoor - Hack tool that exploits vulnerabilities on Android operating ...

TalkTalk hit by record £400000 fine over data breach

ComputerWeekly.com-Oct 5, 2016

"The attacker used a common technique known as SQL injection to access the data. SQL injection is well understood, defences exist and ...

Hacker Rasputin Breaches Over 60 Universities and Government ...

BleepingComputer-Feb 15, 2017

Hacker Rasputin Breaches Over 60 Universities and the UK, and federal, state, and local SQL injection (SQLi) attacks, one of the ...

Building a Holistic Cyberhealth Immune System

Security Intelligence (blog)-May 5, 2017

... SQL injection (SQLi) and OS command injection (CMDi) attacks representing a combined 48 percent of attacks in 2016. Health care records

XSS flaw found in the Google's PHP API client enables phishing ...

SC Magazine UK-May 15, 2017

XSS flaw found in the Google's PHP API client enables phishing attacks ... of the cross-site scripting flaw carry out a phishing attack.

Critical Medical Equipment Vulnerable to LDAP and SQL Injection ...

Softpedia News-Dec 2, 2015

According to Alex Lauerman of TrustFoundry, the older 3.3 branch of this tool is vulnerable to SQL and LDAP injection attacks (CVE-2015-6537 ...

Researcher hacks city's WiFi service using buffer-overflow exploit

SC Magazine-Nov 15, 2016

Researcher hacks city's WiFi service using buffer-overflow exploit ... Routers are increasingly used to launch DDoS attacks, although many ...

SQL Injection flaw found in Ninja Forms WordPress plugin

SC Magazine-Aug 17, 2016

A dangerous **SQL Injection** vulnerability has been disclosed and ... impacting the 600,000 sites using that website construction software.

IBM: Financial services industry bombarded by malware, security threats

IBM X Force says financial services are targeted 65% more by cyber-attacks than the average organization



Unpatched Vulnerability on Wix.com Puts Millions of Sites at Risk

Threatpost-Nov 2, 2016

Update Cloud-based web host Wix.com is vulnerable to a DOM-based **cross-site scripting** vulnerability that can give attackers control over any ...

New Joomla SQL Injection Flaw Is Ridiculously Simple to Exploit

BleepingComputer-May 17, 2017

The Joomla CMS project released today Joomla 3.7.1 to fix an **SQL injection** flaw that allows attackers to execute custom SQL code on affected ...

Spotify Hacked? Thousands Of Accounts' Login Credentials ...

International Business Times-1 hour ago
If true, and your account details are in that list, it is all the more reason ... Late Monday night, a credentials

A lot of these are result of common coding errors, especially missing input validation

TalkTalk hit by record £400000 fine over data breach

ComputerWeekly.com-Oct 5, 2016

"The attacker used a common technique known as **SQL injection** to access the data. **SQL injection** is well understood, defences exist and ...

Hacker Rasputin Breaches Over 60 Universities and Government ...

BleepingComputer-Feb 15, 2017

Hacker Rasputin Breaches Over 60 Universities and the UK, and federal, state, and local **SQL injection (SQLi)** attacks, one of the

Building a Holistic Cyberhealth Immune System

Security Intelligence (blog)-May 5, 2017

... **SQL injection (SQLi)** and **OS command injection (CMDi)** attacks representing a combined 48 percent of attacks in 2016. Health care records

XSS flaw found in the Google's PHP API client enables phishing ...

SC Magazine UK-May 15, 2017

XSS flaw found in the Google's PHP API client enables phishing attacks ... of the cross-site scripting flaw carry out a phishing attack.

Critical Medical Equipment Vulnerable to LDAP and SQL Injection ...

Softpedia News-Dec 2, 2015

According to Alex Lauerman of TrustFoundry, the older 3.3 branch of this tool is vulnerable to **SQL and LDAP injection** attacks (CVE-2015-6537 ...

So, when to fix these issues?

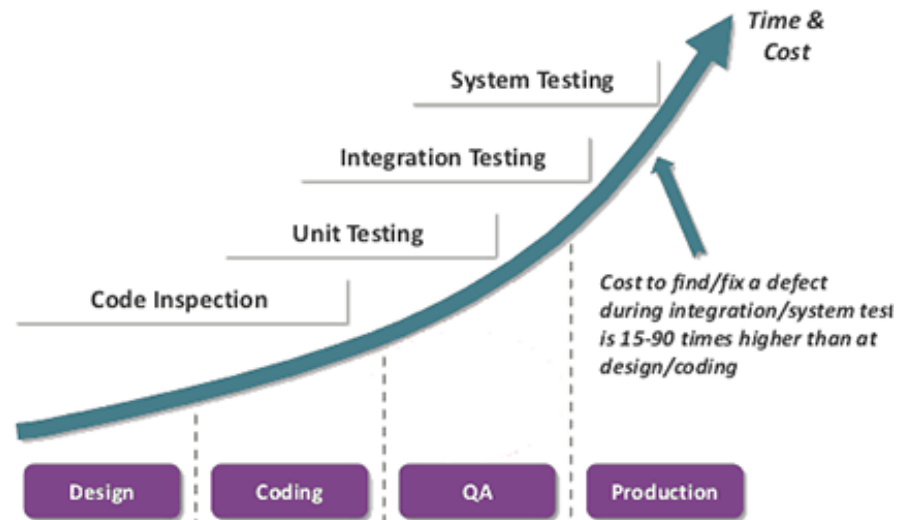


Image source: Checkmarx, Data source: NIST

So, when to fix these issues?

Better to do at coding phase!

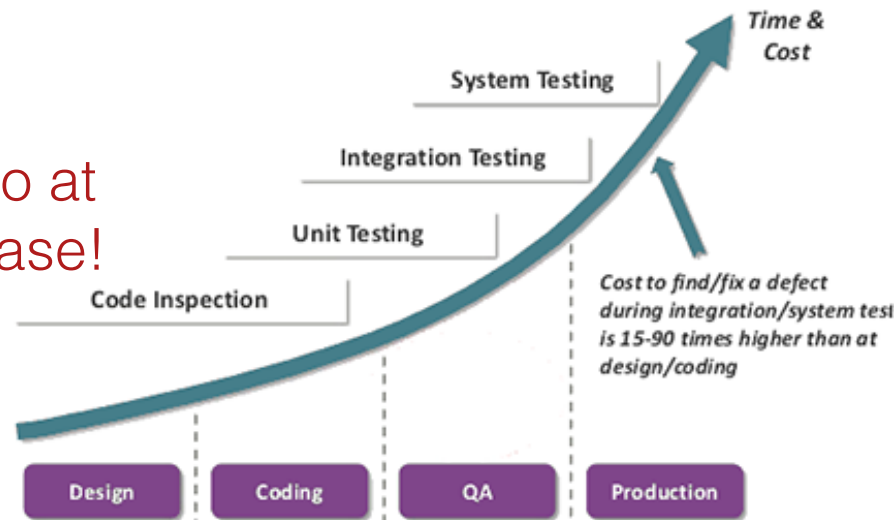
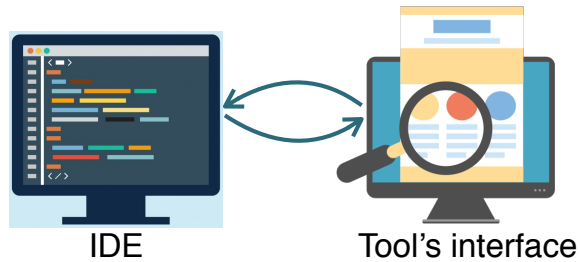


Image source: Checkmarx, Data source: NIST

Problems with secure coding with analysis tools

Problems with secure coding with analysis tools

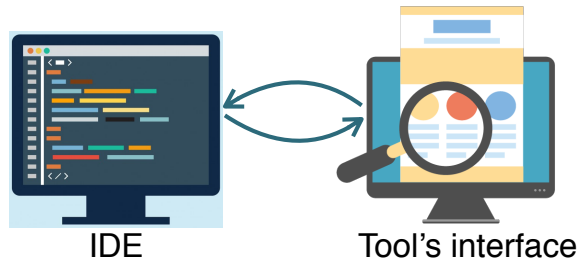


► Separate tool disrupts work-flow

Reference:

1. Johnson *et al.*, “Why don’t software developers use static analysis tools to find bugs?”, ICSE’13
2. Oliveira *et al.*, “It’s the psychology stupid: how heuristics explain software vulnerabilities and how priming can illuminate developer’s blind spots”, ACSAC’14

Problems with secure coding with analysis tools



- ▶ Separate tool disrupts work-flow

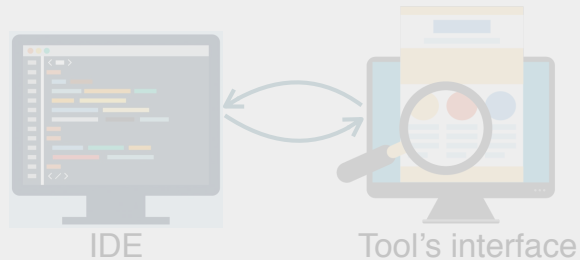


- ▶ Correlating previously learned security issues with code in hand is hard
- ▶ Outputs are hard to understand

Reference:

1. Johnson *et al.*, “Why don’t software developers use static analysis tools to find bugs?”, ICSE’13
2. Oliveira *et al.*, “It’s the psychology stupid: how heuristics explain software vulnerabilities and how priming can illuminate developer’s blind spots”, ACSAC’14

Problems with secure coding with analysis tools

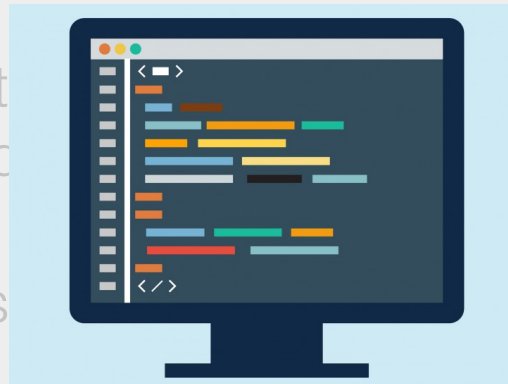


► Separate tool disrupts work-flow

More helpful ..



- Correlate security issues with code
- Outputs and



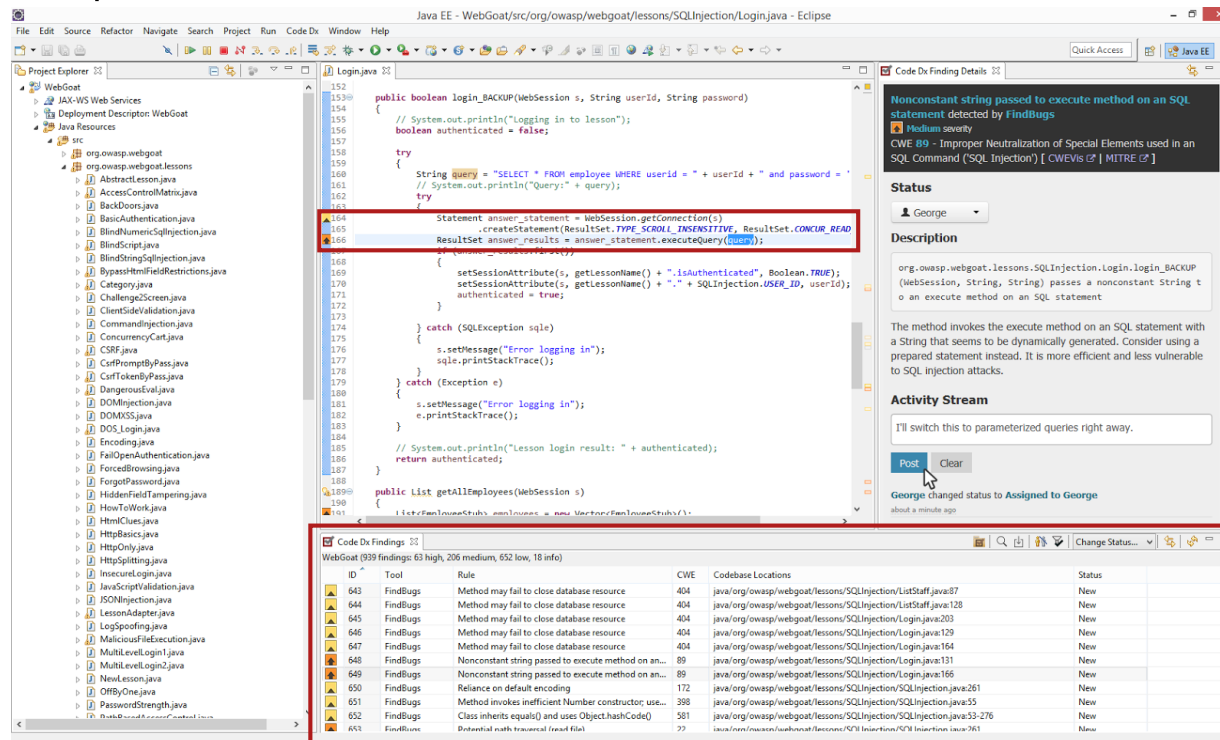
IDE + security analysis

Reference:

1. Johnson *et al.*, “Why don’t software developers use static analysis tools to find bugs?”, ICSE’13
2. Oliveira *et al.*, “It’s the psychology stupid: how heuristics explain software vulnerabilities and how priming can illuminate developer’s blind spots”, ACSAC’14

IDE security plugins

- ▶ Start analysis within IDE
- ▶ Compiler like output
 - list of identified flaws in an informational pane
 - problem markers in code editor



Source: Code DX

This work

This work



- ▶ Availability + Source code + IDE and language support + Feedback styles + Features + Vulnerability support + Uptake + ..

This work



- ▶ Availability + Source code + IDE and language support + Feedback styles + Features + Vulnerability support + Uptake + ..



- ▶ Plugin listings of IDEs + Static analysis tool lists + Academic papers + Forum discussions

This work



- ▶ Availability + Source code + IDE and language support + Feedback styles + Features + Vulnerability support + Uptake + ..

- ▶ Focus on **input-validation-related** vulnerabilities

- ▶ From the **perspective of a regular developer**



- ▶ Plugin listings of IDEs + Static analysis tool lists + Academic papers + Forum discussions

We got ...

Android Lint
ASIDE
Checkmarx CxSAST
CodeDX
Codepro AnalytiX
ESVD
Findbugs
Fortify
FxCop
Goanna Studio
Klocwork Insight
LAPSE+
SecureAssist
SensioLabsInsight
SonarLint
SSVChecker
Veracode

We got ...

Android Lint

ASIDE

Checkmarx CxSAST

CodeDX

Codepro AnalytiX

ESVD

Findbugs

Fortify

FxCop

Goanna Studio

Klocwork Insight

LAPSE+

SecureAssist

SensioLabsInsight

SonarLint

SSVChecker

Veracode

► Total 17 plugins

We got ...

Android Lint



ASIDE

Checkmarx CxSAST

CodeDX

Codepro AnalytiX



ESVD

Findbugs

Fortify

FxCop

Goanna Studio

Klocwork Insight



LAPSE+

SecureAssist

SensioLabsInsight

SonarLint







SSVChecker

Veracode

► Total 17 plugins

► 4 of them are academic

	Availability
Android Lint	Free and open source
 ASIDE	Free and open source
Checkmarx CxSAST	Commercial
CodeDX	Commercial
Codepro AnalytiX	Free
 ESVD	Free
Findbugs	Free and open source
Fortify	Commercial
FxCop	Free
Goanna Studio	Commercial
Klocwork Insight	Commercial
 LAPSE+	Free and open source
SecureAssist	Commercial
SensioLabsInsight	Both
SonarLint	Free and open source
 SSVChecker	Free
Veracode	Commercial





	Availability
Android Lint	Free and open source
🎓 ASIDE	Free and open source
Checkmarx CxSAST	Commercial
CodeDX	Commercial
Codepro AnalytiX	Free
🎓 ESVD	Free
Findbugs	Free
Fortify	Com
FxCop	Free
Goanna Studio	Commercial
Klocwork Insight	Commercial
🎓 LAPSE+	Free and open source
SecureAssist	Commercial
SensioLabsInsight	Both
SonarLint	Free and open source
🎓 SSVChecker	Free
Veracode	Commercial



How easy/hard to access security plugins?

► 9 free, 8 commercial

► 5 open source

	Availability	Introduced	Last update
Android Lint	Free and open source	—	—
 ASIDE	Free and open source	Feb 2013	Sept 2014
Checkmarx CxSAST	Commercial	—	—
CodeDX	Commercial	Jan 2015	Feb/Mar 2016
Codepro AnalytiX	Free	Feb 2005	Oct 2010
 ESVD	Free	July 2014	Nov 2016
Findbugs	Free and open source	—	—
Fortify	Commercial	—	Feb/Mar 2017
FxCop	Free	—	—
Goanna Studio	Commercial	—	—
Klocwork Insight	Commercial	—	—
 LAPSE+	Free and open source	Mar 2011	Mar 2011
SecureAssist	Commercial	—	—
SensioLabsInsight	Both	Oct 2014	Jan 2017
SonarLint	Free and open source	Oct 2015	Feb 2017
 SSVChecker	Free	May 2010	Nov 2016
Veracode	Commercial	—	Feb 2017

	Availability	Introduced	Last update
Android Lint	Free and open source	—	—
ASIDE	Free and open source	Feb 2013	Sept 2014
Checkmarx CxSAST	Commercial	—	—
CodeDX	Commercial	Jan 2015	Feb/Mar 2016
Codepro Analy	—	—	Oct 2010
ESVD	—	—	Nov 2016
Findbugs	—	—	—
Fortify	—	—	Feb/Mar 2017
FxCop	—	—	—
Goanna Studio	Commercial	—	—
Klocwork Insight	Commercial	—	—
LAPSE+	Free and open source	Mar 2011	Mar 2011
SecureAssist	Commercial	—	—
SensioLabsInsight	Both	Oct 2014	Jan 2017
SonarLint	Free and open source	Oct 2015	Feb 2017
SSVChecker	Free	May 2010	Nov 2016
Veracode	Commercial	—	Feb 2017



Is there continued support?

- ▶ mostly yes
- ▶ no for 2 of the academics

	Availability	Introduced	Last update
Android Lint	Free and open source	—	—
ASIDE	Free and open source	Feb 2013	Sept 2014
Checkmarx CxSAST	Commercial	—	—
CodeDX	Commercial	Jan 2015	Feb/Mar 2016
Codepro Analy	—	—	Oct 2010
ESVD	—	—	Nov 2016
Findbugs	—	—	—
Fortify	—	—	Feb/Mar 2017
FxCop	—	—	—
Goanna Studio	Commercial	—	—
Klocwork Insight	Commercial	—	—
LAPSE+	Free and open source	Mar 2011	Mar 2011
SecureAssist	Commercial	—	—
SensioLabsInsight	Both	Oct 2014	Jan 2017
SonarLint	Free and open source	Oct 2015	Feb 2017
SSVChecker	Free	May 2010	Nov 2016
Veracode	Commercial	—	Feb 2017








Is there continued support?

- ▶ mostly yes
- ▶ no for 2 of the academics



No recent update does not necessarily mean missed

 Android Lint
 ASIDE
 Checkmarx CxSAST
 CodeDX
 Codepro AnalytiX
 ESVD
 Findbugs
 Fortify
 FxCop
 Goanna Studio
 Klocwork Insight
 LAPSE+
 SecureAssist
 SensioLabsInsight
 SonarLint
 SSVChecker
 Veracode

Supported IDEs

Eclipse ▫ Android Studio
 Eclipse
 Eclipse ▫ Visual Studio ▫ IntelliJ
 Eclipse ▫ Visual Studio
 Eclipse
 Eclipse
 Eclipse ▫ NetBeans ▫ IntelliJ ▫ Android Studio
 Eclipse ▫ Visual Studio
 Visual Studio
 Eclipse ▫ Visual Studio
 Eclipse ▫ Visual Studio ▫ IntelliJ
 Eclipse
 Eclipse ▫ Visual Studio ▫ IntelliJ
 PHPStorm
 Eclipse ▫ Visual Studio ▫ IntelliJ
 Eclipse
 Eclipse ▫ Visual Studio ▫ IntelliJ

Languages/Platforms















































   
 
     
  
  





 
    

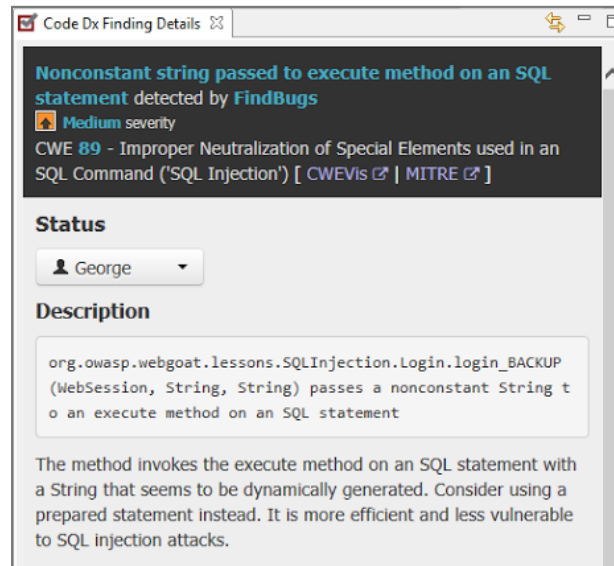
    
       

	Supported IDEs	Languages/Platforms
Android Lint	Eclipse ▫ Android Studio	   
 ASIDE	Eclipse	 
Checkmarx CxSAST	Eclipse ▫ Visual Studio ▫ IntelliJ	     
CodeDX	Eclipse ▫ Visual Studio	  
Codepro AnalytiX	Eclipse	  
 ESVD	 Do these plugins support mainstream IDEs and languages/platforms? <ul style="list-style-type: none"> ▸ mostly yes ▸ but not much focused on mobile platforms like Android 	
Findbugs		
Fortify		
FxCop		
Goanna Studio		
Klocwork Insight	Eclipse ▫ Visual Studio ▫ IntelliJ	 
 LAPSE+	Eclipse	
SecureAssist	Eclipse ▫ Visual Studio ▫ IntelliJ	  
SensioLabsInsight	PHPStorm	
SonarLint	Eclipse ▫ Visual Studio ▫ IntelliJ	    
 SSVChecker	Eclipse	  
Veracode	Eclipse ▫ Visual Studio ▫ IntelliJ	       

	Vulnerability description
Android Lint	Short
 ASIDE	Detailed
Checkmarx CxSAST	Detailed
CodeDX	Short
Codepro AnalytiX	Detailed
 ESVD	Just vuln. name
Findbugs	Detailed
Fortify	Detailed
FxCop	Short
Goanna Studio	Detailed
Klocwork Insight	Detailed
 LAPSE+	Just rule name
SecureAssist	Detailed
SensioLabsInsight	Short
SonarLint	Short
 SSVChecker	Short
Veracode	Detailed

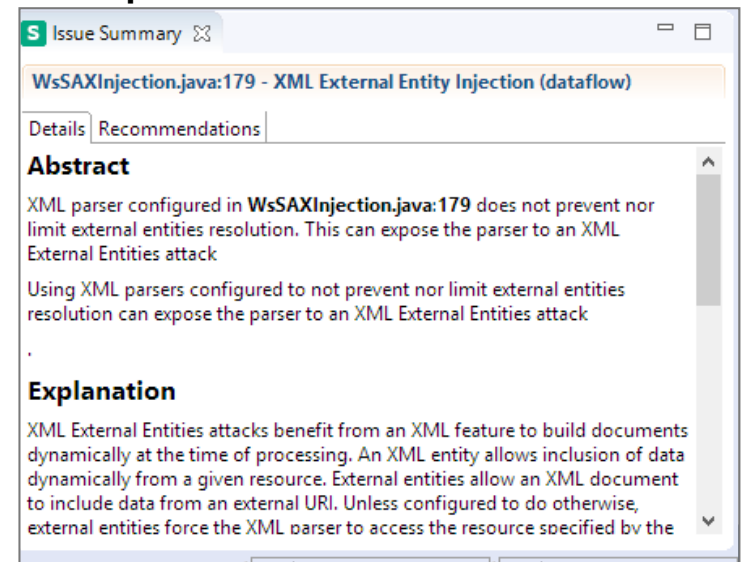
	Android Lint	Short
🎓	ASIDE	Detailed
	Checkmarx CxSAST	Detailed
	CodeDX	Short
	Codepro AnalytiX	Detailed
🎓	ESVD	Just vuln. name
	Findbugs	Detailed
	Fortify	Detailed
	FxCop	Short
	Goanna Studio	Detailed
	Klocwork Insight	Detailed
🎓	LAPSE+	Just rule name
	SecureAssist	Detailed
	SensioLabsInsight	Short
	SonarLint	Short
🎓	SSVChecker	Short
	Veracode	Detailed

Example: Short







Source: CodeDx

Example: Detailed



Source: Fortify

	Vulnerability description	Mitigation
Android Lint	Short	—
 ASIDE	Detailed	Quick fix
Checkmarx CxSAST	Detailed	—
CodeDX	Short	—
Codepro AnalytiX	Detailed	Quick fix
 ESVD	Just vuln. name	—
Findbugs	Detailed	—
Fortify	Detailed	General
FxCop	Short	General
Goanna Studio	Detailed	—
Klocwork Insight	Detailed	General
 LAPSE+	Just rule name	—
SecureAssist	Detailed	General
SensioLabsInsight	Short	—
SonarLint	Short	—
 SSVChecker	Short	—
Veracode	Detailed	General







	Vulnerability description	Mitigation	Select/unselect checks	Suppress warnings
Android Lint	Short	—	✓	✓
ASIDE	Detailed	Quick fix	—	—
Checkmarx CxSAST	Detailed	—	—	—
CodeDX	Short	—	—	✓
Codepro AnalytiX	Detailed	Quick fix	—	—
ESVD	Just vuln. name	—	—	—
Findbugs	Detailed	—	—	—
Fortify	Detailed	General	—	—
FxCop	Short	General	—	✓
Goanna Studio	Detailed	—	✓	✓
Klocwork Insight	Detailed	General	—	—
LAPSE+	Just rule name	—	—	—
SecureAssist	Detailed	General	—	—
SensioLabsInsight	Short	—	—	—
SonarLint	Short	—	—	—
SSVChecker	Short	—	—	✓
Veracode	Detailed	General	—	—

	CWE 20 Improper Input Validation	CWE 77 Command Injection	CWE 77 OS Command Injection	CWE 20 Cross-site scripting	CWE 77 SQL Injection	CWE 77 LDAP Injection	CWE 20 XML Injection	CWE 77 Unsafe Reflection	CWE 77 Path Injection
Android Lint	—	—	—	—	—	—	✓	—	—
ASIDE	✓	—	—	—	—	—	—	—	—
Checkmarx CxSAST	—	✓	✓	✓	✓	✓	—	—	✓
CodeDX									
Codepro AnalytiX									
ESVD	—	✓	—	✓	✓	✓	—	✓	✓
Findbugs	—	✓	✓	✓	✓	✓	—	—	✓
Fortify	—	—	—	✓	✓	—	—	—	—
FxCop	—	—	—	✓	✓	—	—	—	—
Goanna Studio	—	✓	✓	—	—	—	—	—	—
Klocwork Insight	—	—	—	✓	✓	—	—	—	—
LAPSE+	—	✓	—	✓	✓	✓	✓	—	✓
SecureAssist	—	—	—	—	✓	✓	—	—	—
SensioLabsInsight									
SonarLint	—	—	—	—	✓	—	—	—	—
SSVChecker									
Veracode	—	—	—	—	✓	—	—	—	—

	CWE 20 Improper Input Validation	CWE 77 Command Injection	CWE 77 OS Command Injection	CWE 20 Cross-site scripting	CWE 77 SQL Injection	CWE 77 LDAP Injection	CWE 20 XML Injection	CWE 77 Unsafe Reflection	CWE 77 Path Injection
Android Lint	—	—	—	—	—	—	✓	—	—
ASIDE	✓	—	—	—	—	—	—	—	—
Checkmarx CxSAST	—	✓	✓	✓	✓	✓	—	—	✓
CodeDX	—	—	—	—	—	—	—	—	—
Codepro AnalytiX	—	—	—	—	—	—	—	—	—
ESVD	—	✓	—	✓	✓	✓	—	✓	✓
Findbugs	—	✓	✓	✓	✓	✓	—	—	✓
Fortify	—	—	—	✓	✓	—	—	—	—
FxCop	—	—	—	—	—	—	—	—	—
Goanna Studio	—	✓	—	—	—	—	—	—	—
Klocwork Insight	—	—	—	—	—	—	—	—	—
LAPSE+	—	✓	—	✓	✓	✓	✓	—	✓
SecureAssist	—	—	—	—	✓	✓	—	—	—
SensioLabsInsight	—	—	—	—	—	—	—	—	—
SonarLint	—	—	—	—	✓	—	—	—	—
SSVChecker	—	—	—	—	—	—	—	—	—
Veracode	—	—	—	—	✓	—	—	—	—



Uses multiple tools, combined list is not available






 Android Lint
 ASIDE
 Checkmarx CxSAST
 CodeDX
 Codepro AnalytiX
 ESVD
 Findbugs
 Fortify
 FxCop
 Goanna Studio
 Klocwork Insight
 LAPSE+
 SecureAssist
 SensioLabsInsight
 SonarLint
 SSVChecker
 Veracode

	CWE 20 Improper Input Validation	CWE 77 Command Injection	CWE 77 OS Command Injection	CWE 20 Cross-site scripting	CWE 77 SQL Injection	CWE 77 LDAP Injection	CWE 20 XML Injection	CWE 77 Unsafe Reflection	CWE 77 Path Injection
Android Lint	—	—	—	—	—	—	✓	—	—
ASIDE	✓	—	—	—	—	—	—	—	—
Checkmarx CxSAST	—	✓	✓	✓	✓	✓	—	—	✓
CodeDX	—	—	—	—	—	—	—	—	—
Codepro AnalytiX	—	—	—	—	—	—	—	—	—
ESVD	—	✓	—	✓	✓	✓	—	✓	✓
Findbugs	—	✓	✓	✓	✓	✓	—	—	✓
Fortify	—	—	—	✓	✓	—	—	—	—
FxCop	—	—	—	—	—	—	—	—	—
Goanna Studio	—	✓	✓	—	—	—	—	—	—
Klocwork Insight	—	—	—	✓	✓	—	—	—	—
LAPSE+	—	✓	—	✓	✓	✓	✓	—	✓
SecureAssist	—	—	—	—	✓	✓	—	—	—
SensioLabsInsight	—	—	—	—	—	—	—	—	—
SonarLint	—	—	—	—	✓	—	—	—	—
SSVChecker	—	—	—	—	—	—	—	—	—
Veracode	—	—	—	—	✓	—	—	—	—



Full list is not available

	CWE 20 Improper Input Validation	CWE 77 Command Injection	CWE 77 OS Command Injection	CWE 20 Cross-site scripting	CWE 77 SQL Injection	CWE 77 LDAP Injection	CWE 20 XML Injection	CWE 77 Unsafe Reflection	CWE 77 Path Injection
Android Lint	—	—	—	—	—	—	✓	—	—
ASIDE	✓	—	—	—	—	—	—	—	—
Checkmarx CxSAST	—	✓	✓	✓	✓	✓	—	—	✓
CodeDX									
Codepro AnalytiX									
ESVD	—	✓	—	✓	✓	✓	—	✓	✓
Findbugs	—	✓	✓	✓	✓	✓	—	—	✓
Fortify	—	—	—	✓	✓	—	—	—	—
FxCop	—	—	—	✓	✓	—	—	—	—
Goanna Studio	—	✓	✓	—	—	—	—	—	—
Klocwork Insight	—	—	—	✓	✓	—	—	—	—
LAPSE+	—	✓	—	✓	✓	✓	✓	—	✓
SecureAssist	—	—	—	—	✓	✓	—	—	—
SensioLabsInsight									
SonarLint	—	—	—	—	✓	—	—	—	—
SSVChecker									
Veracode	—	—	—	—	✓	—	—	—	—

 Android Lint
 ASIDE
 Checkmarx CxSAST
 CodeDX
 Codepro AnalytiX
 ESVD
 Findbugs
 Fortify
 FxCop
 Goanna Studio
 Klocwork Insight
 LAPSE+
 SecureAssist
 SensioLabsInsight
 SonarLint
 SSVChecker
 Veracode

	CWE 20 Improper Input Validation	CWE 77 Command Injection	CWE 77 OS Command Injection	CWE 20 Cross-site scripting	CWE 77 SQL Injection	CWE 77 LDAP Injection	CWE 20 XML Injection	CWE 77 Unsafe Reflection	CWE 77 Path Injection
Android Lint	—	—	—	—	—	—	✓	—	—
ASIDE	✓	—	—	—	—	—	—	—	—
Checkmarx CxSAST	—	✓	✓	✓	✓	✓	—	—	✓
CodeDX	—	—	—	—	—	—	—	—	—
Codepro AnalytiX	—	—	—	—	—	—	—	—	—
ESVD	—	✓	—	✓	✓	✓	—	✓	✓
Findbugs	—	✓	✓	✓	✓	✓	—	—	✓
Fortify	—	—	—	✓	✓	—	—	—	—
FxCop	—	—	—	✓	✓	—	—	—	—
Goanna Studio	—	✓	✓	—	—	—	—	—	—
Klocwork Insight	—	—	—	✓	✓	—	—	—	—
LAPSE+	—	✓	—	✓	✓	✓	✓	—	✓
SecureAssist	—	—	—	—	✓	✓	—	—	—
SensioLabsInsight	—	—	—	—	—	—	—	—	—
SonarLint	—	—	—	—	✓	—	—	—	—
SSVChecker	—	—	—	—	—	—	—	—	—
Veracode	—	—	—	—	✓	—	—	—	—



Most of the plugins support SQLi and XSS

What made us sad ..



- ▶ No separate “security” category in IDE plugin listings

What made us sad ..



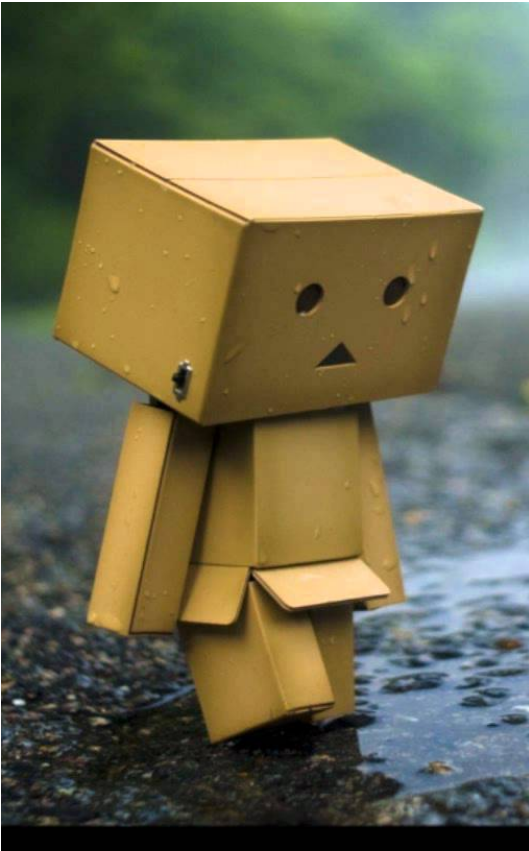
- ▶ No separate “security” category in IDE plugin listings
 - exception Visual Studio, though primarily intended for code obfuscation and group code access

What made us sad ..



- ▶ No separate “security” category in IDE plugin listings
 - exception Visual Studio, though primarily intended for code obfuscation and group code access
 - Visual Studio = 22, Eclipse = 51, IntelliJ = 50, NetBeans = 24

What made us sad ..



- ▶ No separate “security” category in IDE plugin listings
 - exception Visual Studio, though primarily intended for code obfuscation and group code access
 - Visual Studio = 22, Eclipse = 51, IntelliJ = 50, NetBeans = 24
- ▶ Lack of documentation about supported vulnerability checks

What made us sad ..



- ▶ No separate “security” category in IDE plugin listings
 - exception Visual Studio, though primarily intended for code obfuscation and group code access
 - Visual Studio = 22, Eclipse = 51, IntelliJ = 50, NetBeans = 24
- ▶ Lack of documentation about supported vulnerability checks
- ▶ No benchmark result on detection accuracy

What made us sad ..



- ▶ No separate “security” category in IDE plugin listings
 - exception Visual Studio, though primarily intended for code obfuscation and group code access
- ▶ **Frustrated developer → Low adoption**
Visual Studio = 22, Eclipse = 51, IntelliJ = 50, NetBeans = 24
- ▶ Lack of documentation about supported vulnerability checks
- ▶ No benchmark result on detection accuracy

So, what next ..

So, what next ..



- ▶ Initial setup
- ▶ Feedback style

So, what next ..



- ▶ Initial setup
- ▶ Feedback style



- ▶ Vulnerability detection performance
- ▶ Using existing (e.g., OWASP) or new

So, what next ..



- ▶ Initial setup
- ▶ Feedback style



- ▶ Vulnerability detection performance
- ▶ Using existing (e.g., OWASP) or new



- ▶ Applicability in programming language education
- ▶ Re-designing course/assignments to incorporate use of these IDE plugins

Thank You!



Aniqua Baset, aniqua@cs.utah.edu