Metrics for Insights on State of Application Security

Veracode, Inc.

Presented by:

Ashish Larivee, Veracode
Betsy Nichols, PlexLogic

VERACODE

Is there lead paint in your code?

Who we are

Ashish Larivee
Veracode

Ashish Larivee is currently Vice President of Business Development at Veracode and is responsible for driving Veracode's global partnering strategy. Previously, as Vice President of Product Management, she was responsible for the direction, definition and design of Veracode's core cloud-based security service and was a key contributor to the initial launch of the service as well as the company. As one of the early members of the team at Veracode, she was instrumental in defining and executing the strategic and technical vision of the company. Prior to Veracode, Ashish was Director of Product Marketing at Novell Inc. for their Identity, Access Management and Web Services business as well as having held several product strategy, marketing and technical positions at SilverStream and BBN. Ashish has her Masters in Computer Science and has been involved in the software industry for the last 18 years both in the U.S and in India.

Elizabeth A. Nichols, Ph.D.
PlexLogic

Betsy Nichols is Co-Founder and CTO of PlexLogic LLC. Over her 30 year career, she has applied mathematics and computer technologies to develop systems for war gaming, economic modeling, reliability growth analysis, system performance optimization, industrial process control, network and systems management, and most recently, security metrics. She has started three companies, the most recent being PlexLogic. Founded in 2008, PlexLogic offers a Metrics On-Demand service called MetricsCenter which offers both a for-profit security metrics service at www.metricscenter.net as well as an open and free public resource for security metrics at www.MetricsCenter.org. She has helped organize several MetriCon and MetriSEC Workshops and has contributed chapters on security metrics to two books: Andrew Jaquith's book published by Addison-Wesley in 2007 and a new O'Reilly book called "Beautiful Security" for release in April 2009. Betsy graduated with an A.B. from Vassar College and a Ph.D. in Mathematics from Duke University.

Outline

1. Basis for insights on software security

2. Dataset and Sample Distribution

3. Overall state of software security

4. Industry segment and supplier type

5. OWASP and SANS standards

6. Top Vulnerabilities in our dataset

7. Visualization aids

8. Technology

Background – Basis for insights

- For over three years, Veracode has been providing automated security analysis of software to large and small enterprises across various industry segments.

- One of the residual effects is the wealth of security metrics derived from the anonymized data across varied industries and types of applications.

- These metrics offer valuable insights on the quality of application security and issues related to the current state-of-practice and maturity of security in software.

- Veracode was founded in 2006 by application security experts from @stake, Guardent, Symantec, and VeriSign.

- Veracode provides automated security assessment capabilities in the cloud. Automated techniques include static binary analysis and dynamic analysis. Manual test data (if performed) is included in the analysis
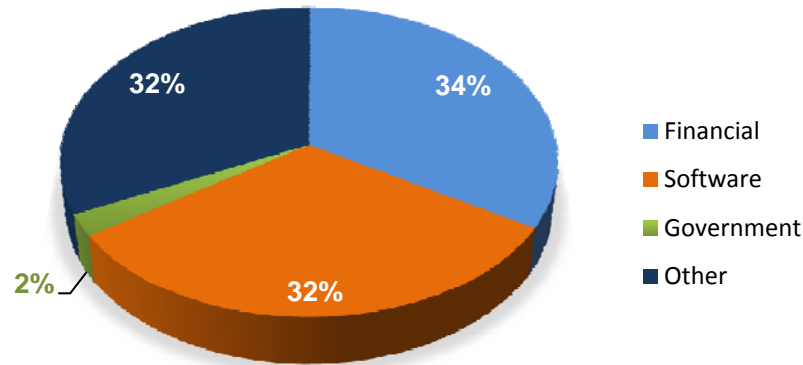
The Data Set + Metrics

- **Enterprise**
  - Industry vertical (enumerated)

- **Application**
  - Application Supplier Type (internal, purchased, outsourced, open source)
  - Application Type (Web facing / Non-web)
  - Assurance Level (1 to 5)
  - Language (enumerated)
  - Platform (enumerated)

- **Scan**
  - Scan Number
  - Scan Date
  - Lines of Code

- **Metrics**
  - Flaw Count
  - FlawPercent
  - ApplicationCount
  - First Scan Acceptance Rate
  - Veracode Risk Adjusted Score
  - MeanTimeBetweenScans
  - Days to Remediation
  - Scans to Remediation
  - PCI pass/fail
  - SANS Top25 pass/fail
  - OWASP pass/fail)
  - Two flavors: '04 and '07

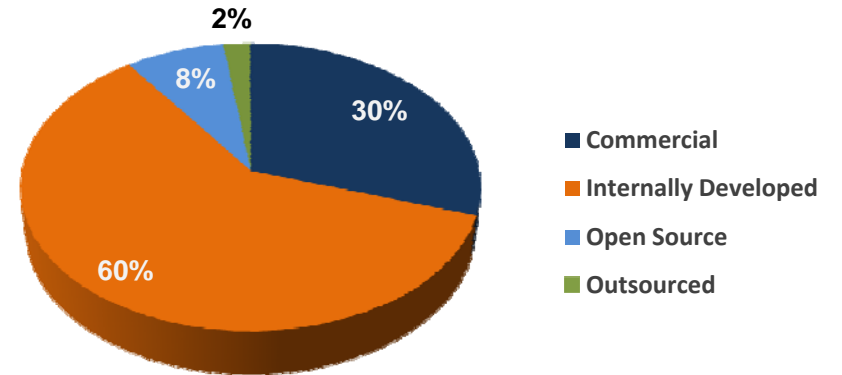# Good News – Statistically significant sample size

- **Sample size this large enable us to report findings with a reasonable degree of confidence:**
- **Type I Error**
  - Probability of stating that something is FALSE when it is in fact TRUE: < .05
- **Type II Error**
  - Probability of stating that something is TRUE when it is in fact FALSE: < .20
- **Margins of Error for estimates of various metrics:**
  - Flaw Count: 10%
  - First Scan Acceptance Rate: 15%
  - Veracode Risk Adjusted Score: 10%
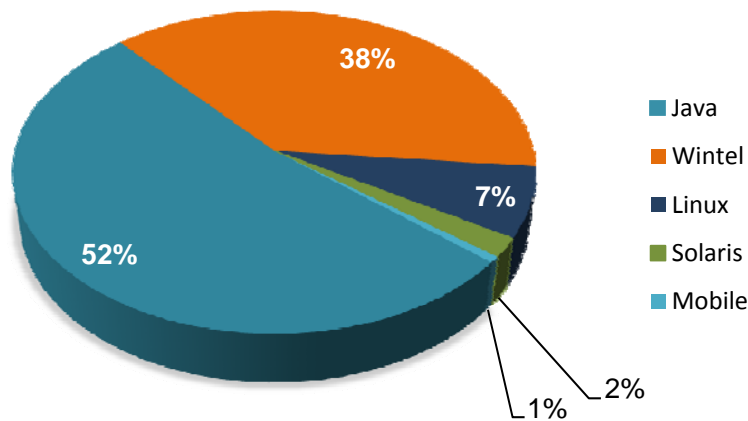 - Remediation Time: 10%
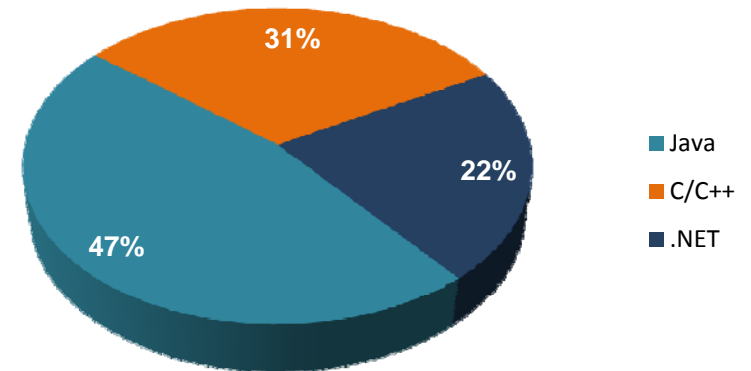
Sample Distribution

Applications by Industry

- Financial — 34%
- Software — 32%
- Government — 2%
- Other — 32%

Applications by Supplier

- Commercial — 30%
- Internally Developed — 60%
- Open Source — 8%
- Outsourced — 2%

Applications by Platform

- Java — 52%
- Wintel — 38%
- Linux — 7%
- Solaris — 2%
- Mobile — 1%

Applications by Language

- Java — 47%
- C/C++ — 31%
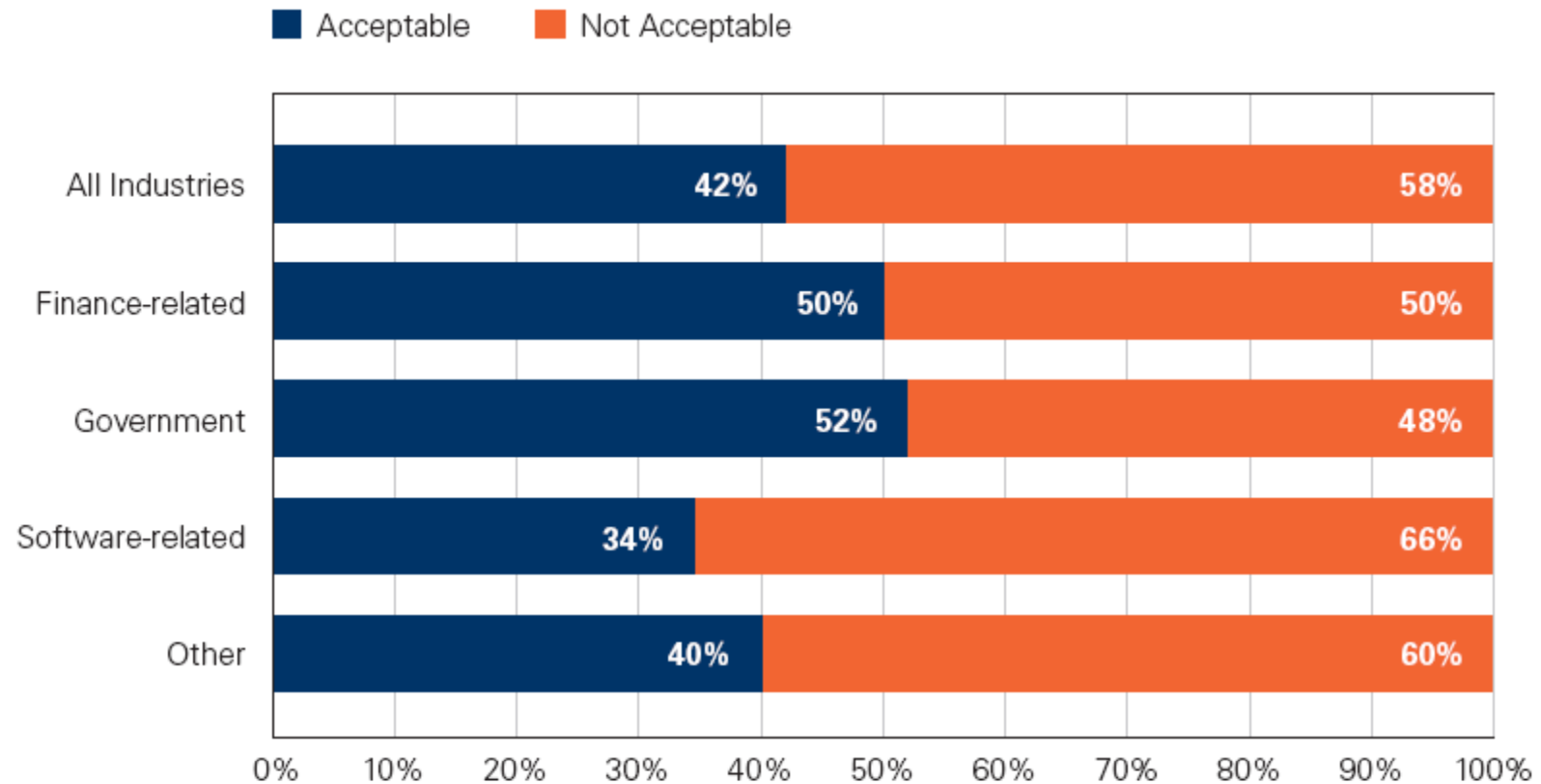- .NET — 22%

Majority of software is insecure

Pass: 42%

Fail: 58%

From all (self-selected) set of applications that were submitted to Veracode for assessment

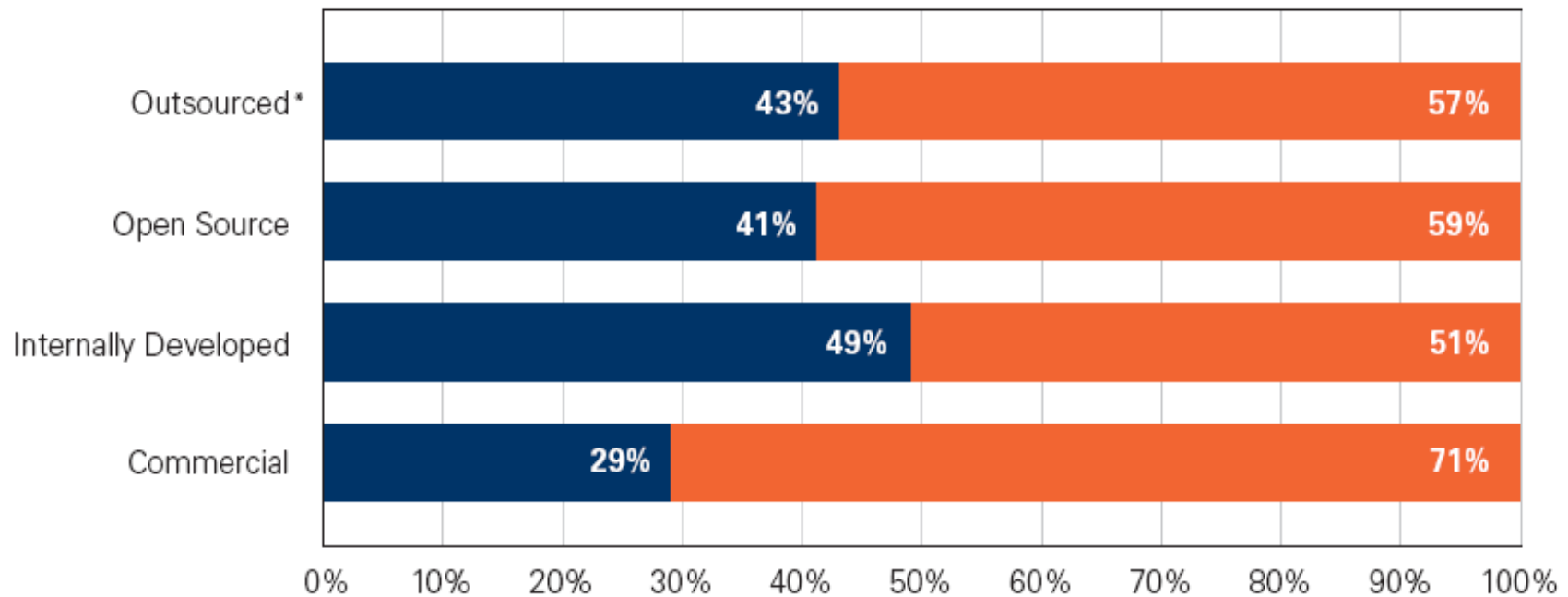# Financial Services and Government fare best
Software not so much

Application Performance by Industry on First Submission (Adjusted for Business Criticality)

■ Acceptable ■ Not Acceptable

Industry	Acceptable	Not Acceptable
All Industries	42%	58%
Finance-related	50%	50%
Government	52%	48%
Software-related	34%	66%
Other	40%	60%

Internal Apps have Best First Scan Acceptance Rate

**Supplier Performance on First Submission
(Adjusted for Business Criticality)**

■ Acceptable ■ Not Acceptable

Category	Acceptable	Not Acceptable
Outsourced*	43%	57%
Open Source	41%	59%
Internally Developed	49%	51%
Commercial	29%	71%

Commercial has longest remediation cycles

Remediation Performance by Supplier

Legend: Internally Developed | Commercial | Open Source | Overall

Average Days to Remediate:
- Internally Developed: 48
- Commercial: 82
- Open Source: 36
- Overall: 59

Average Remediation Submissions to Pass:
- Internally Developed: 1.42
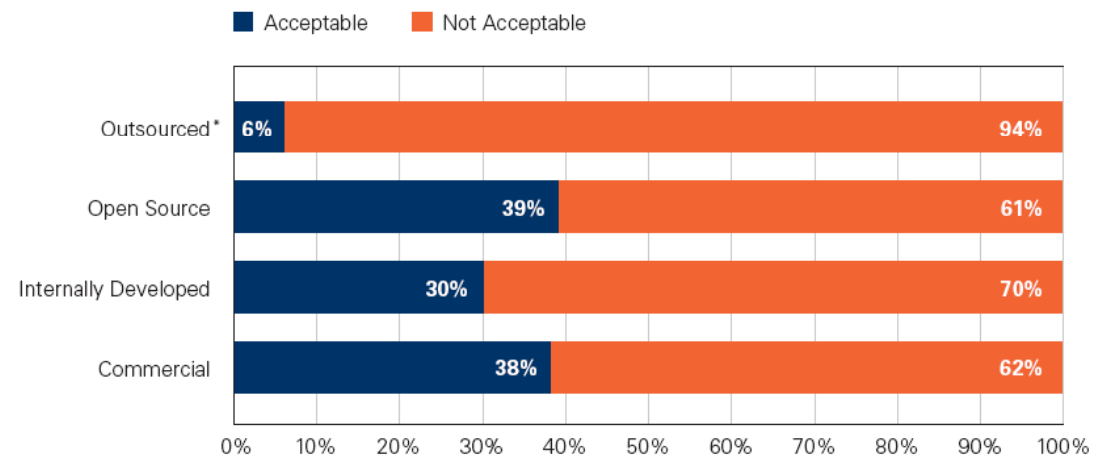- Commercial: 1.26
- Open Source: 1.11
- Overall: 1.36
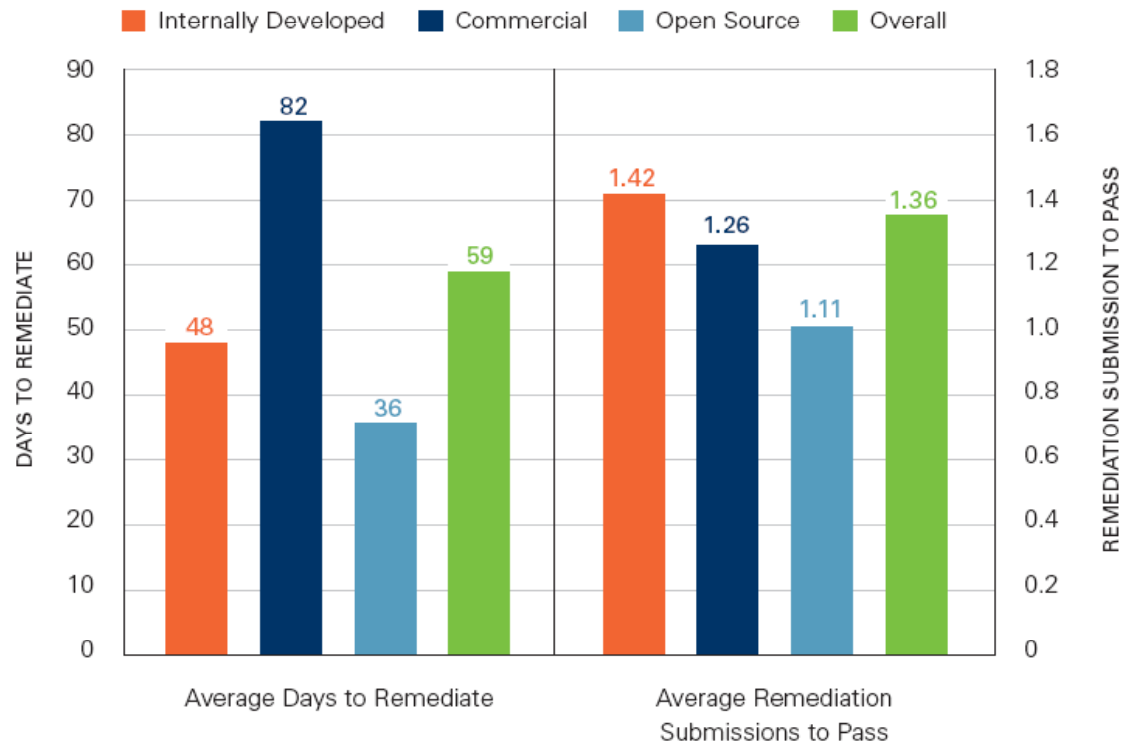
while Open Source is shortest

Majority not compliant with OWASP or SANS Top 25

OWASP Top 10 Compliance by Supplier on First Submission

■ Acceptable ■ Not Acceptable

Supplier	Acceptable	Not Acceptable
Outsourced*	4%	96%
Open Source	53%	47%
Internally Developed	12%	88%
Commercial	37%	63%

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
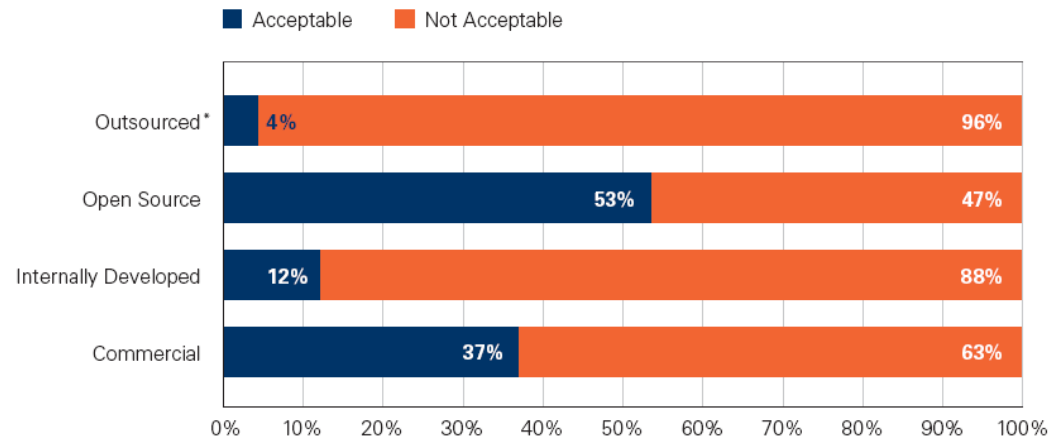
CWE/SANS Top 25 Compliance by Supplier on First Submission

■ Acceptable ■ Not Acceptable

Supplier	Acceptable	Not Acceptable
Outsourced*	6%	94%
Open Source	39%	61%
Internally Developed	30%	70%
Commercial	38%	62%

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

All Applications Suffer Least from SANS Top 25 Flaws
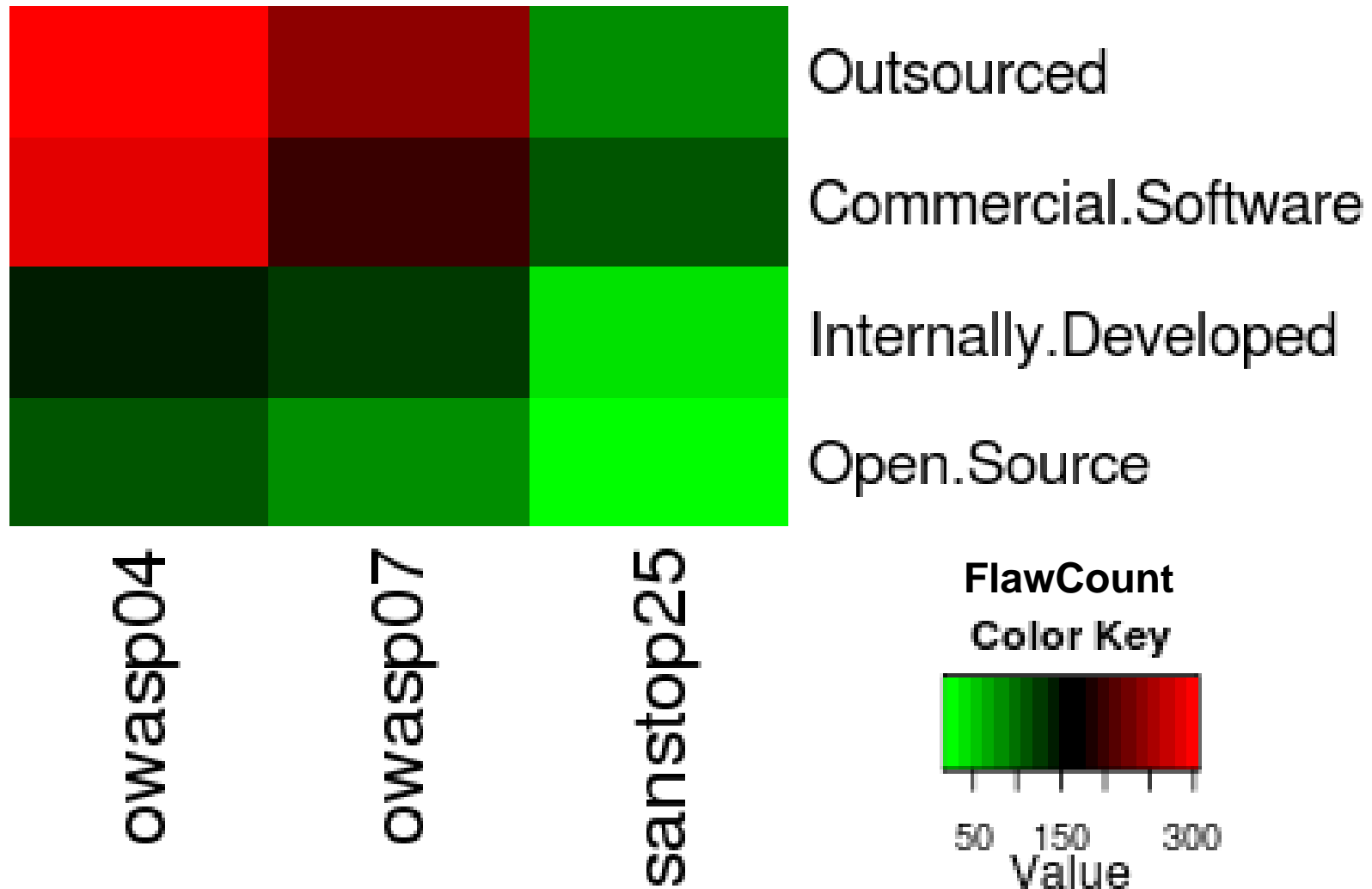
Cryptographic Issues Most Common in Applications

Top Vulnerability Categories (Percent of Application Affected)

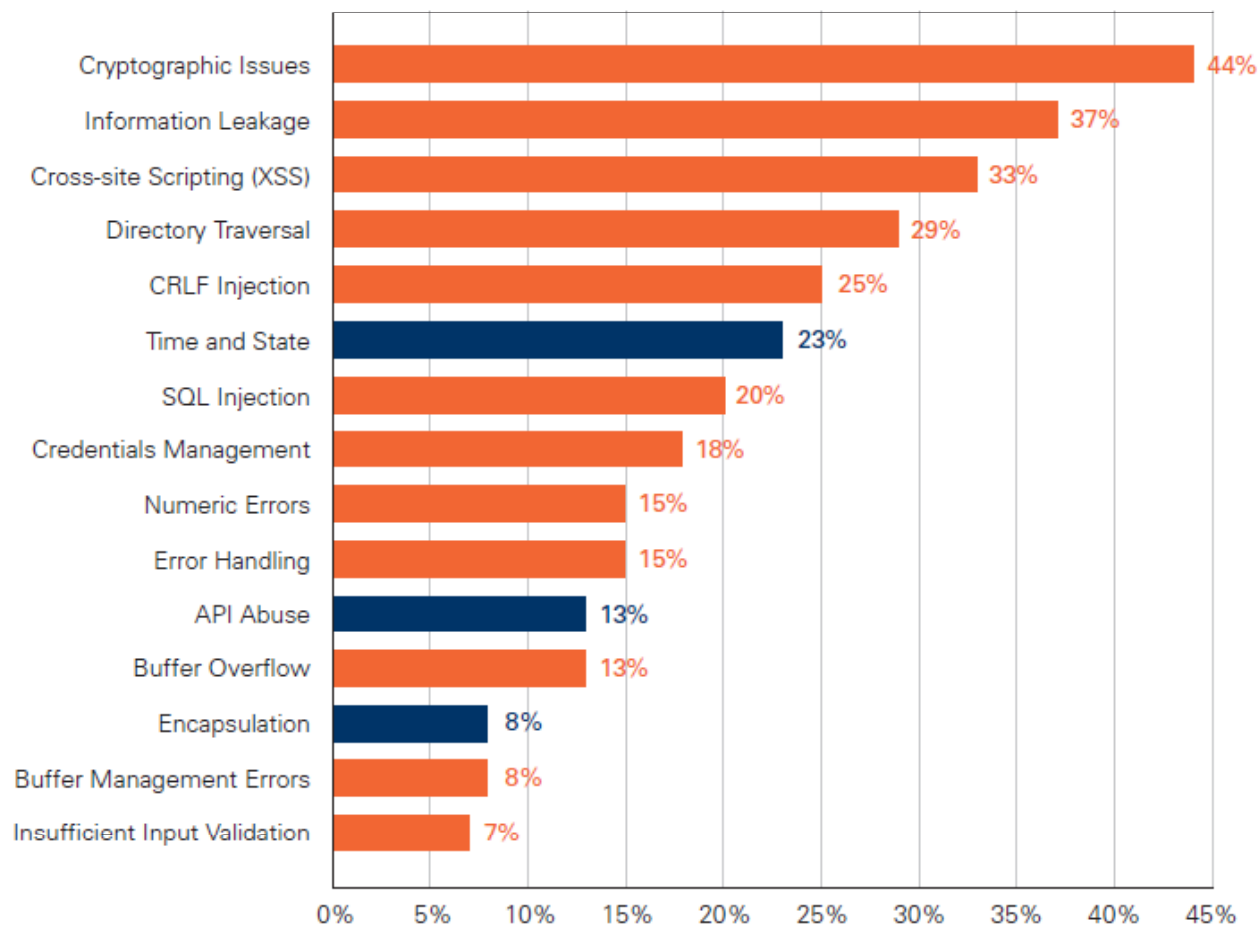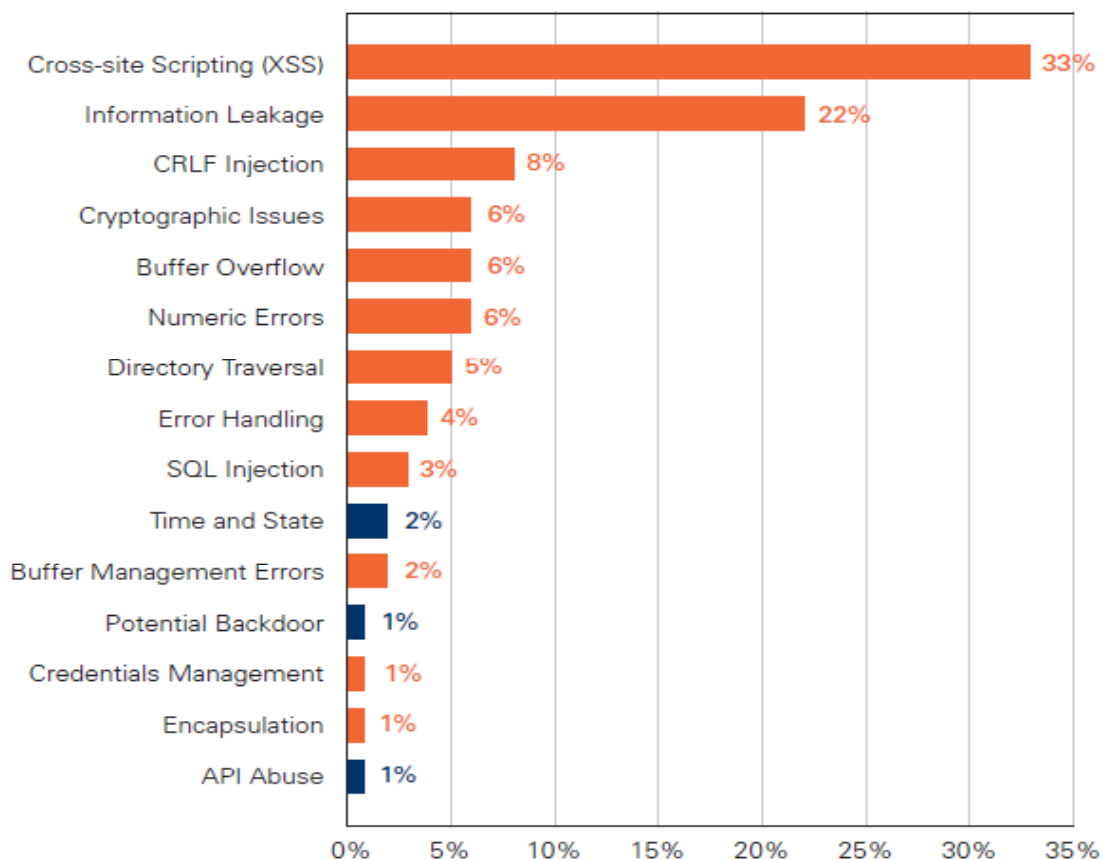■ Indicate categories that are in the OWASP Top 10
or CWE/SANS Top 25

Figure 11: Top Vulnerability Categories (Percent of Application Affected)

Cross-site Scripting easy to fix but still most prevalent

Top Vulnerability Categories (Overall Prevalence)

Indicate categories that are in the OWASP Top 10
or CWE/SANS Top 25

Category	Percent
Cross-site Scripting (XSS)	33%
Information Leakage	22%
CRLF Injection	8%
Cryptographic Issues	6%
Buffer Overflow	6%
Numeric Errors	6%
Directory Traversal	5%
Error Handling	4%
SQL Injection	3%
Time and State	2%
Buffer Management Errors	2%
Potential Backdoor	1%
Credentials Management	1%
Encapsulation	1%
API Abuse	1%

Figure 10: Top Vulnerability Categories (Overall Prevalence)

Flaw Percent = Flaw Count / Total

This yields a very Different List

Visualization using metrics – Fix First Chart

Remediation Effort
Hard — Easy

Plan to Fix — Fix Now

Severity Level
High
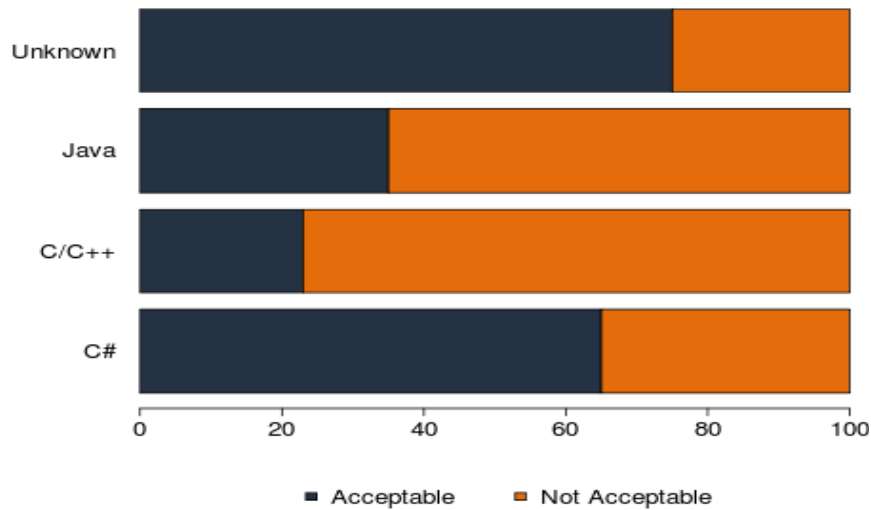Low

Accept Risk — Fix Later

Veracode recommends that developers prioritize remediation efforts in terms of a combination of flaw severity and effort, with high severity/low effort flaws being prioritized to "fix first".
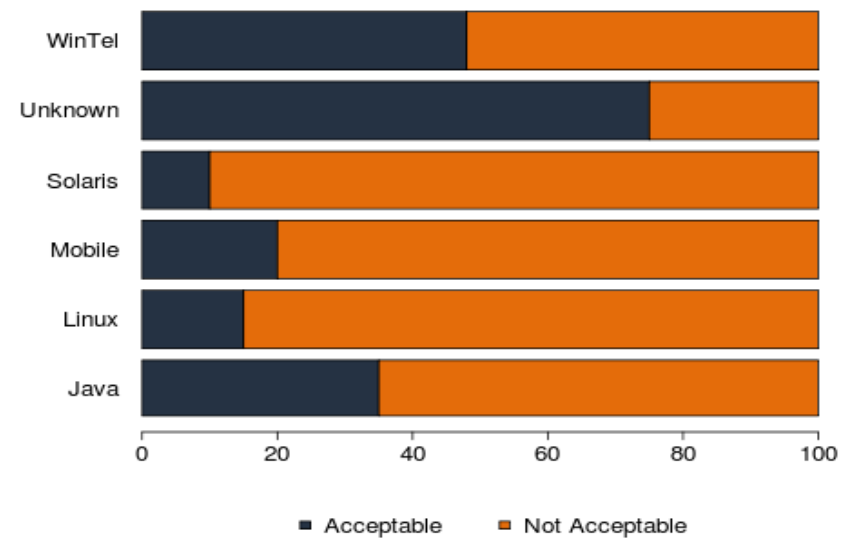
< Click on the red circles to the left to browse your application flaws by their "fix first" status.
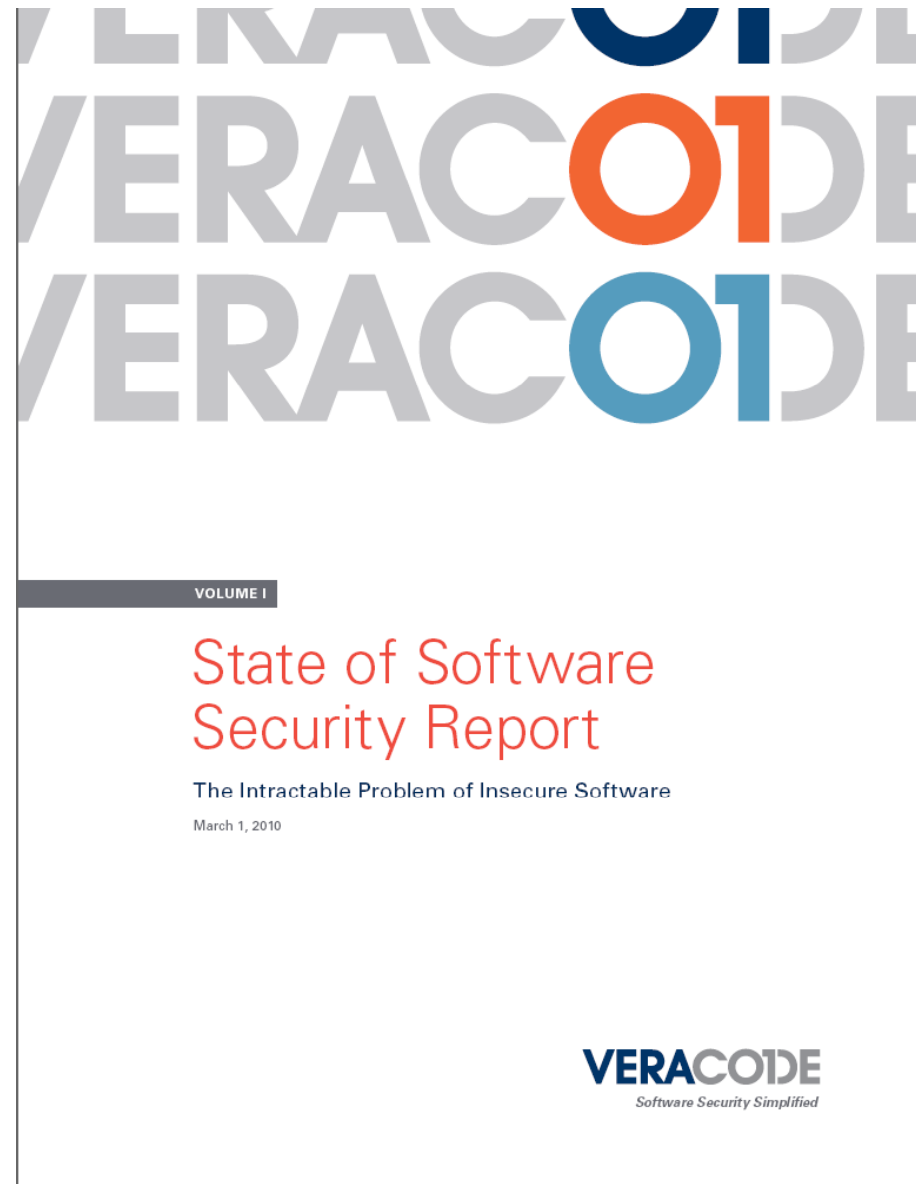
C# and WinTel Leads on First Scan Acceptance Rate

More in a detailed report launched today

Thank You

Questions?

VERACODE