



We See the Future and It Isn't Pretty

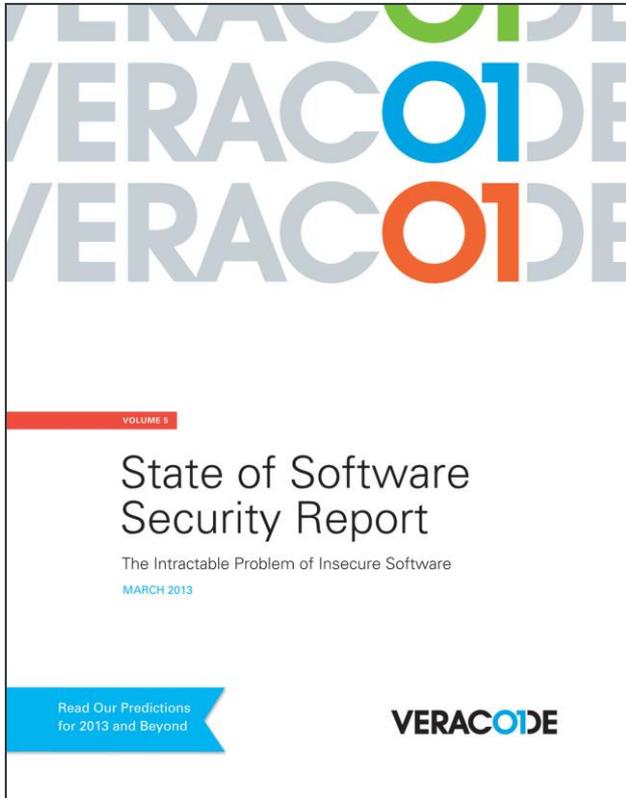
Chris Eng

Vice President of Research, Veracode

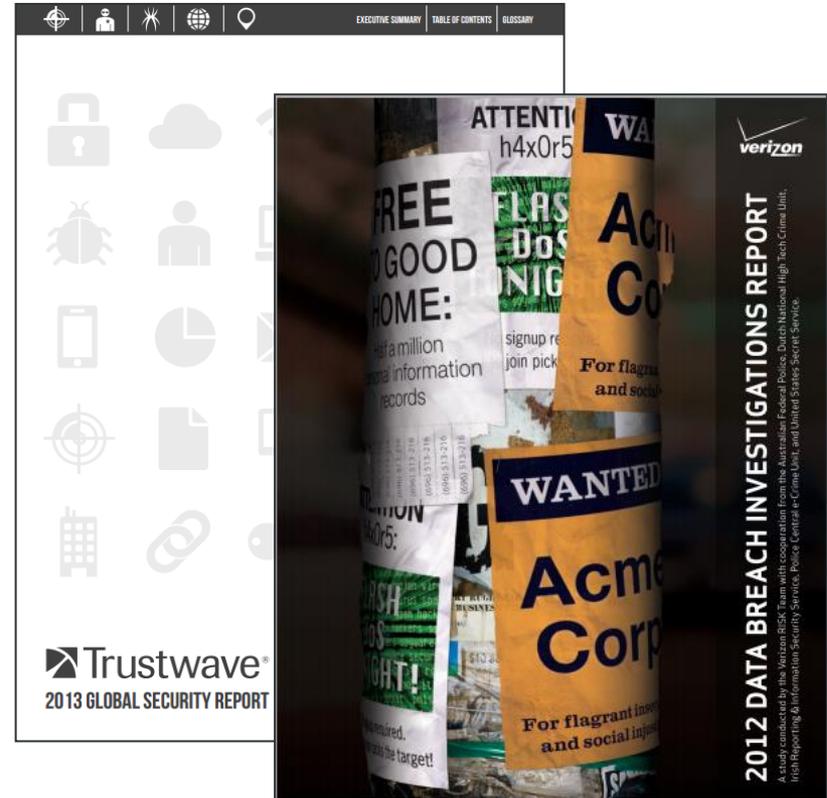
June 5, 2013

What is the SoSS Report?

SoSS is the “BEFORE”



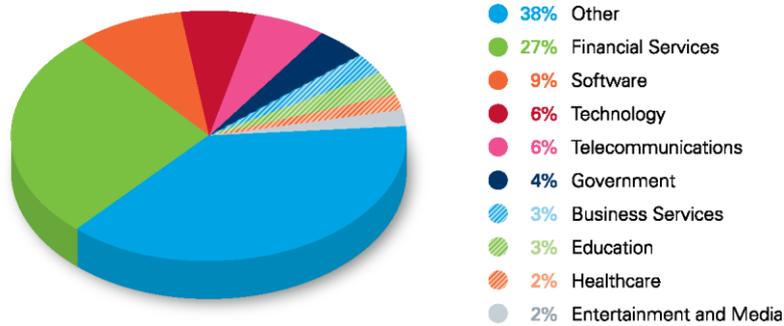
Breach Reports are the “AFTER”



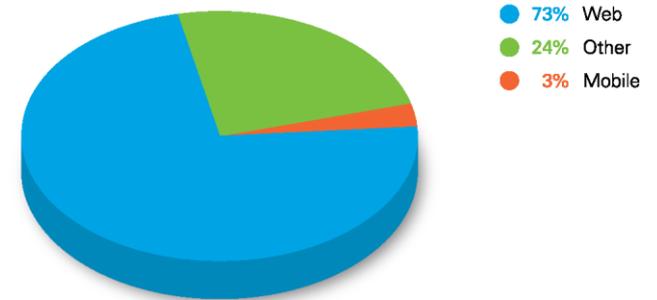
Dataset Overview

22,430 application builds from Jan 2011 to Jun 2012

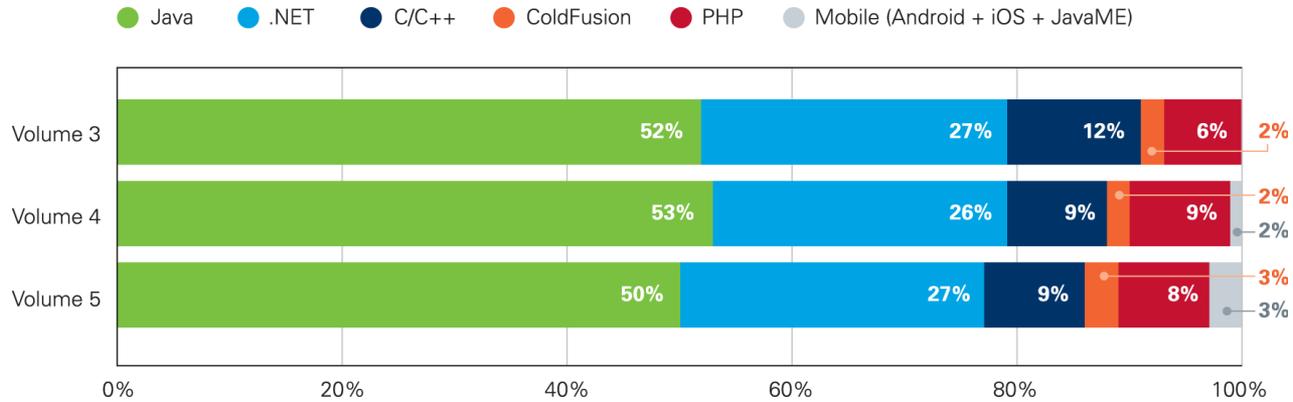
Distribution of Applications by Industry



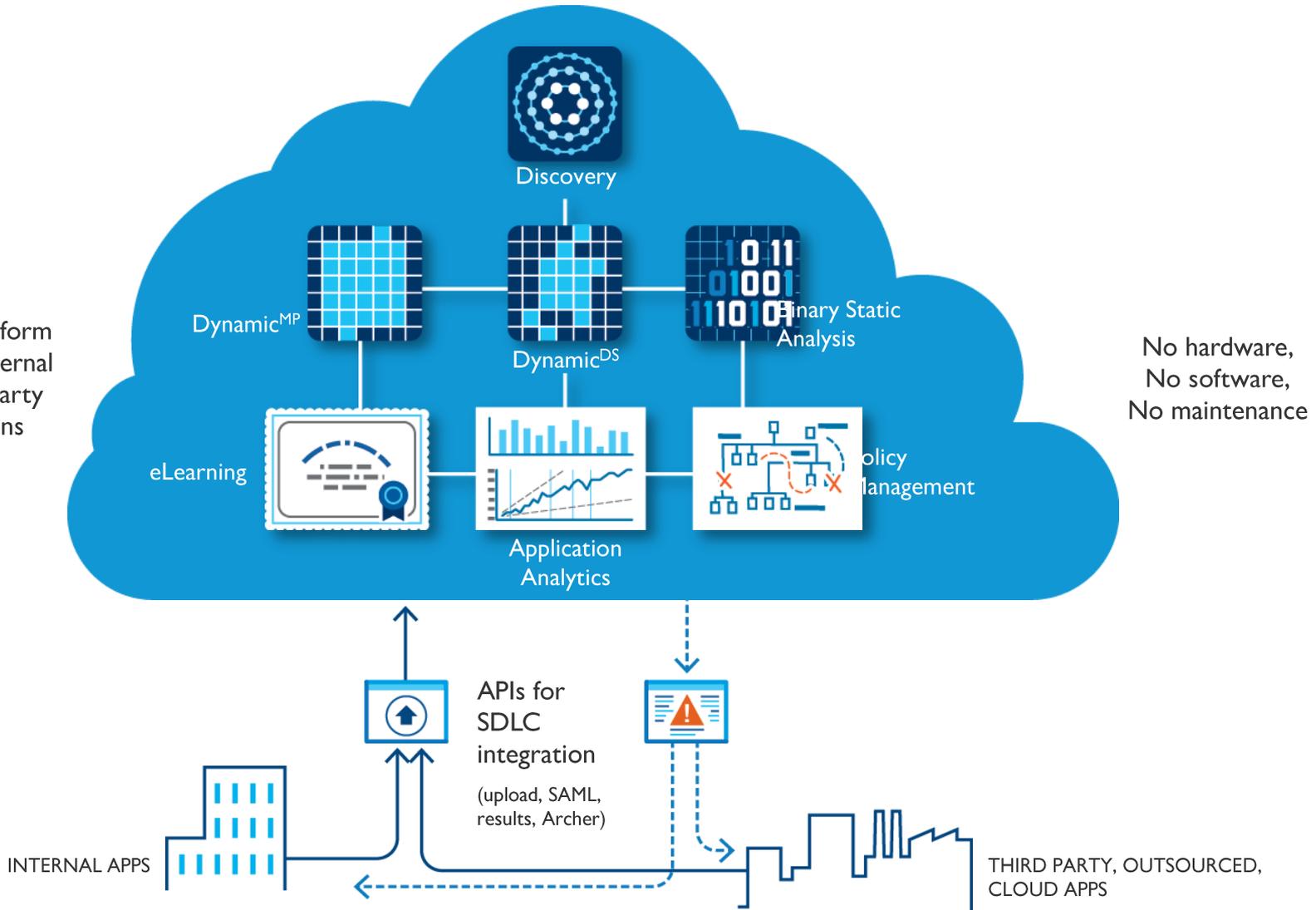
Distribution of Web, Mobile and Other Applications



Distribution by Language: Apps



Central platform supports internal and third-party applications



No hardware,
No software,
No maintenance

Application Metadata

- ▶ Industry vertical
- ▶ Supplier (internal, third-party, open source, etc.)
- ▶ Application type
- ▶ Business criticality
- ▶ Language
- ▶ Platform

Scan Data

- ▶ Scan number
- ▶ Scan date
- ▶ Lines of code

Enterprise Metrics

- ▶ Flaw counts
- ▶ Flaw percentages
- ▶ Application count
- ▶ Risk-adjusted rating
- ▶ First scan acceptance rate
- ▶ Time between scans
- ▶ Days to remediation
- ▶ Scans to remediation
- ▶ Team comparisons
- ▶ Custom policies
- ▶ PCI-DSS[†]
- ▶ CWE/SANS Top25[†]
- ▶ OWASP Top Ten[†]

[†] Pass/Fail only

Caveats

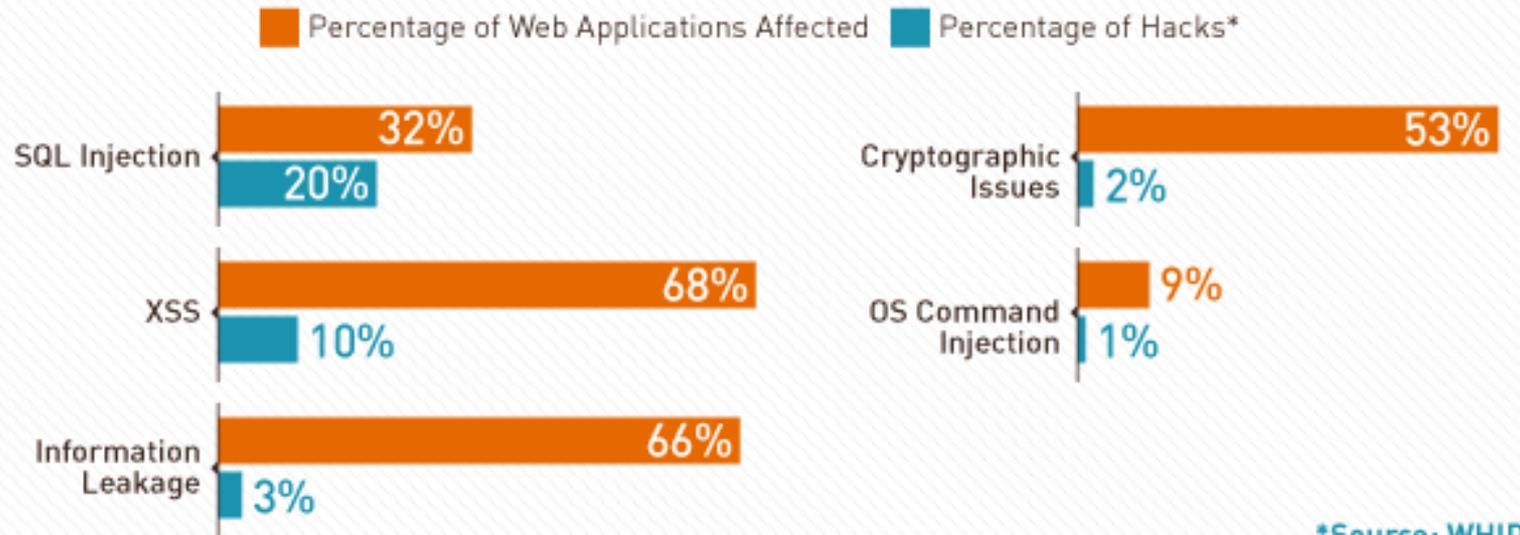
- ✓ Customer base is already security-conscious
- ✓ Bias toward business critical applications
- ✓ Applications are at inconsistent phases in the SDLC
- ✓ Not all flaws are easy to exploit
- ✓ Analysis technology is continuously being improved
- ✓ All security testing has False Negatives



Latent
Vulnerabilities
vs.
Attacks



Top 5 Attacked Web Application Vulnerabilities



While other flaws such as XSS account for a higher volume of findings, SQL injection accounts for 20 percent of hacks.

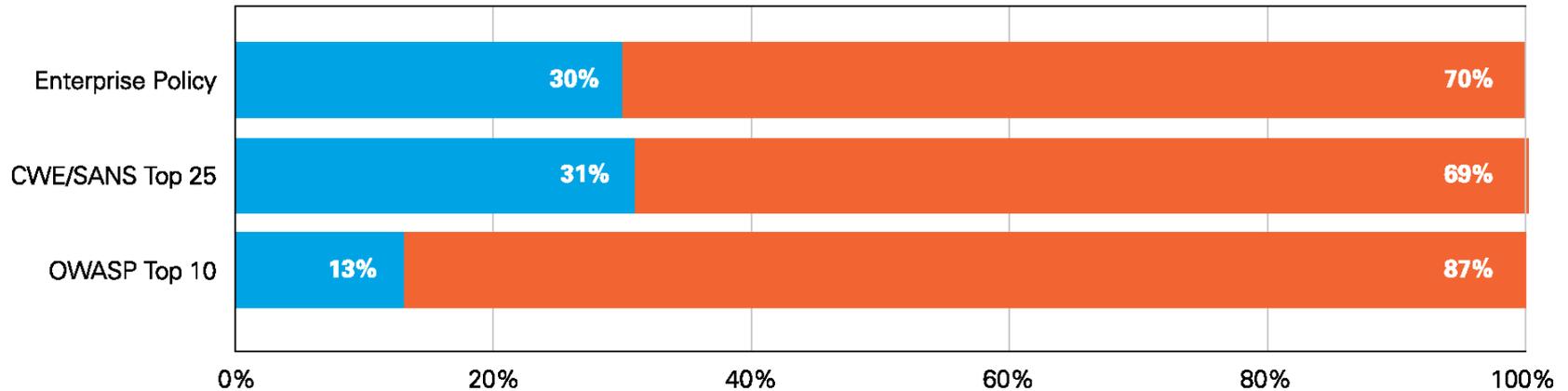
Key Finding

70% of applications failed to comply with enterprise security policies on first submission

New Applications have **Known** and **Exploitable** Vulnerabilities

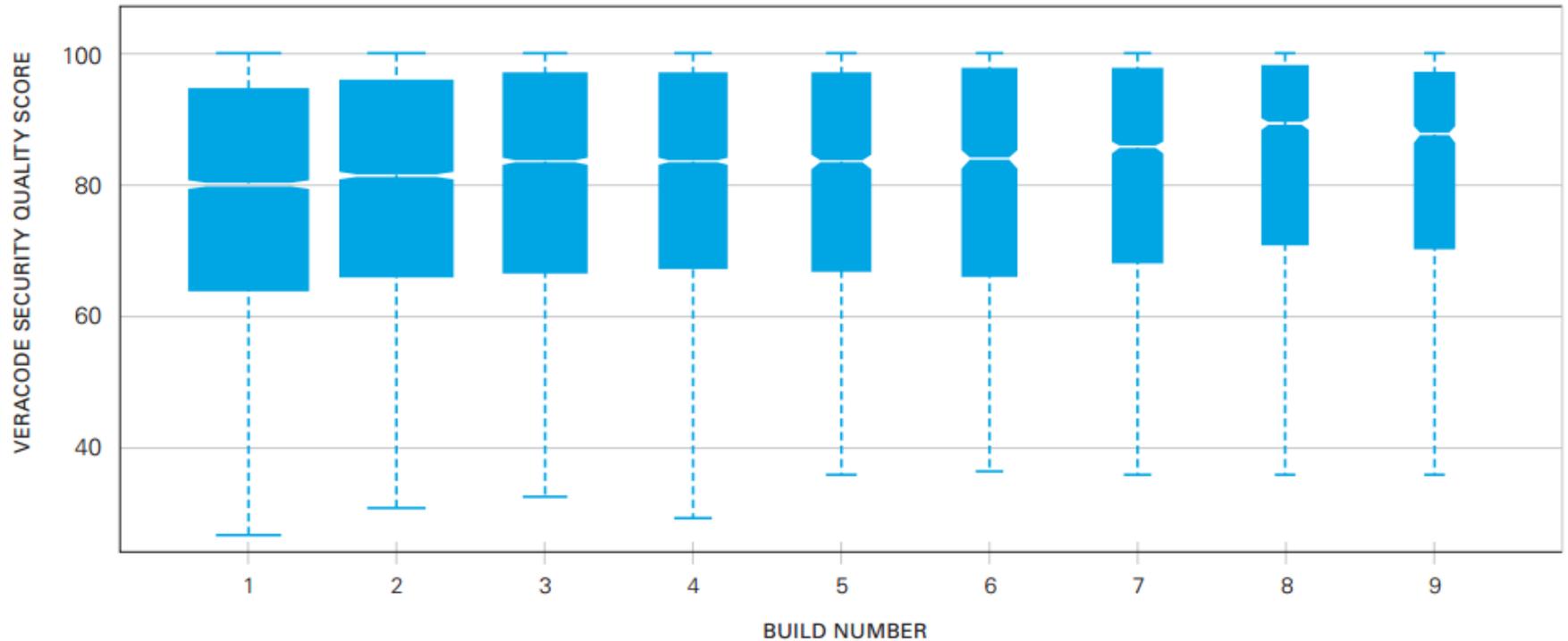
Compliance with Policies Upon First Submission

● Compliant ● Out of Compliance



Build Over Build Improvement

Veracode Security Quality Score by Build



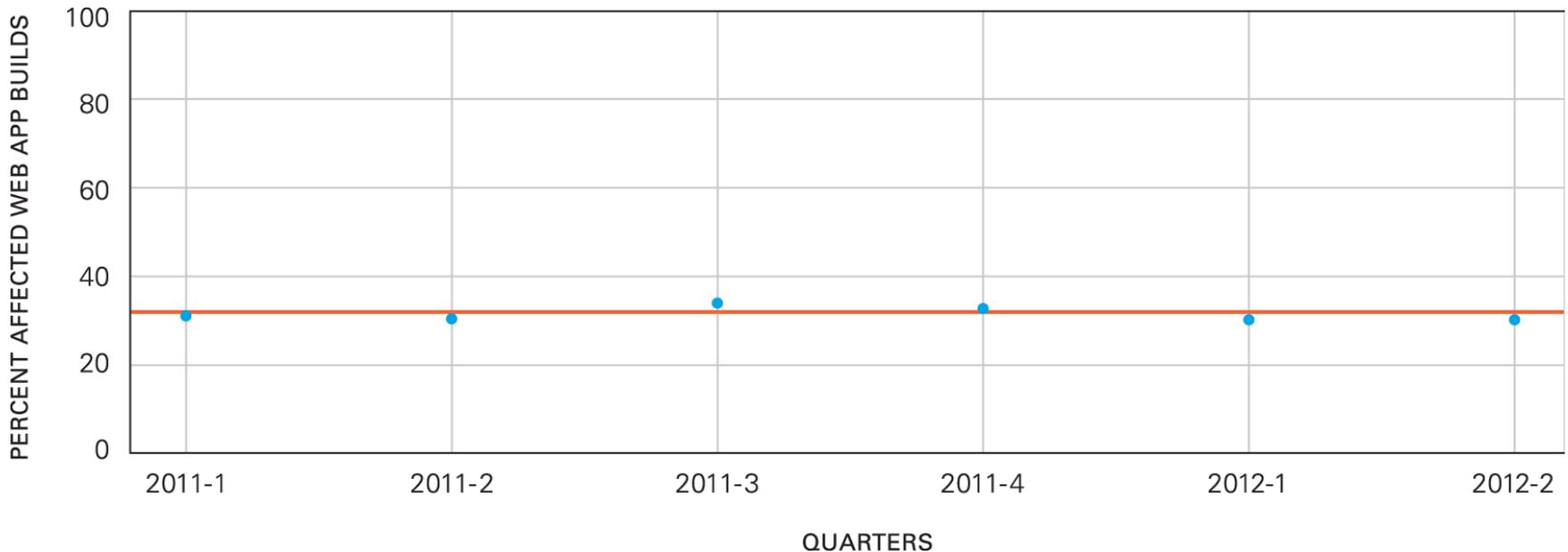
Key Finding

SQL injection prevalence has plateaued, affecting approximately 32% of web applications

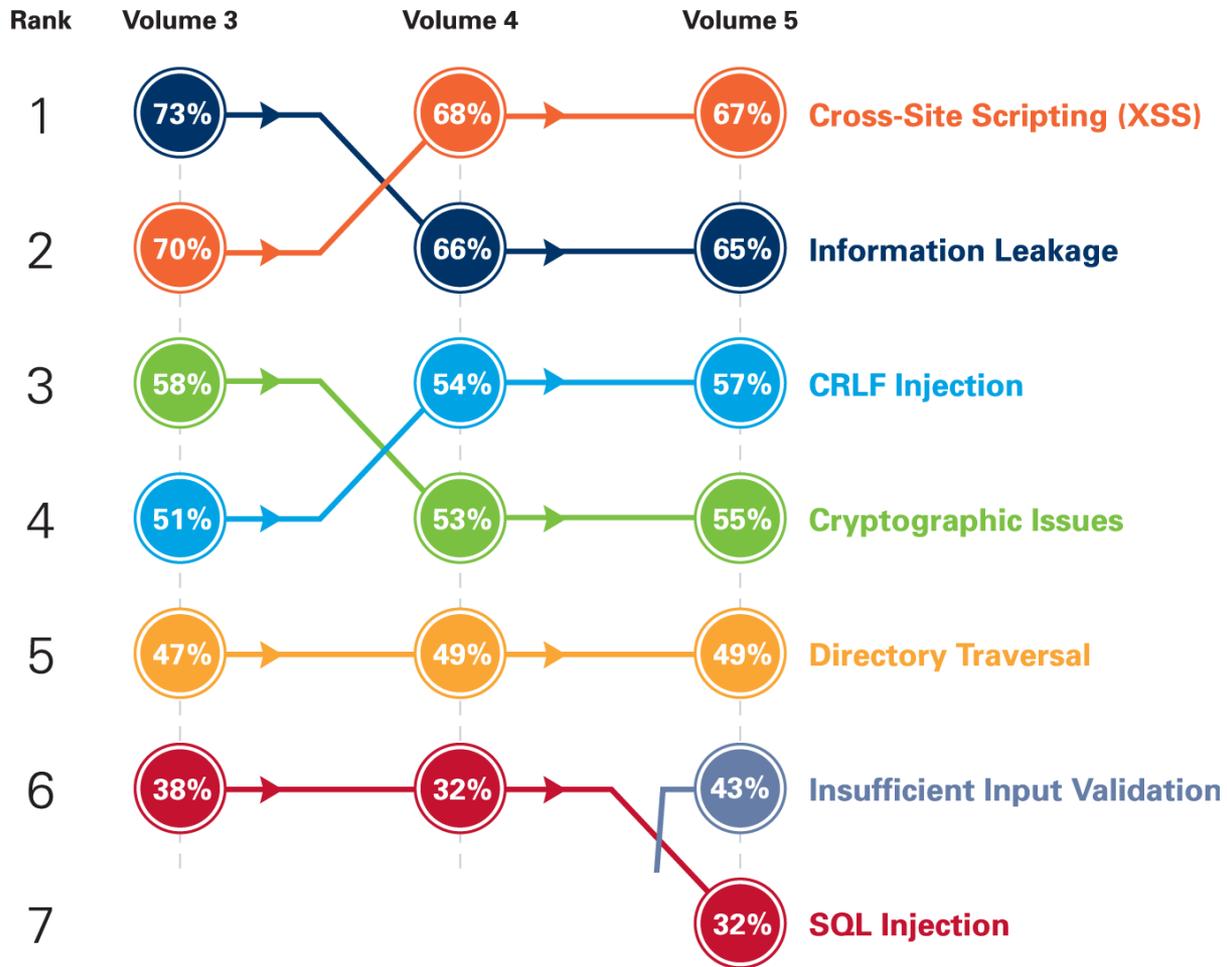
Flat SQL Injection Trend Enables Ongoing Attacks in 2013

Quarterly Trend for SQL Injection Prevalence (Percent of Web Applications Affected)

pvalue = 0.868



Top Vulnerability Categories (Percentage of Affected Web Application Builds)

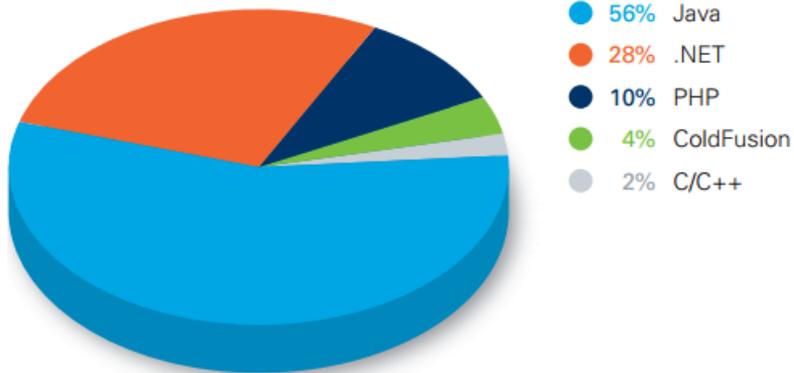


THE TIOBE INDEX: AN INDICATOR OF THE POPULARITY OF VARIOUS LANGUAGES, BASED UPON GLOBAL NUMBERS OF ENGINEERS, COURSES, AND THIRD-PARTY VENDORS

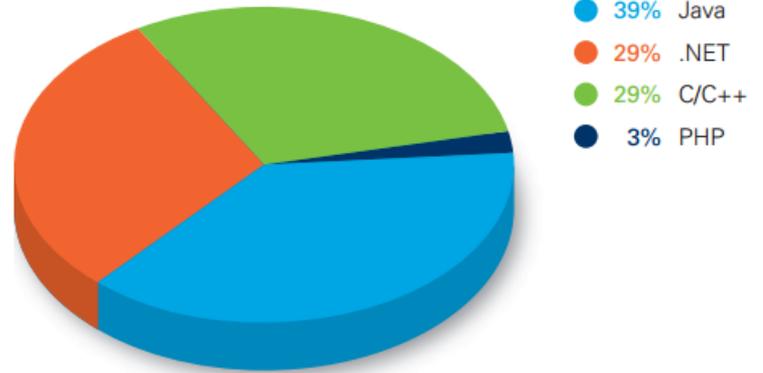
POSITION MARCH 2013	POSITION MARCH 2012	DELTA IN POSITION	PROGRAMMING LANGUAGE	RATINGS MARCH 2013	DELTA MARCH 2012
1	1	=	Java	18.156%	+1.05%
2	2	=	C	17.141%	+0.05%
3	5	↑↑	Objective-C	10.230%	+2.49%
4	4	=	C++	9.115%	+1.07%
5	3	↓↓	C#	6.597%	-1.65%
6	6	=	PHP	4.809%	-0.75%
7	7	=	(Visual)Basic	4.607%	+0.24%
8	9	↑	Python	4.388%	+1.10%
9	13	↑↑↑↑	Ruby	2.150%	+0.74%
10	10	=	Perl	1.959%	-0.74%

Language Details

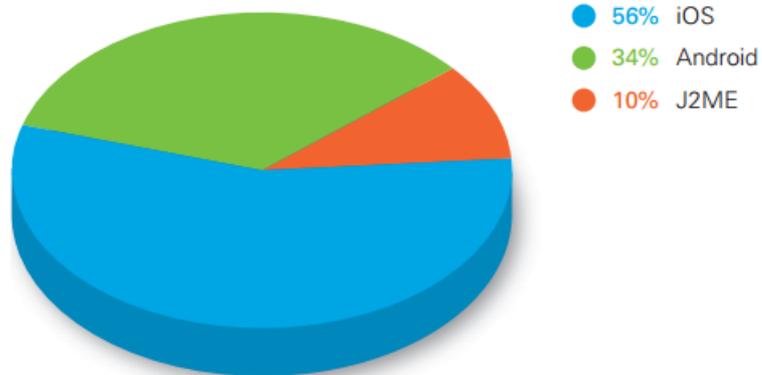
Distribution of Web Applications by Language



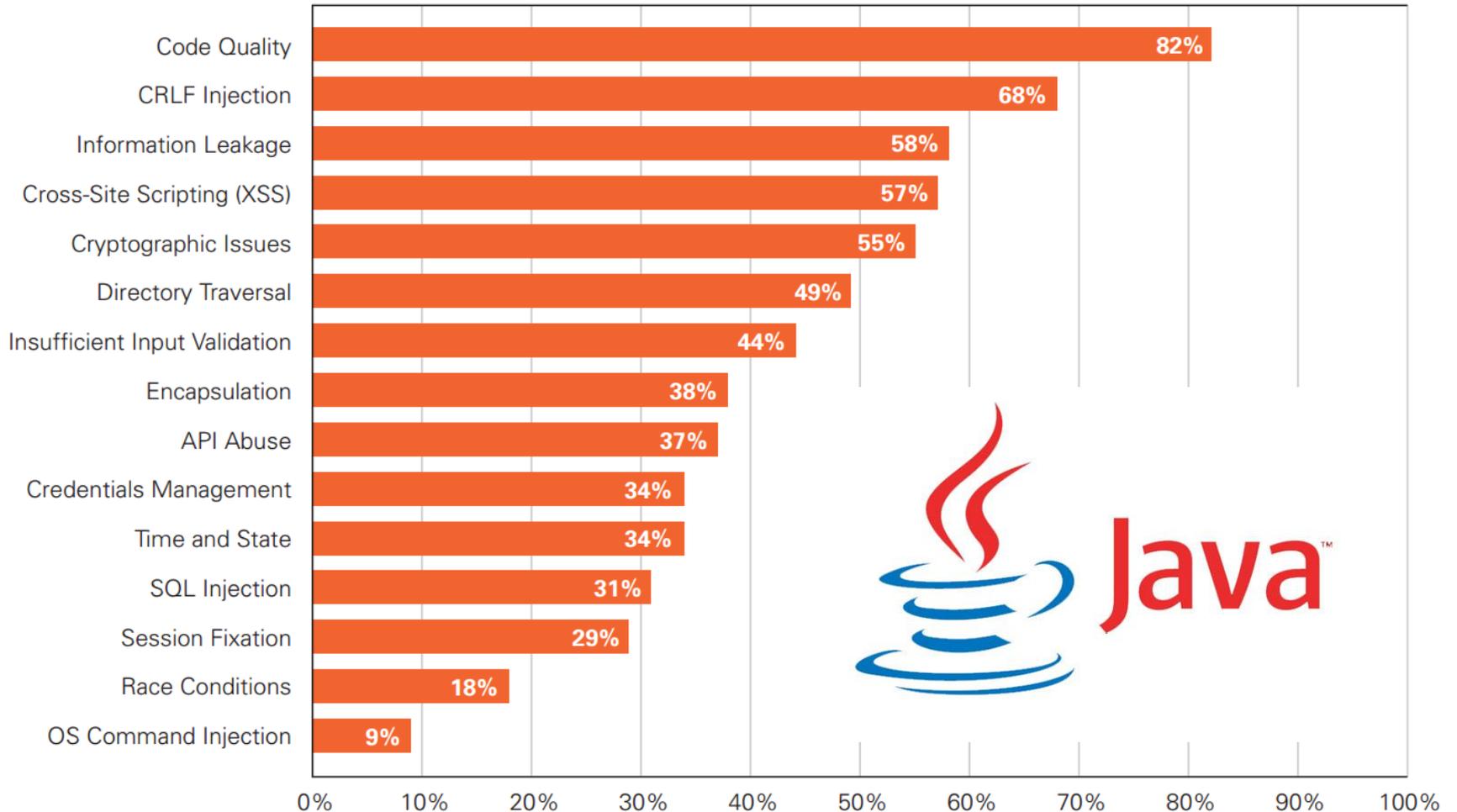
Distribution of Non-Web Applications by Language



Distribution of Mobile Applications by Platform

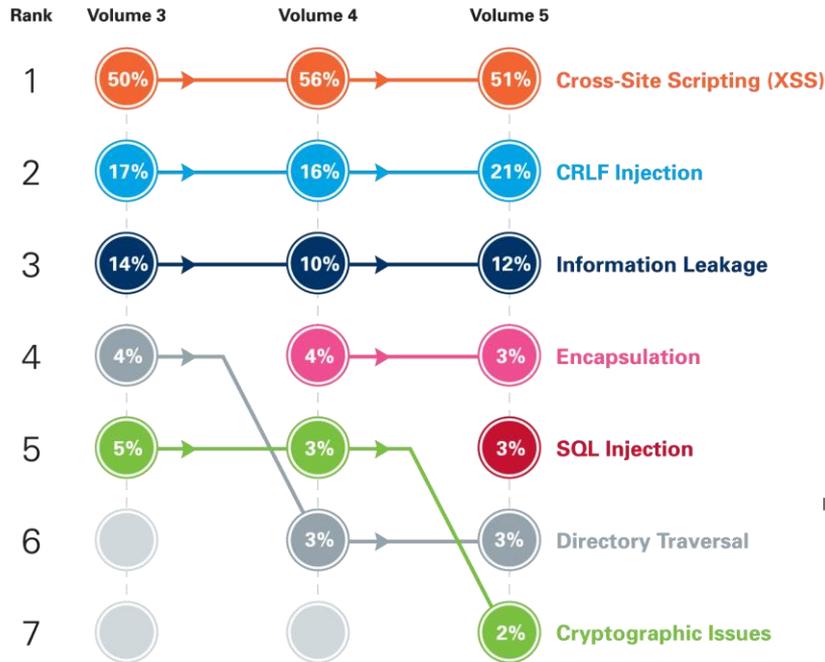


Vulnerability Prevalence in Java Applications (Percentage of Applications Affected)



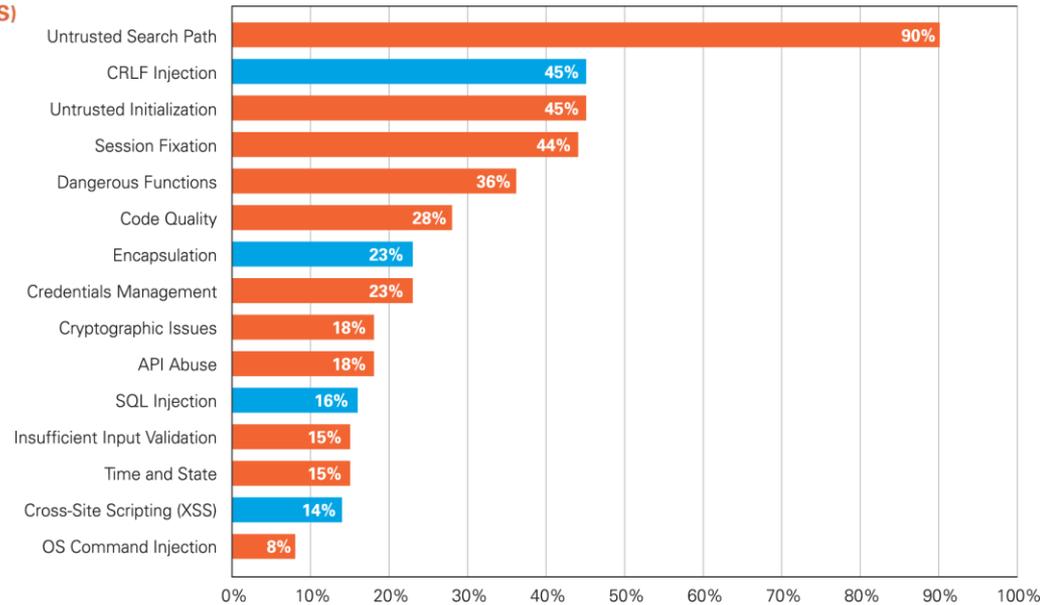
Java Applications

Vulnerability Distribution Trends for Java Applications (Share of Total Vulnerabilities Found)

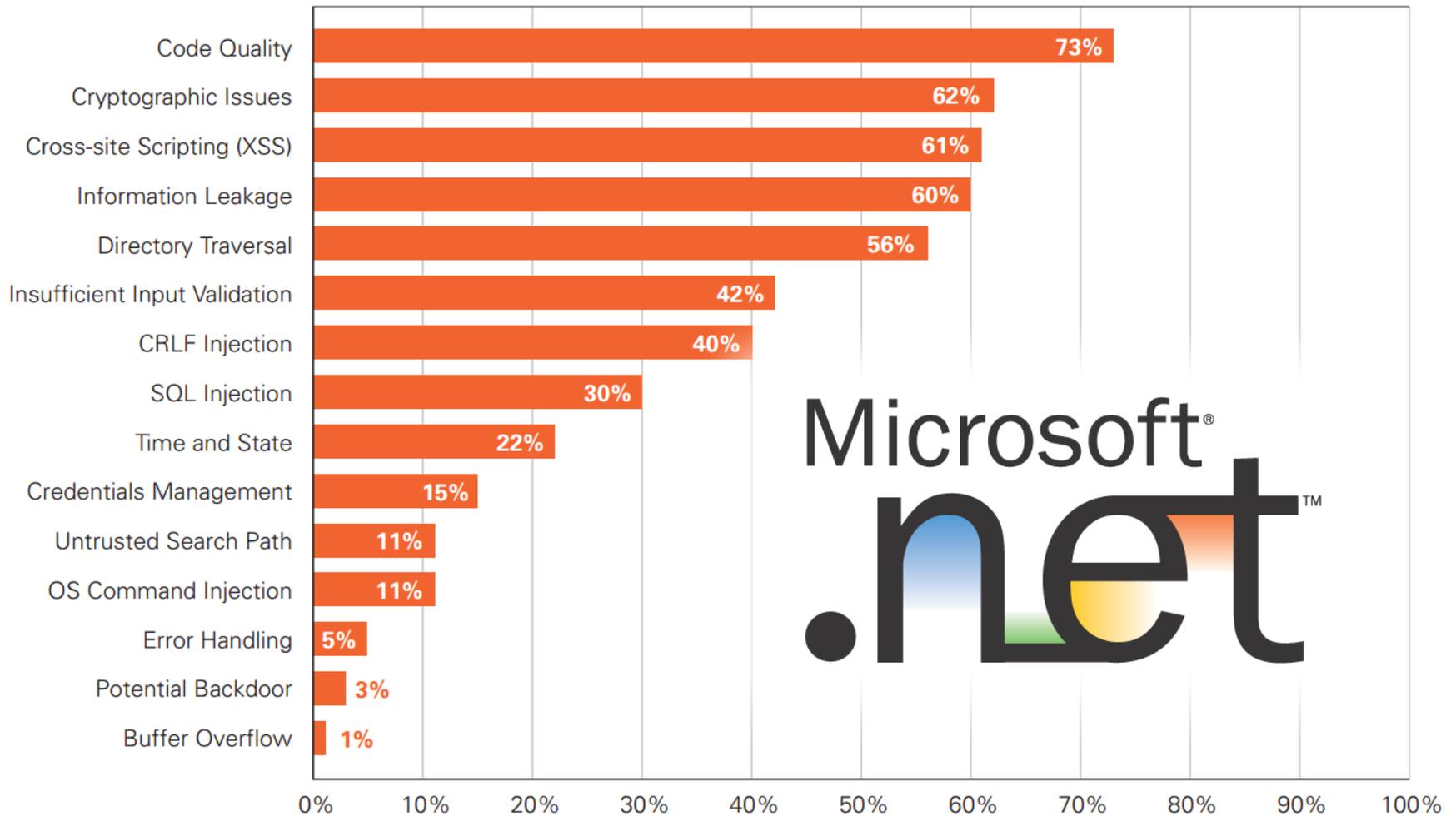


Percent Improvement in Java Vulnerability Distribution from First to Second Submission

● Indicates categories with the highest vulnerability distribution in Java

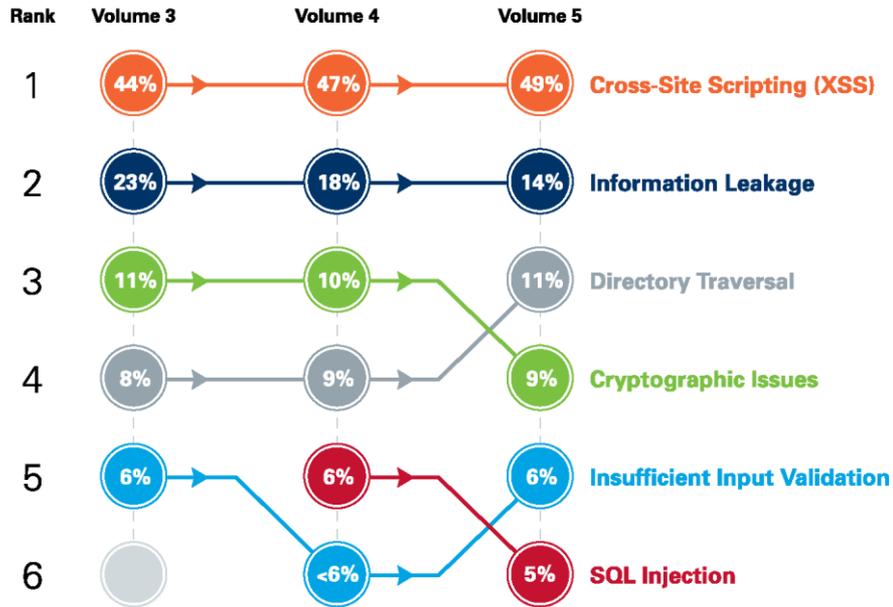


Vulnerability Prevalence in .NET Applications (Percentage of Applications Affected)

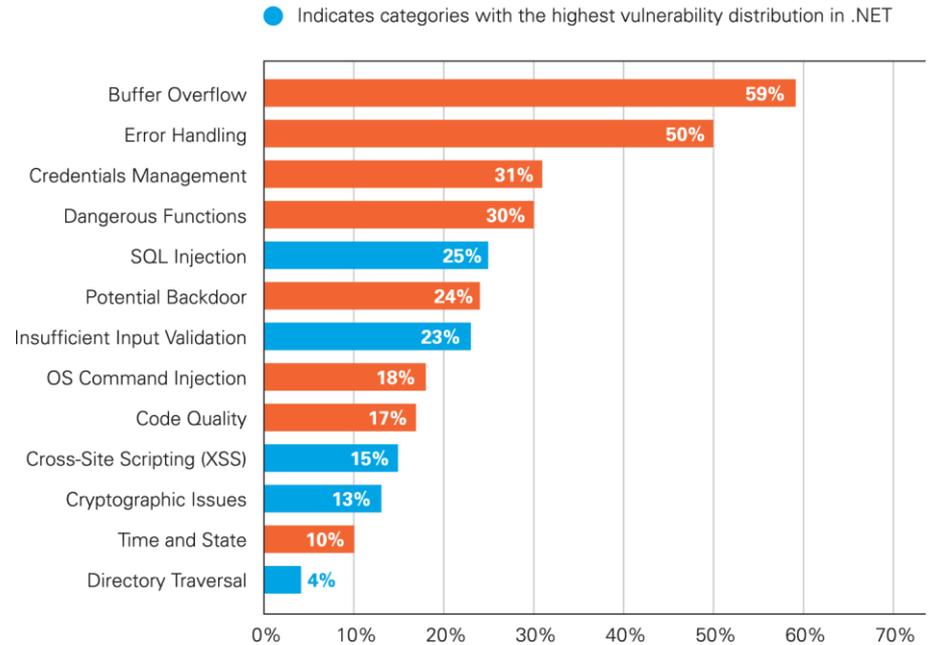


.NET Applications

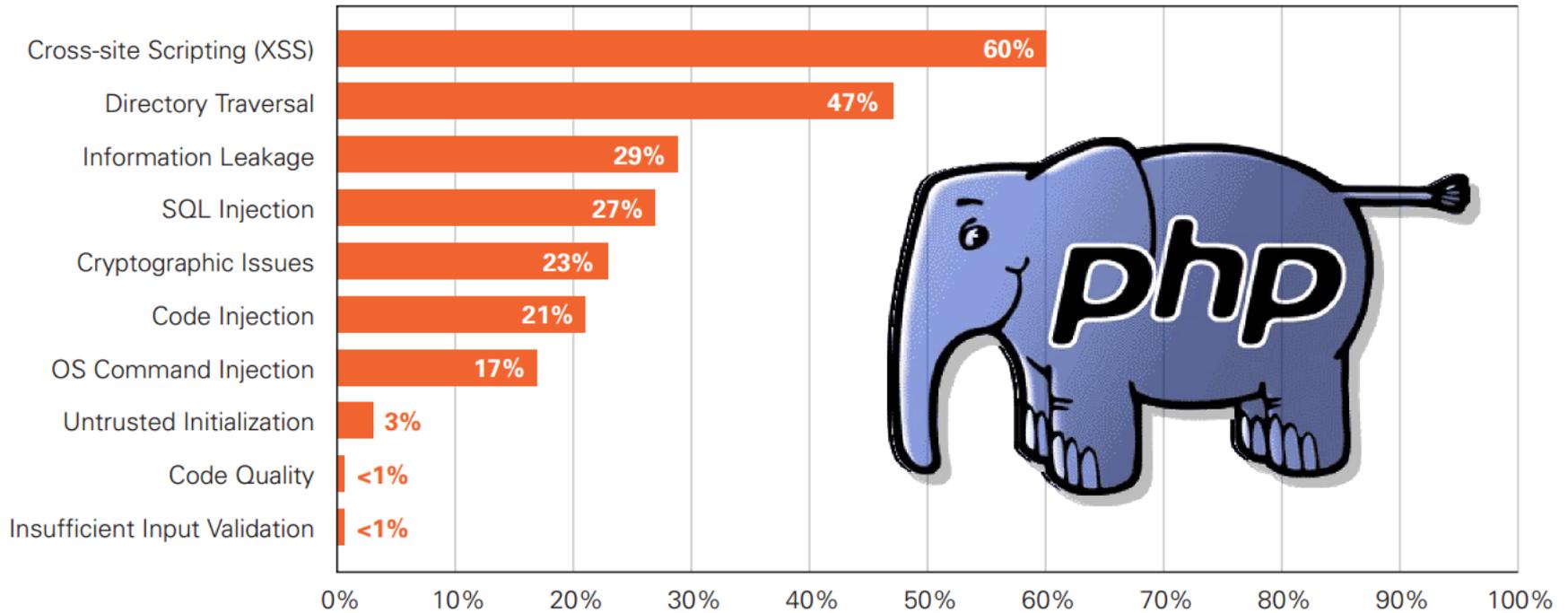
Vulnerability Distribution Trends for .NET Applications (Share of Total Vulnerabilities Found)



Percent Improvement in .NET Vulnerability Distribution from First to Second Submission



Vulnerability Prevalence in PHP Applications (Percentage of Applications Affected)

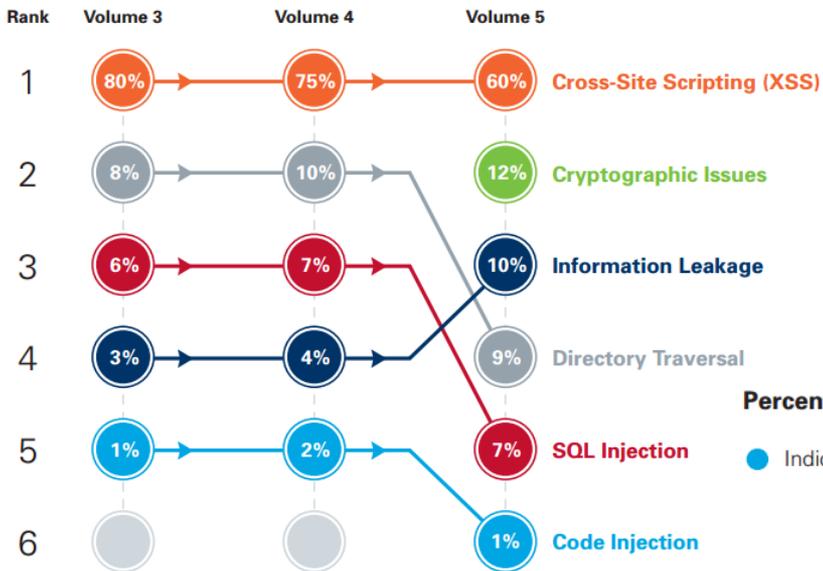


PHP Applications

FAST, SECURE, BUG FREE
User friendly
100 % satisfaction guaranteed

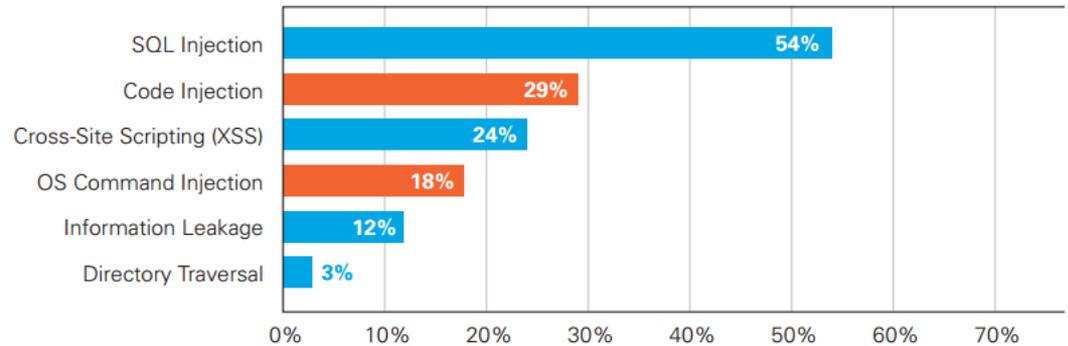


Vulnerability Distribution Trends for PHP Applications (Share of Total Vulnerabilities Found)

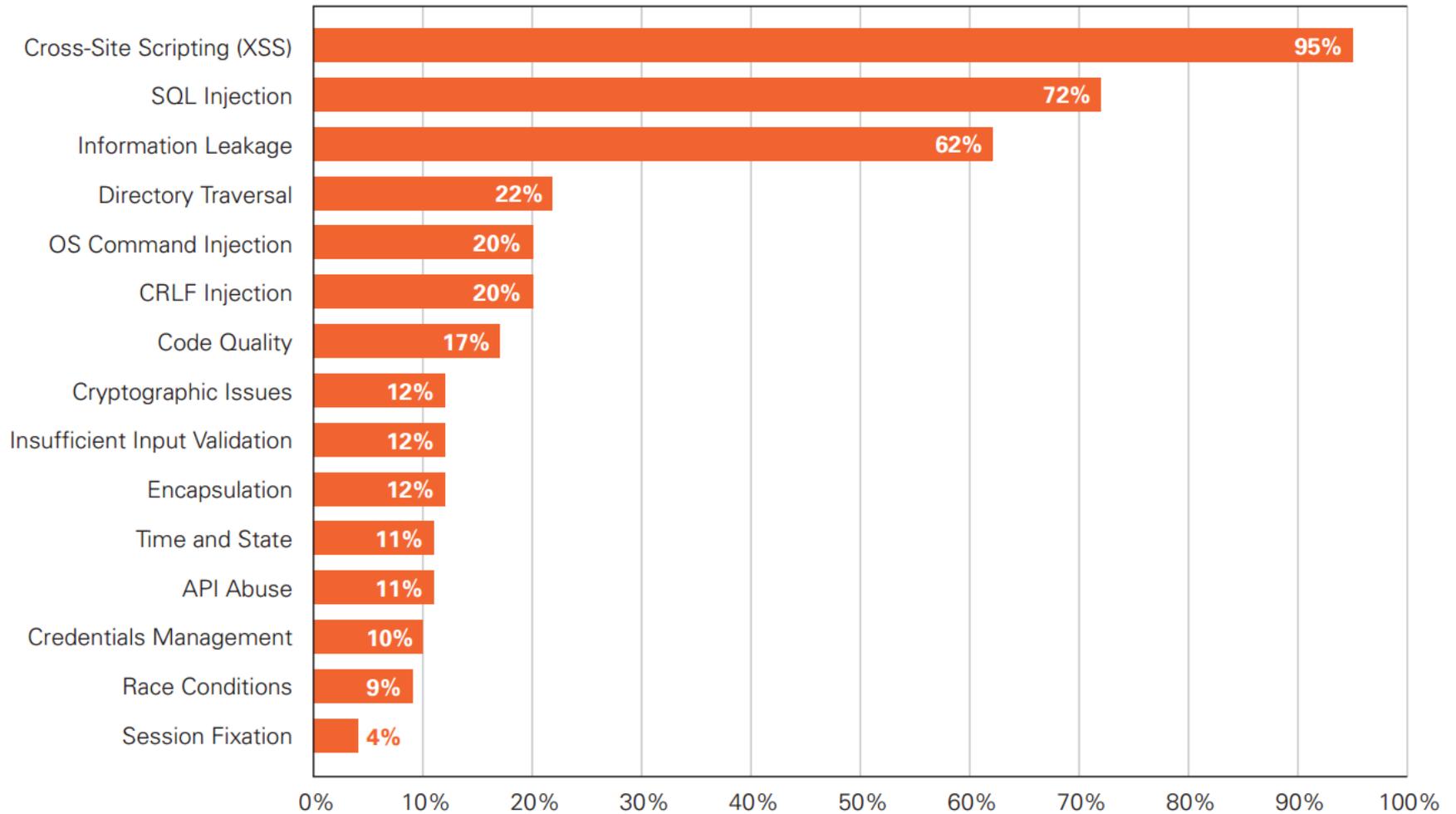


Percent Improvement in PHP Vulnerability Distribution from First to Second Submission

● Indicates categories with the highest vulnerability distribution in PHP

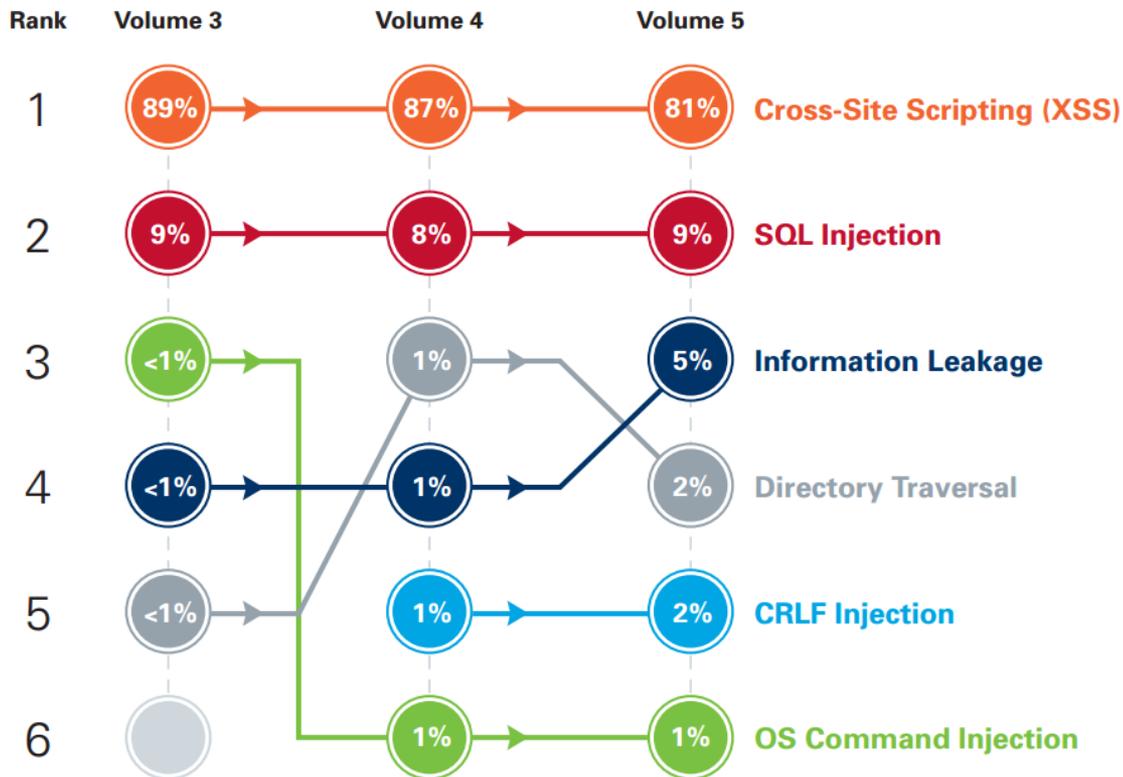


Vulnerability Prevalence in ColdFusion Applications (Percentage of Applications Affected)

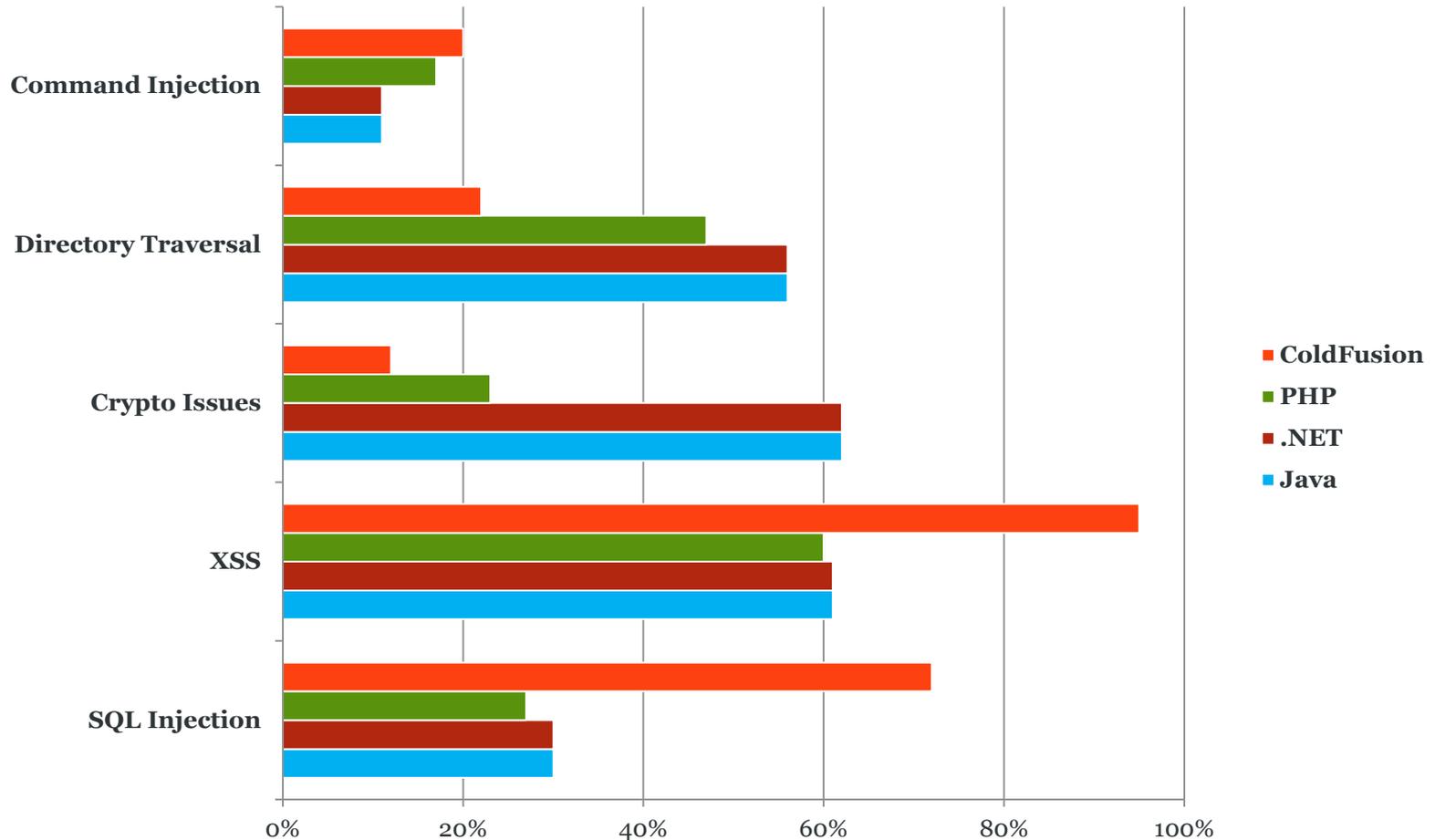


ColdFusion Applications

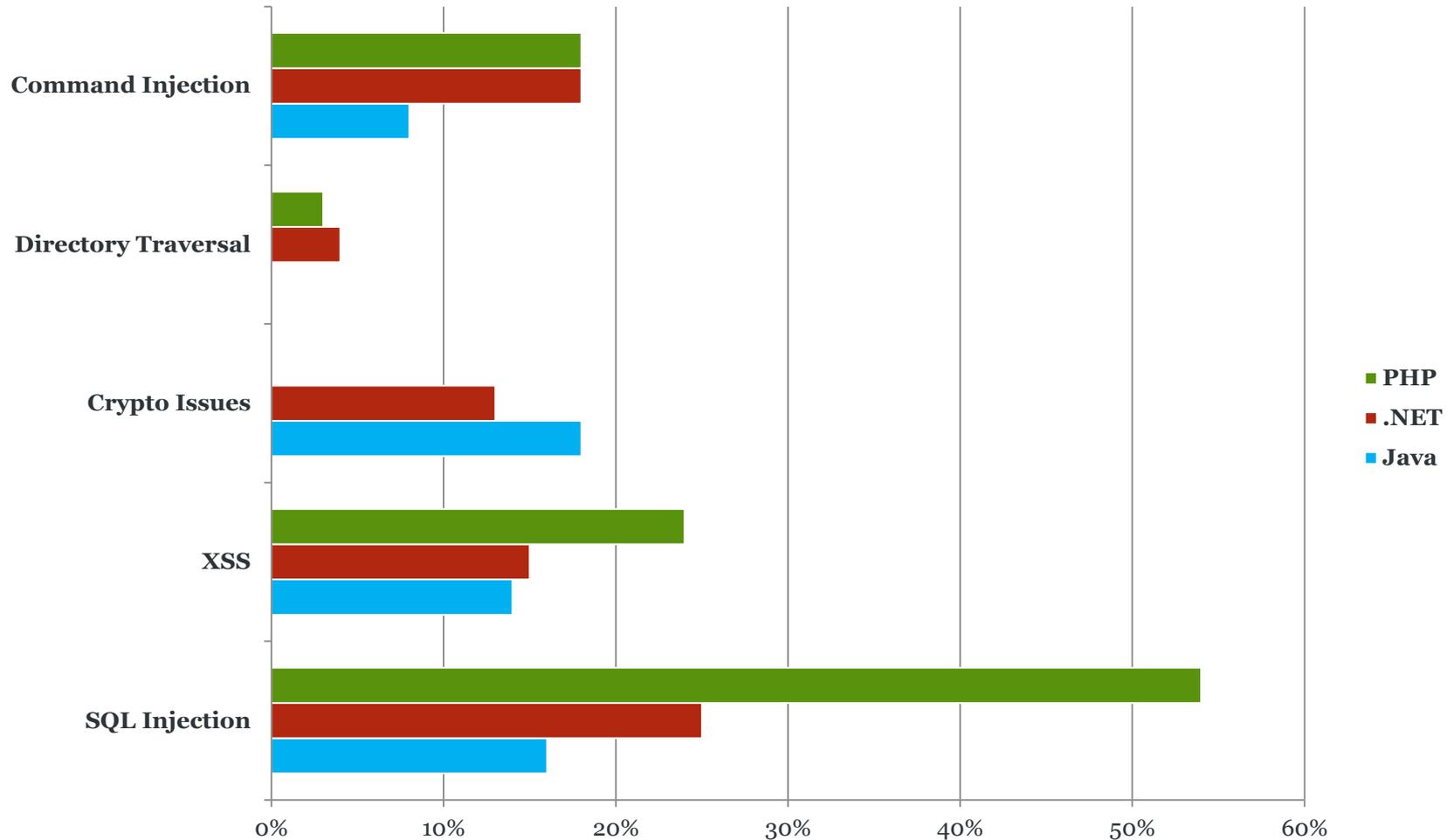
Vulnerability Distribution Trends for ColdFusion Applications (Share of Total Vulnerabilities Found)



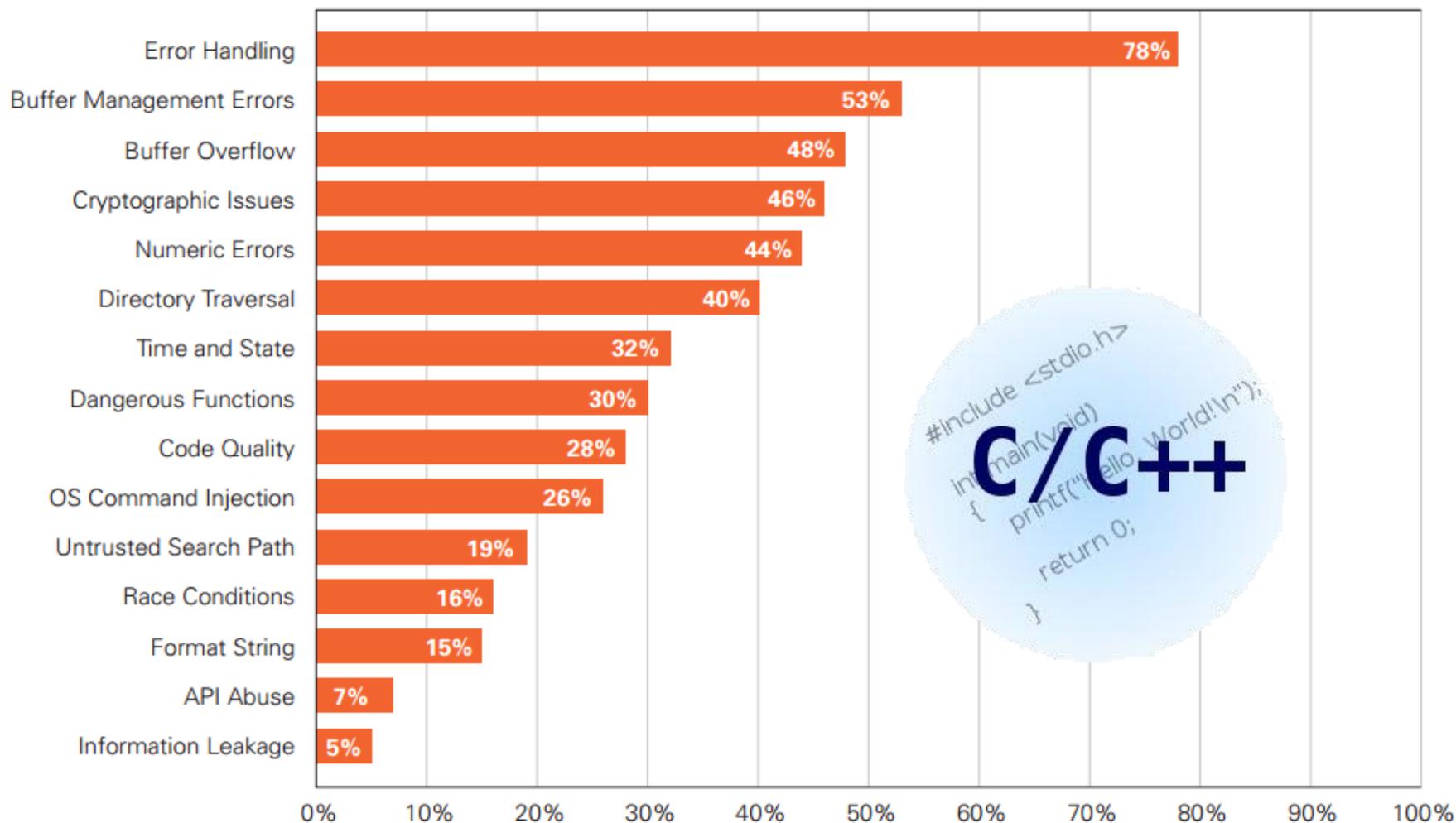
Flaw Prevalence by Language



Improvement by Language, 1st to 2nd Scan

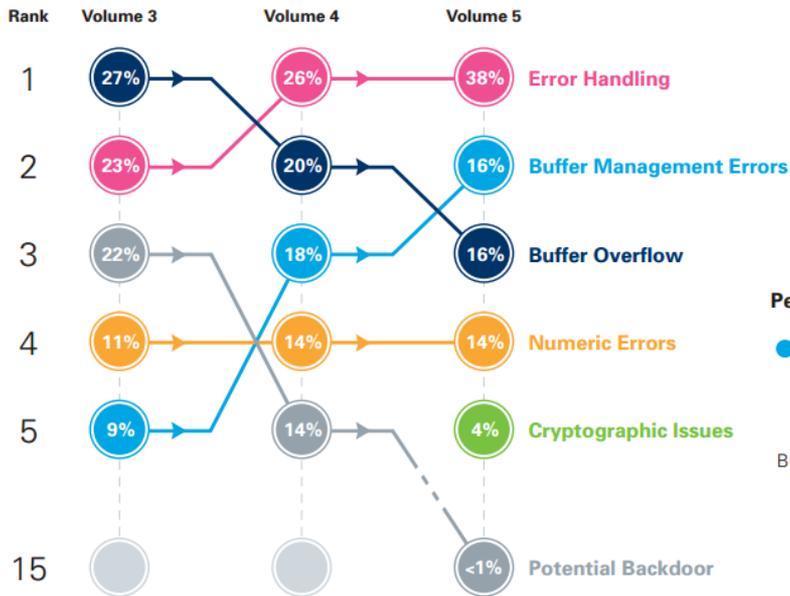


Vulnerability Prevalence in C/C++ Applications (Percentage of Applications Affected)



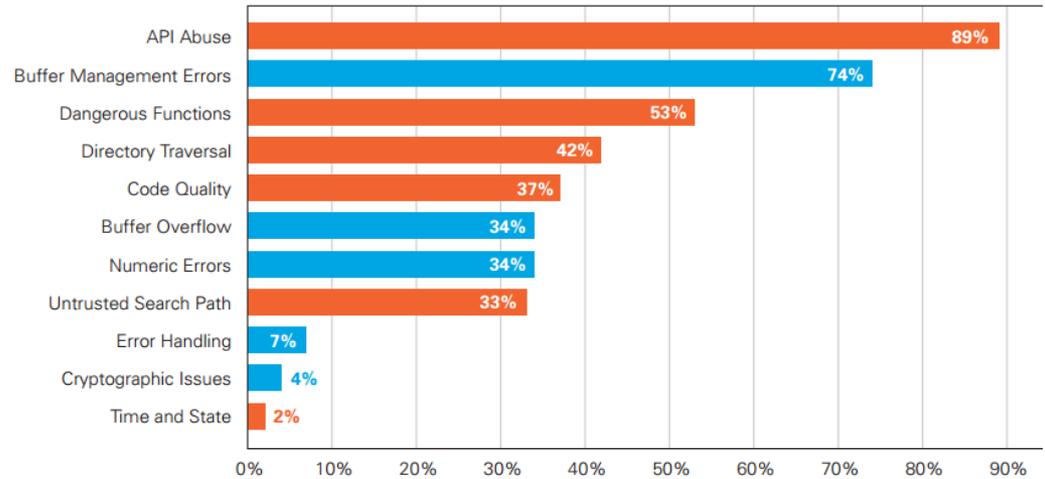
C/C++ Applications

Vulnerability Distribution Trends for C/C++ Applications (Share of Total Vulnerabilities Found)



Percent Improvement in C/C++ Vulnerability Distribution from First to Second Submission

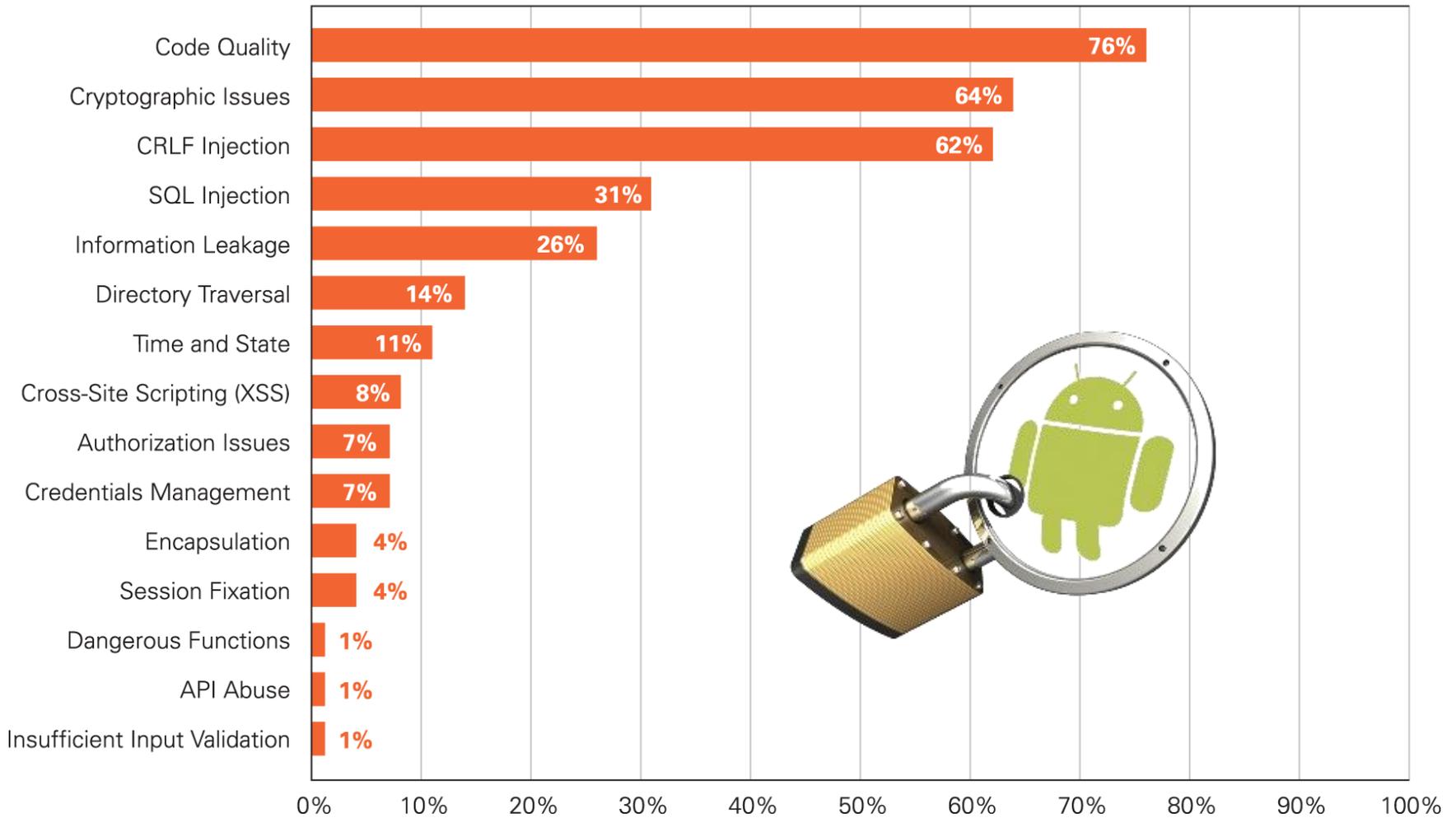
● Indicates categories with the highest vulnerability distribution in C/C++



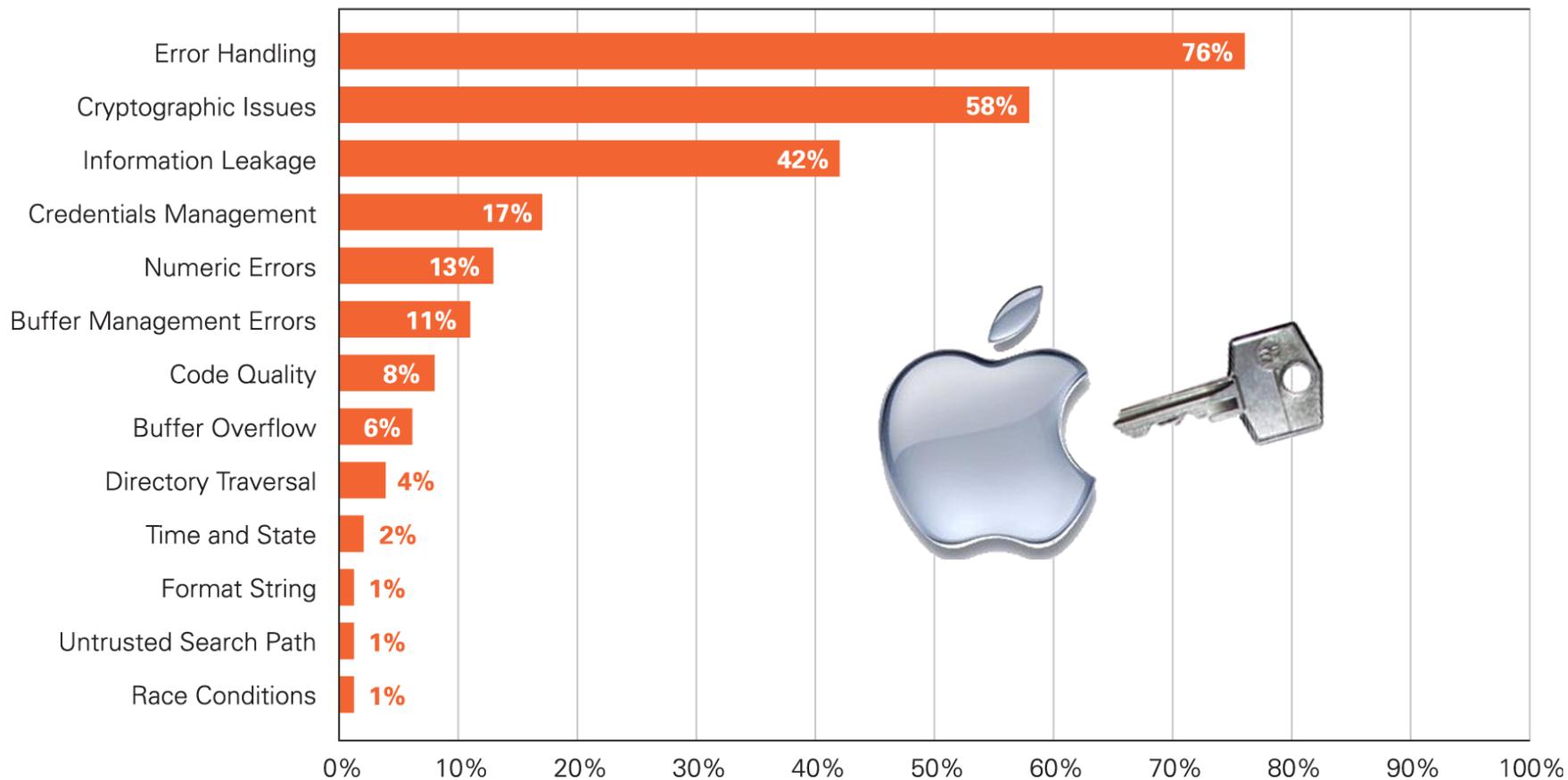
Key Finding

Cryptographic issues affect a sizeable portion of Android (64%) and iOS (58%) applications

Android Vulnerability Prevalence (Percentage of Applications Affected)



iOS (ObjectiveC) Vulnerability Prevalence (Percentage of Applications Affected)



Vulnerability Distribution for Mobile Platforms (Share of Total Vulnerabilities Found)

Android		iOS		Java ME	
CRLF Injection	37%	Information Leakage	62%	Cryptographic Issues	47%
Cryptographic Issues	33%	Error Handling	20%	Information Leakage	47%
Information Leakage	10%	Cryptographic Issues	7%	Directory Traversal	3%
SQL Injection	9%	Directory Traversal	6%	Insufficient Input Validation	2%
Time and State	4%	Buffer Management Errors	3%	Credentials Management	<1%



Key Findings

- ✓ 70% of applications failed to comply with enterprise security policies on first submission
- ✓ SQL injection prevalence has plateaued, affecting approximately 32% of web applications
- ✓ Eradicating SQL injection in web applications remains a challenge as organizations make tradeoffs around what to remediate first
- ✓ Cryptographic issues affect a sizeable portion of Android (64%) and iOS (58%) applications

Predictions

- ✓ Average CISO tenure continues to decline
- ✓ The rise of the “Everyday Hacker”
- ✓ Decreased job satisfaction/ higher turnover for security professionals
- ✓ Default encryption, not opt-in, will become the norm

Questions?

Thank You!



@chriseng