VERACODE

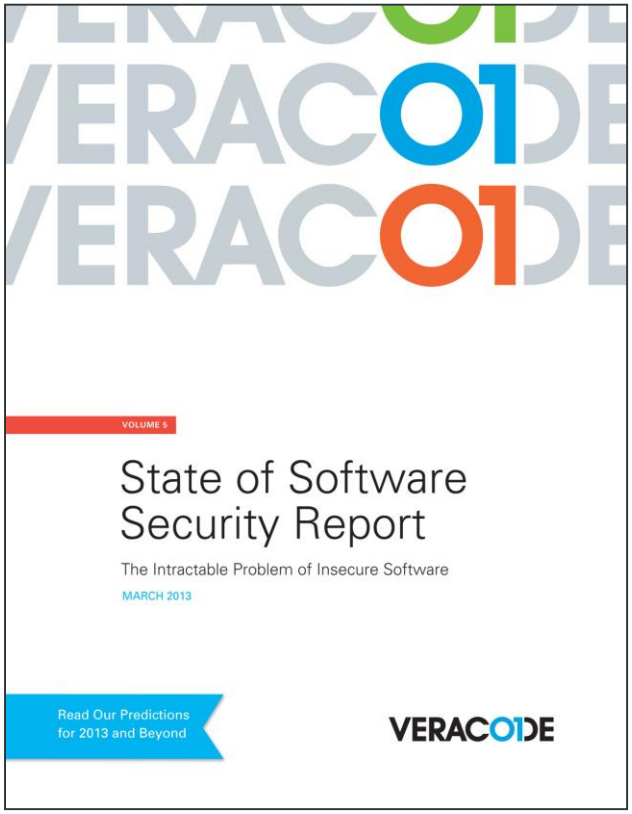
We See the Future and it's Not Pretty

Predicting the future using vulnerability data

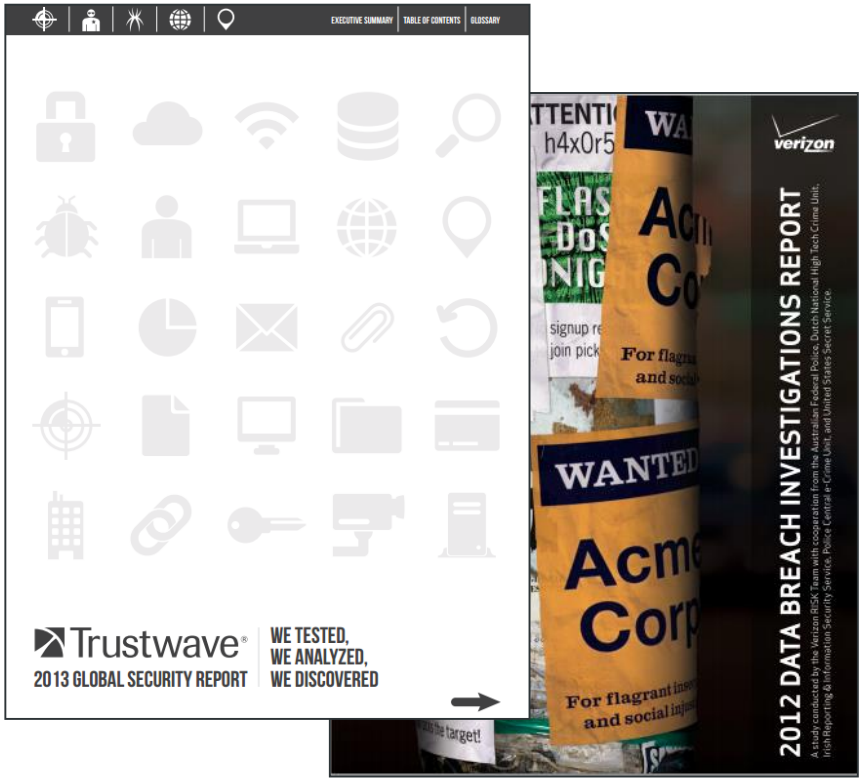
Chris Wysopal, CTO & Co-founder, Veracode

What is the SoSS Report?

SoSS is the "BEFORE"



Breach Reports are the "AFTER"

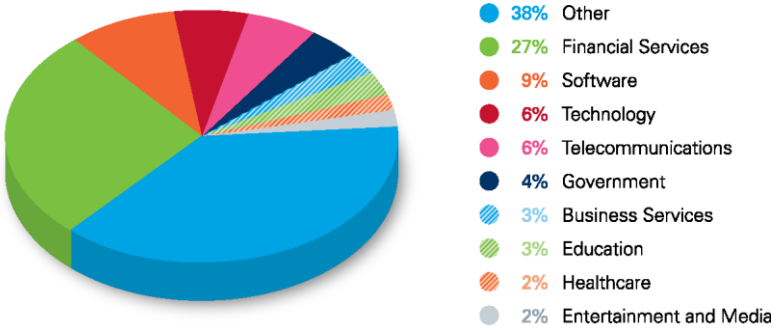


A CRYSTAL BALL FOR DATA BREACH PREDICTIONS

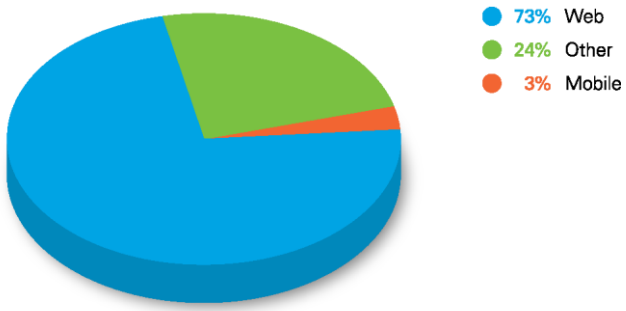
Dataset Overview

22,430 application builds from Jan 2011 to Jun 2012

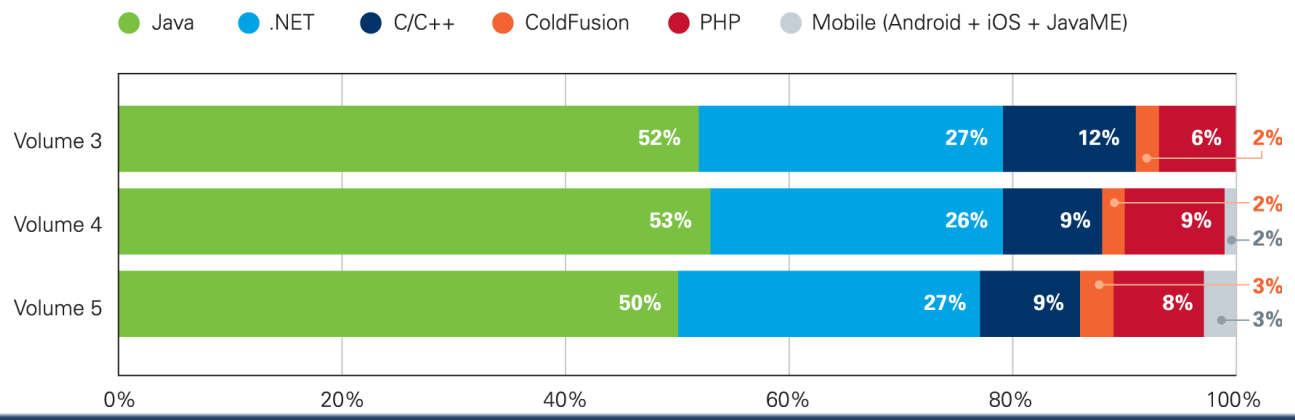
Distribution of Applications by Industry



Distribution of Web, Mobile and Other Applications



Distribution by Language: Apps



VERACODE

Application Metadata

- Industry vertical
- Application supplier (internal, third-party, etc.)
- Application type
- Assurance level
- Language
- Platform

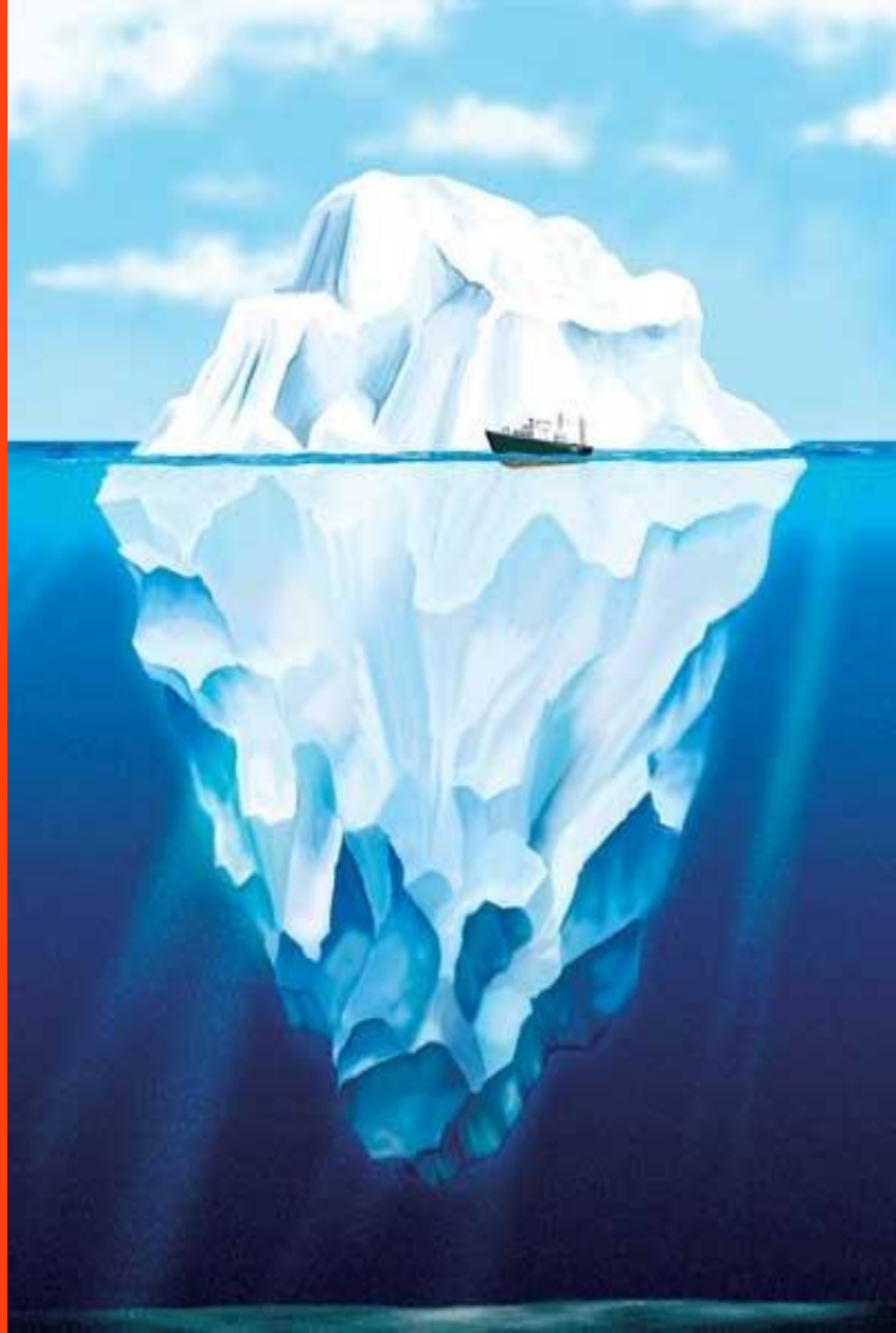
Scan Data

- Scan number
- Scan date
- Lines of code
- Flaw type

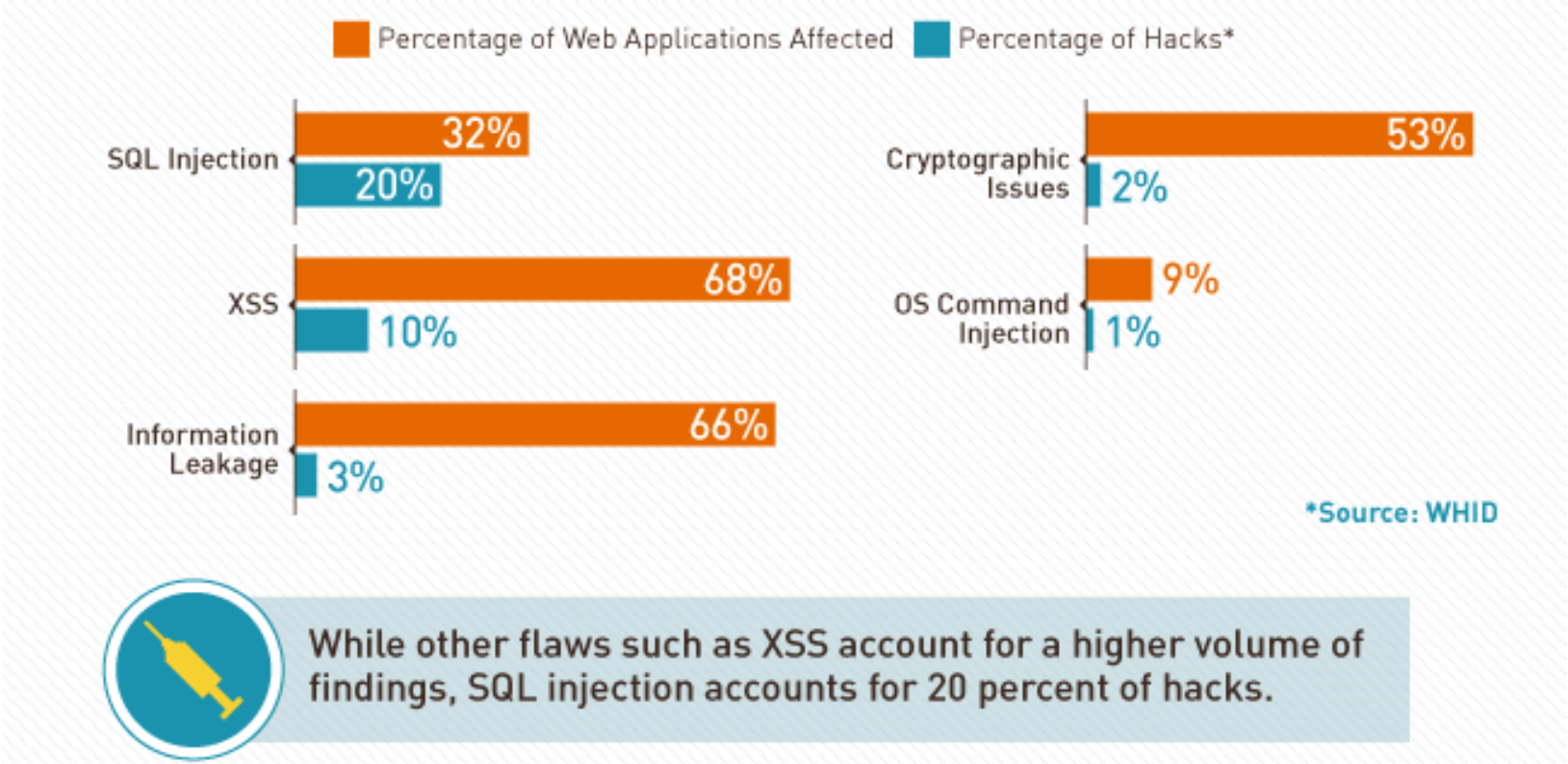
Application Security Metrics

- Flaw counts
- Flaw percentages
- Application count
- Risk-adjusted rating
- First scan acceptance rate
- Time between scans
- Days to remediation
- Scans to remediation
- CWE/SANS Top25 (pass/fail)
- OWASP Top Ten (pass/fail)
- Custom policies

The latent
Vulnerabilities
vs.
The Attacks



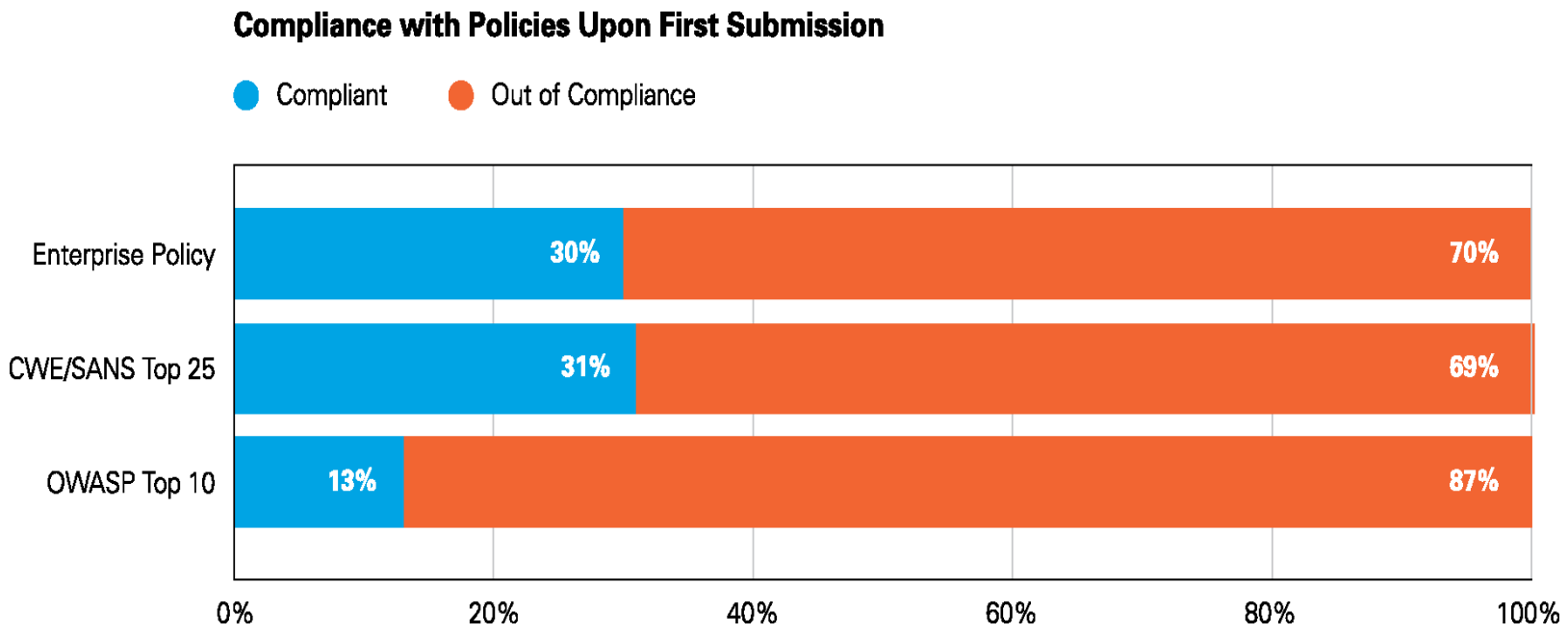
Top 5 Attacked Web Application Vulnerabilities



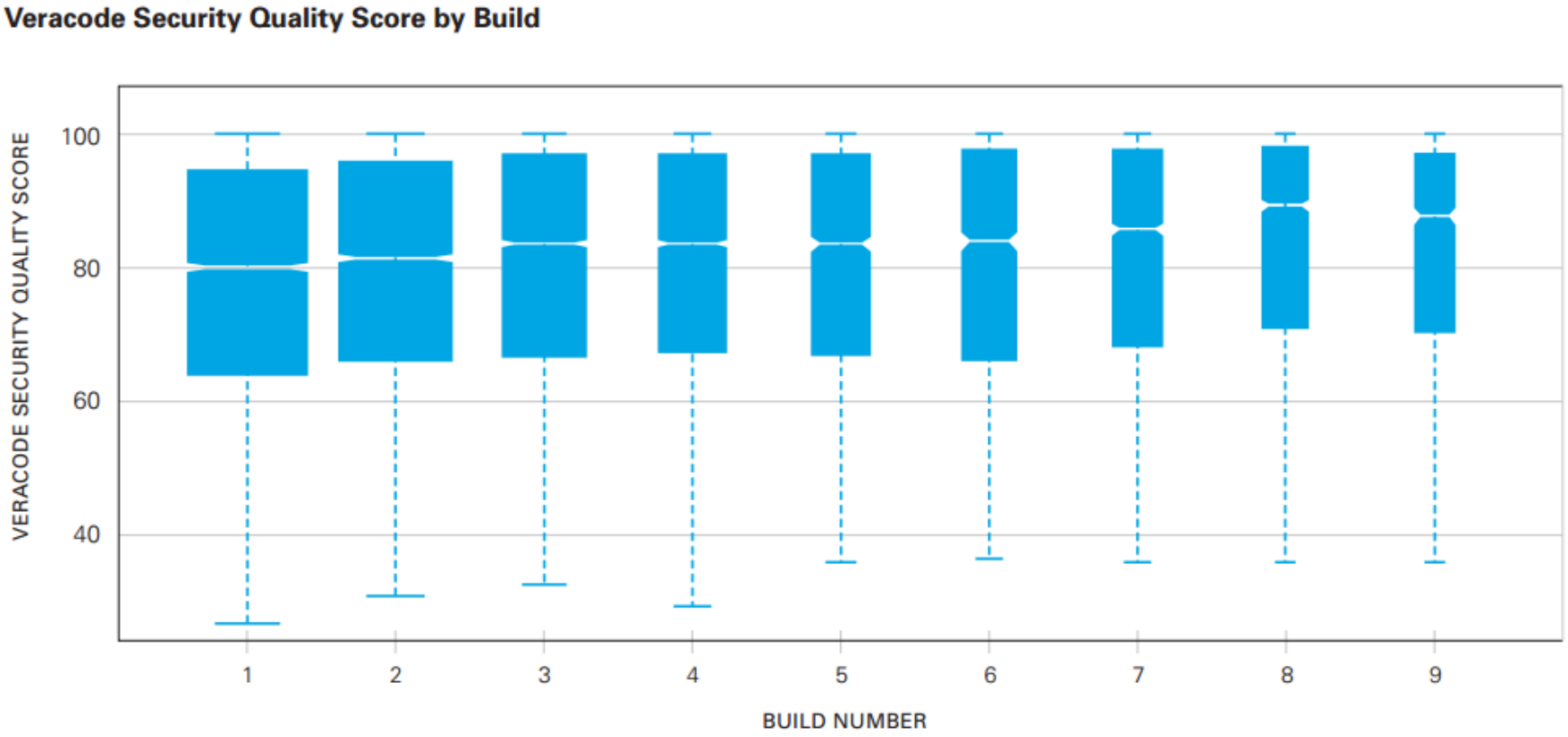
Key Finding:

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

New applications have known and exploitable vulnerabilities



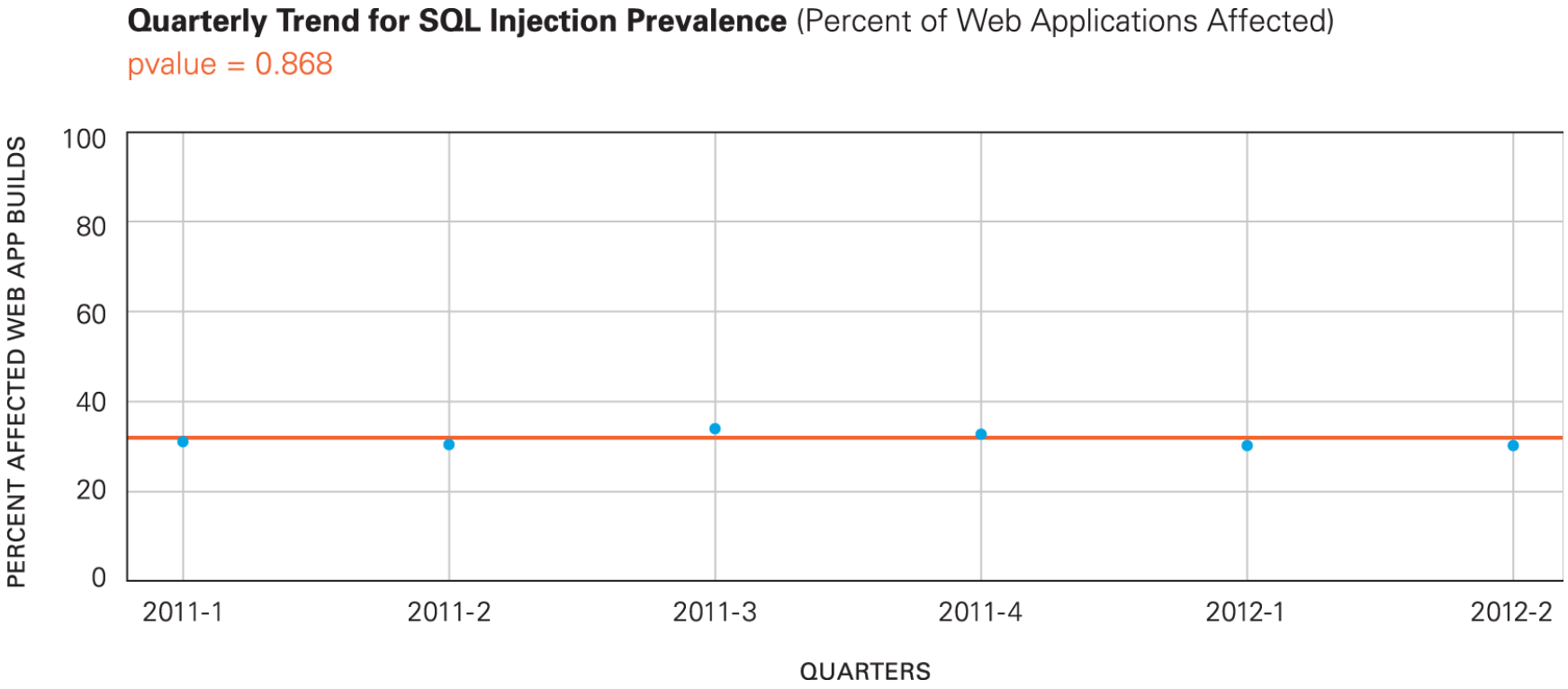
Build over Build Improvement



Key Finding:

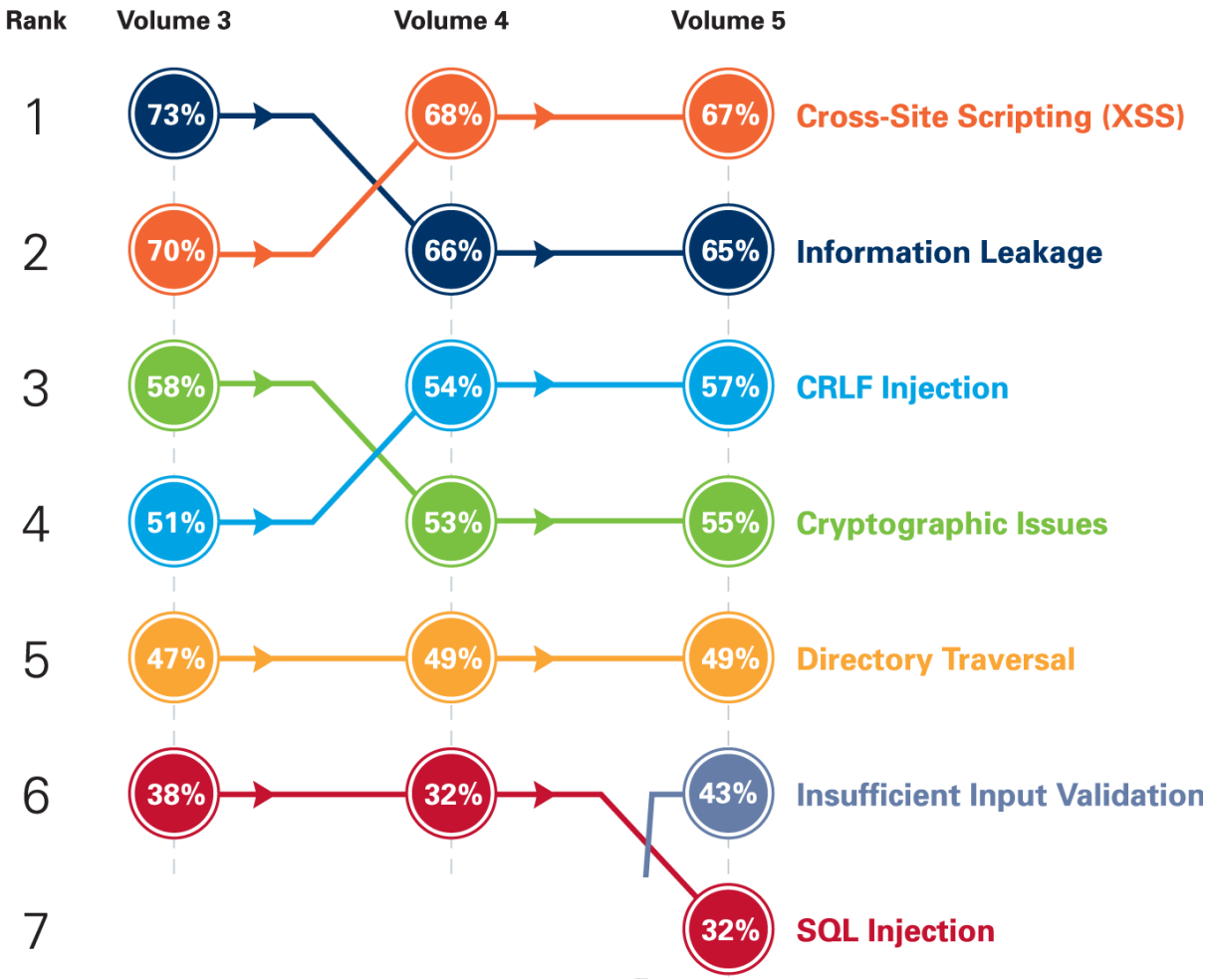
SQL injection prevalence has plateaued, affecting approximately 32% of web applications.

Flat SQL injection trend suggests more attacks in 2013

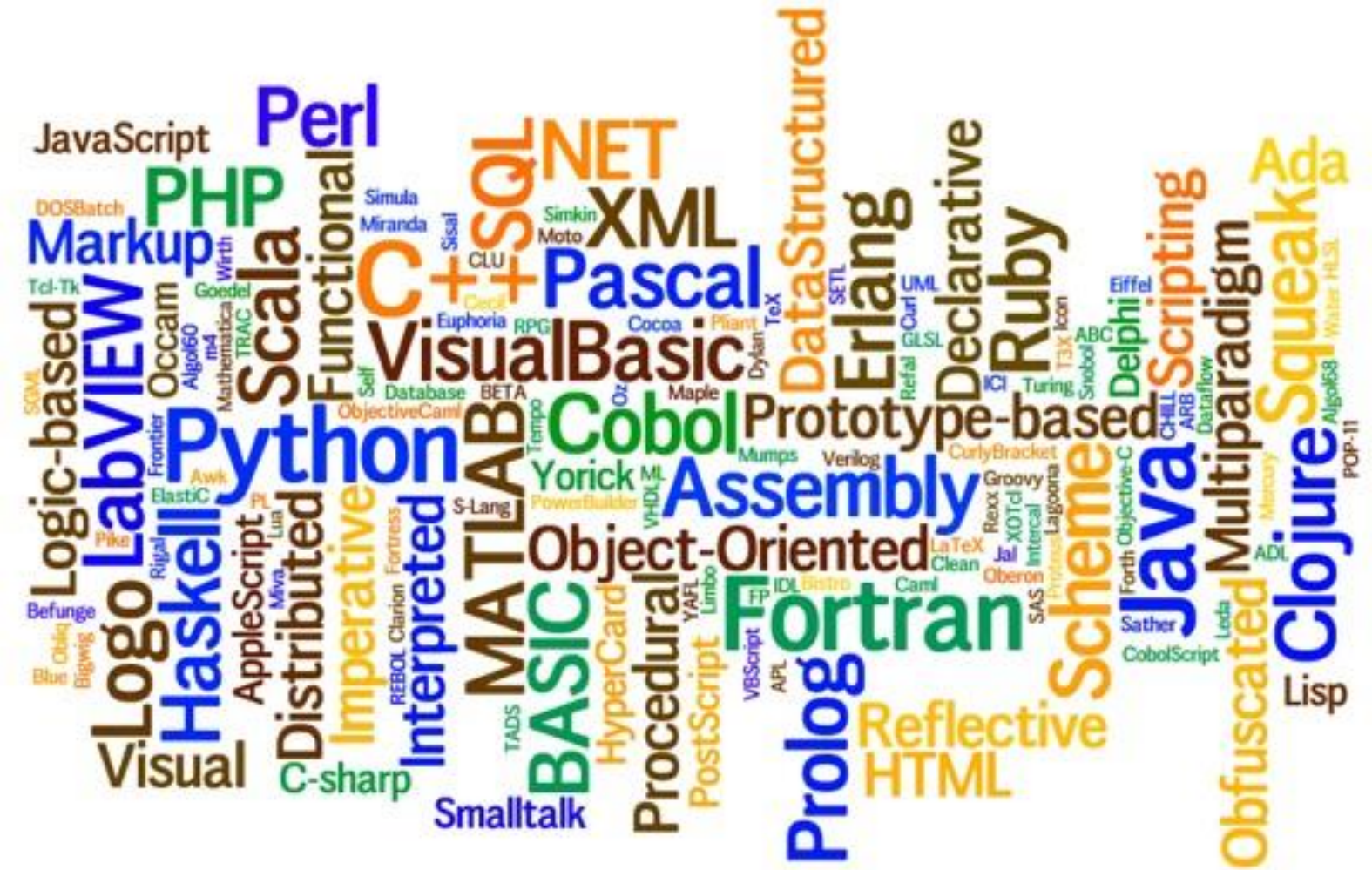


VERACODE

Top Vulnerability Categories (Percentage of Affected Web Application Builds)



Programming Language Selection Matters

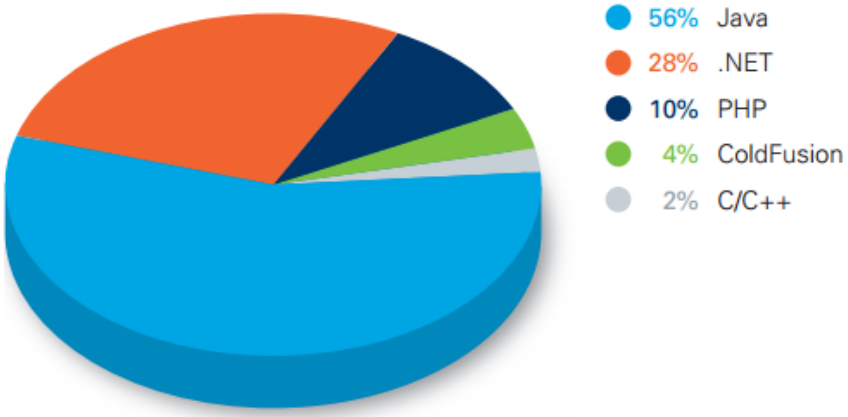


THE TIOBE INDEX: AN INDICATOR OF THE POPULARITY OF VARIOUS LANGUAGES, BASED UPON GLOBAL NUMBERS OF ENGINEERS, COURSES, AND THIRD-PARTY VENDORS

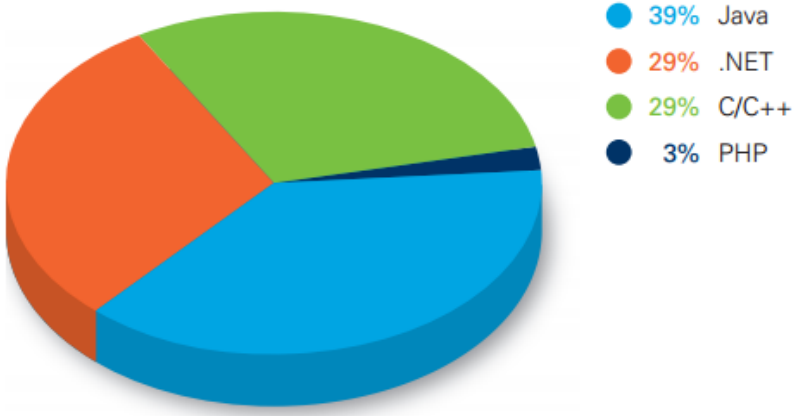
POSITION MARCH 2013	POSITION MARCH 2012	DELTA IN POSITION	PROGRAMMING LANGUAGE	RATINGS MARCH 2013	DELTA MARCH 2012
1	1	=	Java	18.156%	+1.05%
2	2	=	C	17.141%	+0.05%
3	5	↑↑	Objective-C	10.230%	+2.49%
4	4	=	C++	9.115%	+1.07%
5	3	↓↓	C#	6.597%	-1.65%
6	6	=	PHP	4.809%	-0.75%
7	7	=	(Visual)Basic	4.607%	+0.24%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

Language Details

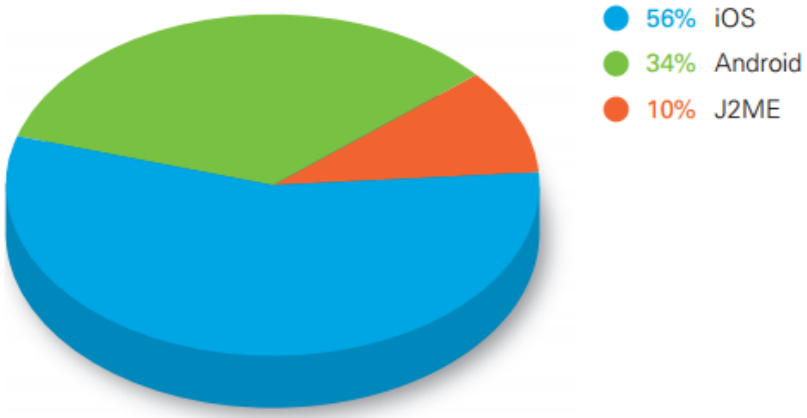
Distribution of Web Applications by Language



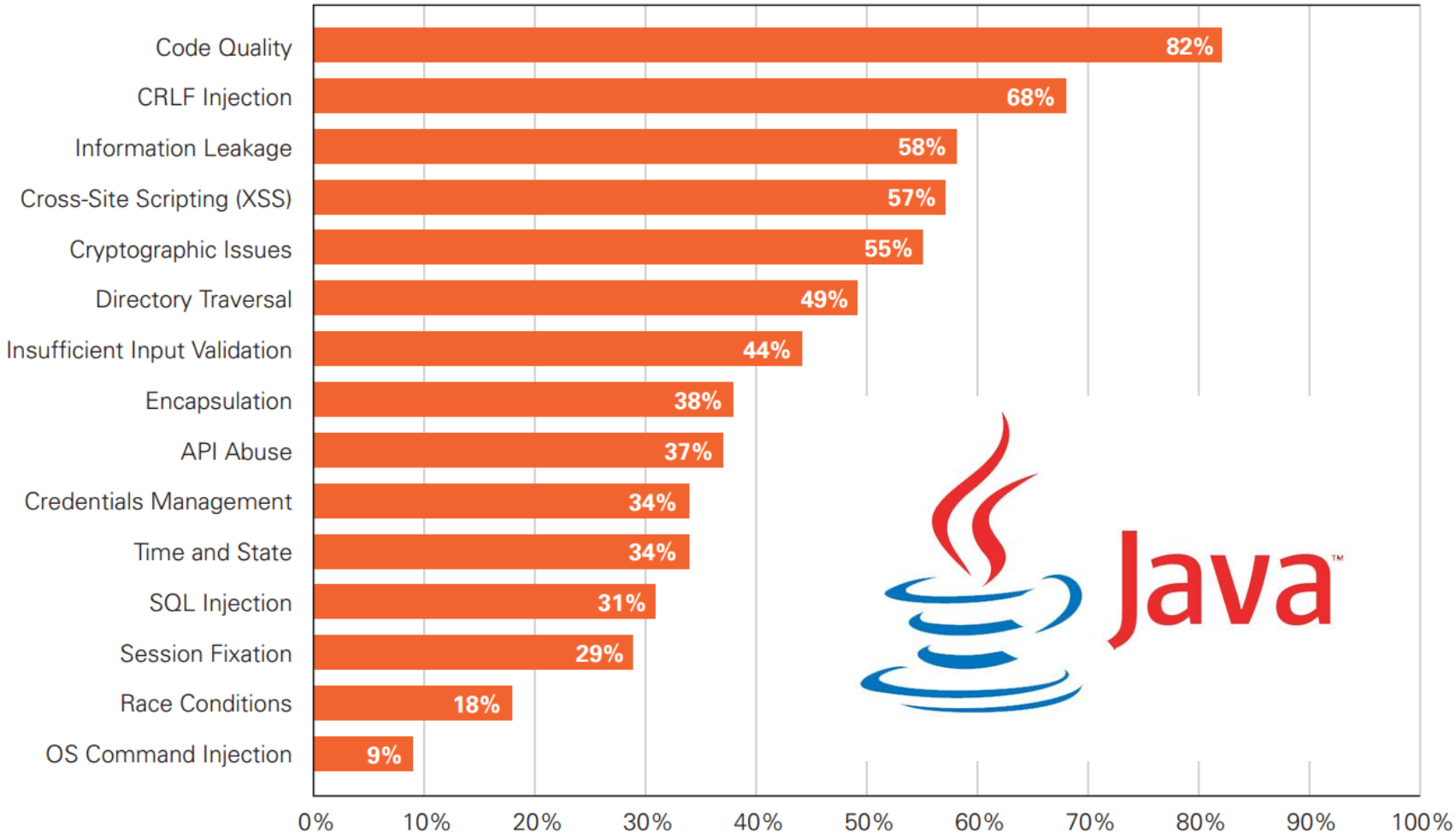
Distribution of Non-Web Applications by Language



Distribution of Mobile Applications by Platform



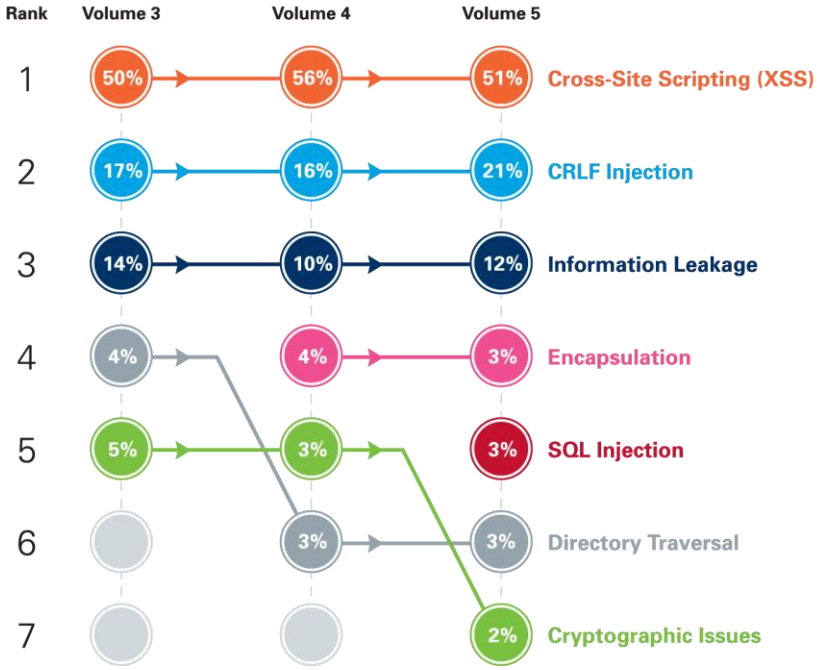
Vulnerability Prevalence in Java Applications (Percentage of Applications Affected)



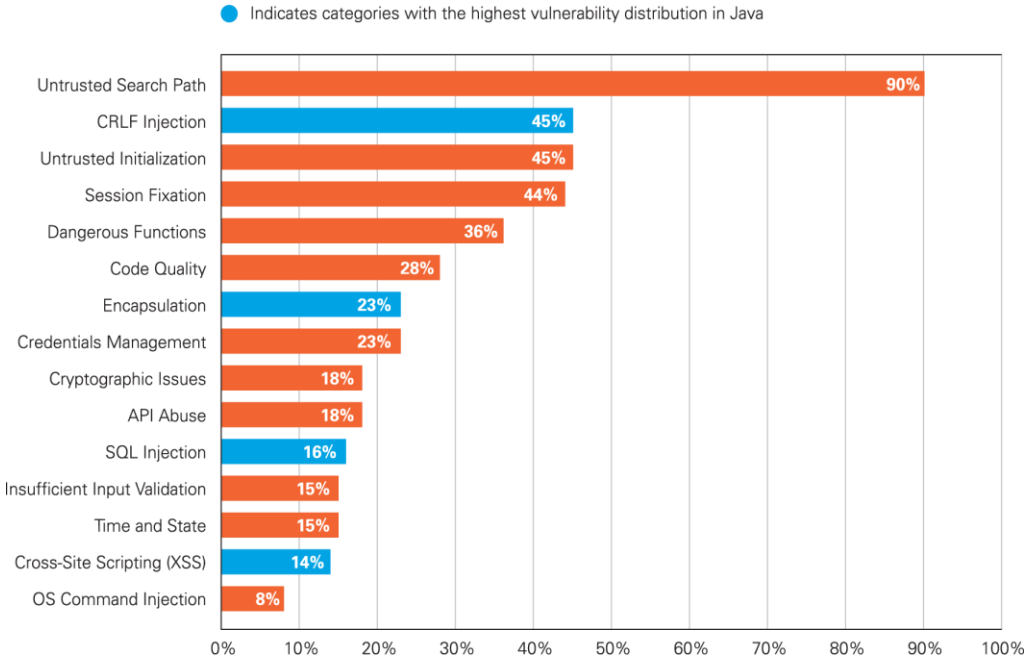
VERACODE

Java Applications

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

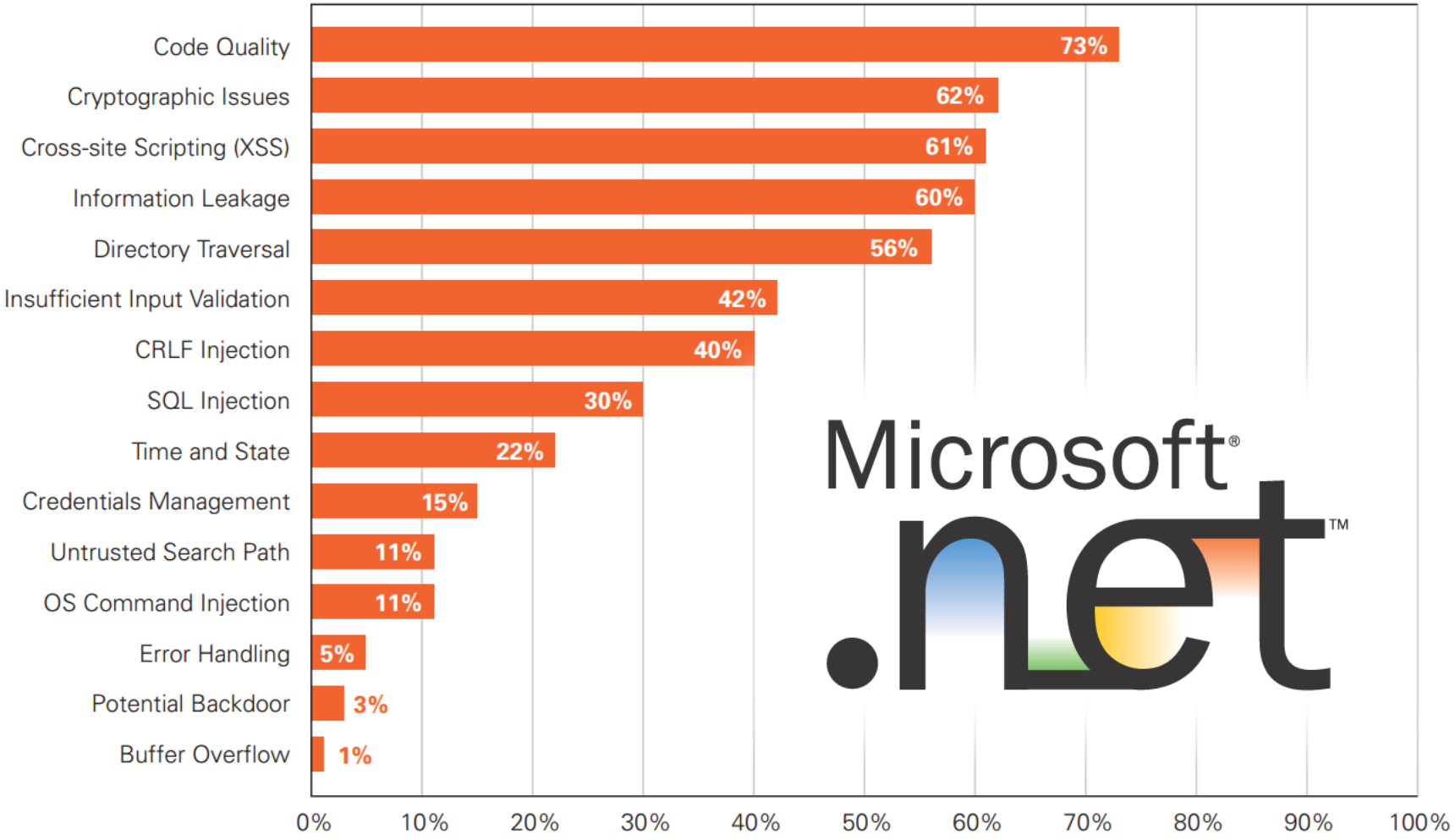


Percent Improvement in Java Vulnerability Distribution from First to Second Submission



VERACODE

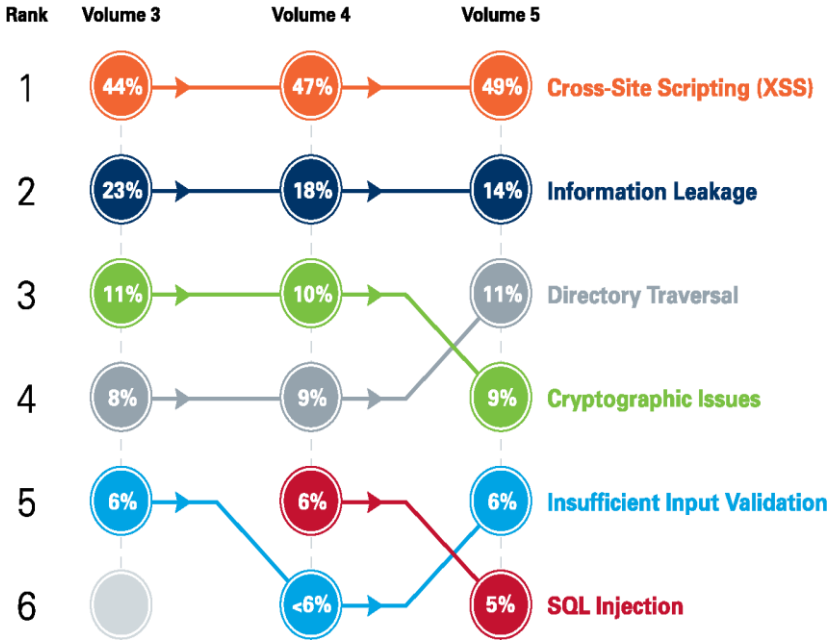
Vulnerability Prevalence in .NET Applications (Percentage of Applications Affected)



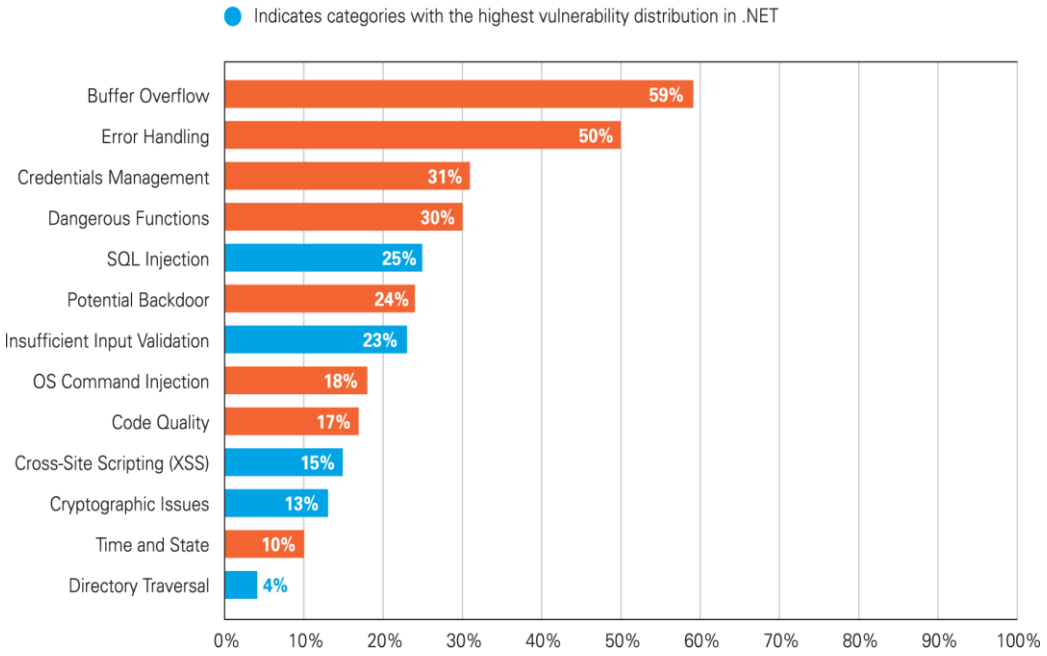
VERACODE

.Net Applications

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

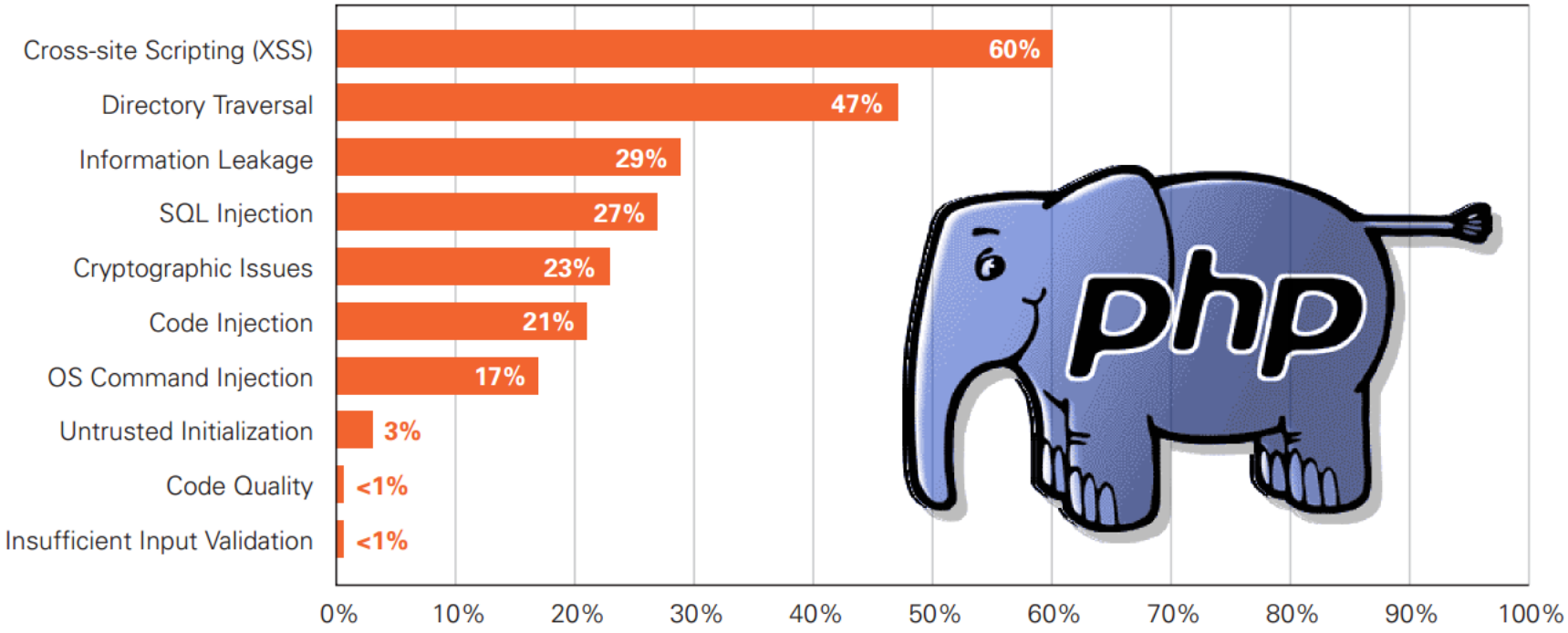


Percent Improvement in .NET Vulnerability Distribution from First to Second Submission



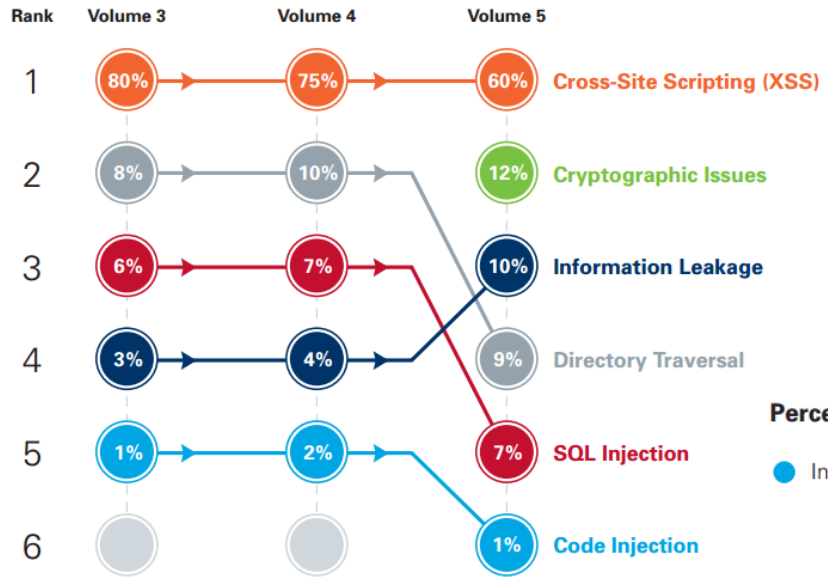
VERACODE

Vulnerability Prevalence in PHP Applications (Percentage of Applications Affected)



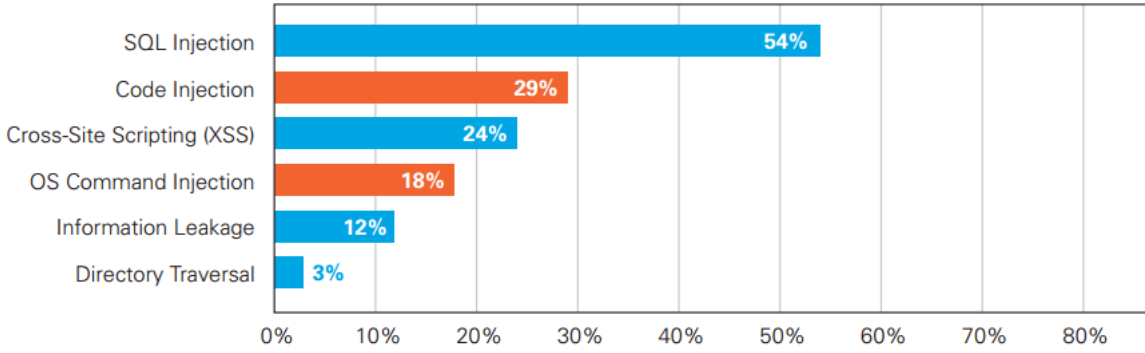
PHP Applications

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



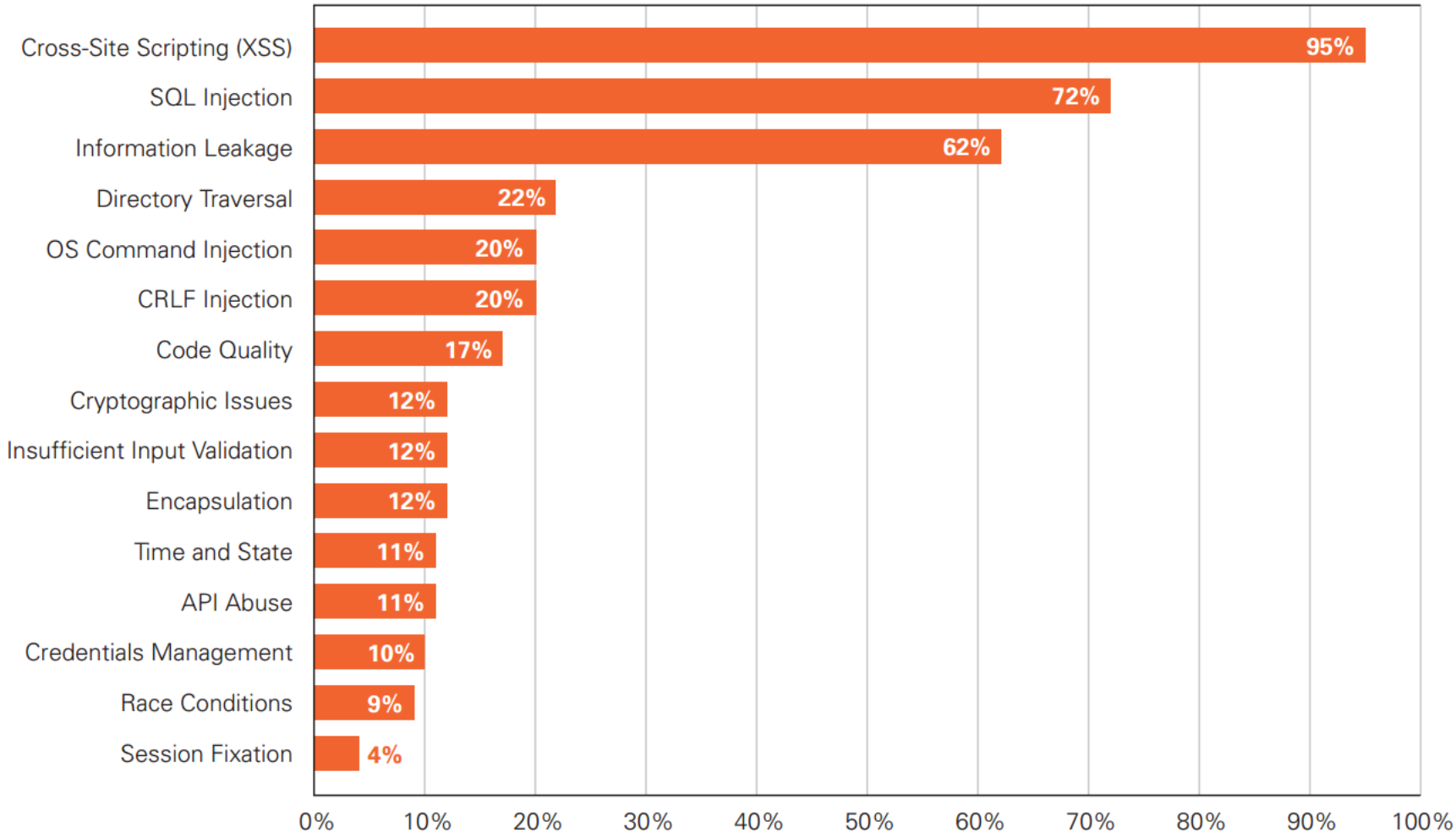
Percent Improvement in PHP Vulnerability Distribution from First to Second Submission

● Indicates categories with the highest vulnerability distribution in PHP



VERACODE

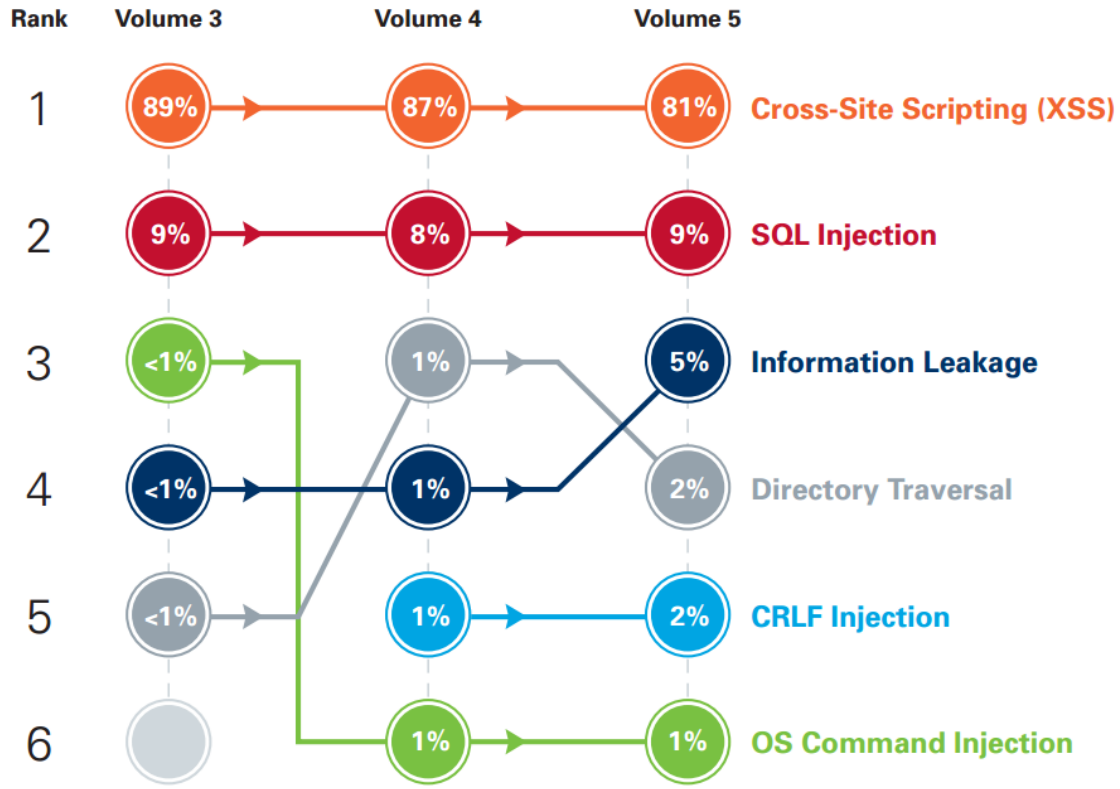
Vulnerability Prevalence in ColdFusion Applications (Percentage of Applications Affected)



VERACODE

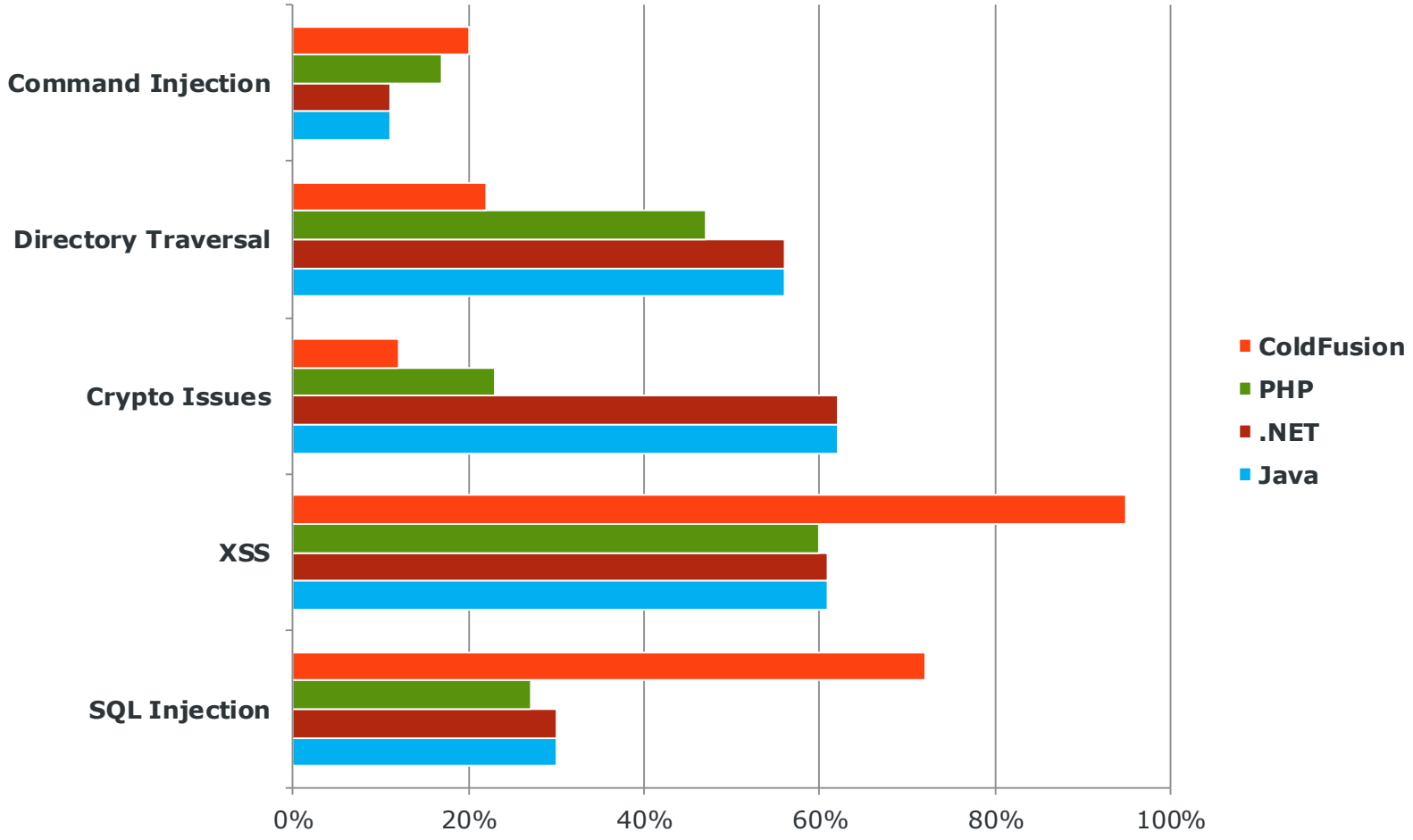
Cold Fusion

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

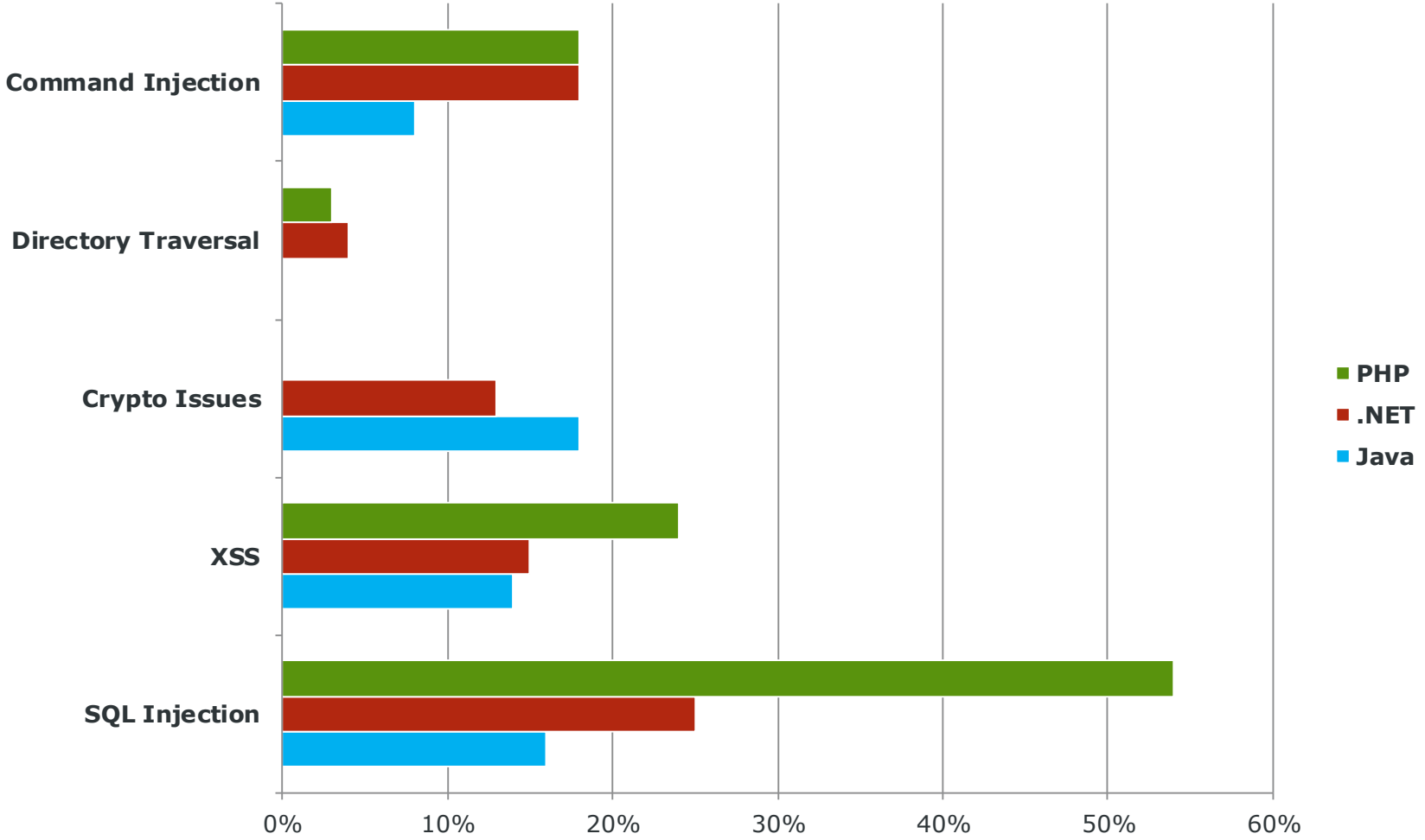


VERACODE

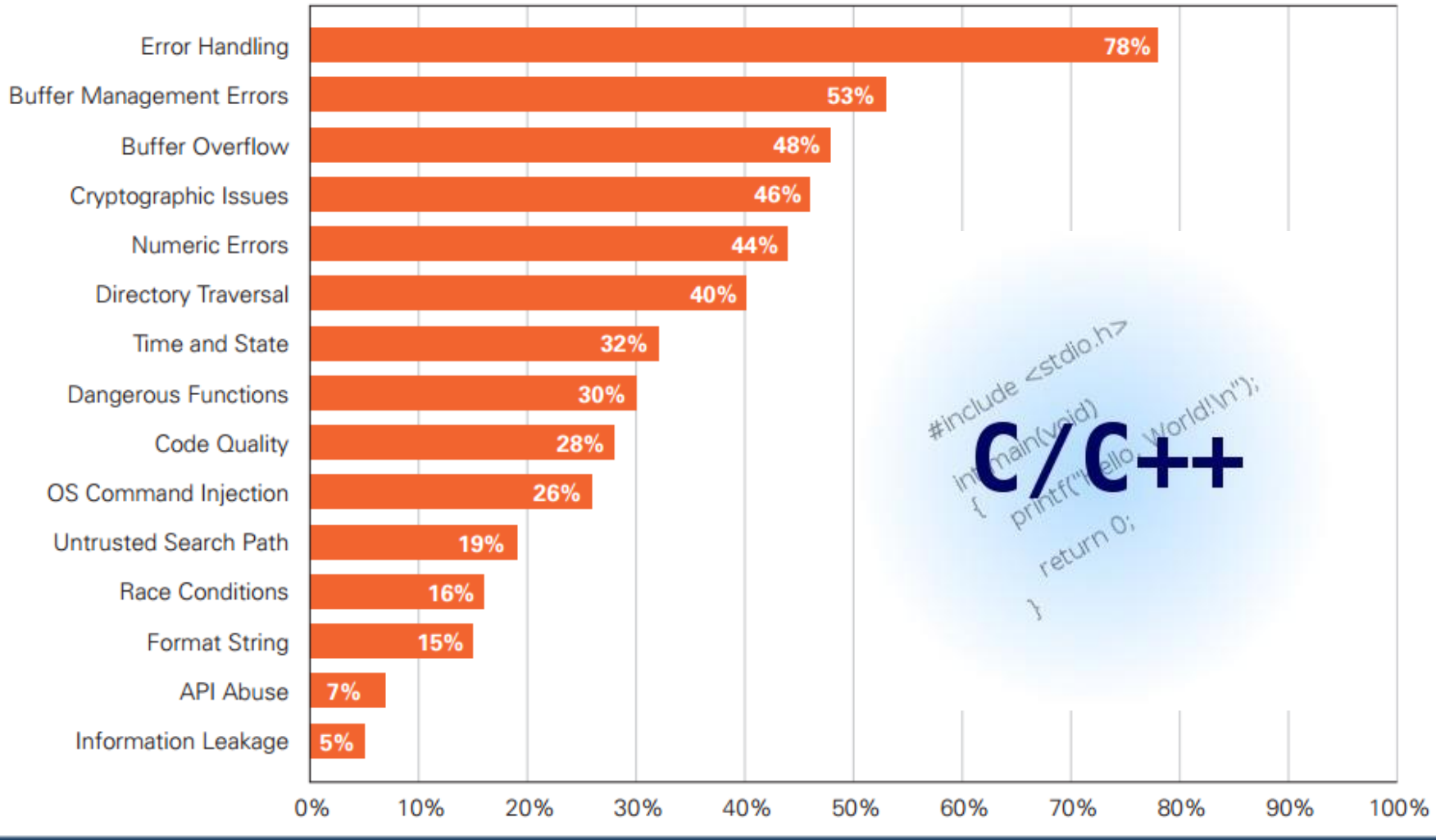
Prevalence of Apps With Flaws by Language



1st to 2nd Test Improvement by Language

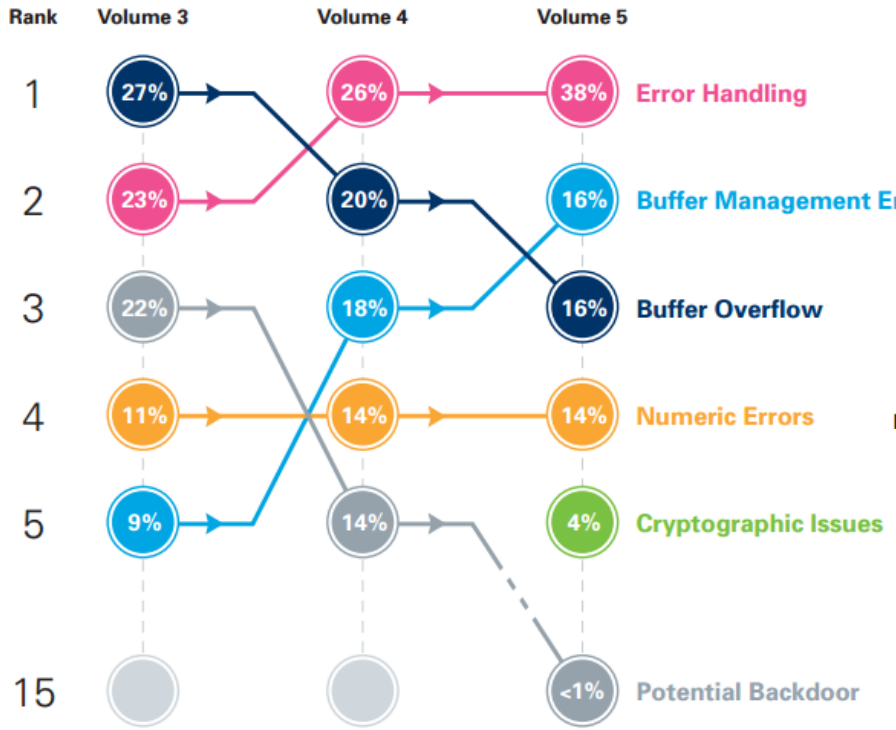


Vulnerability Prevalence in C/C++ Applications (Percentage of Applications Affected)



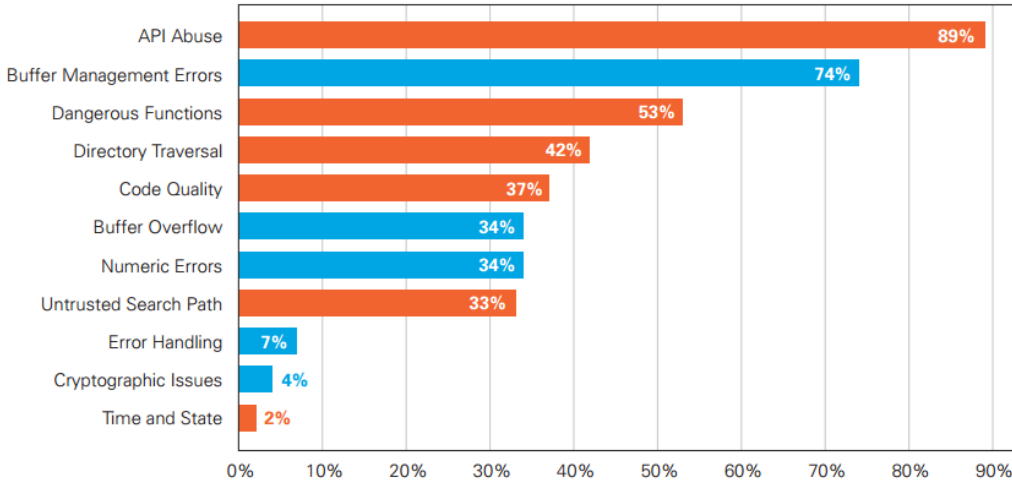
VERACODE

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++

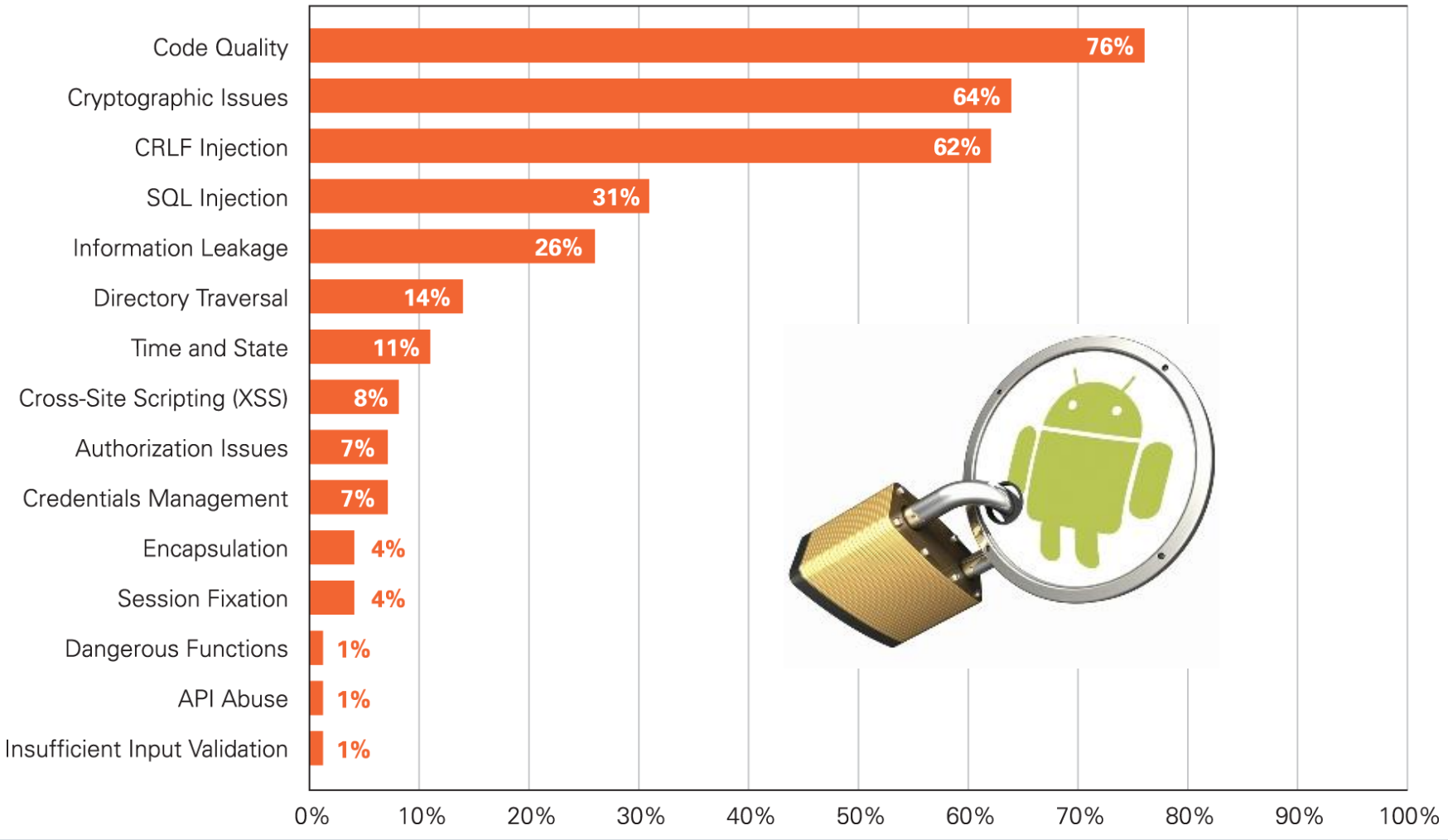


VERACODE

Key Finding:

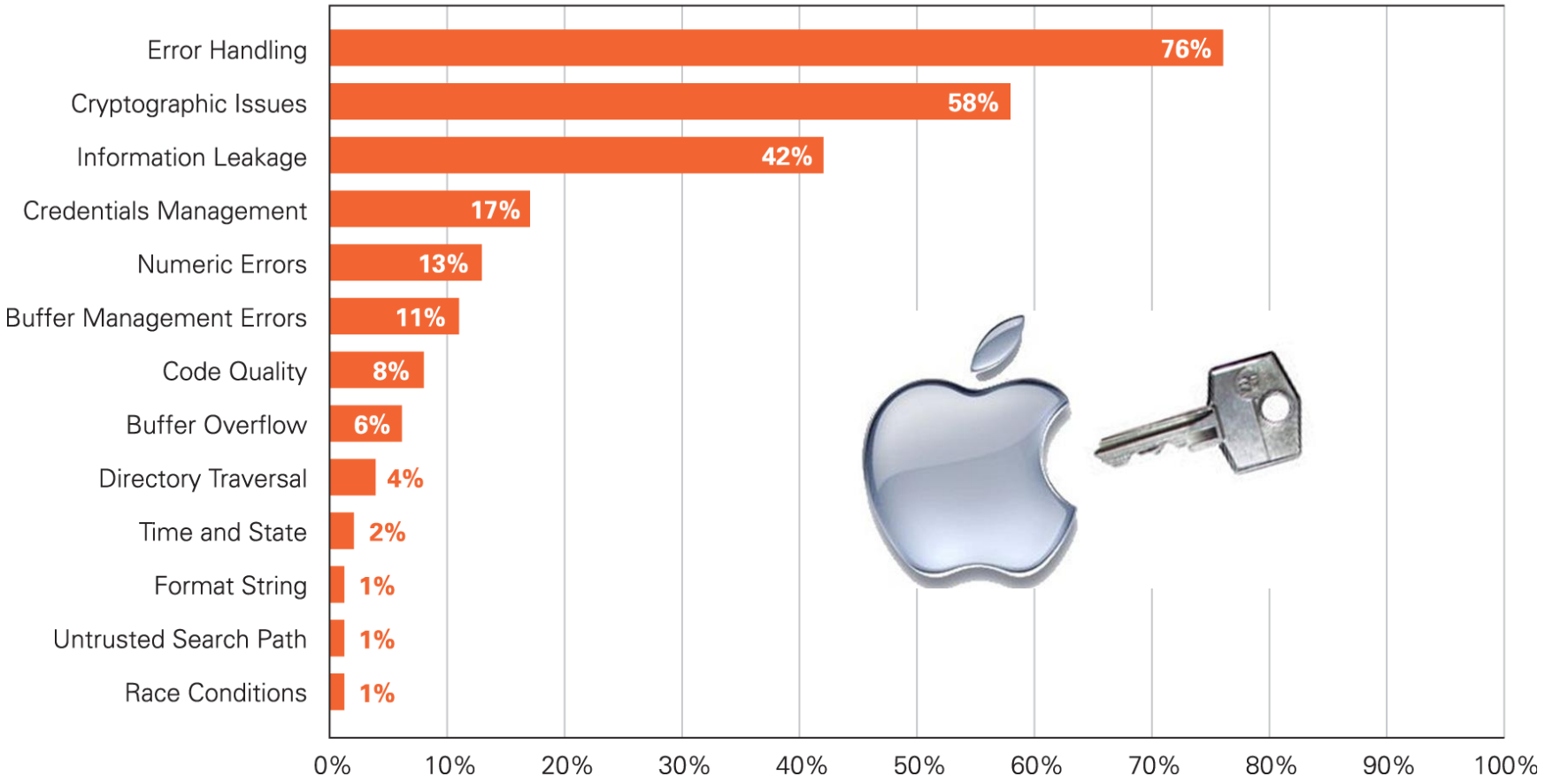
Cryptographic issues affect a sizeable portion of Android (64%) and iOS (58%) applications.

Android Vulnerability Prevalence (Percentage of Applications Affected)



VERACODE

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



VERACODE

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%

VERACODE

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 Turn-over for Security Professionals.
- Default Encryption, Not “Opt-in,” Will Become the Norm.

Questions?

cwysopal@veracode.com
@weldpond