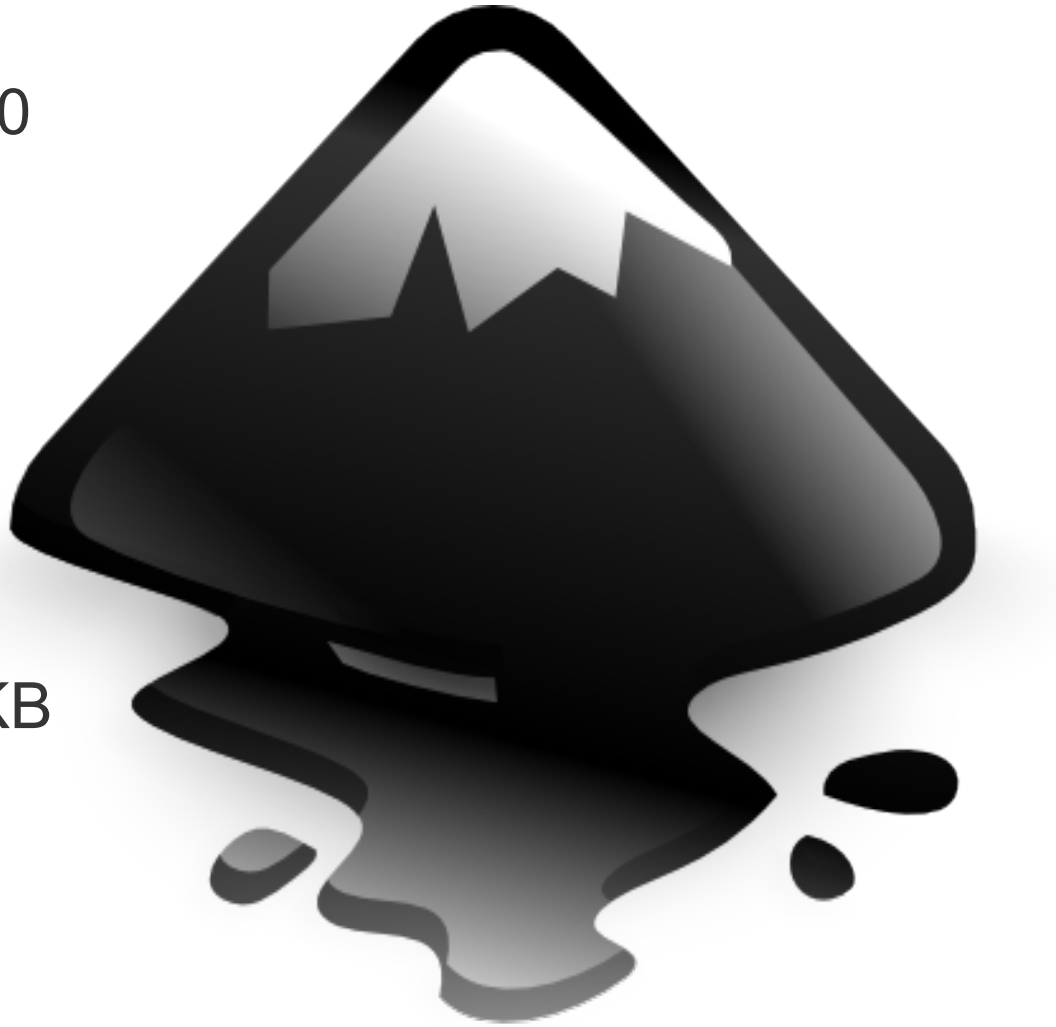
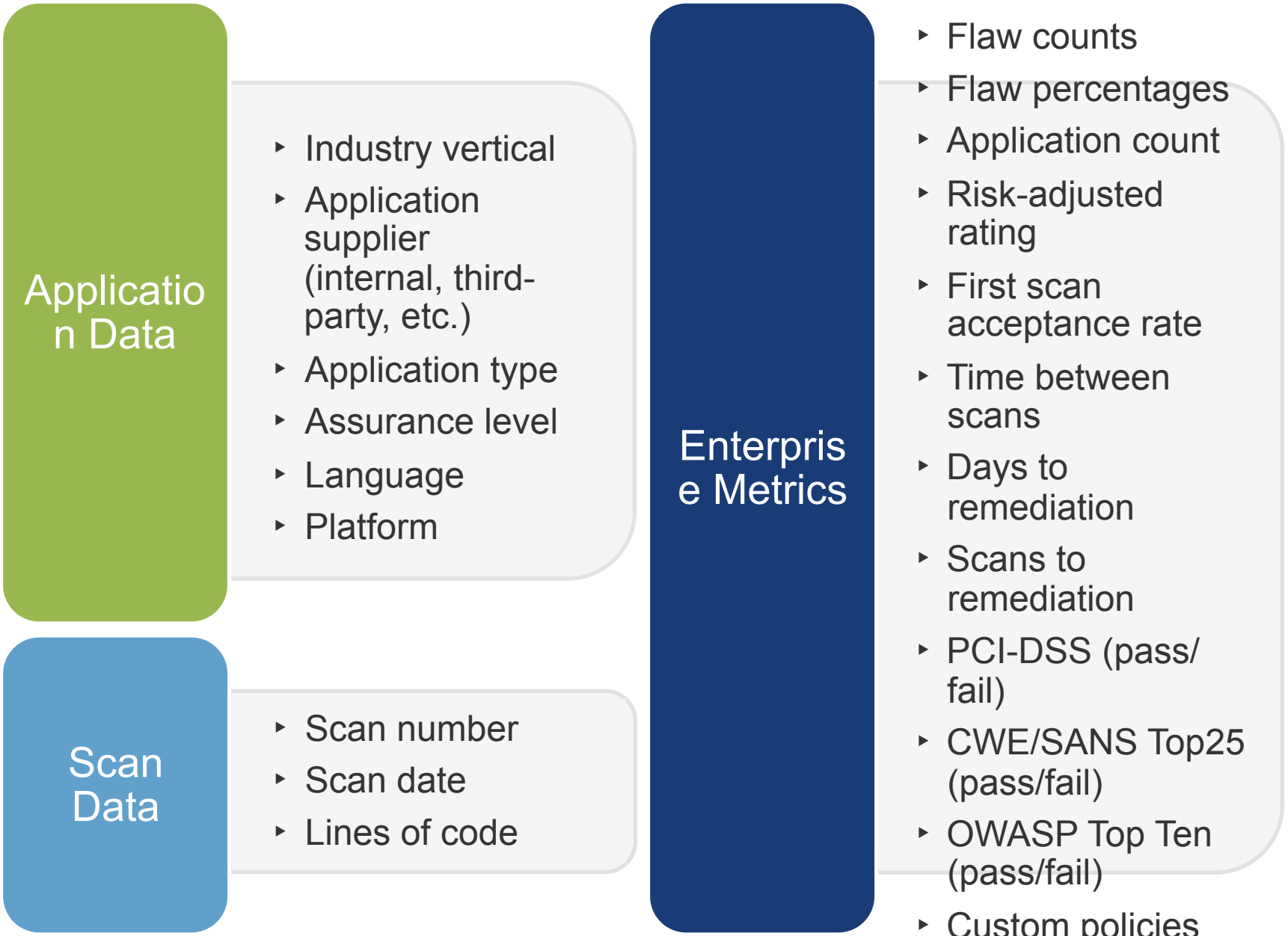
Data Mining a Mountain of Zero Day Vulnerabilities

Chris Wysopal
CTO & Co-founder

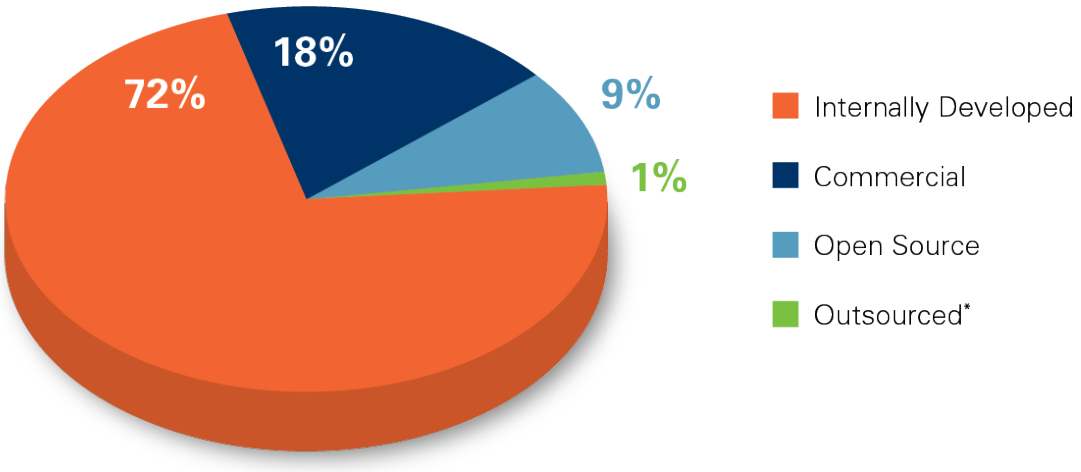
The Data Set

- Applications from over 300 commercial and US government customers
- **Scanned** 9,910 applications over past 18 months
- Ranged in size from 100KB to 6GB
- Software was pre-release and in production
- Internally built, outsourced, and commercial ISV code

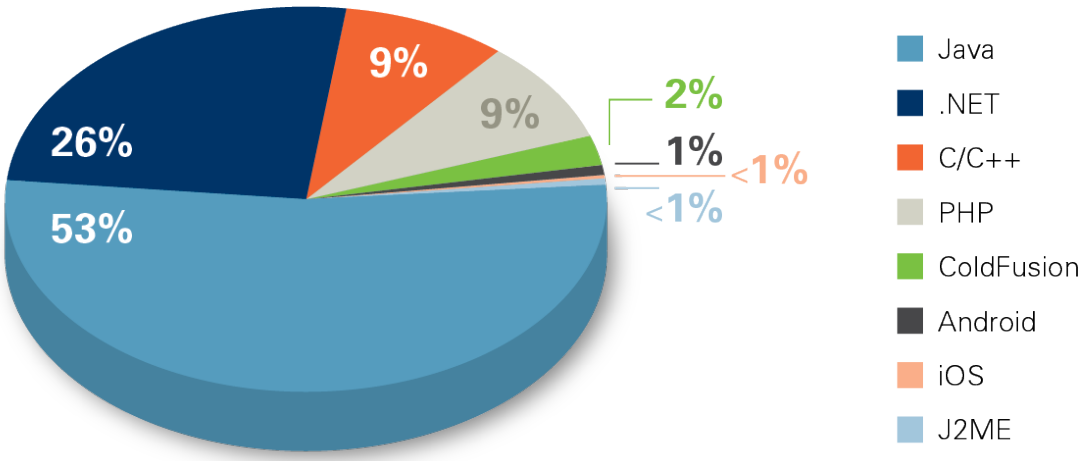



Application Data
Industry vertical
Application supplier (internal, third-party, etc.)
Application type
Assurance level
Language
Platform
Scan Data
Scan number
Scan date
Lines of code
Enterprise Metrics
Flaw counts
Flaw percentages
Application count
Risk-adjusted rating
First scan acceptance rate
Time between scans
Days to remediation
Scans to remediation
PCI-DSS (pass/fail)
CWE/SANS Top25 (pass/fail)
OWASP Top Ten (pass/fail)
Custom policies

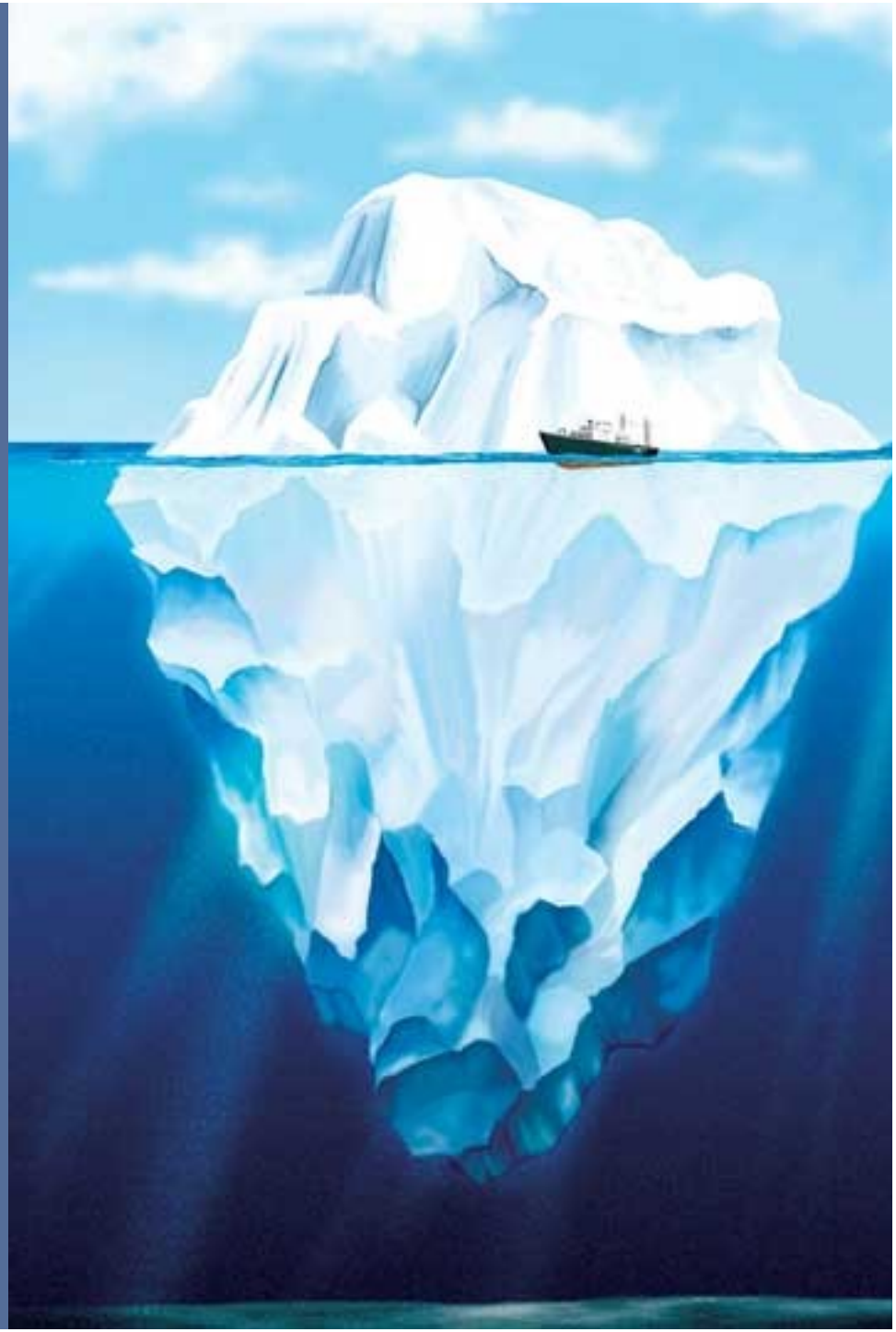
Applications by Supplier Type



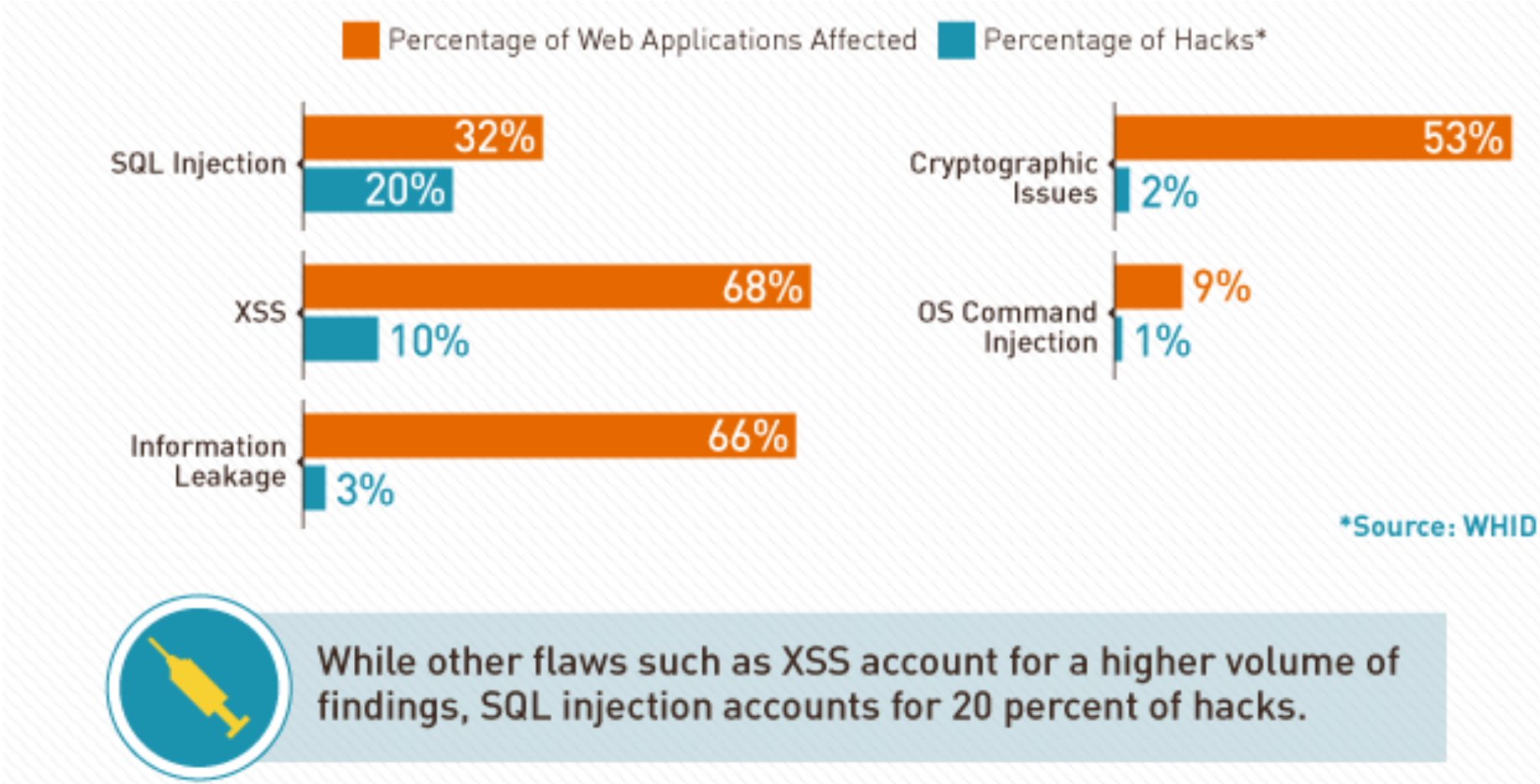
Applications by Language Family



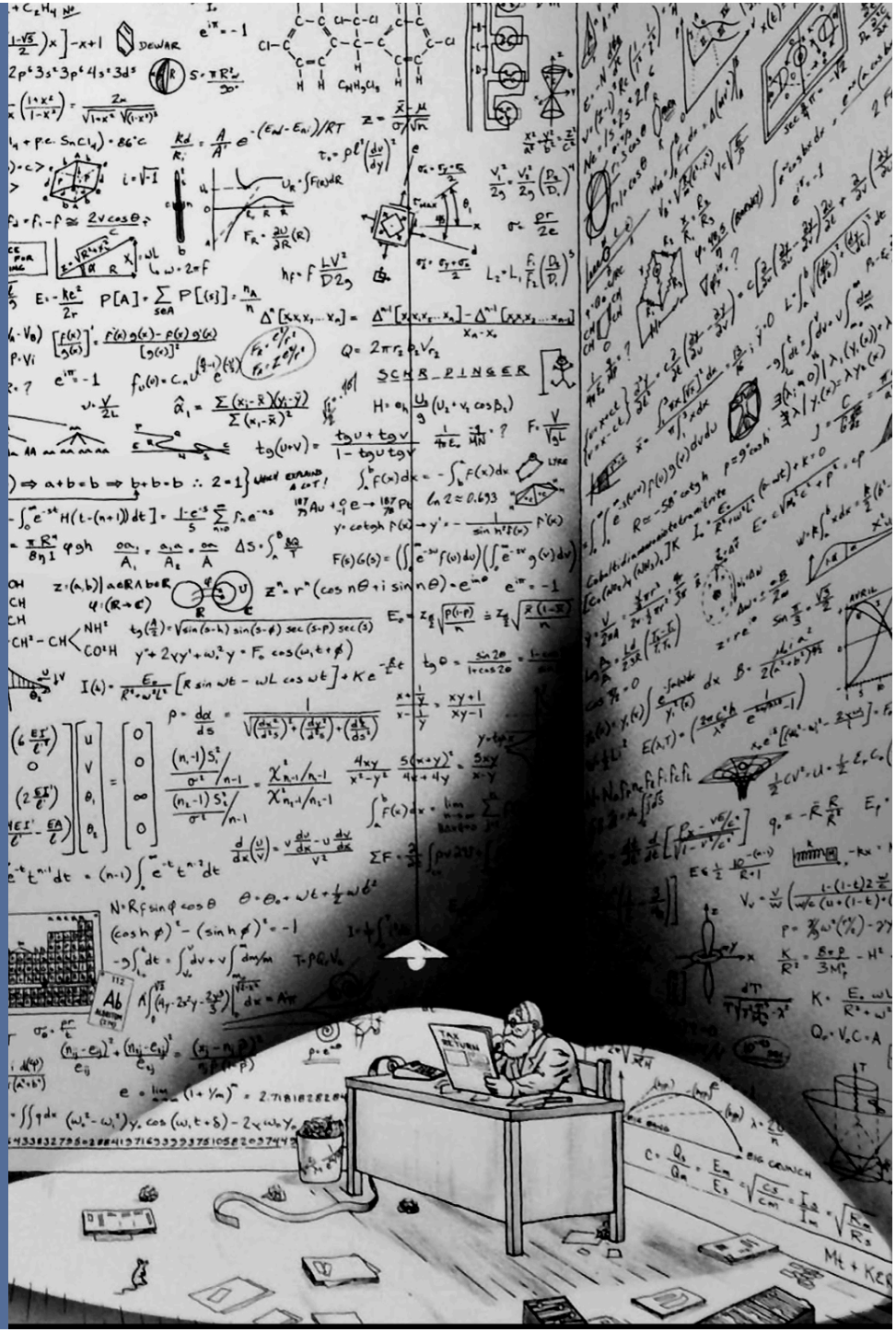
The latent Vulnerabiliesvs. The Attacks



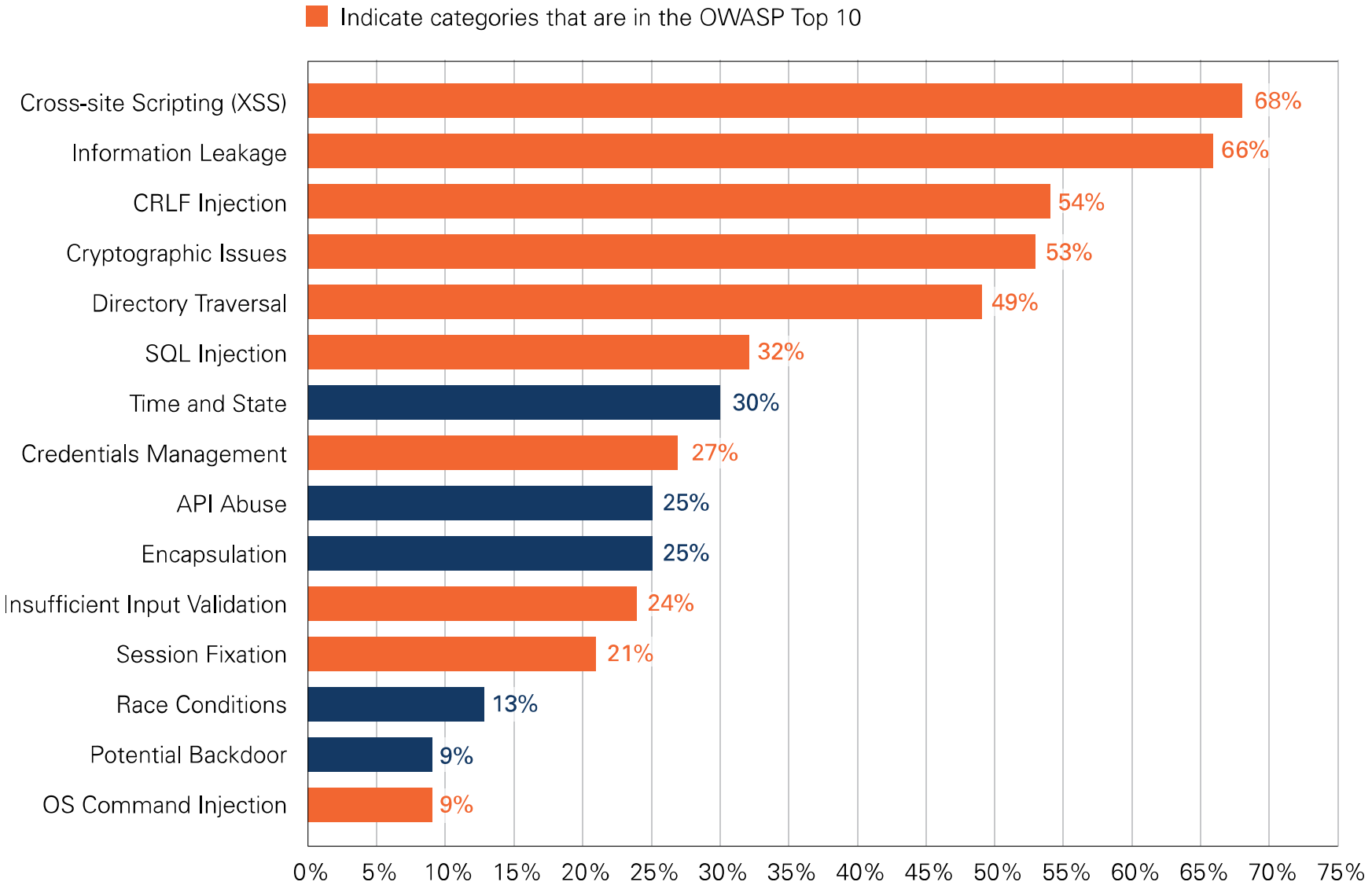
Top 5 Attacked Web Application Vulnerabilities



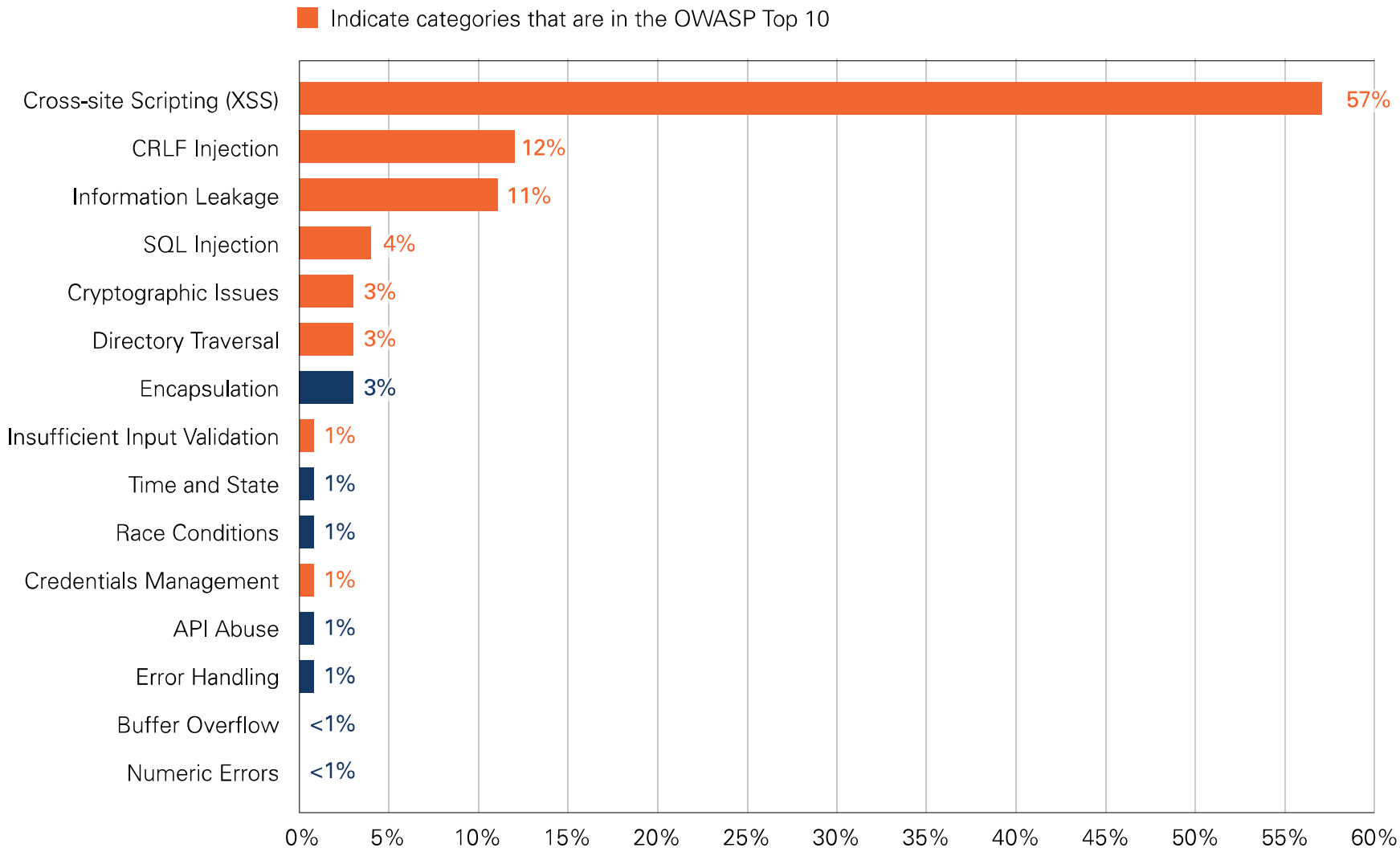
Let’s take a closer look at the numbers



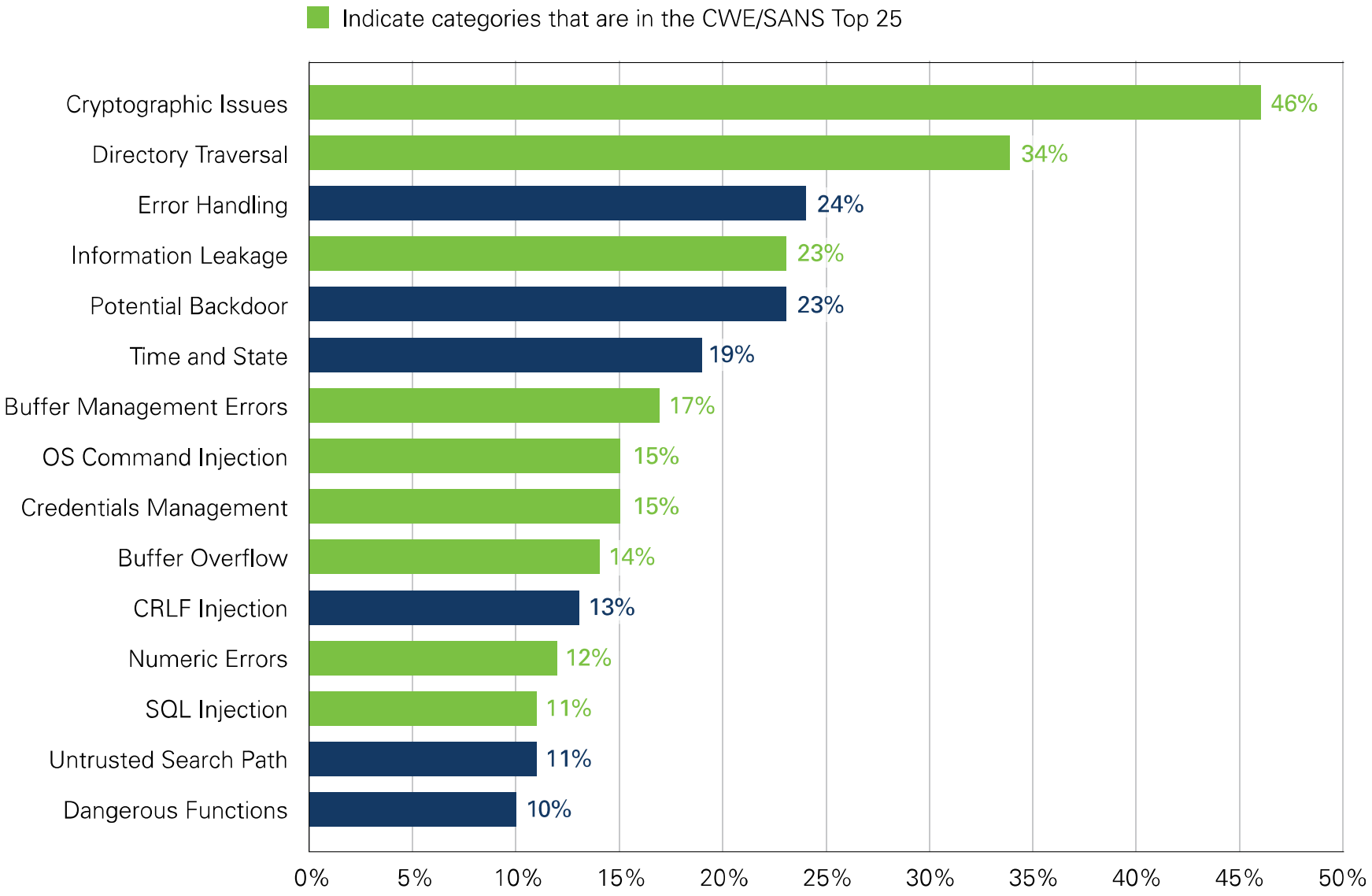
Top Vulnerability Categories
(Percent of Applications Affected for Web Applications)



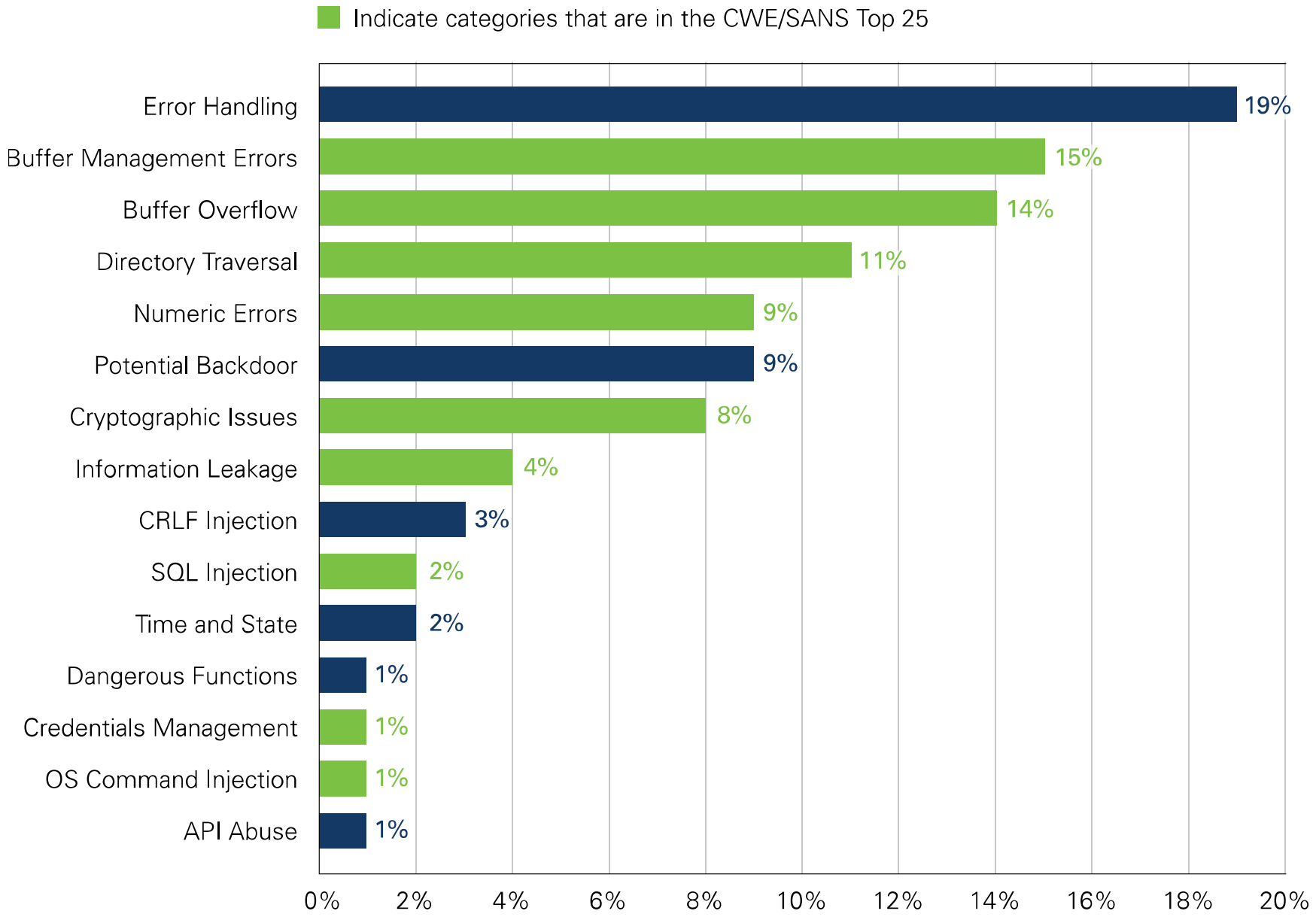
Top Vulnerability Categories
(Overall Prevalence for Web Applications)



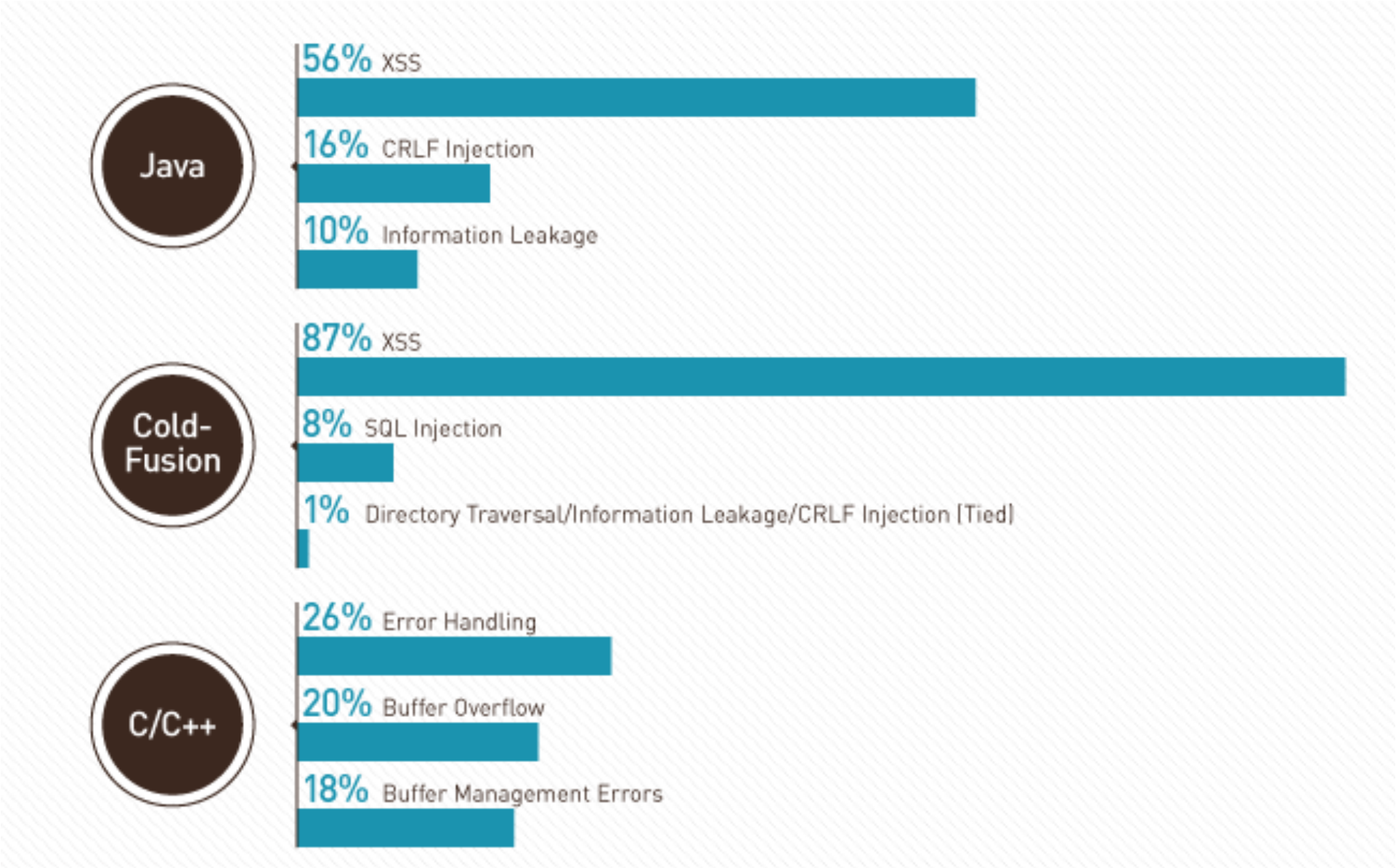
Top Vulnerability Categories
(Percentage of Applications Affected for Non-Web Applications)



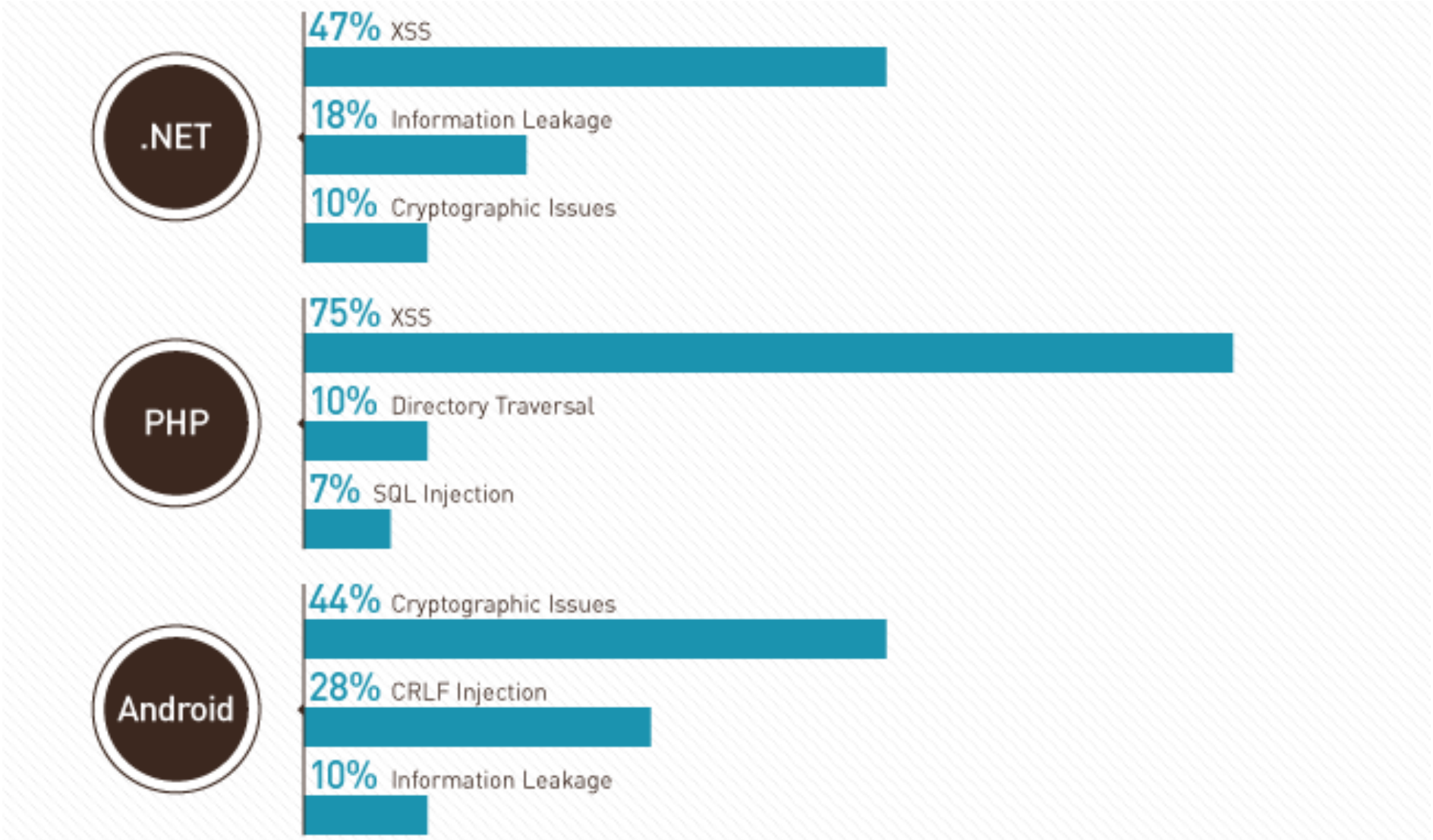
Top Vulnerability Categories
(Overall Prevalence for Non-Web Applications)



Top 3 Vulnerabilities by Language



Top 3 Vulnerabilities by Language



Different developers deliver different vulns

Vulnerability Distribution by Supplier

Internally Developed		Commercial		Open Source		Outsourced*	
Cross-site Scripting (XSS)	58%	Cross-site Scripting (XSS)	44%	Cross-site Scripting (XSS)	41%	CRLF Injection	47%
CRLF Injection	12%	Information Leakage	11%	Directory Traversal	13%	Cross-site Scripting (XSS)	28%
Information Leakage	10%	CRLF Injection	8%	Information Leakage	13%	Information Leakage	6%
SQL Injection	4%	Directory Traversal	6%	CRLF Injection	11%	Encapsulation	6%
Cryptographic Issues	3%	Error Handling	5%	Cryptographic Issues	8%	Cryptographic Issues	5%
Encapsulation	3%	Cryptographic Issues	5%	SQL Injection	3%	Credentials Mgmt	3%
Directory Traversal	3%	Buffer Mgmt Errors	4%	Error Handling	2%	Directory Traversal	2%
Insufficient Input Validation	1%	Buffer Overflow	3%	Time and State	2%	API Abuse	1%
Time and State	1%	Potential Backdoor	3%	API Abuse	2%	Time and State	1%
Race Conditions	1%	SQL Injection	3%	Insufficient Input Validation	1%	Insufficient Input Validation	1%

Table 2: Vulnerability Distribution by Supplier

*(*Small sample size)*

Different developers deliver different vulns

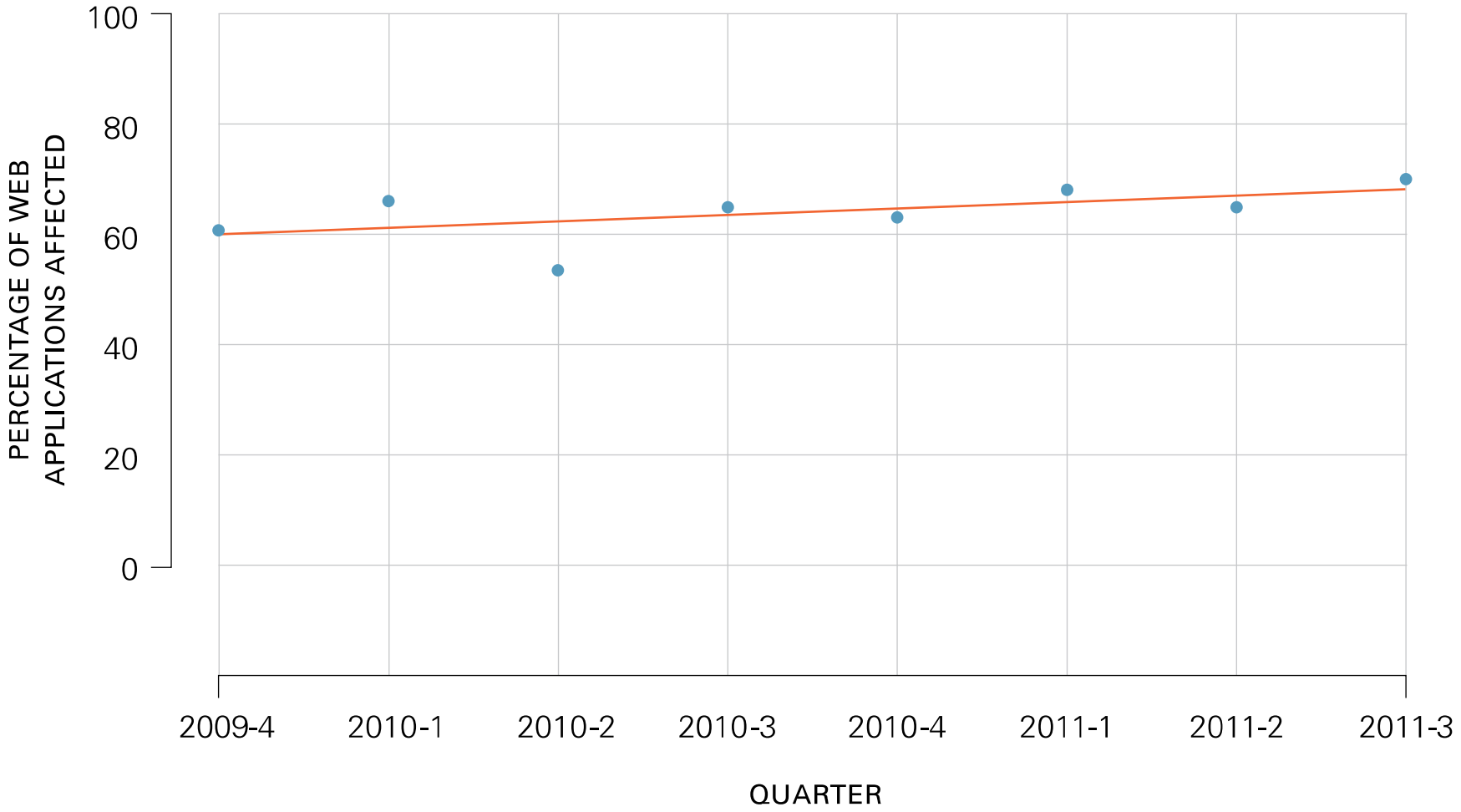
Vulnerability distribution by industry

Government		Finance		Software	
Cross-site Scripting (XSS)	75%	Information Leakage	68%	Cryptographic Issues	59%
Information Leakage	66%	Cross-site Scripting (XSS)	67%	Information Leakage	59%
SQL Injection	40%	Cryptographic Issues	53%	Cross-site Scripting (XSS)	55%
Cryptographic Issues	35%	CRLF Injection	51%	CRLF Injection	54%
Directory Traversal	31%	Directory Traversal	47%	Directory Traversal	54%
Insufficient Input Validation	27%	Insufficient Input Validation	30%	Time and State	39%
CRLF Injection	27%	SQL Injection	29%	Credentials Mgmt	31%
OS Command Injection	19%	Time and State	28%	SQL Injection	30%
Time and State	18%	API Abuse	26%	API Abuse	25%
Credentials Mgmt	16%	Encapsulation	25%	Encapsulation	23%
API Abuse	14%	Credentials Mgmt	24%	Session Fixation	18%
Potential Backdoor	12%	Session Fixation	19%	OS Command Injection	14%
Session Fixation	11%	Race Conditions	13%	Potential Backdoor	14%
Encapsulation	11%	Potential Backdoor	10%	Race Conditions	13%
Untrusted Search Path	3%	OS Command Injection	6%	Insufficient Input Validation	13%

Are DEVELOPERs making any progress at eradicating cross-site scripting or sql injection?

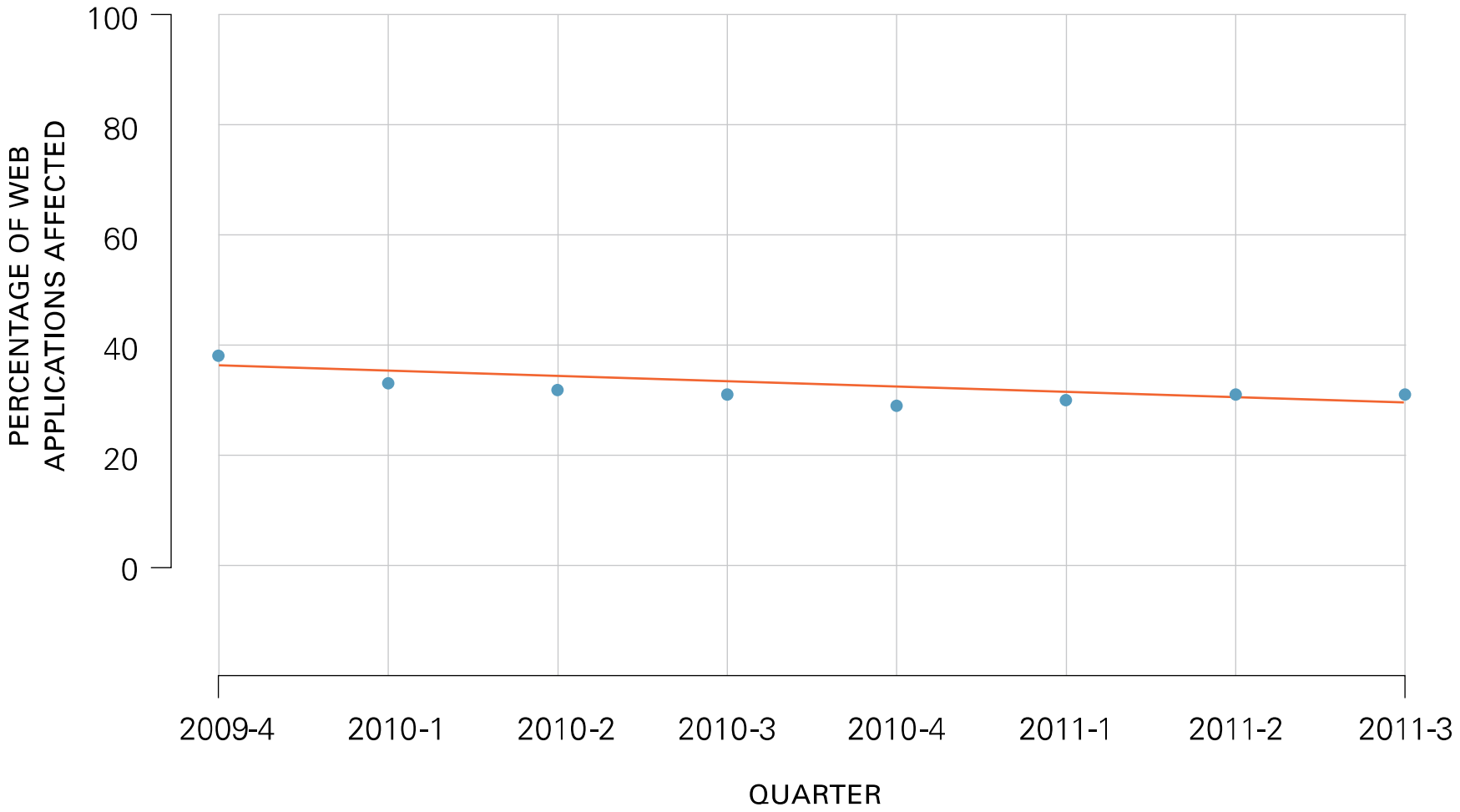
Quarterly Trend for XSS

pvalue = 0.124: Statistically, the trend is flat.



Quarterly Trend for SQL Injection

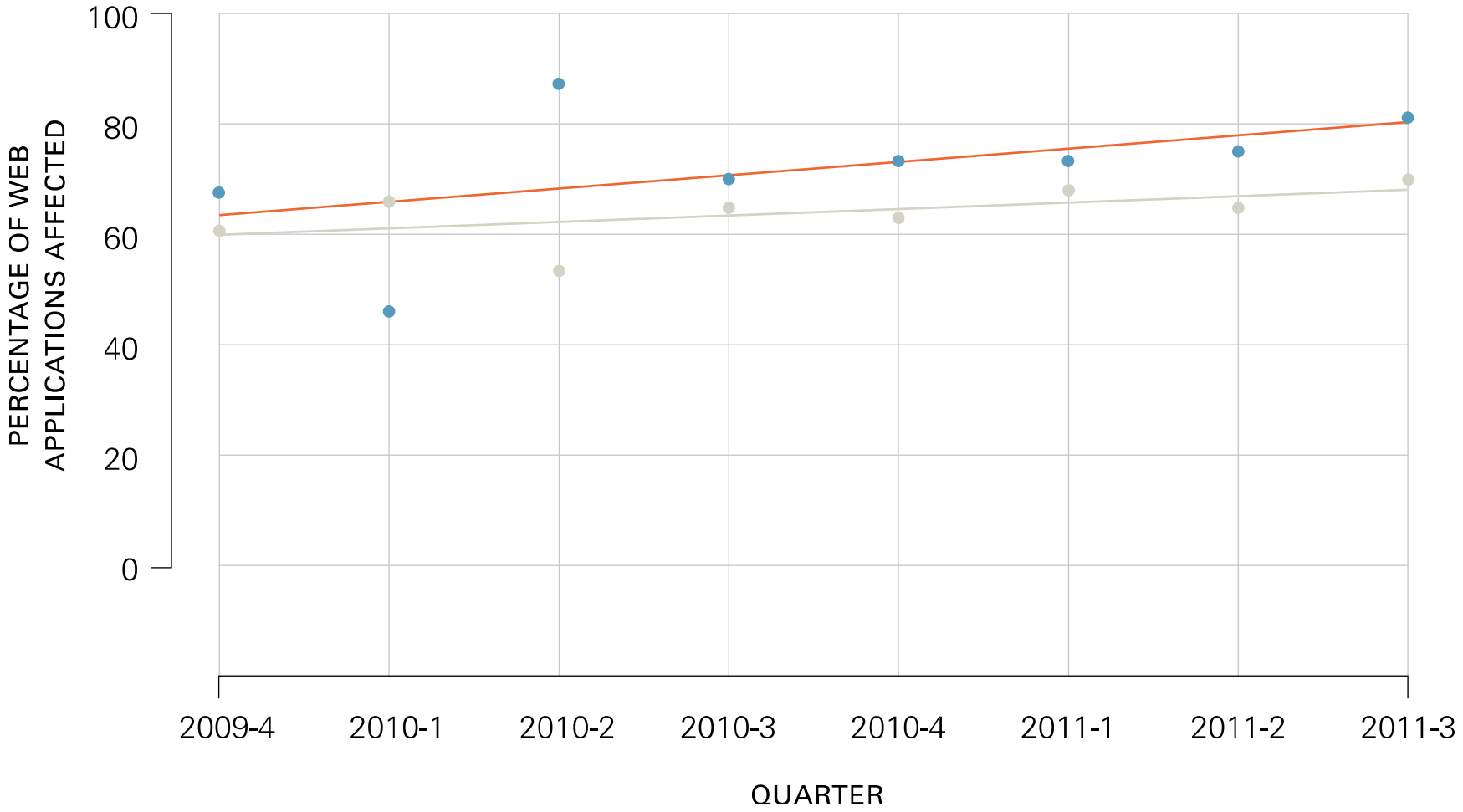
pvalue = 0.048: Statistically, the trend is down.



Dare we ask, How is the U.S. government sector doing?

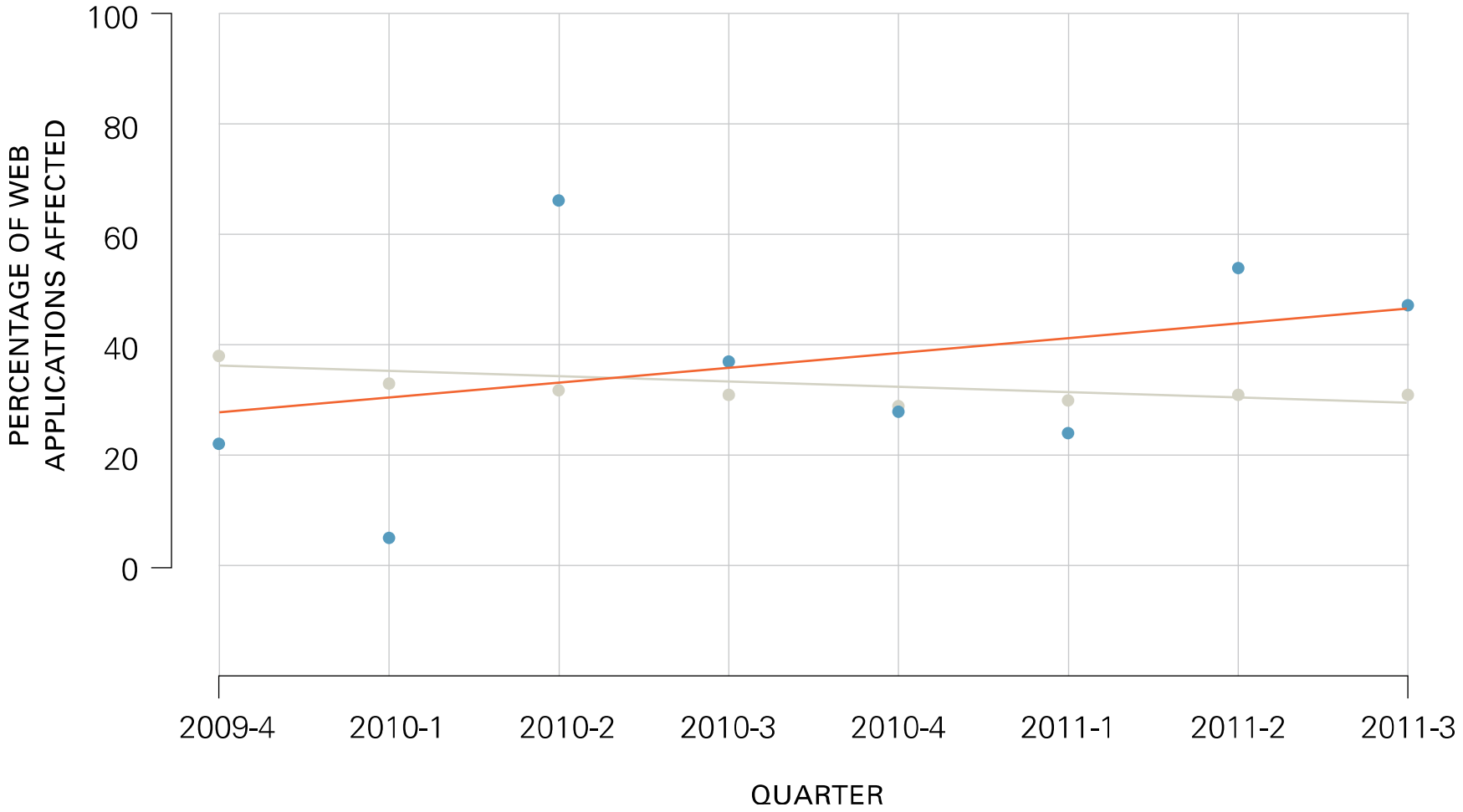
Quarterly Trend for XSS in Government Web Applications

pvalue = 0.215: Statistically, the trend is flat.



Quarterly Trend for SQL Injection in Government Web Applications

pvalue = 0.343: Statistically, the trend is flat.



What percentage of WEB applications fail OWASP TOP TEN?

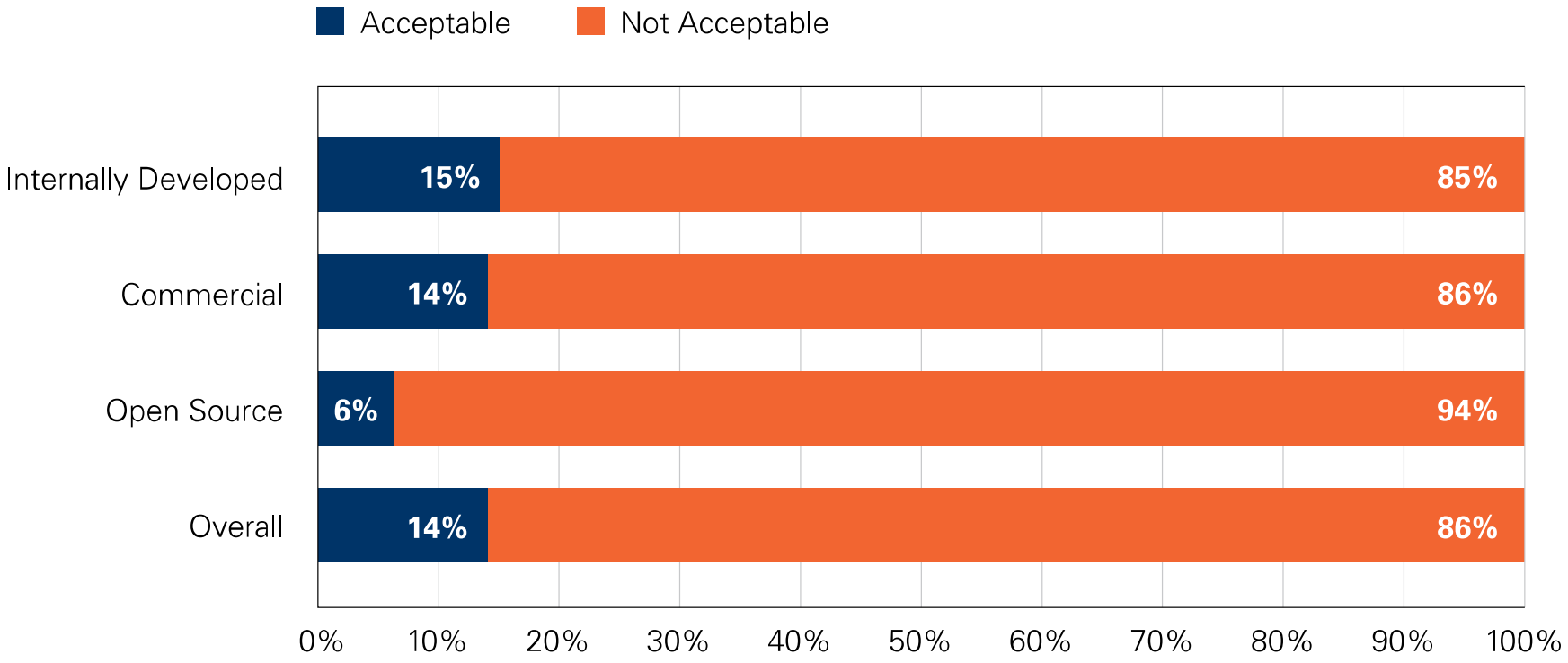
a) 34%

b) 57%

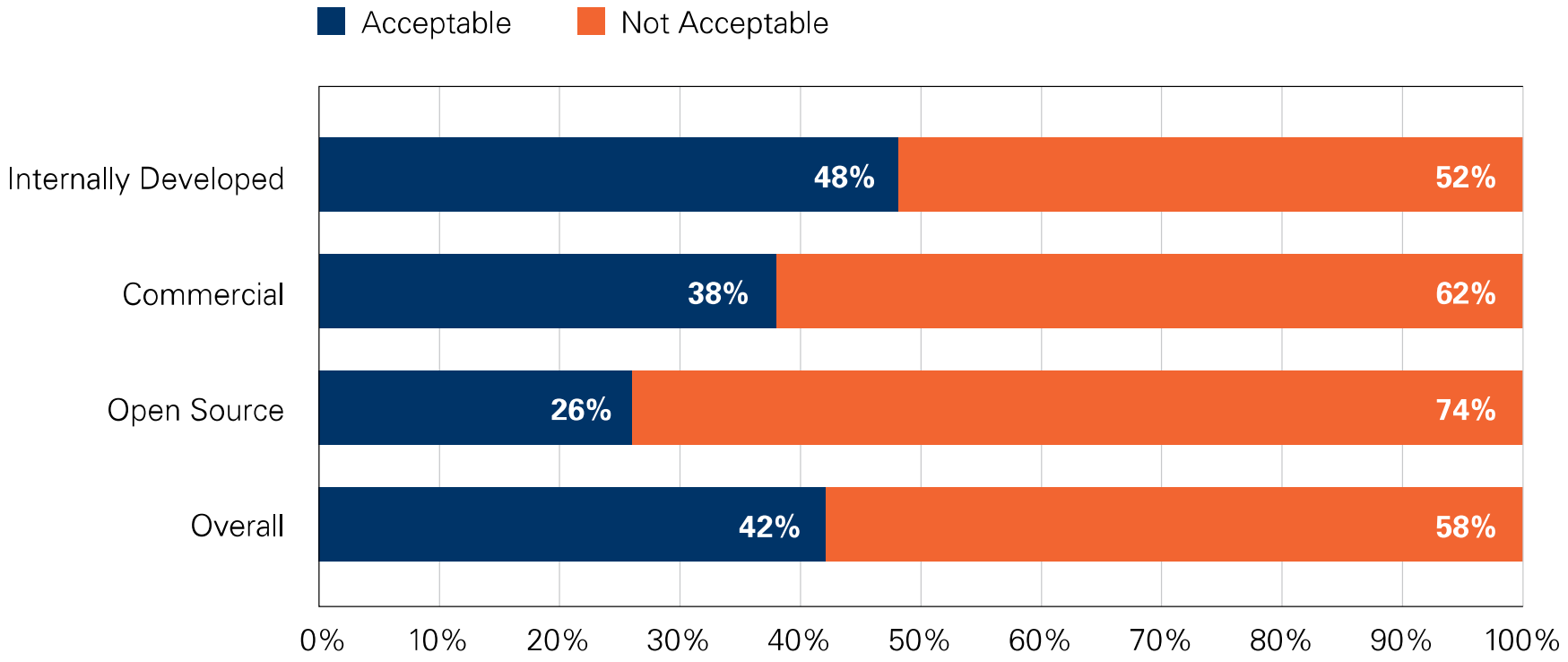
c) 86%

d) 99%

OWASP Top 10 Compliance by Supplier on First Submission
(Web Applications)

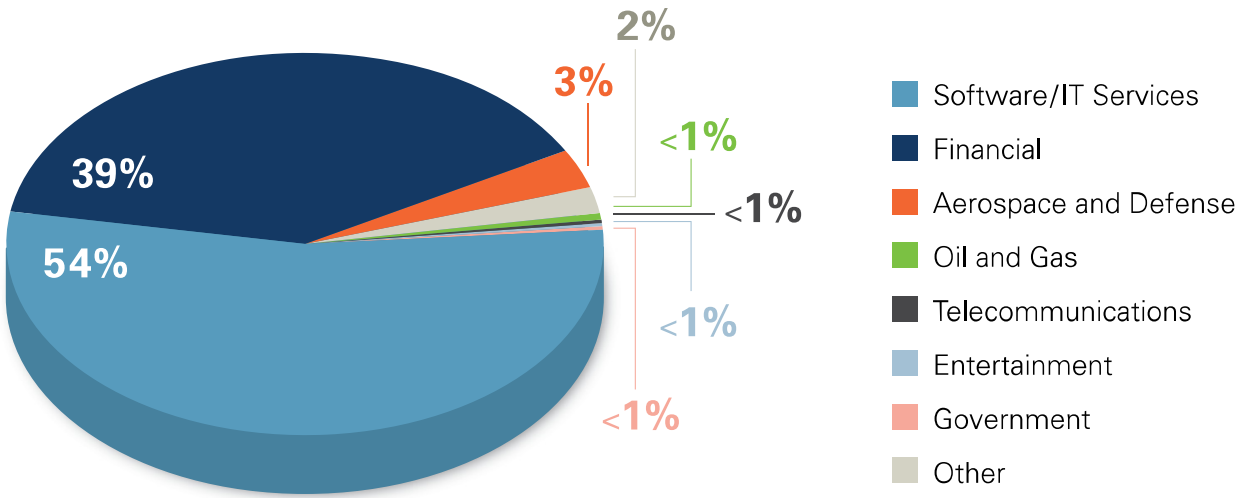


CWE/SANS Top 25 Compliance by Supplier on First Submission
(Non-Web Applications)

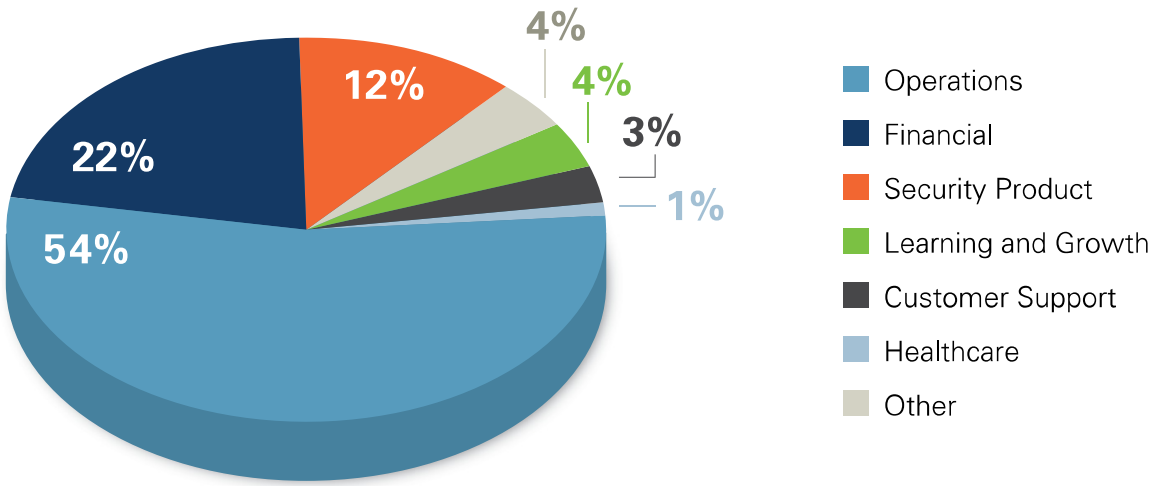


Who is holding their software vendors accountable?

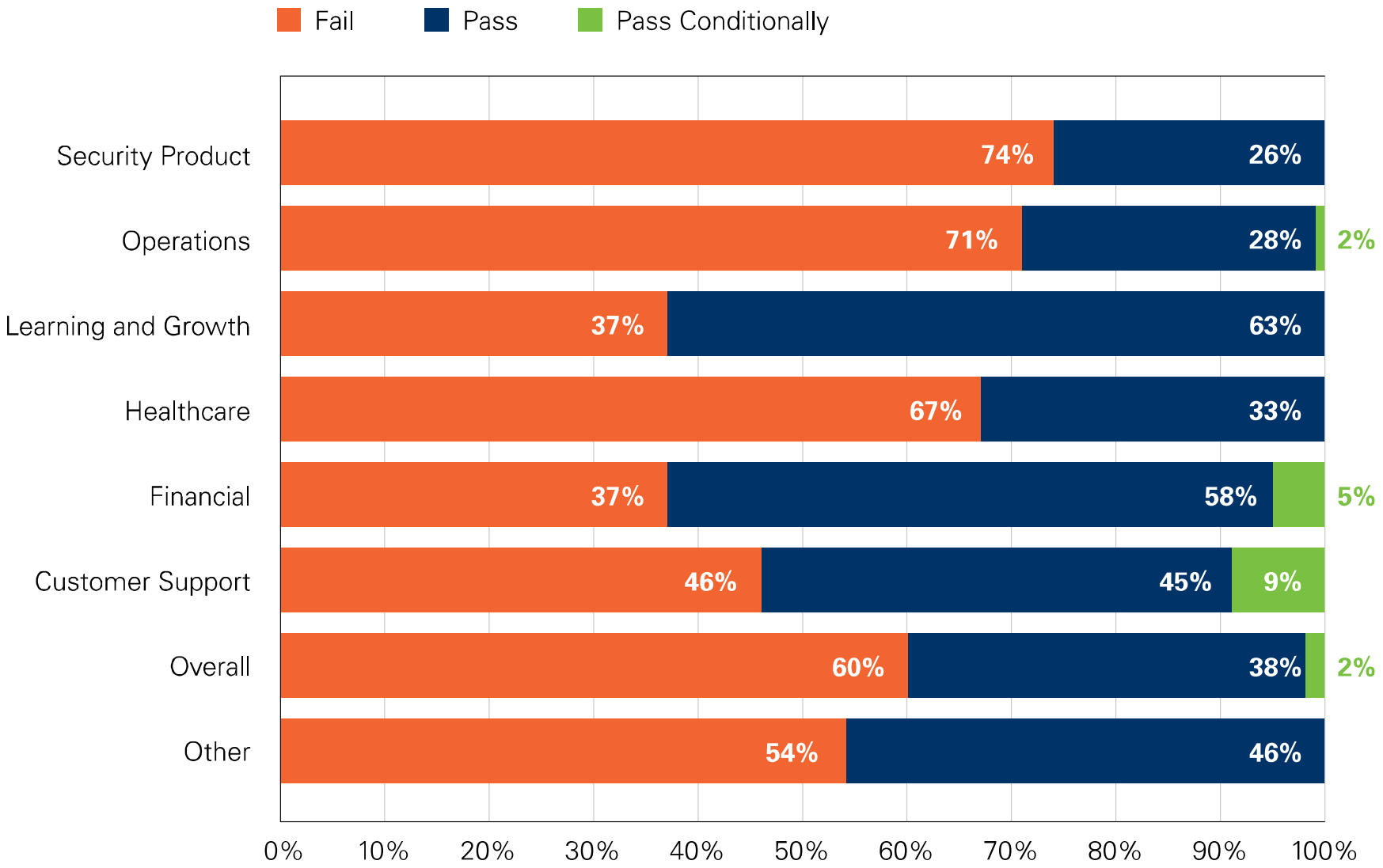
Requestor Type by Industry



Third-party Assessments by Application Purpose

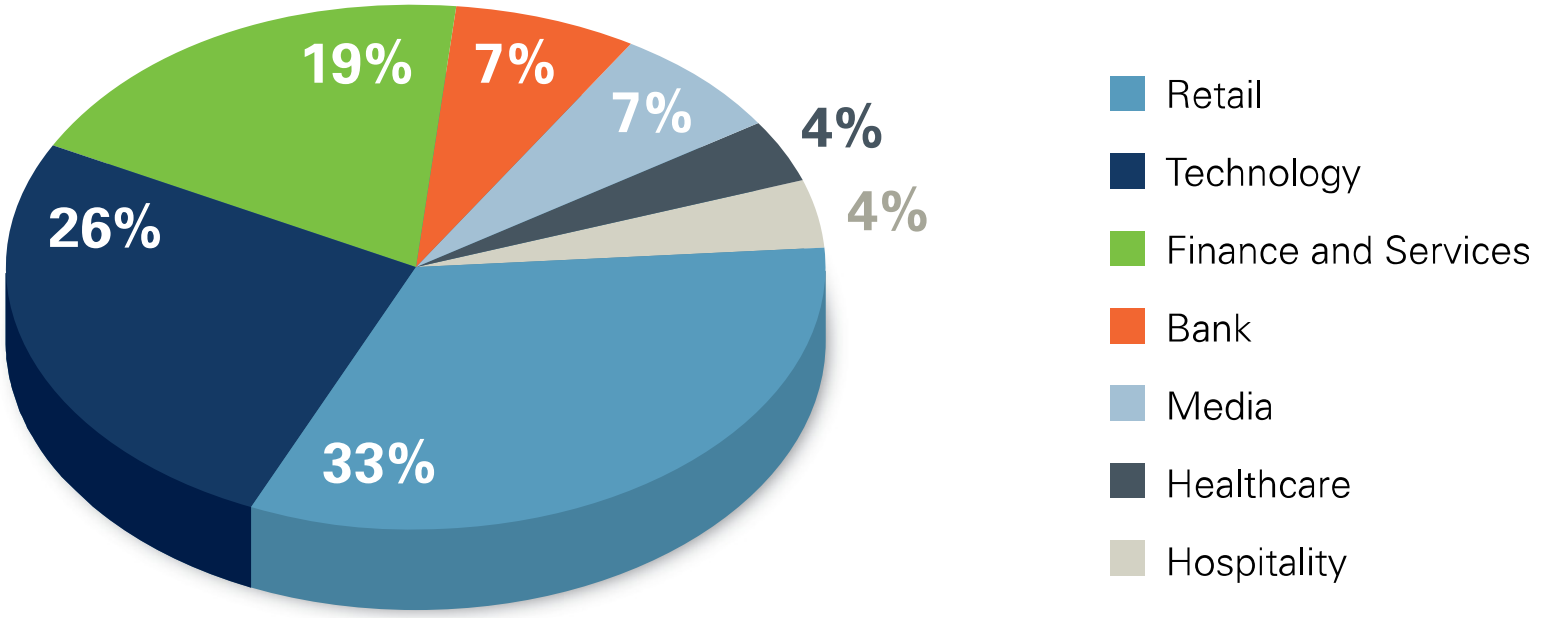


Performance Against Enterprise Policy by Application Purpose



So I hear
you can run
applications on
smart phones?

Android Applications by Industry Vertical



CWE Category	CWE	Percent Applications Affected
Insufficient Entropy	331	61%
Use of Hard-coded Cryptographic Key	321	42%
Information Exposure Through Sent Data	201	39%
Information Exposure Through Error Message	209	6%

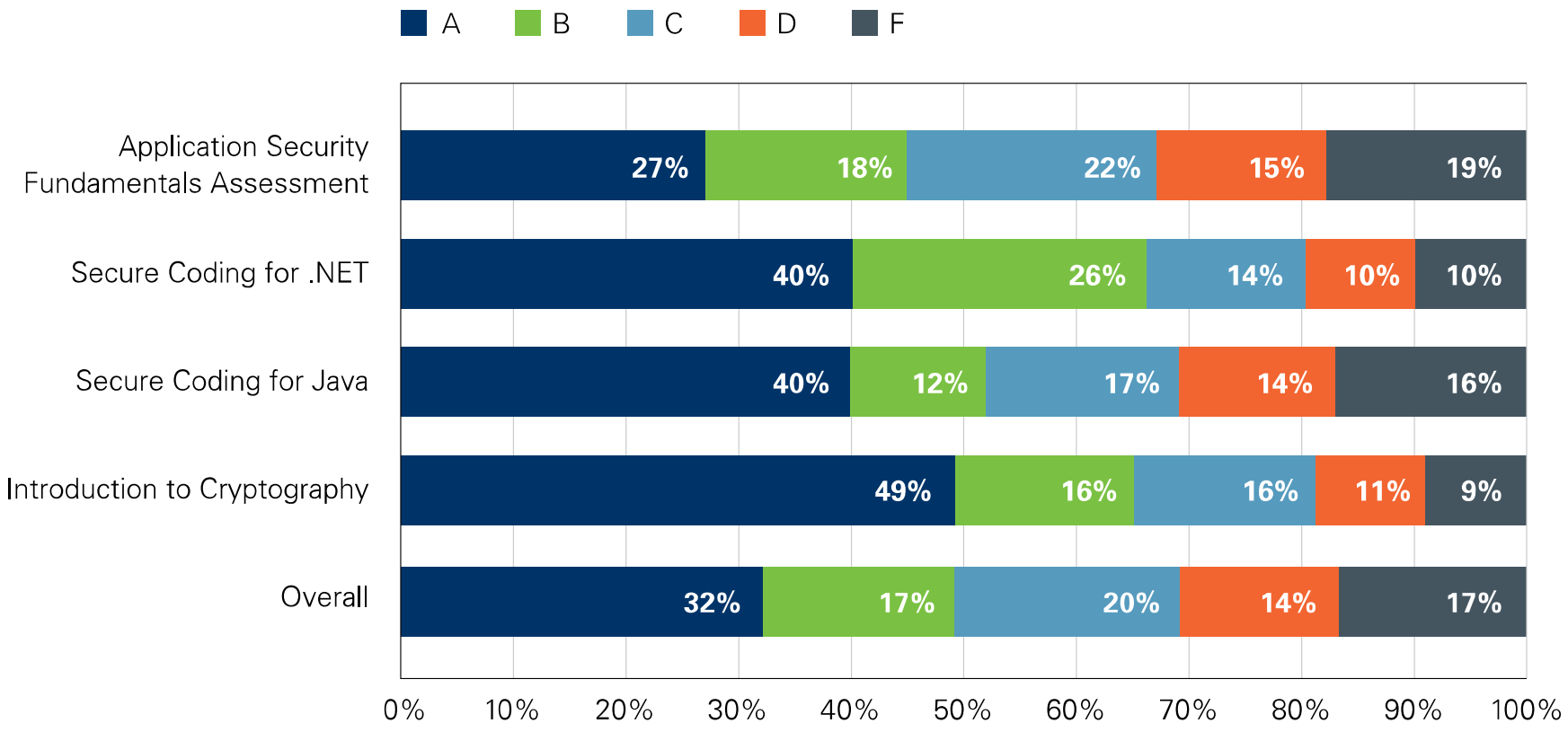
When given an exam on application security fundamentals, over half of developers…

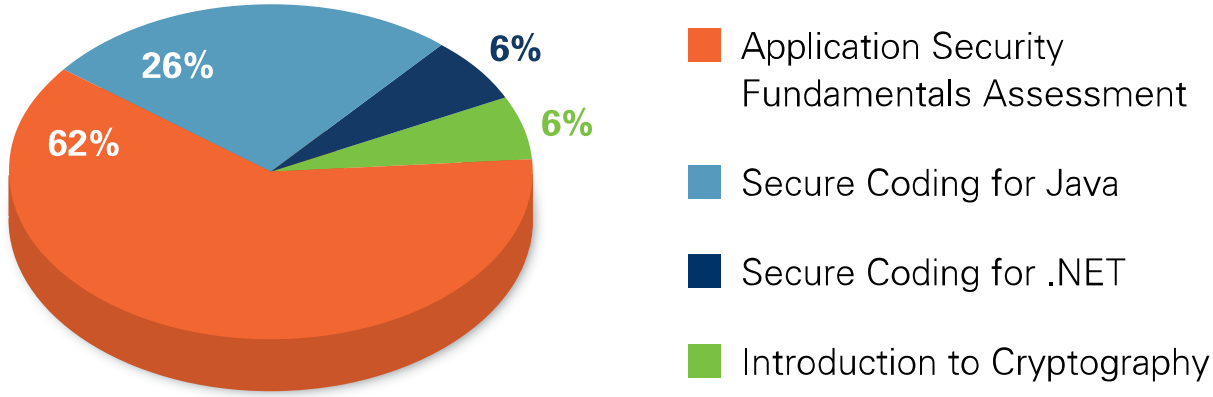
a) Receive an A

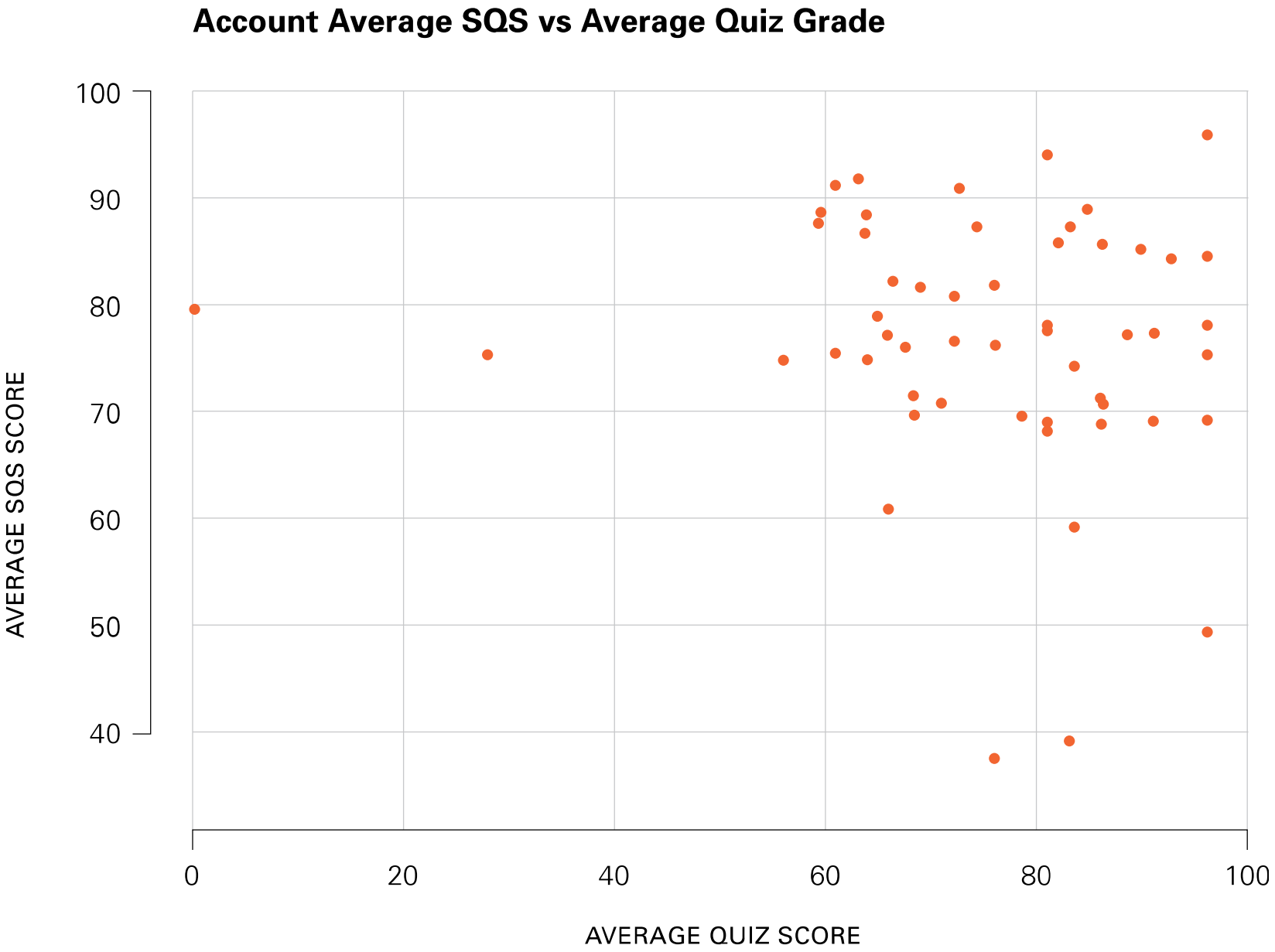
b) Receive a B or worse

c) Receive a C or worse

d) Fail (receive a D or F)


A
B
C
D
F
Application Security Fundamentals Assessment
27%
18%
22%
15%
19%
Secure Coding for .NET
40%
26%
14%
10%
10%
Secure Coding for Java
40%
12%
17%
14%
16%
Introduction to Cryptography
49%
16%
16%
11%
9%
Overall
32%
17%
20%
14%
17%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%


6%
26%
6%
62%
Application Security Fundamentals Assessment
Secure Coding for Java
Secure Coding for .NET
Introduction to Cryptography


Account Average SQS vs Average Quiz Grade
AVERAGE SQS SCORE
100
90
80
70
60
50
40
0
20
40
60
80
100
AVERAGE QUIZ SCORE

QUESTIONS?

Chris Wysopal
cwysopal@veracode.com
@weldpond