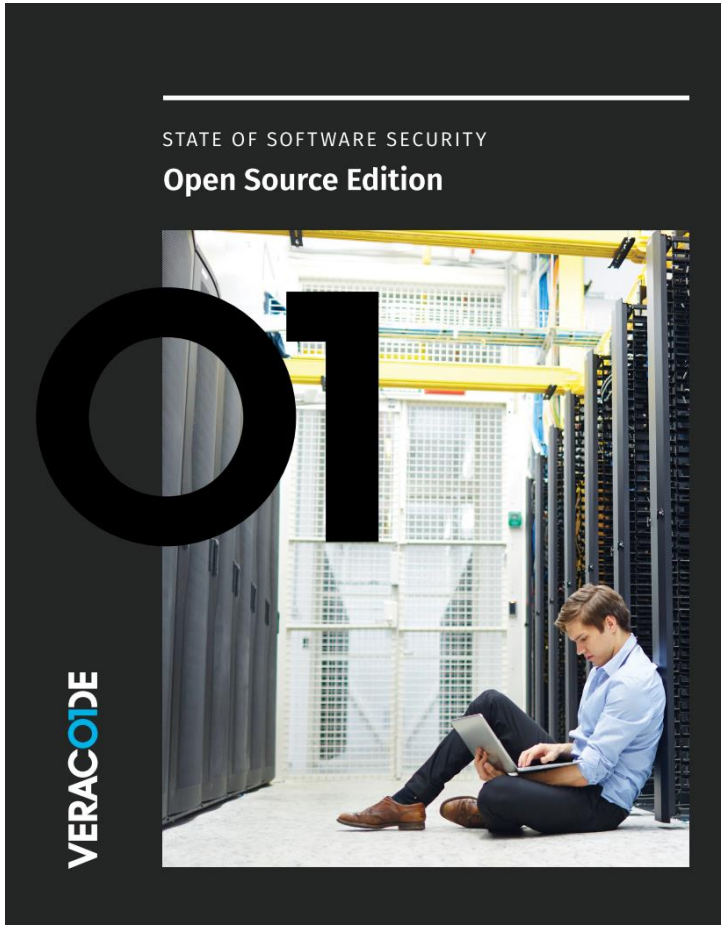
```
for line in future.readlines():
    line.secure()
```

Some of Them Want to Use You; Some of Them Want to Get Used By You

Chris Wysopal
@weldpond
Founder & CTO

06.04.2020

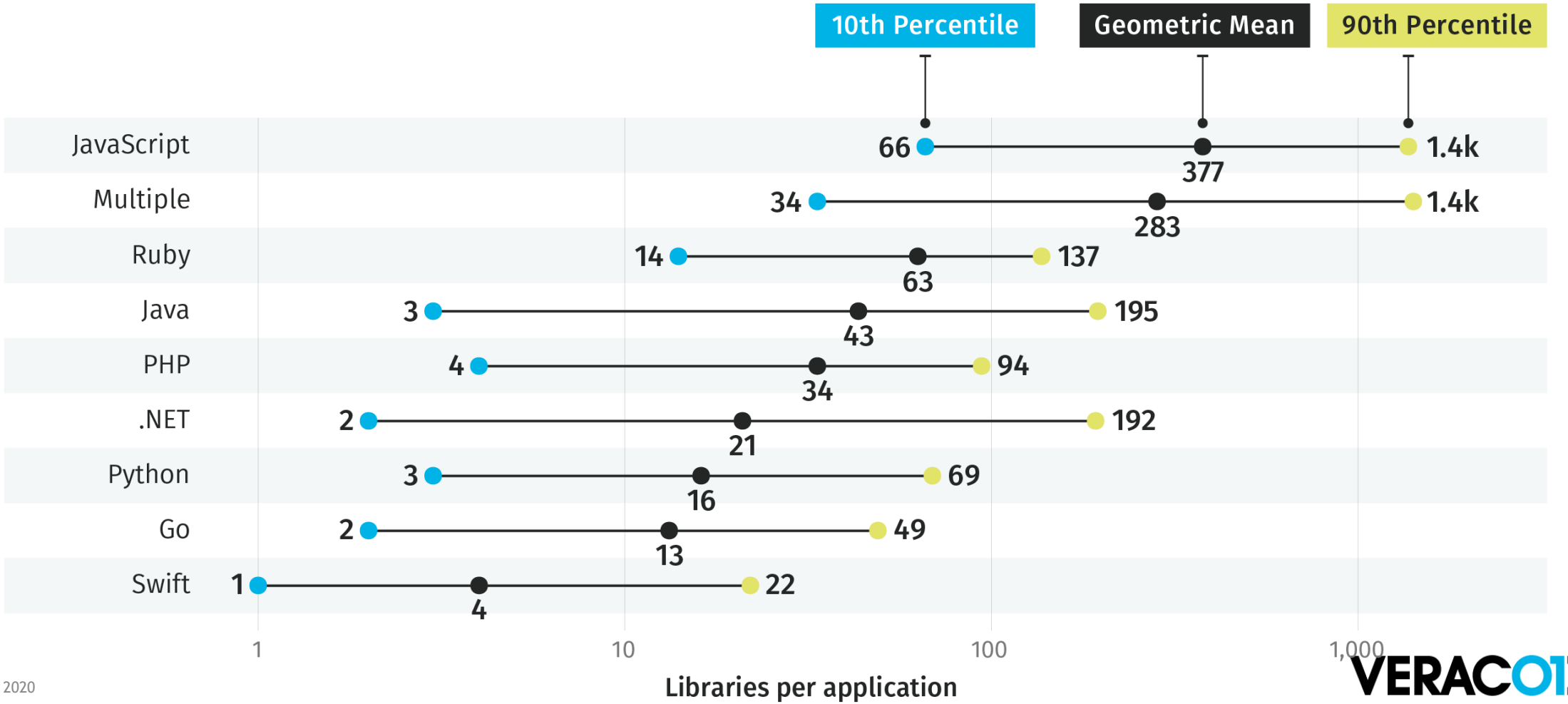
The Data



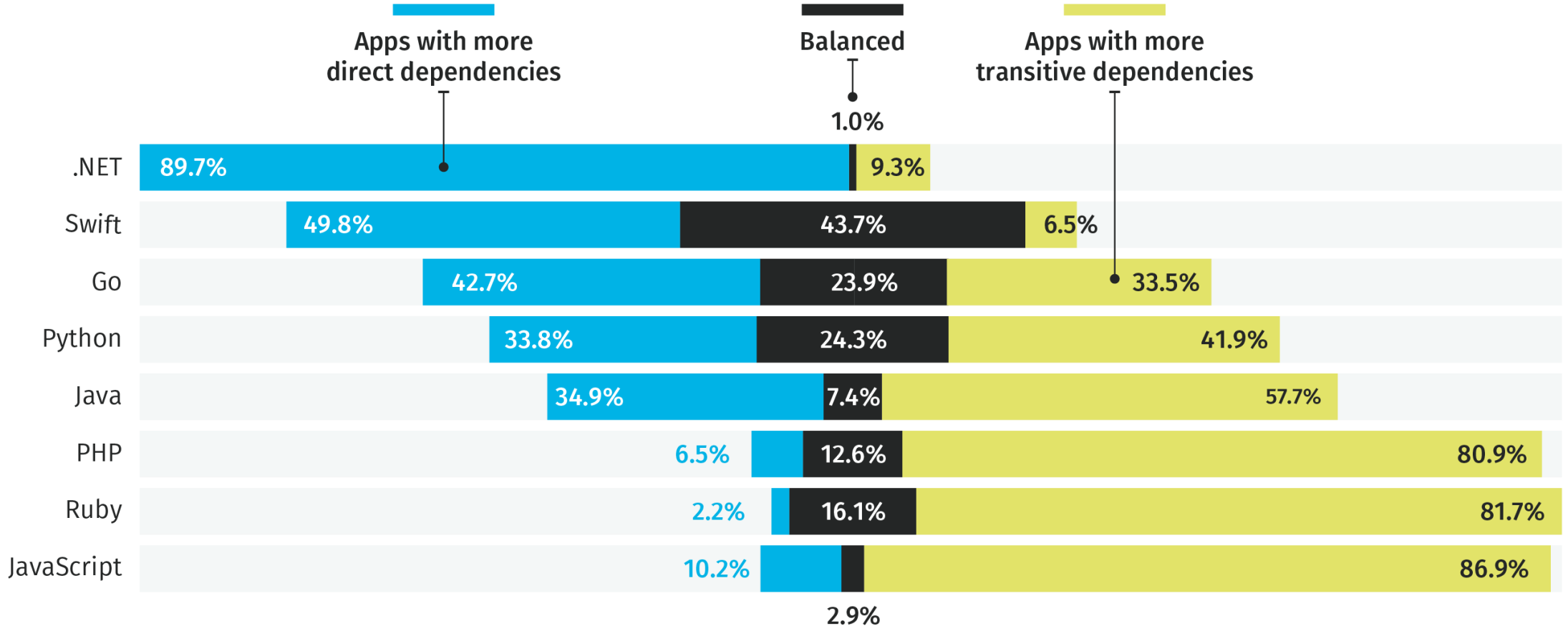
Analysis of the open source libraries contained in 85,000 applications – accounting for over 351,000 unique external libraries.

Open Source Library Use

Open source libraries make up a significant portion of most application's code.

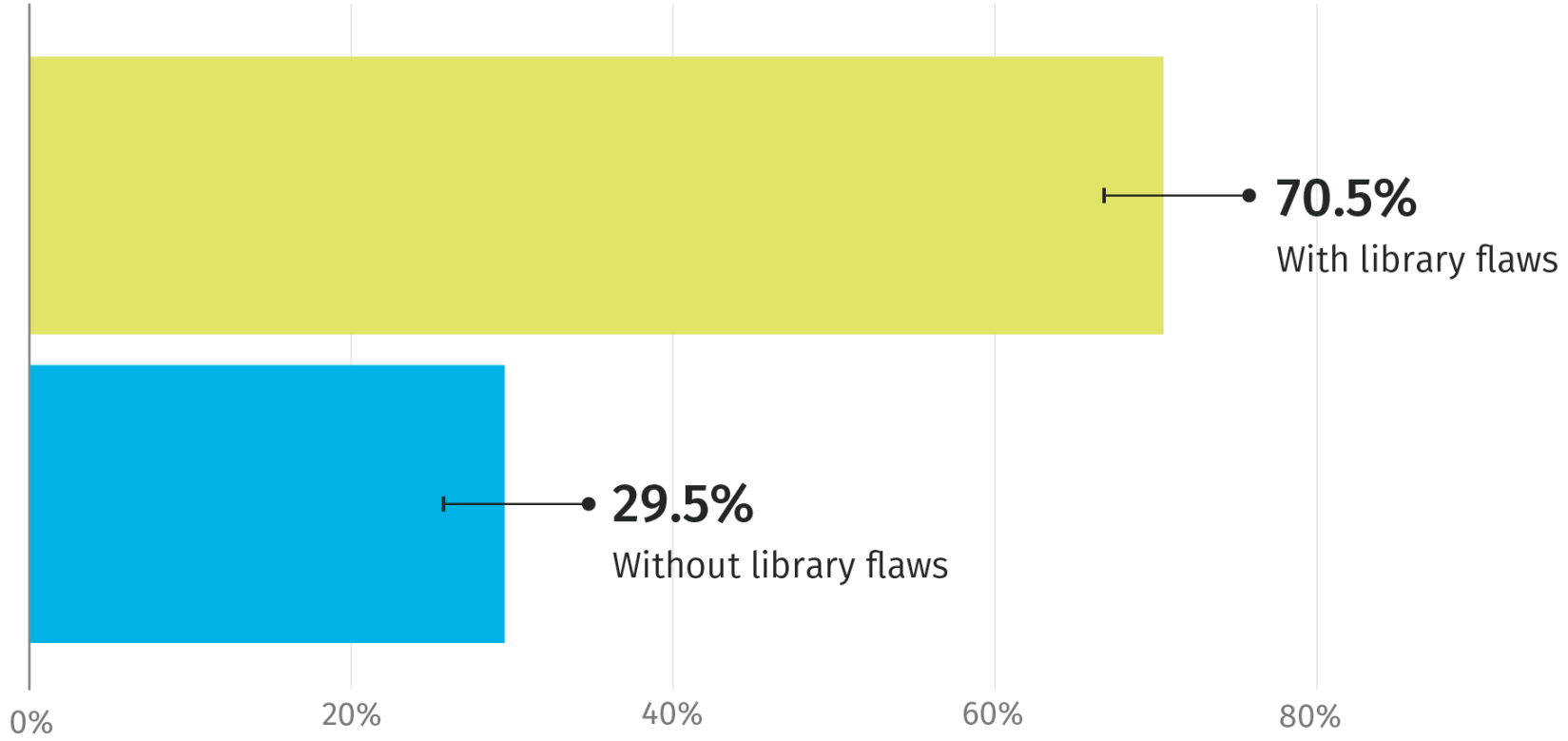


The Open Source Library Dependency Chain

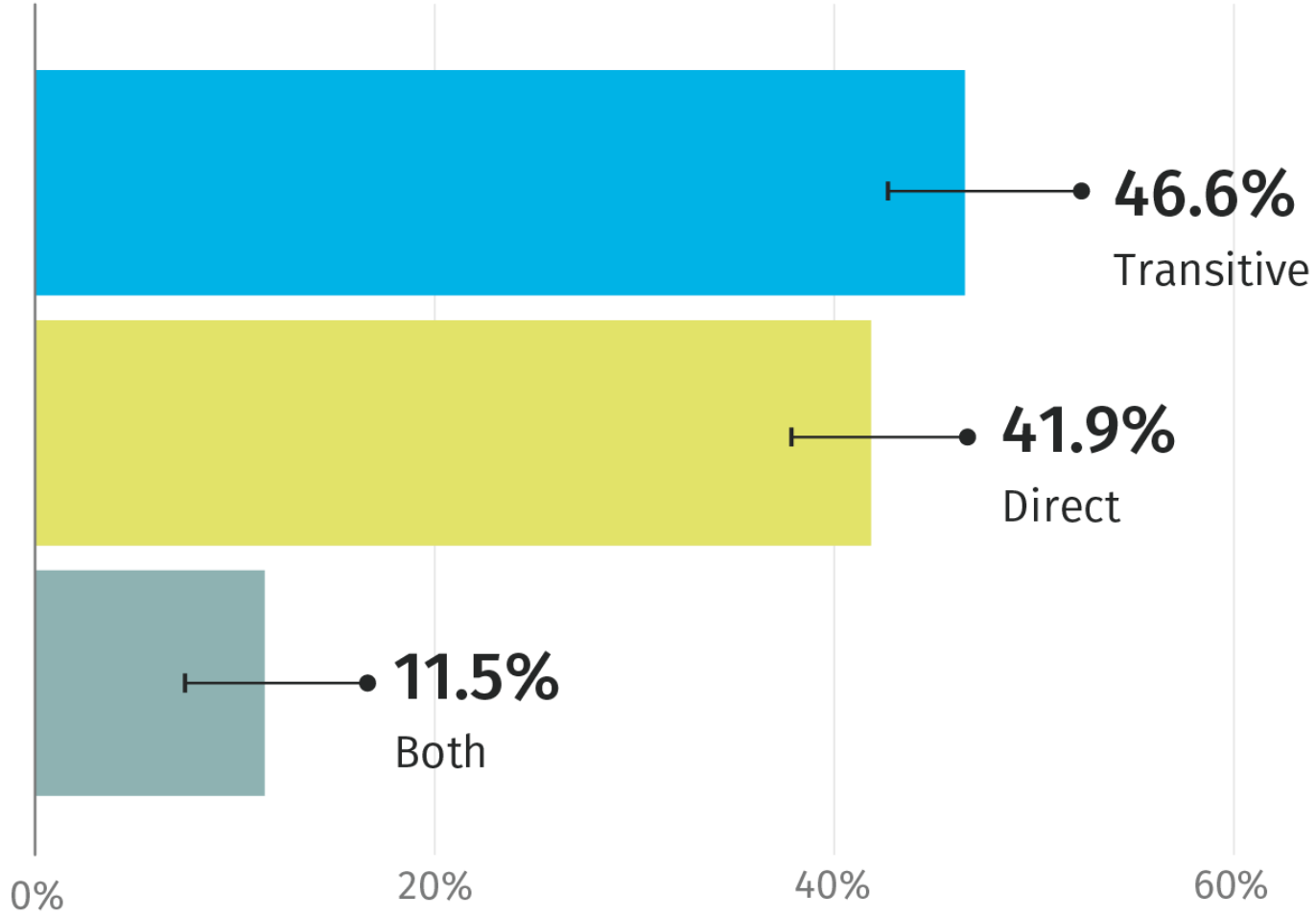


Open Source Library Security

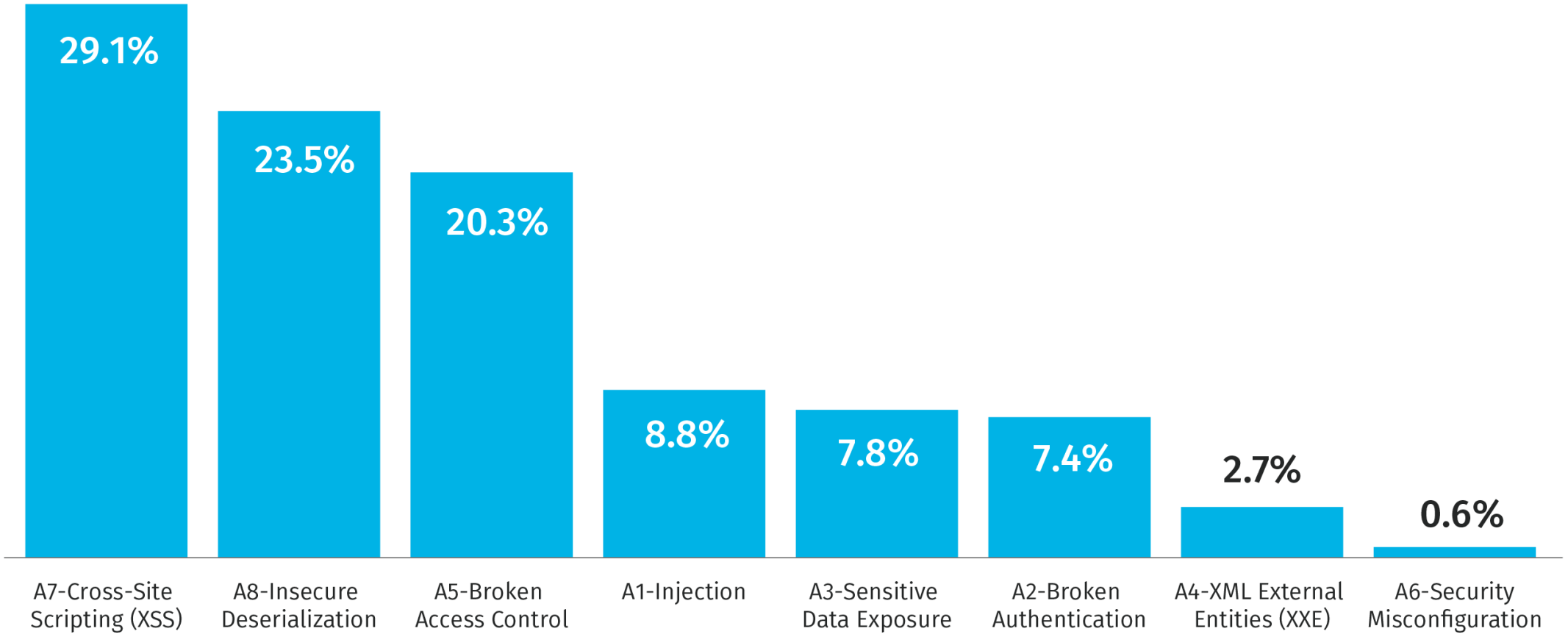
70% of applications have a security flaw in an open source library on initial scan.



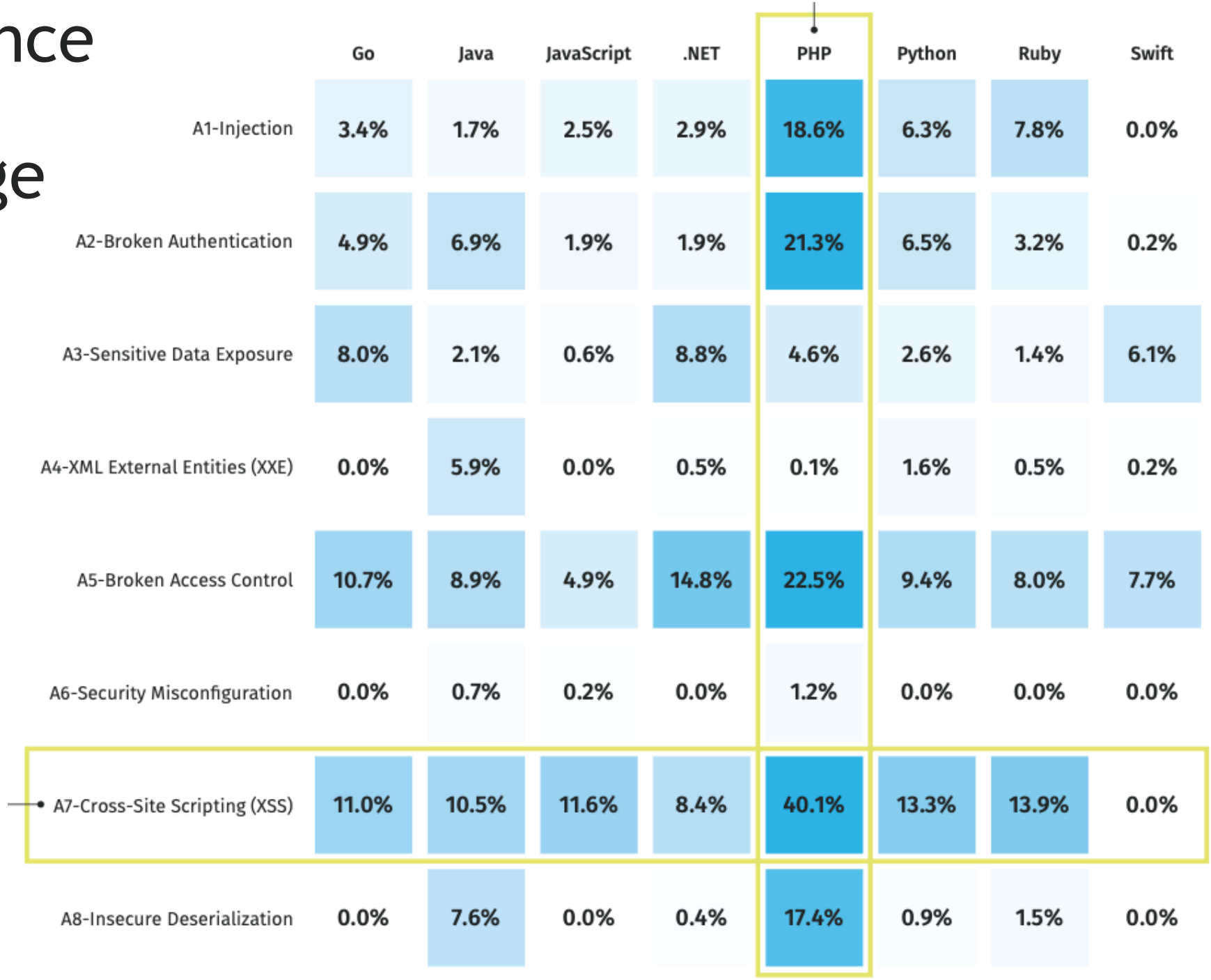
How Flaws in Open Source Libraries Are Included in Applications



Categories of Discovered Flaws Across All Libraries



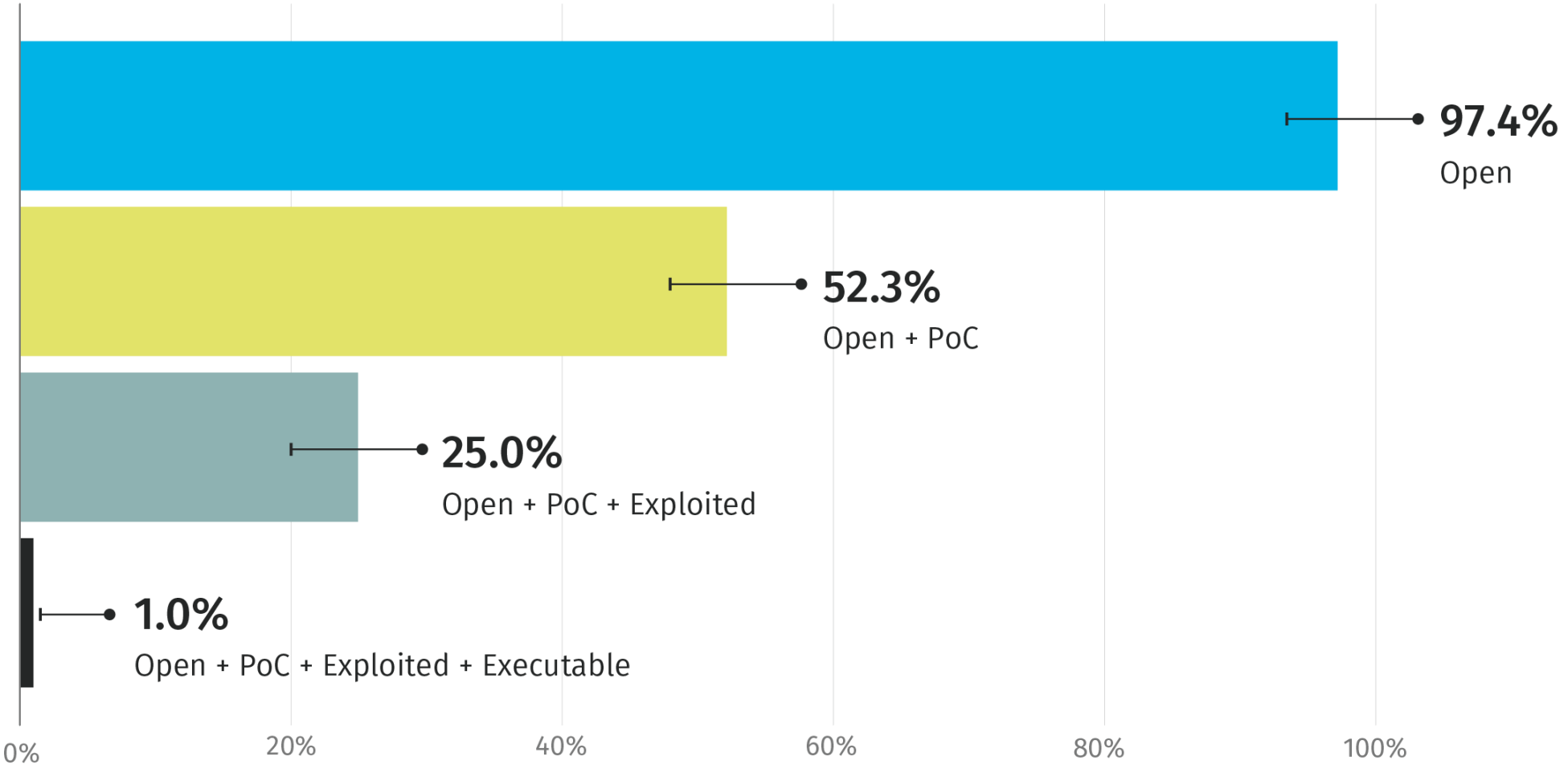
Prevalence by Language



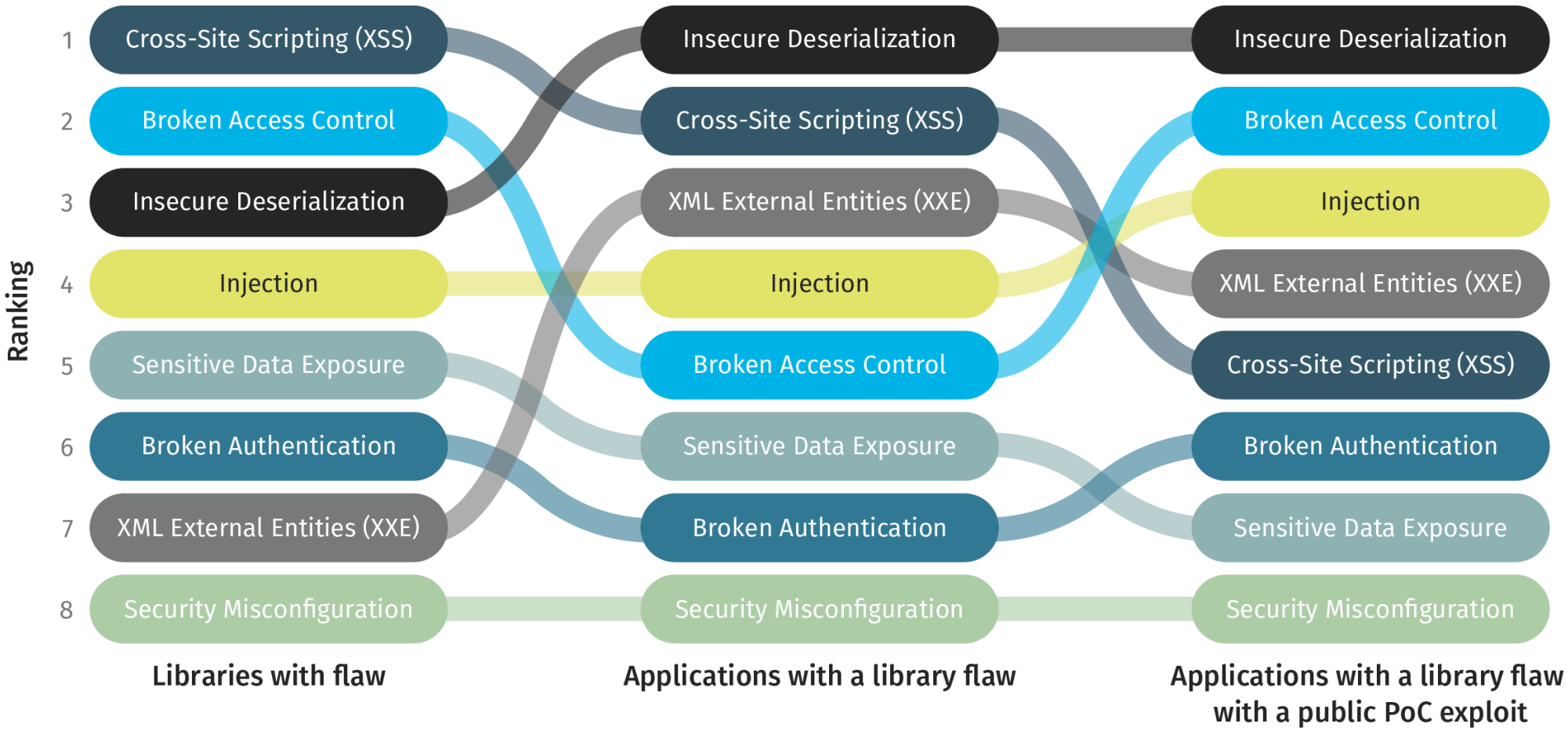
	Go	Java	JavaScript	.NET	PHP	Python	Ruby	Swift
A1-Injection	3.4%	1.7%	2.5%	2.9%	18.6%	6.3%	7.8%	0.0%
A2-Broken Authentication	4.9%	6.9%	1.9%	1.9%	21.3%	6.5%	3.2%	0.2%
A3-Sensitive Data Exposure	8.0%	2.1%	0.6%	8.8%	4.6%	2.6%	1.4%	6.1%
A4-XML External Entities (XXE)	0.0%	5.9%	0.0%	0.5%	0.1%	1.6%	0.5%	0.2%
A5-Broken Access Control	10.7%	8.9%	4.9%	14.8%	22.5%	9.4%	8.0%	7.7%
A6-Security Misconfiguration	0.0%	0.7%	0.2%	0.0%	1.2%	0.0%	0.0%	0.0%
A7-Cross-Site Scripting (XSS)	11.0%	10.5%	11.6%	8.4%	40.1%	13.3%	13.9%	0.0%
A8-Insecure Deserialization	0.0%	7.6%	0.0%	0.4%	17.4%	0.9%	1.5%	0.0%

VERACODE

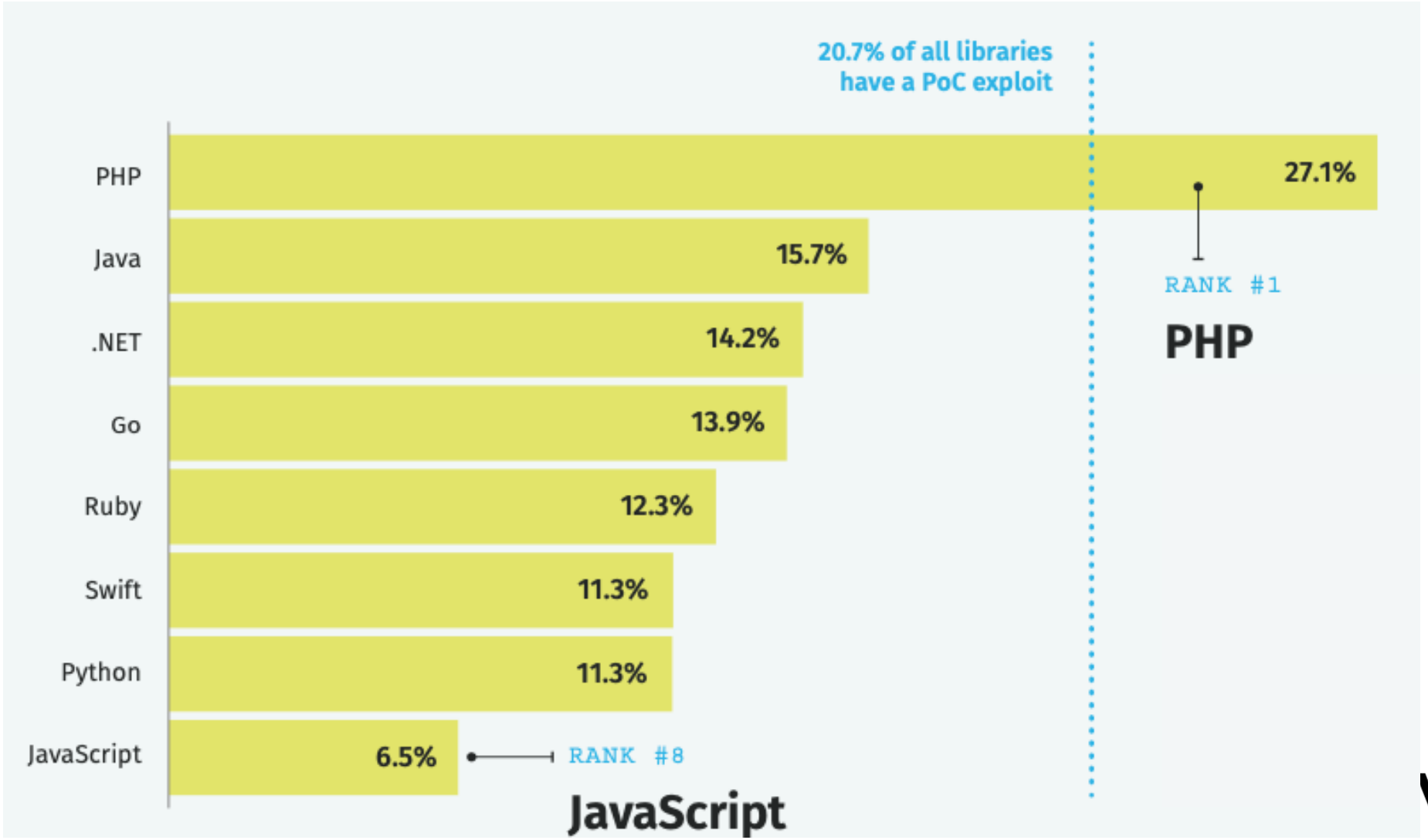
Qualifying the Flaws in Open Source Libraries



Open Source Flaw Types by Exploitability



% of Flawed Libraries With a PoC



VERACODE

Thank You!

Chris Wysopal
@weldpond