WHAT YOU CAN LEARN FROM THE OWASP TOP 10 DATACALL

Infosec 2018 Nashville

Sept 7, 2018

BRIAN GLAS

@infosecdad

OWASP TOP 10 OVERVIEW

- First version was released in 2003
- Updated in 2004, 2007, 2010, 2013, 2017
- Started as an awareness document
- Now widely considered the global baseline
- Is a standard for vendors to measure against

HUMAN-AUGMENTED TOOLS (HAT) VS. TOOL-AUGMENTED HUMANS (TAH)

- Frequency of findings
- Context (or lack thereof)
- Natural Curiosity
- Scalability
- Consistency

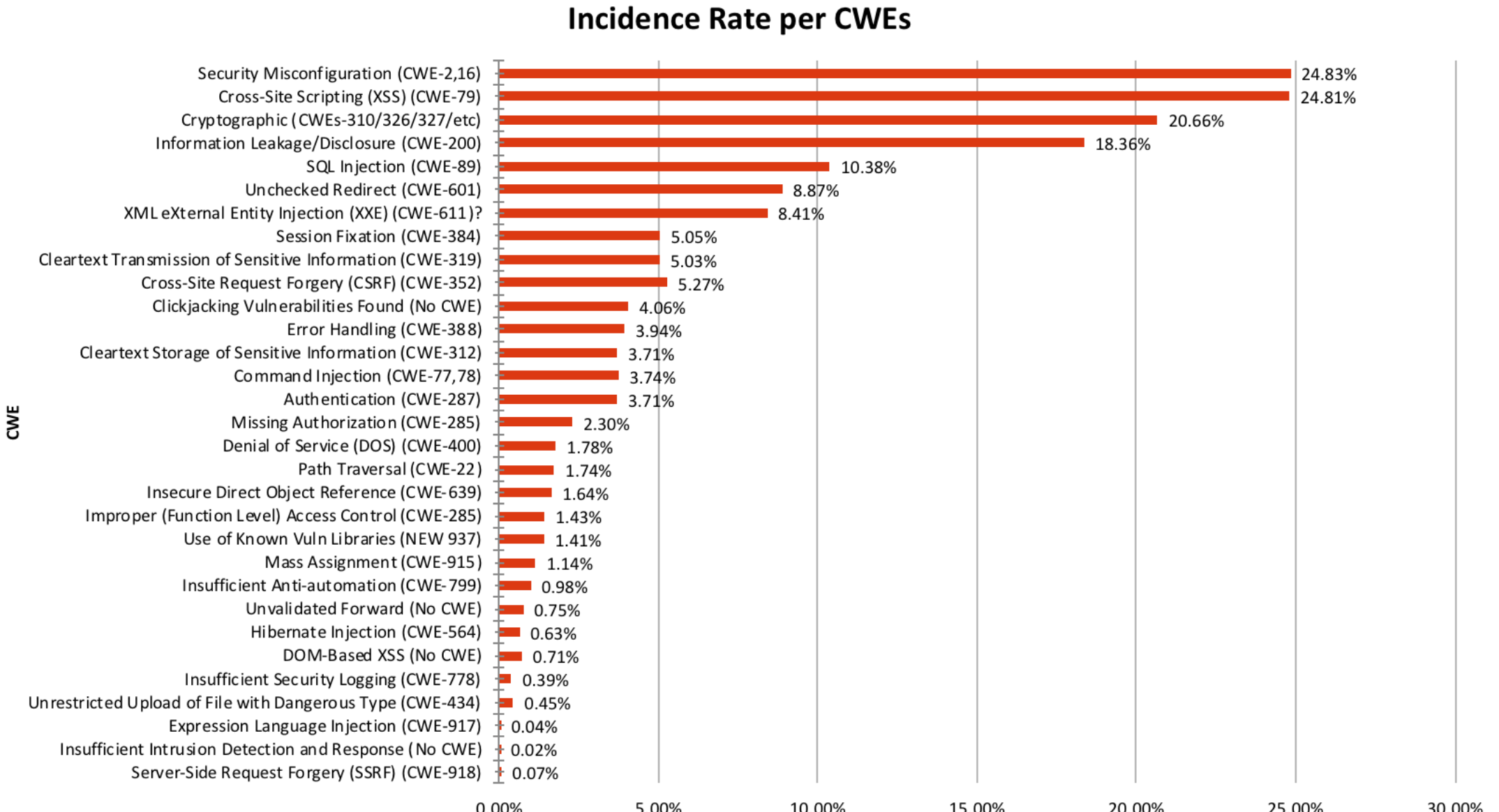
HAT VS TAH

Type of Testing	# Webapps	Companies	# Vulnerabilities	Avg per App	Classification
Manual expert code review with commercial SAST tool(s)	54	1	11456	212.1	Human Augemented Tool
Combined manual expert code review and penetration testing with only free tools	114	2	7062	61.9	Human Augemented Tool
Raw output of automated analysis tools, using rules tuned by earlier stage manual false positive analysis	44627	1	2201970	49.3	Human Augemented Tool
Raw (untriaged) output of automated analysis tool results using default rules	5244	3	90760	17.3	Tool
Combined manual expert code review and penetration testing with free and commercial tools	7	1	106	15.1	Tool Augmented Human
Manual expert penetration testing (Expected to be tool assisted w/ free DAST tool(s))	30	4	415	13.8	Tool Augmented Human
Output from manually tailored automated analysis tool(s) - with manual false positive analysis/elimination	519	4	5979	11.5	Tool Augmented Human
manual expert penetration testing or/and code review coupled with commercial DAST/SAST/IAST tools and free DAST/SAST tools	155	1	1531	9.9	Tool Augmented Human
Combined manual expert code review and penetration testing with only commercial tools	200	1	1844	9.2	Tool Augmented Human
Manual expert penetration testing with commercial DAST tool(s)	1477	3	12512	8.5	Tool Augmented Human
Combined manual expert code review and penetration testing with free and commercial tools, Automated analysis tool results - with manual false positive analysis/elimination	2490	1	19508	7.8	Tool Augmented Human
manual expert penetration testing or/and code review coupled with commercial as well as free DAST and SAST tools	111	1	839	7.6	Tool Augmented Human
Automated analysis tool results - with manual false positive analysis/elimination	6	1	20	3.3	Tool Augmented Human

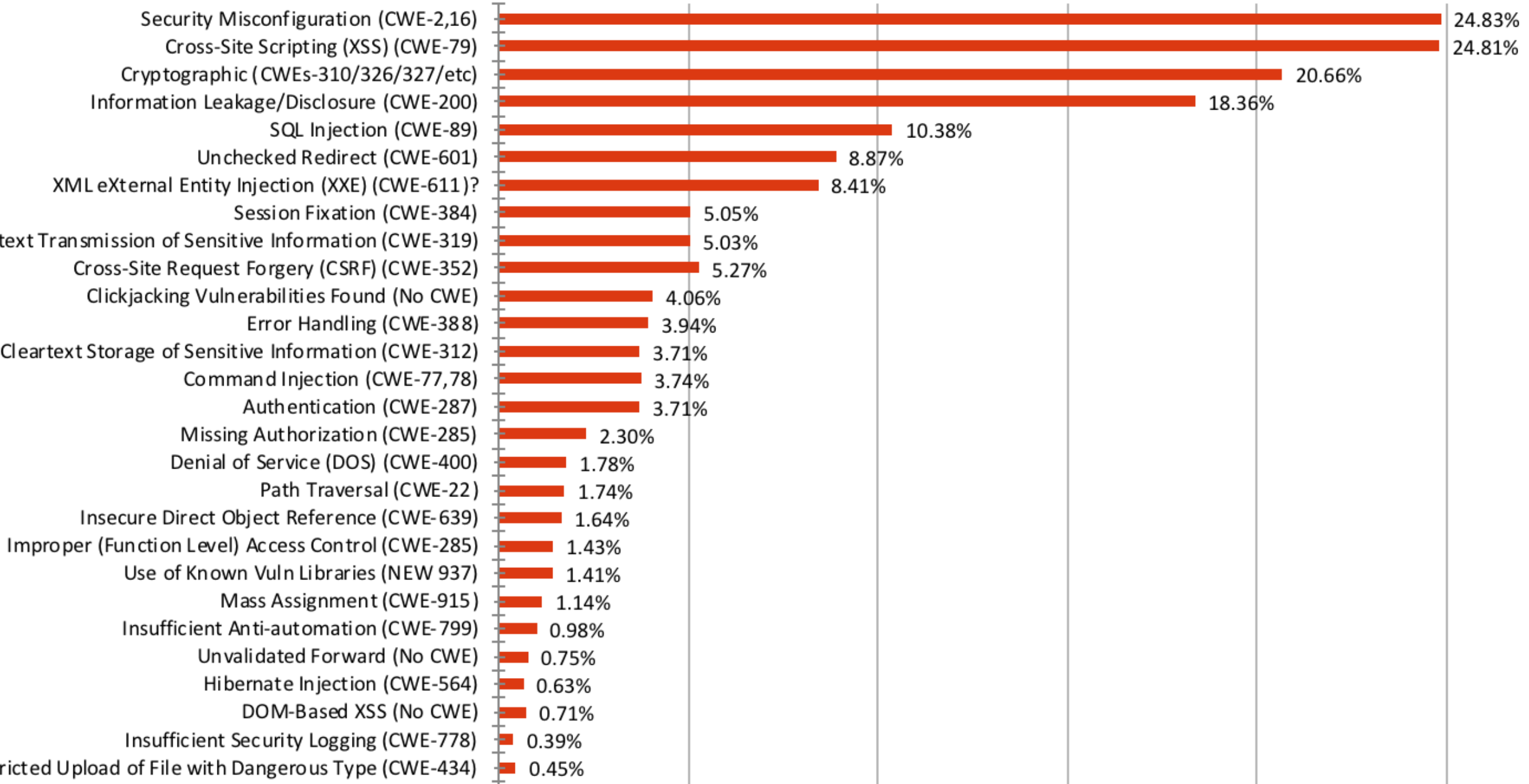
DATA CALL RESULTS

- A change from frequency to incident rate
- Extended Data Call added: More Veracode, Checkmarx, Micro Focus (Fortify), Synopsys, Bug Crowd, and others
- Data for over 114,000 applications

DATA CALL RESULTS



Incidence Rate per CWEs



DATA CALL RESULTS

Source	MicroFocus		Checkmarx		Bugcrowd		Veracode16		Veracode15		Veracode14		Synopsis		Softtek	
Number of Apps	7,086		3,423		635		46,260		31,309		19,718		5,955		2,490	
Cross-Site Scripting (XSS) (CWE-79)	2019	28.49%	3423	100.00%	635	100.00%	7513	16.24%	6130	19.58%	4501	22.83%	336	5.64%	1626	65.30%
Security Misconfiguration (CWE-2,16)	4390	61.95%	0	0.00%	355	55.91%	20059	43.36%	0	0.00%	0	0.00%	205	3.44%	2490	100.00%
Authentication (CWE-287)	216	3.05%	0	0.00%	246	38.74%	6	0.01%	21	0.07%	18	0.09%	289	4.85%	2490	100.00%
Information Leakage/Disclosure (CWE-200)	2953	41.67%	86	2.51%	245	38.58%	5493	11.87%	4990	15.94%	3216	16.31%	1622	27.24%	1716	68.92%
Cryptographic (CWEs-310/326/327/etc)	2787	39.33%	721	21.06%	26	4.09%	10226	22.11%	3998	12.77%	2848	14.44%	1118	18.77%	69	2.77%
Insecure Direct Object Reference (CWE-639)	786	11.09%	0	0.00%	92	14.49%	30	0.06%	11	0.04%	0	0.00%	0	0.00%	56	2.25%
Cleartext Transmission of Sensitive Information (CWE-319)	3452	48.72%	81	2.37%	67	10.55%	0	0.00%	0	0.00%	0	0.00%	63	1.06%	407	16.35%
Error Handling (CWE-388)	1426	20.12%	0	0.00%	158	24.88%	202	0.44%	210	0.67%	171	0.87%	79	1.33%	676	27.15%
Clickjacking Vulnerabilities Found (No CWE)	3033	42.80%	30	0.88%	42	6.61%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	48	1.93%
Missing Authorization (CWE-285)	68	0.96%	6	0.18%	246	38.74%	3	0.01%	0	0.00%	0	0.00%	57	0.96%	727	29.20%
Use of Known Vuln Libraries (NEW 937)	889	12.55%	25	0.73%	36	5.67%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
SQL Injection (CWE-89)	522	7.37%	1111	32.46%	147	23.15%	3896	8.42%	2238	7.15%	2627	13.32%	47	0.79%	267	10.72%
Cross-Site Request Forgery (CSRF) (CWE-352)	3257	45.96%	845	24.69%	344	54.17%	89	0.19%	10	0.03%	2	0.01%	180	3.02%	498	20.00%
Session Fixation (CWE-384)	221	3.12%	165	4.82%	54	8.50%	1562	3.38%	1468	4.69%	1088	5.52%	53	0.89%	4	0.16%
Path Traversal (CWE-22)	6	0.08%	633	18.49%	158	24.88%	157	0.34%	137	0.44%	88	0.45%	322	5.41%	67	2.69%
Improper (Function Level) Access Control (CWE-285)	150	2.12%	6	0.18%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	58	0.97%	727	29.20%
Insufficient Anti-automation (CWE-799)	313	4.42%	0	0.00%	107	16.85%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	28	1.12%
Denial of Service (DOS) (CWE-400)	126	1.78%	490	14.31%	157	24.72%	0	0.00%	0	0.00%	0	0.00%	2	0.03%	55	2.21%
Insufficient Security Logging (CWE-778)	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	7	0.28%
Unchecked Redirect (CWE-601)	728	10.27%	802	23.43%	146	22.99%	3146	6.80%	2755	8.80%	2224	11.28%	36	0.60%	220	8.84%
Command Injection (CWE-77,78)	155	2.19%	149	4.35%	92	14.49%	1664	3.60%	1197	3.82%	838	4.25%	28	0.47%	22	0.88%
DOM-Based XSS (No CWE)	425	6.00%	0	0.00%	145	22.83%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	121	4.86%
Insufficient Intrusion Detection and Response (No CWE)	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	15	0.60%
Hibernate Injection (CWE-564)	20	0.28%	0	0.00%	1	0.16%	271	0.59%	239	0.76%	148	0.75%	0	0.00%	4	0.16%
Cleartext Storage of Sensitive Information (CWE-312)	3320	46.85%	25	0.73%	5	0.79%	54	0.12%	43	0.14%	7	0.04%	3	0.05%	515	20.68%
Unvalidated Forward (No CWE)	728	10.27%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	50	2.01%
XML eXternal Entity Injection (XXE) (CWE-611)?	693	9.78%	102	2.98%	101	15.91%	4641	10.03%	2570	8.21%	1303	6.61%	3	0.05%	10	0.40%
Server-Side Request Forgery (SSRF) (CWE-918)	3	0.04%	0	0.00%	70	11.02%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%
Mass Assignment (CWE-915)	338	4.77%	0	0.00%	1	0.16%	679	1.47%	166	0.53%	11	0.06%	0	0.00%	78	3.13%
Unrestricted Upload of File with Dangerous Type (CWE-434)	0	0.00%	70	2.04%	214	33.70%	6	0.01%	12	0.04%	3	0.02%	130	2.18%	0	0.00%
Expression Language Injection (CWE-917)	36	0.51%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	0	0.00%	4	0.16%

Vulnerability	Found 1+
Cross-Site Scripting (XSS) (CWE-79)	96.15%
Authentication (CWE-287)	84.62%
SQL Injection (CWE-89)	84.62%
Path Traversal (CWE-22)	80.77%
Security Misconfiguration (CWE-2,16)	76.92%
Cryptographic (CWEs-310/326/327/etc)	76.92%
Missing Authorization (CWE-285)	76.92%
Cross-Site Request Forgery (CSRF) (CWE-352)	76.92%
Information Leakage/Disclosure (CWE-200)	73.08%
Cleartext Transmission of Sensitive Information (CWE-319)	73.08%
Session Fixation (CWE-384)	73.08%
Unchecked Redirect (CWE-601)	73.08%
Command Injection (CWE-77,78)	73.08%
Error Handling (CWE-388)	69.23%
Cleartext Storage of Sensitive Information (CWE-312)	69.23%
Insecure Direct Object Reference (CWE-639)	65.38%
Clickjacking Vulnerabilities Found (No CWE)	57.69%
Improper (Function Level) Access Control (CWE-285)	57.69%
Denial of Service (DOS) (CWE-400)	57.69%
Use of Known Vuln Libraries (NEW 937)	50.00%
DOM-Based XSS (No CWE)	50.00%
Insufficient Anti-automation (CWE-799)	46.15%
XML eXternal Entity Injection (XXE) (CWE-611)?	46.15%
Mass Assignment (CWE-915)	38.46%
Hibernate Injection (CWE-564)	30.77%
Unvalidated Forward (No CWE)	30.77%
Unrestricted Upload of File with Dangerous Type (CWE-434)	30.77%
Server-Side Request Forgery (SSRF) (CWE-918)	26.92%
Insufficient Security Logging (CWE-778)	19.23%

DATA CALL RESULTS

- Percentage of submitting organizations that found at least one instance in that vulnerability category

WHAT CAN THE DATA TELL US

- Humans still find more diverse vulnerabilities
- Tools only look for what they know about
- Tools can scale on a subset of tests
- You need both
- We aren’t looking for everything…

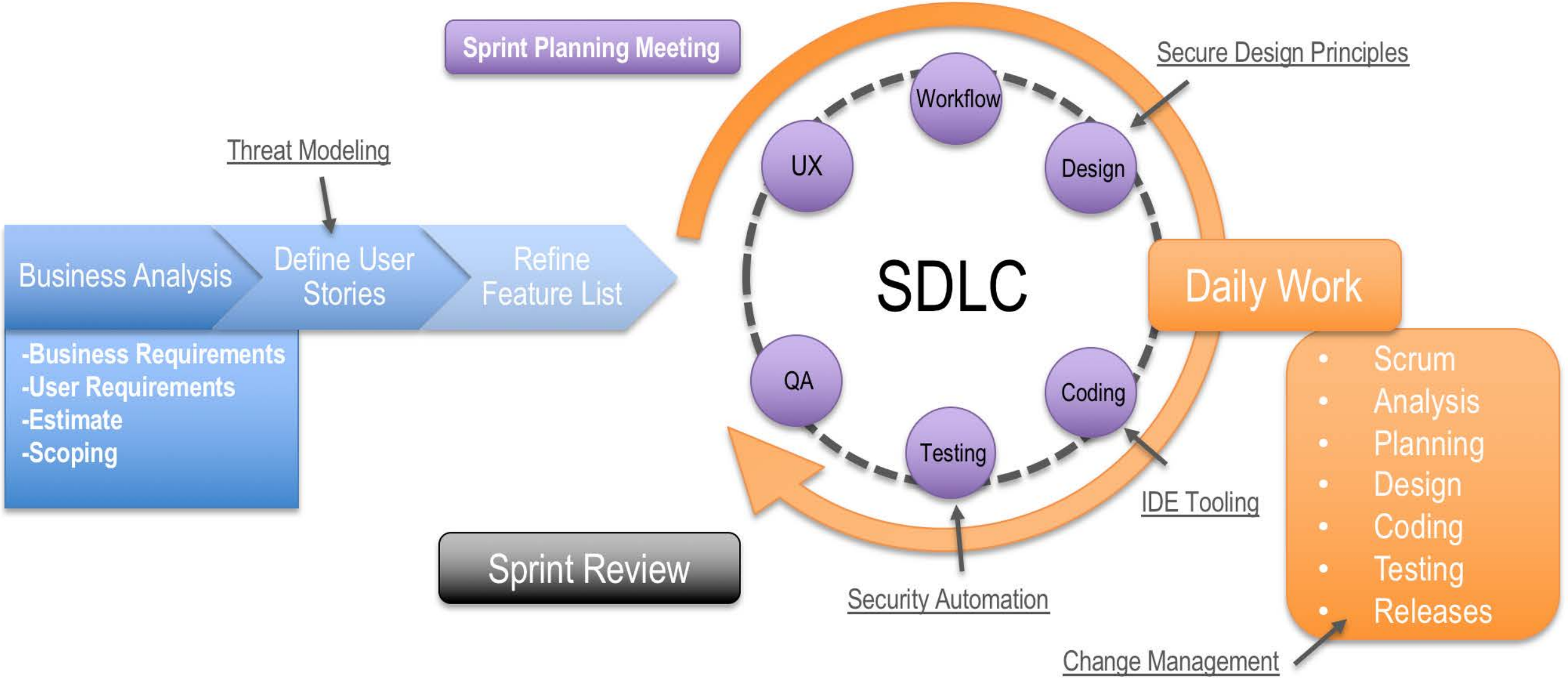
WHAT CAN THE DATA NOT TELL US

- Is a language or framework more susceptible
- Are the problems systemic or one-off
- Is developer training effective
- Are IDE plug-ins effective
- How unique are the findings?
- Consistent mapping?
- Still only seeing part of the picture

VULN DATA STRUCTURES

- CWE Reference
- Related App
- Date
- Language/Framework
- Point in the process found
- Severity (CVSS/CWSS/Something)
- Verified

VULN DATA IN SECURITY STORIES



WHAT ABOUT TRAINING DATA?

- How are you measuring training?
- Are you correlating data from training to testing automation?
- Can you track down to the dev?
- Do you know your Top 10?

WHAT CAN YOU DO?

- Think about what story to tell, then figure what data is needed to tell that story
- Structure your data collection
- Keep your data as clean and accurate as possible
- Write stories
- Consider contributing to Top 10 2020

THAT'S ALL FOLKS

THANK YOU!

- Brian Glas
- @infosecdad
- brian.glas@gmail.com