Comparative Analysis and New Solutions to Reduce SQL Injections

Joshua Gitter
Research Advisor: Dr. Paolina Centonze

Iona College - New Rochelle, NY

Latest SQL Research in the Field

Detection and Prevention of SQL Injection Attack by Dynamic Analyzer and Testing Model - Nadeem et al. @ UAF Sub Campus Burewala, Pakistan, Jan 2017

Analysis of SQL Injection Detection Techniques – Singh et al. @ Concordia University, Montreal, Canada, Jan 2017

S.No.	Technique	Blind SQL Injection	FF_SQLI	SQLI_XSS	SQLI_DNS	SQLI_CDP	SQLI_DDoS	SQLI_In_Authen
1.	Crypto Graphical Hash Functions	p	x	x	x	x	x	+
2.	Dynamic Cookies Rewriting	x	x	+	p	x	x	p
3.	Execution Flow Mechanism	x	x	*	x	x	x	x
4.	Static Code Analysis	o	x	o	x	*	x	x
5.	Dynamic Data Tainting	x	x	*	x	x	x	x
6.	Run Time Monitoring	p	+	*	x	x	x	x
7.	Machine Learning	x	o	*	x	x	o	x

TABLE I: The different techniques for Detection and Prevention of an Attack

S.No.	Tools	Blind SQL Injection	FF_SQLI	SQLI_XSS	SQLI_DNS	SQLI_CDP	SQLI_DDoS	SQLI_In_Authen
1.	Ardilla Tool	x	x	o	x	o	x	x
2.	Noxes	x	x	p	x	+	x	x
3.	Session Shield	x	x	*	p	x	x	p
4.	AMNESIA	*	x	p	x	x	x	x
5.	SQLMap	o	x	o	p	x	o	o
6.	Fast Flux Monitor	x	o	x	o	x	x	x

TABLE II: The Evaluation of different tools for Detection and Prevention of an Attack

Contributions of work done here

Our Research Contributions

X – can detect this form of injection

S. No	Tools	Blind SQLi	In-band SQLi
1	Vega (Static)	x	x
2	.NET Security Guard (Static)		x
3	Burp Suite (Dynamic)	x	
4	RAT (Dynamic)	x	x

Our Research Contributions Cont.

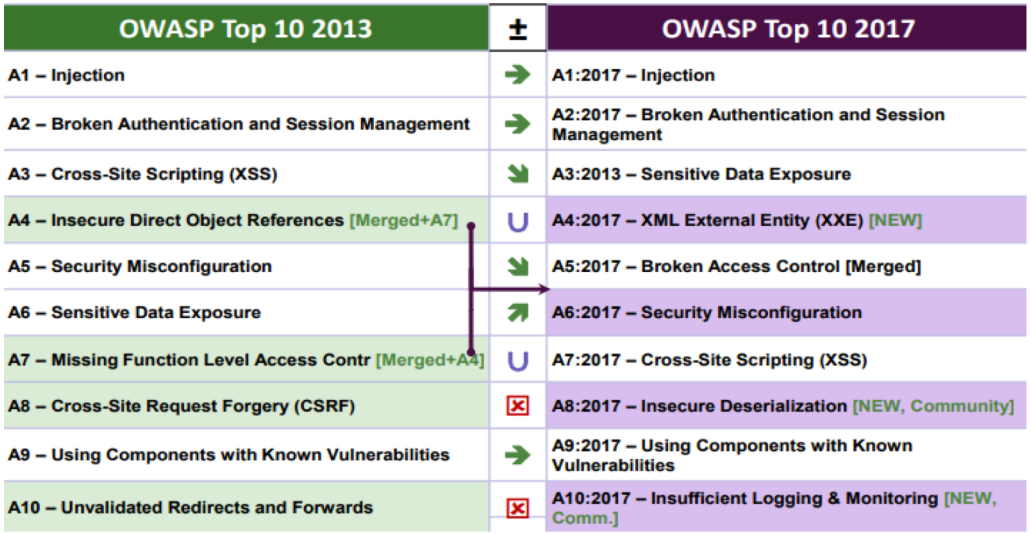
- Static analyzers are prone false positives
- Both Static and Dynamic analyzers can give false negatives
- New SQL Injection techniques - Fast Flux SQL Injection and Compounded SQL Injection

Website Name	VEGA Results (Static analyzer)	Burp Suite (Dynamic analyzer)
Hack Yourself First	4	5
Vicnum	3	3
Altoro Mutual	0	4
Acunetix(Forum ASP)	1	2
JuiceShop	0	5

Program Analysis For Database Injection – Ramsingh, Iona College, May 2017

Future Work

- Improve program analysis tools for SQL injections (combination of static and dynamic analyzers)
- Analyze and understand why some of these tools have a high percentage of false negatives and false positives



OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Injection	→	A1:2017 – Injection
A2 – Broken Authentication and Session Management	→	A2:2017 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	↘	A3:2013 – Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017 – XML External Entity (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017 – Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017 – Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017 – Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017 – Insufficient Logging & Monitoring [NEW, Comm.]