Database Management System

Report – SQL Injection

By Lakshya Gupta

17BCS015

1. Introduction

1. Scope of the topic

The topic that I have chosen is SQL Injection. This topic is widely discussed and continuous improvements have been made to detect and prevent SQL injection attacks. The papers that are chosen discuss the different methods to detect and prevent SQL injection attacks.

The chosen topic has not yet been fully explored since as the detection and prevention techniques improve, the SQL injection attacks become more complex and harder to detect. There hasen't been a sure solution to these attacks thus all the proposed solutions are being tested and those with the maximum detection rates are being implemented.

In the present day, every company has atleast one online database or databases that can be accessed online. This makes every company is susceptible to SQL Injection. The papers propose solutions to detect SQL Injection.

The paper, "Detection of SQL Injection Attacks by Removing the Parameter Values of SQL Query", detects SQL injection attacks by removing the parameters and match the left out query with a statically defined query and if that query matches then it is an SQL attack. This paper implemented this solution on a Login Page, it showed a detection rate of 96% for SQLIA. It showed a significant improvement in response time as well which leads me to believe that this solution can be implemented in real time applications.

The paper, "Encountering SQL Injection in Web Applications", educates us on the different types of SQL Injection and the different ways that hackers try to inject attacks into your database. The hackers usually use the techniques described in this paper to perform SQL attacks.

The paper, "Detecting and Preventing SQL Injection Attacks: A Formal Approach", proposes to detect and prevent SQL Injection attacks by using Finite State Automata. The solution implements detection and prevention for languages other than english and this can be extended to other languages. Thus if a hacker uses different languages then that can also be detected and prevented. This solution is implemented in ASP.net and can be tested for JAVA and PHP.

2. Literature Study

Paper 1: Detection of SQL Injection Attacks by Removing the Parameter Values of SQL Query

The following are the previous years solutions along with their advantages and their disadvantages

Method Name	Advantages	Disadvantages
A novel method for SQL injection attack detection based on removing SQL query attribute values [1]	The proposed method cannot only be implemented on web applications but it can also be used on any applications connected to databases. It can be used for SQL query profiling, SQL query listing and modularization of detection programs.	It is independent of the DBMS when compared with other SQLIA detection methods.
Data-mining based SQL injection attack detection using internal query Trees [2]	The proposed method decreases the computation time and increases the probability of correctly detection of SQLIA.	A large amount of time is consumed to generate a multi-dimensional sequence from a query tree.
Defeating SQL Injection [3]	Defensive coding practices are labor-intensive.	Runtime prevention approaches require dynamic monitoring systems but it could prevent all attacks.

SQL Injection: A Demonstration and Implications for Accounting Students [4]	Identifying and understanding the risks of SQL injection and its impact on financial processes.	Identifying and understanding the risks of SQL injection and its impact on financial processes.
Analysis of Field Data on Web Security Vulnerabilities [5]	Applications written in strong typed languages have a smaller number of vulnerabilities and exploits.	Vulnerabilities are not present in the source data analyzed.

Paper 2: Detecting and Preventing SQL Injection Attacks: A Formal Approach

The paper , “Detecting SQL Injections from web applications[6]”, proposed a dynamic detection and prevention solution but they did not take into account the ascii code, hexadecimal code or unicode.

In “ SQLRand: Preventing SQL Injections[7]”, they used randomization to encrypt SQL keywords to prevent SQLIA, but remembering the keywords required a lot of overhead and computation power.

In “Automatic creation of SQL injection and cross site scripting attacks[8]”, they used Ardilla to find cross site scripting attacks and automatically create SQL injection. They statically analyse the code and find the attacks. This is applied to source code of applications, thus posing problems and unnecessary overhead.

Paper 3: Encountering SQL Injection in Web Applications

The following papers are the previous works:

Sr. No	Name	Year	Approach
1	Indrani B., E. Ramaraj[1]	2012	The Text based Key Generator are four types of filtration technique used to detect & prevent SQL Injection Attacks from accessing database
2	Sonam Panda[2]	2013	Rabin & RSA algorithm used for prevention purpose, it is more complex to say which cryptosystem is better
3	Lwin Khin Shar & Hee Beng Kuan[3]	2013	Authors has been Propose use of active attributes to balance static quality in prediction of weakness of security.
4	Pankaj Sharma[4]	2014	Proposed a increasing web applications security to becomes a main worry
5	Amirmohammad S.[5]	2014	The hacker could convert from database or updated entities to database

6	Sampada Gadgil[6]	2015	This research has presented a survey of current techniques of SQL injection as well as a result methodology for avoiding attacks
7	Swapnil Kharche[7]	2015	The proposed scheme is evaluated by using sample of well known attack patterns.
8	Rathod Mahesh P.[8]	2015	The approach of Mapping that requests are mapped on generated issue could be used productively to expose like type of attacks &
			avoidance logic could be applied for attack removal.
9	Nabeel Salih Ali[9]	2016	Proposed a evaluated & analyze explain technique value to effectiveness in practices
10	Kanchan Choudhary, Anuj Kumar Singh[10]	2016	An effectiveness & able scheme is develop to block SQL Injection Attack that is position between web application & database.
11	Manju Khari, Parikshit S.[11]	2016	This paper presented in tabular form to present research done in static & dynamic approaches to tackle web application vulnerabilities

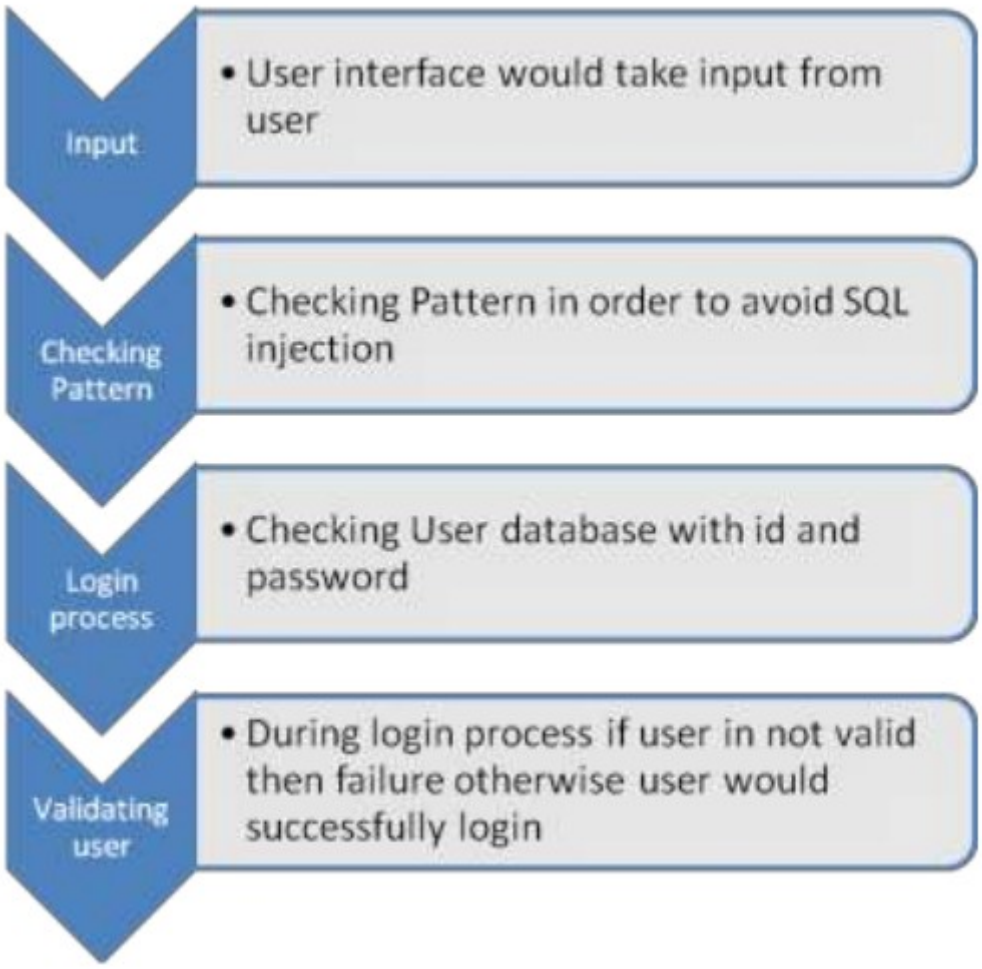
12	Harti Nagpa[12]	2017	This paper presented to hacking any site continue to increase important as hackers are use weakness of security across all geographies & across some types of web technologies.
13	Parveen Sadotra[13]	2017	Proposed a effective analysis of SQL Injection attack, detection & avoidance techniques.
14	Sonewar piyush A,Nalini A[14]	2015	Proposed a framework using .net approach in detecting SQL & XSS vulnerabilities.
15	Mukesh kumar gupta[15]	2015	Presented a survey for vulnerability detection of SQL injection & XSS through Static analysis
16	Kanchan chowdhary[16]	2016	proposed scheme is a combination of two methodology which is known as SQM & Sanitization in Reverse Proxy Server

2. New proposed Solutions - Research papers

2.1 Encountering SQL Injection in Web Applications , Second International Conference on Computing Methodologies and Communication (ICCMC 2018)

The hackers perform built-in save process by using malicious known as SQM & Sanitization in SQL injection codes .The security from SQL injection has Reverse Proxy Server major concern. The prevention of above attack is vital for dynamic web development applications . So the study of threats and their encountering should be required.. In proposed model pattern locking is worked as ascii character checking, token creation and checking of their threshold value. This would make sure that only valid queries should be passed to database server. Some of successful preventions we have studied on this Scheme for Preventing web Application against SQL Injection attack are SQL Cheat Sheet in OWASP ,Use of Parameterized query ,Automatic & dynamic access control list outlining ,Use quote blocking function ,Avoid detailed error message ,Impart limited permissions to users etc.

Proposed Model:

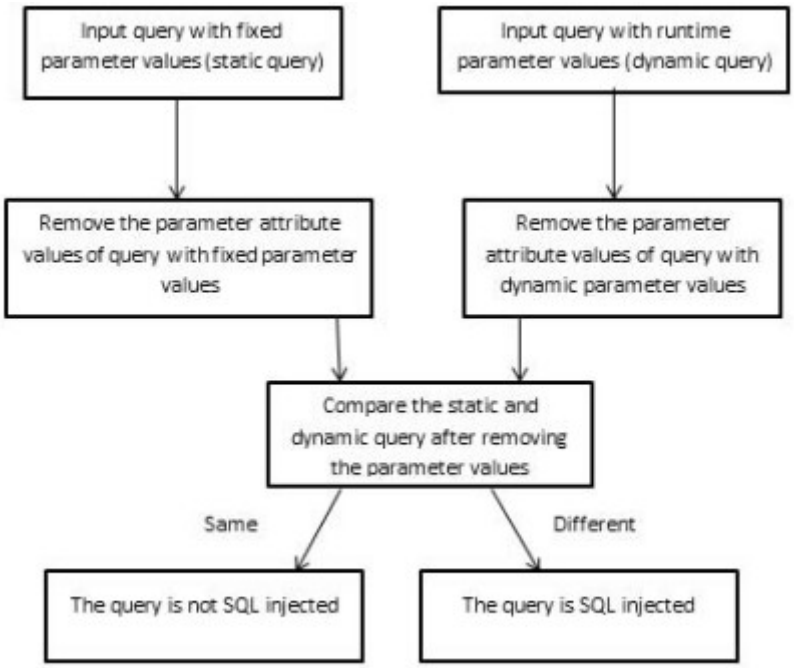


2.2 Detection of SQL Injection Attacks by Removing the Parameter Values of SQL Query, Second International Conference on Inventive Systems and Control (ICISC 2018)

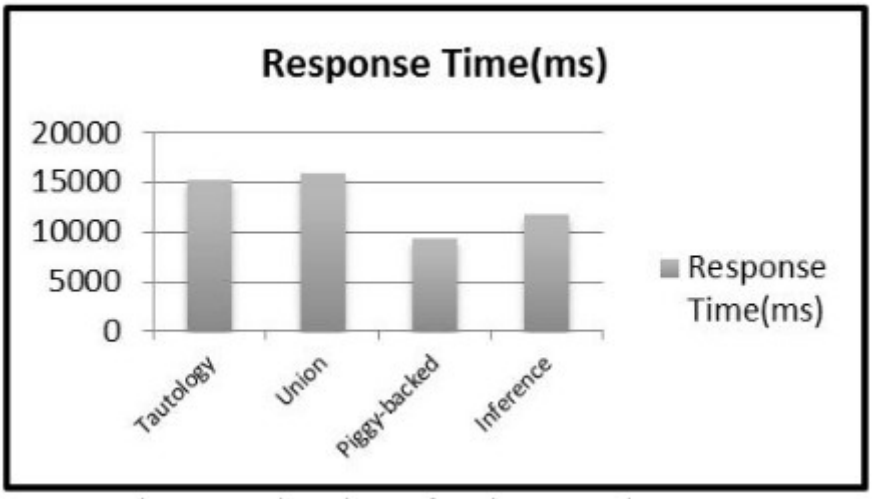
This paper presents the SQL injection detection mechanism and protecting web applications from SQL injection attacks. Digital era of technology expects attack free systems making more secure sharing of data. Proposed method makes web applications with ability to detect the code injection (SQL injection) attacks before losing any data makes systems more secure. Combining existing SQL injection detection mechanisms to develop more strong mechanism to make web application more robust is best with result as it's expected from this proposed method.

Future work should work on efficient methods for detecting the SQL injection attack and methods to prevent it. A less time must be consumed to detect the SQL injections, for this more new and robust methods are to be developed. The impact on the businesses must be understood to reduce the risk of SQL injection attacks.

Proposed Framework:



Response Time :



Advantages :

Detection/ Prevention Method	Source code adjustment	Static analysis	Applicable type of web application	Detected type of attacks
AMNESIA	Not needed	String analysis	Runtime monitoring	All but except stored procedures
Framework and database firewall method	Not needed	W3af	Database firewall	All
Proposed method	Not needed	String analysis	Query string with dynamic parameter.	All

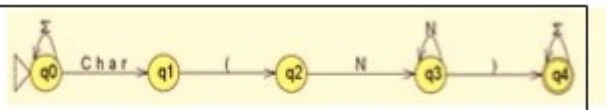
2.3 Detecting and Preventing SQL Injection Attacks: A Formal Approach, 2016 Cybersecurity and Cyberforensics Conference

In this paper, a formal technique to detect and prevent SQLIA is presented. This technique can help researchers,developers and programming laguages designers to detect and prevent SQLIA. This paper compounded theoretical method based on Finite Automata and Regular Expression with the practical aspect by developing ASP.net code.

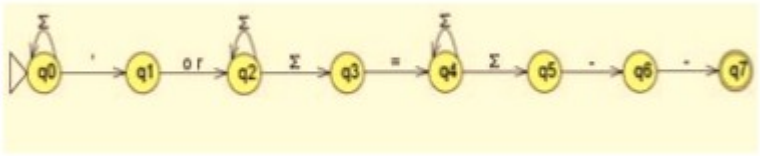
This paper is used to prevent attacks only. This allows users more flexibility. This technique can be applied to different languages such as JAVA and PHP.

Proposed Solution:

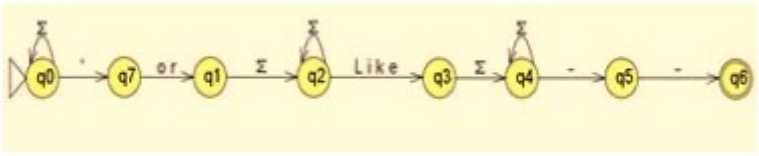
Generalization of the statements, the finite automata states used and the regular expression generalization.

FA	
' RE	$\Sigma^* char(N^+)\Sigma^*$

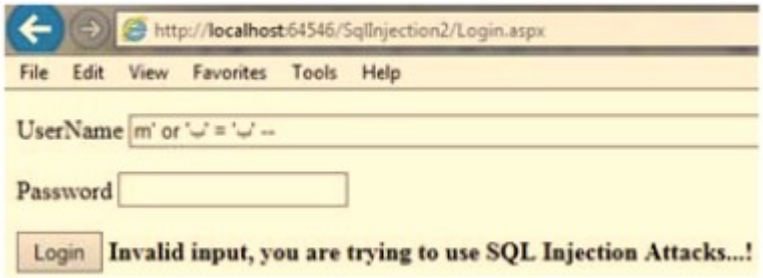
The finite automata states used when “=” sign is used:

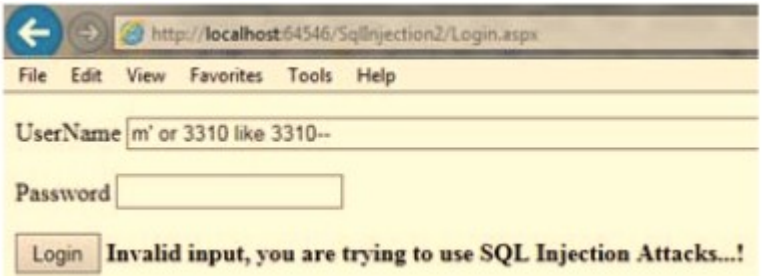


The finite automata states when “like” tesrm is used:



This solution was implemented in ASP.net on a Login Page. The following images were the output:





Thus, as you can see the proposed solution prevents SQLIA. This thoery is implemented for a Login Page but can be extended for queries as well.

3.References

- Lwin Khin Shar & Hee Beng Kuan (2013)Tan Mining SQL Injection & Cross Site Scripting Vulnerabilities using Hybrid Program Analysis
- S. Pankaj Sharma, “Integrated approach to prevent SQL injection attack & reflected cross site scripting attack,” International Journal on Recent & Innovation Trends in Computing & Communication Volume: 1 Issue: 4,2014

- Amirmohammad Sadeghian 2014 SQL Injection Vulnerability General Patch Using Header Sanitization
- Sampada Gadgil 2015 SQL injection attacks & prevention techniques
- Swapnil Kharche Preventing sql injection attack using pattern matching algorithm 2015
- Rathod Mahesh Pandurang 2015 A Mapping-based Podel for Preventing Cross Site
- Inyong Lee, Soonki Jeong, Sangsoo Yeo, Jongsub Moon," A novel method for SQL injection attack detection based on removing SQL query attribute values", Mathematical and Computer Modelling (Elsevier), Volume: 55, Issue: 1-2, PP. 58-68, January 2012.
- Mi-Yeon Kim, Dong Hoon Lee," Data-mining based SQL injection attack detection using internal query Trees," Expert Systems with Applications (Elsevier), Vol. 41, Issue 11, PP. 5416–5430, September 2014.
- Lwin Khin Shar, Hee Beng Kuan Tan," Defeating SQL Injection," Computer: the flagship publication of the IEEE Computer Society (IEEE), Volume: 46, Issue: 3, PP. 69 - 77, March 2013.
- David Henderson, Michael Lapke and Christopher Garcia," SQL Injection: A Demonstration and Implications for Accounting Students," AIS Educator Journal, Vol. 11, Issue 1, PP. 1-8, 2016.