Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

A Detail Review of SQL Injection Discovery and Deterrence Techniques for Web Applications

Prof. Nilima D. Bobade , Prof. Dr. Swati S. Sherekar
Prof. Ram Meghe Institute of Technology & Research Badnera

Abstract:- **In the current scenario use of the Internet for various online services is rising. We are doing online shopping, banking, booking, trading and accessing social networking site with the help of web applications or mobile apps. Database of the web application is the treasure which contains sensitive and valuable information of an individual such as personal, financial, medical and organization .This led to need for assuring confidentiality, Integrity, and availability of user data. Whether it's a small or enterprise web application the data stored by that application is crucial.**

The motive of this paper is to explain sql Injection and SQL Injection attack process . It describes the impact of SQL Injection and types of SQL Injection attack and categorize it. At last it summarizes and review the analysis of SQL Injection detection and prevention technique according to each author on the basis of algorithm technique , dataset , platform used, results and future scope . This analytical review will be helpful to the researcher for further research in the interested area of SQL Injection.

Keywords:-SQL injection, OWASP, Analysis, Detection, Prevention .

I. INTRODUCTION

SQL injection is the vulnerability which gives an attacker the ability to manipulate the Structured Query Language queries that web application supply to back-end database. The first SQL Injection attack that attracted public attention was Rain Forest Puppy in 1998.

There is an online community OWASP i.e Open Web Application Security Project which produce documentation, tools, articles for the security of the web applications. For web application security there is a standard awareness document for developers called OWASP Top 10. In the year 2021 SQL Injection attack was at third rank in the list.[1]

II. WHAT IS SQL INJECTION ?

SQL Injection is one of the most dangerous attack on web application. SQL Injection is an attack technique used to exploit the code by modifying backend SQL statement through manipulating input.

Basically for execution of SQL Injection, in the parameters malicious code is inserted directly that concatenated with SQL query.

When attacker is successful in altering SQL query can damage the back-end database in a variety of ways such as unauthorized manipulation of the database, denial of service to the application.

III. SQL INJECTION ATTACK PROCESS

Web applications having client server architecture are mostly victim of SQL Injection attack. Firstly attacker search any vulnerability in web application. If vulnerability is located then attacker come to know that web application is hackable. After finding vulnerability attacker try to insert malicious query by number of possible ways as his objective is that query must evaluated to true. Once the query is evaluated to true attacker is successful and will get hold on the whole backend database.

Now attacker has control on confidential information stored in the database and can modify or destroy data in the database.

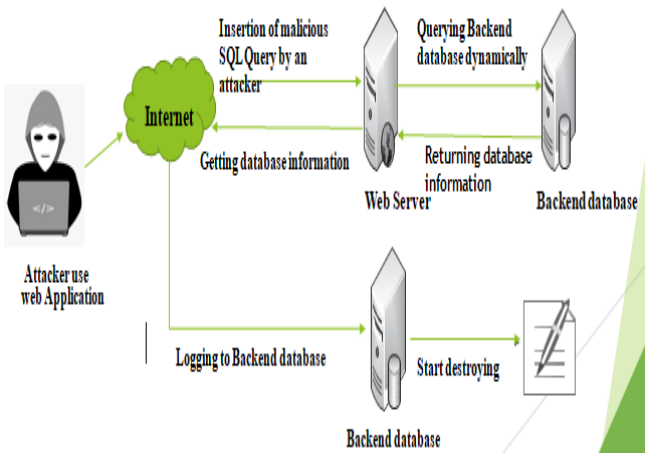

Fig 1 : SQL Injection Injection Process

IV . IMPACT OF SQL INJECTION

SQL Injection attack results in the breaching of CIA triad for data in the database.

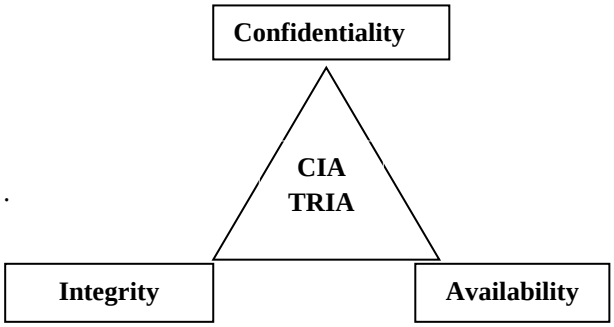

Fig 2: CIA TRIAD

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

Authentication bypass and information disclosure is also the outcome of SQL Injection.

V. CLASSIFICATION OF SQL INJECTION ATTACK

SQL injection attack classified into six types

1) Tautologies
In the condition malicious code is added in such a way that the condition output result to true.

2) Logically Incorrect Queries
The main goal of this attack to collect the relevant information such as structure and type of backend database. The attacker target a weakness that results in the default error page by the application server. As the error page is displayed attacker work is done. That error page is helpful to get description of injectable parameter, tables and columns name.

3) Union Query: - with the help of this attackers connect injected query to original query by using UNION as follows
Union <original query> <injected query>.
This attack returns the dataset from the database which is the collective result of original and injected query.

4) Stored procedure:- Injection applied on a stored procedure in the database.

5) Piggy-Backed Queries: - Attacker tries to inject malicious queries in the original query. Malicious query which is injected in the original query is called piggy backed query.

6) Inference: - In this attack an attacker modify the behavior of a database application.

I. Blind Injection :- Developer conceal the error details which is helpful for attacker in order to compromise database. Attacker get a generic page provided by the developer .

II. Timing Injection Attack:- In this attack attackers gather information based on response time delays in the responses from the database's . [2]

IV. SQL INNJECTION ATTACK DETECTION AND PREVENTION TECHNIQUES

Author Indrani Balasundarama et al. particularly designed an approach to pinpoint SQLIA on the basis of four types of validation model. It uses the blend of static and dynamic analysis. Prevention technique at the static analysis stage consist of three phases Malicious Text Detector, Field Constraint Validation and Static Query Length Validation. After that in the runtime validation stage, validation of the user input data with all these stages is done to check whether the user input is safe or unsafe.

This tool is for .NET based web applications. Author proposed ASCII based string matching algorithm and the databases used were SQL Server and Ms Access. [3]

Author Natarajan et al. proposed dynamic prevention technique using SQL IF algorithm . The algorithm checks for keywords, special characters and boolean keywords used in SQL query. The algorithm is useful to detect union and logical/illegal query attack. The generic detection method checks input fields for suspicious characters and keywords. If Vulnerability is found then sent it to data collector that resets the Http request and warn the iser as soon as the variance is to be found in the parametric values [4]

Author Noor Ashitah Abu Othman et al. projected a technique which combine two methods Query Tokenization and Adaptive for detection and prevention of SQL Injection attack in which through input malicious codes is inserted. Query parse method used by Query Tokenization and adaptive method construct adaptive shell for prevention.

The method is tested and evaluated on a live web application. [5]

Author Nency Patela et al. proposed method that uses modified AhoCorasick Pattern matching algorithm to detect and prevent SQL Injection . The proposed architecture at first phases check input query for injection using SQLMAP tool and AIIDA.

Boolean-based, Time-based , Error-based , UNION , Stacked queries is detected and exploited by SQLMAP. This technique results in less memory consumption than existing system.[6]

Author Debabrata Kar et al. propose a novel technique to detect SQL injection by means of SVM and graph of tokens . Normalized SQL queries into sequence of tokens protect the structural composition and capture the interaction between the tokens in form of a graph. The intention of this approach to work at the database firewall layer .It is implemented in a prototype called SQLiGoT . Using directed and undirected graphs using two different edge-weighting methods the system was thoroughly tested. Single as well as multiple SVMs classifier proposed, tested, and compared. [7]

Author Dr. Ahmad Ghafarian et al. proposed method is combination of static at the Database layer and dynamic at the CGI layer having three phases.

In phase first it advise that tables of all the database be improved to include a record that has only symbols such as Dollar sign. In second phase (CGI), it uses an algorithm that dynamically process and monitor the running of all incoming queries. This algorithm take input of user query and responsible to approve or reject query. At third phase string matching process performed using algorithm between the received SQL queries and previous expected SQL queries. Comparison of result will be matched with the expected valid query automatically. On the basis of the comparison process it detect the existence of SQLIA . If

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

there is SQL injection attack then query will be rejected.[8]

Author Solomon Ogbomon Uwagbole et al. discover the dataset from attack patterns containing SQL tokens which are malicious.
For a test case, construct a web application from list of dictionary word as vector variables to show massive quantities of learning data. In the supervised learning first preprocessing of dataset take place next go for labeling and feature hashing. The trained classifier deployed as a webservice.
Web proxy API is implemented through custom .NET application to detect and accurately predict SQL Injection in web requests for prevention of malicious web requests from the back end protected database.

Author demonstrate a concept for implementation of an Machine Learning predictive analytics and web service deployment for accurately prediction and prevention of SQL Injection with experimental evaluations in the Confusion Matrix and Receiver Operating Curve . [9]

Author Benfano Soewitoa et al. proposed method it uses scanning tools and penetration test to detect vulnerability of SQL Injection. For findining vulnerability URL parameters and user input are checked.

As the vulnerability is the result of the user input and URL parameters that are intentionally queried to the database without any processing,filtering and validation.

Regular expressions, prepare statements, and MySQL escape string techniques are used to implement a solution. [10]

Author Saima Saleem et al. proposed method consists of three important parts. First is setup installation for creation of dataset and training model using windows 10, wamp server ,DVWA. Second is attacking tools such as SQLMAP, Burpsuite , Metasploit are used for log creation. At last data collection, data preprocessing , data classification is done . Machine learning models are trained and tested. [11]

Author Meharaj Begum et al. proposed pattern-based Neural Network model to detect SQL injection .

He uses framework that extracts the WHERE clause of SQL query with the help of SQL parser, tokenize them with the help of word tokenizer and tagging them using tagger. The focus is to get the pattern of WHERE clause of genuine as well as malicious queries and differentiate them by their distinctiveness.

It is noticed while extracting tagged patterns that they are distinct and that distinctness useful for training ,modeling and classifying queries.

The proposed work consists dataset creation , preprocessing phase , parsing , tokenizing , tagging, pattenizing and updating tasks, Learning phase, Evaluation phase. [12]

TABLE I. DETAIL REVIEW OF SQL INJECTION DISCOVERY AND DETERRENCE TECHNIQUES ON THE BASIS OF EACH AUTHOR

Paper Id	Title Of Paper	Author /Publisher	Algorithm Technique	Data Set	Platform	Attributes / Parameters	Results	Future
1	An Efficient Technique for Detection and Prevention of SQL Injection Attack using ASCII Based String Matching , 2011	Indrani Balasundaram a, E. Ramarajb	Combination of static and dynamic analysis		.NET	Sensitive input fields like username ,Password	Able to prevent all web applications attacks.	Making Detection Overhead and prevention Overhead efficient.
2	Generation of SQL-injection free secure algorithm to detect and prevent SQL-injection attacks,2012	Kanchana Natarajan	Use secure algorithm SQL-IF dynamic technique	.	JAVA	Boolean ,Special Keywords and each keyword of SQL query is checked	detect the SQLIAs applied on real web-based applications	Generate parser to detect critical vulnerabilities
3	Secured Web Application Using Combination of Query Tokenization and Adaptive Method in Preventing SQL Injection Attacks,2014	Noor Ashitah Abu Othman, Fakariah Hani Mohd Ali	Query Tokenization and Adaptive Method		Five Test Cases	Input values	Detection and prevention	Enhancement of solution to block the SQL code
4	Implementation of pattern matching algorithm to defend SQLIA 2015	Nency Patela, Narendra Shekokar	modified AhoCorasick Pattern matching algorithm	Training data set	JAVA, SQLMAP tool	username ,Password	Less memory consumption	Construction of SQL parser to detect and prevent attack.
5	SQLiGoT: Detecting SQL	Debabrata Kar , Suvasini	graph , tokens and SVM			Single or multiple SVMs	Detection of SQLIA	Focus on improvement of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

	injection attacks using graph of tokens and SVM,2016	Panigrahi , Srikanth Sundararajan						accuracy
6	A Hybrid Method for Detection and Prevention of SQL Injection Attacks,2017	Dr. Ahmad Ghafarian,	Blend of static and dynamic	String Queries		String Queries	Able to handle queries normal or possible SQLIAs	Extend to include all other types of SQLIAs.
7	Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention, 2017	Solomon Ogbomon Uwagbole	ML predictive analytics	data set of extracted dictionary word ,SQL tokens from Microsoft SQL reserved keywords	Microsoft Azure Machine Learning,.Net Application	Tool used TCSVM classifier	Detect and prevent SQLIA in big data context	Extend to use multi-class classifier to identify and group the different SQLIA types
8	Prevention Structured Query Language Injection Using Regular Expression and Escape String,2018	Benfano Soewitoa, Fergyanto E. Gunawanb, Hirzic, Frumentiusa	Use techniques such as regular expression, prepare statement, and MySQL escape string.	URL Parameters, user input		SQL Map tool	prevention of system from SQL injection.	
9	Web Server Attack Detection using Machine Learning 2020	Saima Saleem , Muhammad Sheeraz , Dr. Muhammad Hanif , Dr. Umar Farooq	Machine Learning Simple classification and Text based classification models	Multi class labeled dataset, URL from each Log		Apache WAMP server, DVWA tool,Burpsuit,Metasploit, Python		Application to the technique on other web server attacks
10	Efficient Detection Of SQL Injection Attack(SQLIA) Using Pattern-based Neural Network Model 2021	Meharaj Begum, Michael Arock	pattern-based Neural Network model		Genuine or malicious queries are stored in spreadsheet.	Where clause in sql query	accuracy of detection and prevention is 94.4%.	extended to discover other types of injection with large dataset

V. CONCLUSION

Online services through web applications serve today's basic needs of people in this modern internet era. According to OWASP , SQL Injection attack is one of the topmost threats for security of web applications. It has become very important challenge for researcher to detect and prevent SQL Injection attack. In this paper we have studied different SQL injection detection and prevention techniques from 2011 to 2021and comparatively analyzed it. In future more research is needed for efficient and accurate detection and prevention of all types of SQL Injection Attack.

REFERENCES

[1] https://owasp.org/www-project-top-ten/
[2] Joshi Padma N etal, **"**Encountering SQL Injection in Web Applications", Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC 2018) IEEE Conference Record # 42656; IEEE Xplore ISBN:978-1-5386-3452-3
[3] Indrani Balasundarama etal ,"An Efficient Technique for Detection and Prevention of SQL Injection Attack using ASCII Based String Matching" ,International Conference on Communication Technology and System Design 2011, 1877-7058 © 2011 Published by Elsevier Ltd., Open access under CC BY-NC-ND license ,Available online at www.sciencedirect.com
[4] Kanchana Natarajan etal "Generation of SQL-injection free secure algorithm to detect and prevent SQL-injection attacks", ISSN: 2212-0173 2012 Published by Elsevier Ltd. doi: 10.1016/j.protcy.2012.05.129
[5] Noor Ashitah Abu Othman etal , "Secured Web Application Using Combination of Query Tokenization and Adaptive Method in Preventing SQL Injection Attacks", 978-1-4799-4555-9/14/$31.00 ©2014 IEEE
[6] Nency Patela etal ,"Implementation of pattern matching algorithm to defend SQLIA", International Conference on Advanced Computing Technologies and Applications (ICACTA-2015),Peer-review under responsibility of scientific committee of International Conference on Advanced Computing Technologies and Applications (ICACTA-2015),1877-0509 © 2015 The Authors. Published by Elsevier B.V. doi:10.1016/j.procs.2015.03.078
[7] *Debabrata Kar etal ,* "SQLiGoT: Detecting SQL injection attacks using graph of tokens and SVM",0167-4048/© 2016
[8] Dr. Ahmad Ghafarian,2017"A Hybrid Method for Detection and Prevention of SQL Injection Attacks", 978-1-5090-5443-5/17/$31.00 ©2017 IEEE
[9] Solomon Ogbomon Uwagbole,2017, "Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention", *IFIP/IEEE IM 2017 Workshop: 3rd International Workshop on Security for Emerging Distributed Network Technologies - Short Paper*
[10] Benfano Soewitoa etal,2018, "Prevention Structured Query Language Injection Using Regular Expression and Escape String", 1877-0509 © 2018 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

Selection and peer-review under responsibility of the 3rd International Conference on Computer Science and Computational Intelligence 2018. 10.1016/j.procs.2018.08.218

[11] Saima Saleem etal ,2020, "Web Server Attack Detection using Machine Learning" , This research work was funded by HEC Pakistan and Ministry of Planning Development and Special Initiatives under National Centre for Cyber Security 978-1-7281-6840-1/20/$31.00 ©2020 IEEE

[12] M. B. A and M. Arock, "Efficient Detection Of SQL Injection Attack(SQLIA) Using Pattern-based Neural Network Model," in *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India, Feb. 2021, pp. 343–347. doi: 10.1109/ICCCIS51004.2021.9397066.