SQL – Attacks, Modes, Prevention

Akarsh Kumar Keshri[1*], Abhinav Sharma[2], Sharon[3], Ayanesh Chowdhury[4],
Shivam Singh Rawat[5], Kanchu Kiran[6]

***Abstract*: SQL insertion attack (SQLIA) is a code injection technique which exploits a protection vulnerability going on in the database layer of an software and a provider. This is most usually observed inside web pages with dynamic content material. Structured Query Language Injection Attack (SQLIA) is the most uncovered to assault on the Internet. From this attack, the attacker can take control of the database that allows you to be capable of interpolate the statistics from the database server for the internet site. We have supplied one of a kind sorts of assault techniques and prevention strategies of SQLIA which have been used to aid the design and implementation of our version. The paper targets to place SQL attack into perspective by outlining a number of the materials and researches that have already been finished. The phase suggesting methods of mitigating SQLIA goals to clarify some misconceptions about SQLIA prevention and offers some beneficial tips to software program builders and database directors to save you the attacks. Web programs are presently utilized for on-line administrations, as an example: lengthy range casual conversation, purchasing and dealing with money owed. It deals with complex person information. Unauthorized get right of entry to can cause disintegrate of a system. SQLIA is a standout among the maximum risky safety dangers to Web programs. This paper indicates approaches to save you SQLIA in saved methods with the assist of parameterized queries in order that the net software is secured from injection attacks. The experiments display that the proposed methods are very powerful and simple than some other methods.**

***Keywords*: SQL, Modes, Attacks, Prevention.**

1. SQL

SQL is a type of internet software protection vulnerability in which an attacker is capable of submit a database SQL command, which can be done by means of an internet application, uncovering the again-cease database. SQL Injection assaults takes location when a web utility appoint user- provided records without perfect validation or encoding as part of a command or query. The particularly crafted person statistics schemes the software into executing unexpected instructions or converting statistics. SQL Injection allows an attacker to create, read, update, regulate, or delete facts saved within the back-quit database. In its maximum commonplace shape, SQL Injection lets in attackers to have access of touchy information together with social safety numbers, credit card range or other economic records.

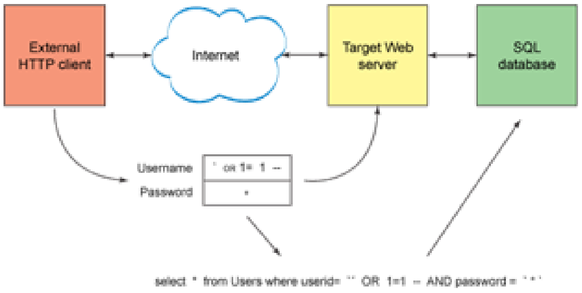


Fig. 1.

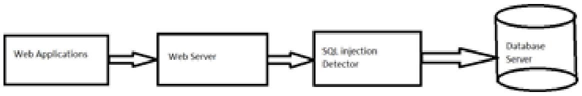


Fig. 2.

A. How Attackers Exploit SQLI Vulnerabilities

Attackers offer specially-crafted enter to trick an application into editing the SQL queries that the utility asks the database to execute. This lets in the attacker to:

- Control application behavior that's primarily based on statistics inside the database, as an example by way of tricking an application into permitting a login without a valid password.
- Alter statistics in the database without authorization, as an instance via developing fraudulent records, adding users or "selling" customers to better get admission to tiers, or deleting statistics.
- Access records without authorization, for example by tricking the database into presenting too many consequences for a question

B. Anatomy of a SQL Injection Attack

A developer defines a SQL question to perform some database movement essential for his or her utility to characteristic. This question has a controversy so that only preferred statistics are lower back, and the fee for that argument can be furnished by a user (as an instance, thru a shape discipline, URL parameter, web cookie, and so on).

A SQLI attack plays out in degrees:

1) Research: Attacker tries submitting diverse sudden values for the argument, observes how the software responds, and determines an assault to strive.
2) Attack: Attacker offers a cautiously-crafted enter value that, when used as an argument to a SQL question, could be interpreted as part of a SQL

[*] Corresponding author: akarshkeshri8@gmail.com

command rather than simply records; the database then executes the SQL command as modified with the aid of the attacker.

The research and assault levels can be without difficulty automatic by using conveniently-to be had tools.

2. Defending Against SQLI Attacks

There are easy approaches to avoid introducing SQLI vulnerabilities in an utility, and to limit the damage they can motive.

- Discover SQLI vulnerabilities with the aid of robotically trying out your programs both the usage of static checking out and dynamic checking out.
- Avoid and repair SQLI vulnerabilities via the use of parameterized queries. These varieties of queries specify placeholders for parameters so that the database will usually treat them as information rather than a part of a SQL command. Prepared statements and object relational mappers (ORMs) make this smooth for builders.
- Remediate SQLI vulnerabilities in legacy systems via escaping inputs before adding them to the query. Use this approach only where prepared statements or comparable centers are unavailable.
- Mitigate the impact of SQLI vulnerabilities by implementing least privilege on the database. Ensure that every utility has its personal database credentials, and that these credentials have the minimum rights the software needs.

Paper –1: A Novel method for SQL injection attack detection based on removing SQL query attribute. Inyong Lee (2011) proposed the method removes the value of an SQL query attribute of web pages when parameters are submitted and then compares it with a predetermined one. This method uses combined static and dynamic analysis for the detection of the SQL injection attacks.

Paper – 2: Study on SQL injection attacks: Mode, Detection and prevention. Subhranil Som (2016) proposed the method which detects SQL injection attacks in stored procedures and gave certain prevention measures for such attacks.

Paper – 3: SQL Injection Impact on Web Server and Their Risk Mitigation Policy Implementation Techniques: An Ultimate solution to Prevent Computer Network from Illegal Intrusion. Parveen Sadotra (2017) analyzed the existing detection and prevention techniques for SQL injection and provided description of how attacks of that type could be performed. It provided an easy solution to prevent computer Network for Illegal intrusion.

Paper – 4: Detection and prevention of SQL injection attack using novel method in Web Applications. Tejinderdeep (2015) proposed the method which uses test queries for SQL injections and gave a preventive measures for such kind of SQL injection vulnerabilities.

Paper – 5: Detecting SQL injection attack using query result size. Young-Su Jang (2014) proposed the technique which dynamically analyzes the developer- intended query result size for any input, and detects attacks by comparing this against the result of the actual query. This technique is implemented in a tool for protecting Java-based web applications. This method is experimentally found to be effective against SQL injection vulnerabilities.

Paper – 6: A survey of SQL injection attack detection and prevention. Khaled Elshazly (2014) proposed some useful tips for software developers and database administrators for preventing the intrusion in the database. It details the creation of filtering proxy server used to prevent SQL injection attack and analyses the performance impact of the filtering process in the web application.

Paper – 7: SQL injection Attacks: Detection in a Web Application environment. DB networks (2016) provided the detailed study of different SQL injection attacks and the detection of attacks on the Web based Application environment.

Paper–8: An Efficient Technique for Detection and Prevention of SQL Injection Attack using ASCII Based String Matching Indrani Balasundaram (2011) proposed the method which uses the prevention of SQL injection attack using ASCII Based String Matching. This security prevents the unauthorized access to your database and also it prevents your data from being altered or deleted by users without the appropriate permissions. Malicious Text Detector, Constraint Validation, Query length validation and Text based Key Generator are the four types of filtration technique which is used to detect and prevent the SQL Injection Attacks from accessing the database.

Paper – 9: SQL injection attack detection and prevention methods: A critical review. Dr. Manju Kaushik (2014) studied the various SQL injection prevention techniques and discuss it and find a better methodology in order to design better attack detection and prevention methods. For better security it has also discussed encryption and decryption techniques.

Paper–10: Classification of SQL injection Detection and prevention measure. Muhammad Saidu Aliero (2016) provided the programmers with common issues that need to be considered before choosing a particular technique and to raise awareness of issues related to such techniques as many of those techniques were not meant for the purpose of protection of SQLIA. In addition, it provided researchers by shedding light on how to develop good SQLI (SQL Injection) protection tools as most of the SQLI protection tools were developed using combination an of two or more defensive coding techniques. Lastly we provide recommendations on avoiding such issues.

Paper – 11: SQL UnitGen: Test Case Generation for SQL Injection Detection. Yonghee Shin (2006) proposed an method for SQL injection vulnerability detection, computerized by using a prototype tool SQLUnitGen. It additionally checks it in two small net packages and the approach is determined to be effective for the detection of SQL injection attacks.

Paper–12: Generation of SQL-Injection free comfortable algorithm to detect and prevent SQL- Injection Attacks. Kanchana Natarajan (2011) proposed SQL-IF at ease set of rules. The generated set of rules has been integrated into the runtime surroundings even as the implementation has been accomplished thru Java. The set of rules describes the method that how we comply with the tactics for stopping SQL-injection attacks. The paper presented the SQL-IF comfy algorithm and common sense of the generated code. Comparison of comparable styles of assault along with distinct features is finished. The empirical effects and its evaluation prove that the algorithm works efficaciously to stumble on the SQLIAs.

Paper–13: SQL Injection assault and defend Technical Research XuePing-Chen (2011) provided the precise research of SQL injection assault on net surroundings and gives preventive measures for such attacks resisting hackers from illegally getting into the database and additionally save you other malicious harm.

Paper–14: SQL-injection vulnerability scanning tool for computerized creation of SQL-injection attacks Abdul Bashah Mat Ali (2010) proposed the certain discussion for the development of new scanning tool for SQL injection vulnerabilities. The experiments shows that the proposed work is determined to be effective for preventing such injection assaults.

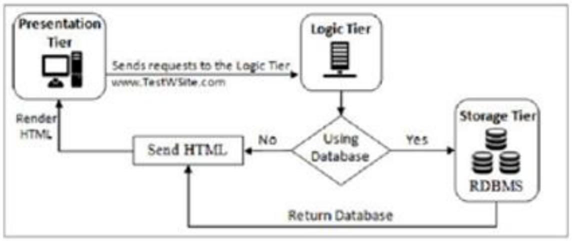


Fig. 3.

A. *Problem Definition*

There are exclusive form of SQL injection assaults and every attack is finished for some precise functions. Purposes such as Identifying Injectable Parameters, performing database fingerprinting, determining database schema, extracting information, Adding or Modifying facts, Bypassing Authentication, and so on. SQL injection is a type of software program vulnerability. In this the statistics that's entered by using the consumer is dispatched to the SQL interpreter as part of an SQL question. An attacker who carry out such attacks provides mainly designed enter facts to the SQL interpreter and traps the interpreter to execute the unintentional instructions. This sort of attacks are the important threats to the web based totally programs and web sites which store the net database including college web sites. This type of SQL injection assaults exploits safety vulnerability on the database layer. By exploiting the SQL injection fault, attackers can create, examine, adjust or delete touchy information. So we want a few effective measures to save you these type of SQL injection attacks.

Proposed Methodology:

To avoid these SQL injection attacks we need to use parameterized queries like as shown below:

Example Queries:

SqlCommand cmd = new SqlCommand("select Name, Total=value from countrydetails where value =@value", con);

cmd.Parameters.AddWithValue("@value",txtSearch.Text); SqlDataAdapter da = new SqlDataAdapter(cmd);

There are many architectures that can control and arrange any facts-driven systems, however the maximum not unusual architecture which is used is the three-tier architecture that relies upon on dividing the gadget into three degrees as follows:

1) Presentation Tier (a Web browser or rendering engine).
2) Logic Tier (a server code, including C#, ASP, .NET, PHP, JSP, and many others.).
3) Storage Tier (a database together with Microsoft SQL Server, MySQL, Oracle, and many others.).

The proposed approach takes a look at that if a few classic SQL injection Test queries does now not satisfy the Password authentication. (Test Queries along with Test'or1=1--) These type of Test queries is Specially crafted by means of the attackers in this sort of manner that the SQL interpreter is not able to Distinguish among the meant queries and the attacker's crafted facts. The interpreter is in one of these manner is tricked into looking forward to surprising instructions. So we use the parameterized Queries to keep away from such injection assaults. If the Test queries is not able to access the database, then there may be no SQL injection and using the parameterized queries we are capable of prevent it So there's no SQL injection attack within the website.

Implementation:

Tools used: Created free database as provided by the 000Webhost and personal free website Created by connecting the database using PHP queries.

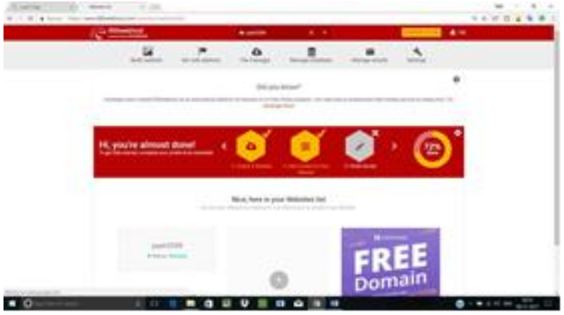
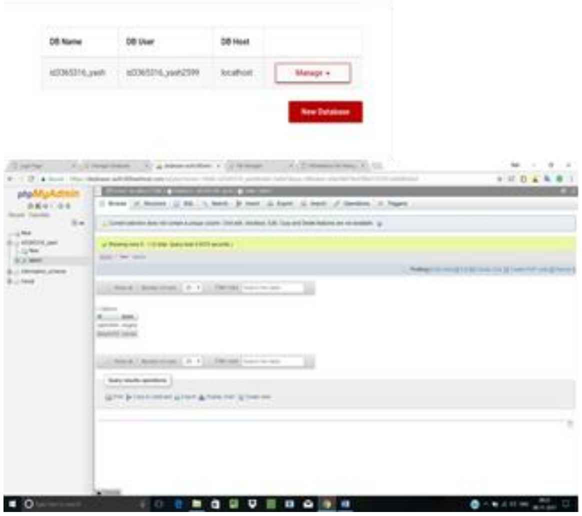


Fig. 4.

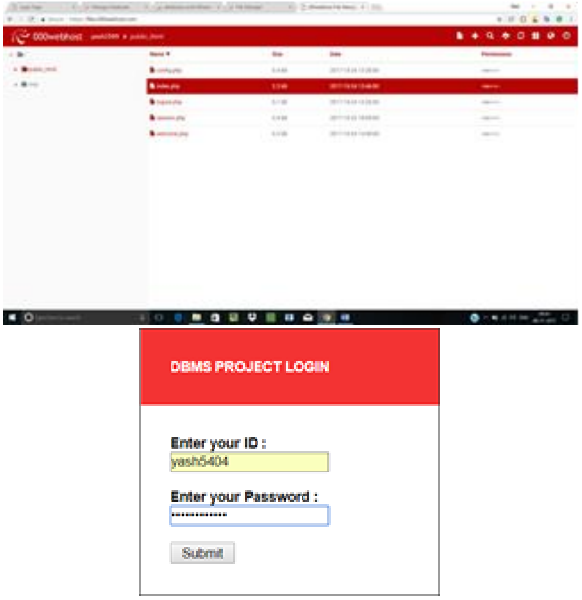
Database Created:



DB Name	DB User	DB Host	
id3365316_yash	id3365316_yash2599	localhost	Manage ▾

Fig. 5.

Queries written for creating a website:



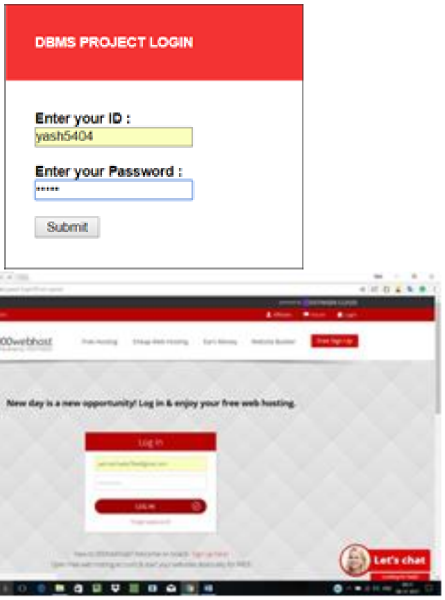
DBMS PROJECT LOGIN

Enter your ID : yash5404

Enter your Password : ••••••••••••••

Fig. 6.

Login Page of the Website:



DBMS PROJECT LOGIN

Enter your ID : yash5404

Enter your Password : •••••

Submit
000webhost
New day is a new opportunity! Log in & enjoy your free web hosting.
Log in
Let's chat

Fig. 7.

Connecting to the database with the correct password:

Connection to the database established with the correct password:

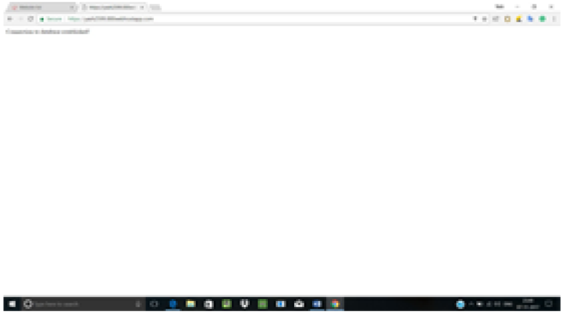
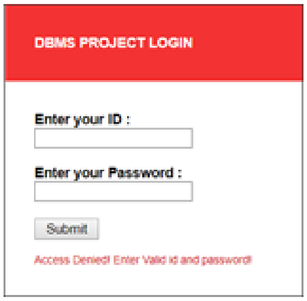


Fig. 8.

Trying to connect to the database with the crafted Test Query:

Access denied using the Test query as the password so the SQL injection is prevented.



DBMS PROJECT LOGIN

Enter your ID :

Enter your Password :

Access Denied! Enter Valid id and password!

Fig. 9.

3. Conclusion

The suggested compound technique successfully detects the SQL injection attack with the input test queries. The test queries such as (for example: TEST’ or 1=1--) are used for checking whether the site has SQL injection or not. The attacker is prevented to access the database with such specially designed crafty queries which can be result into the illegal access of the database and permits to make changes to sensitive information in the database. The prevention of such vulnerabilities is achieved with the help of use of parameterized queries. The proposed method is found to be effective for prevention of SQL injection attacks.

References

[1] Inyong Lee, Soonki Jeong, Sangsoo Yeoc, Jongsub Moon, A Novel method for SQL injection attack detection based on removing SQL query attribute, 2011.

[2] Subhranil Som, Sapna Sinha, Ritu Kataria, Study on SQL injection attacks: Mode, Detection and prevention, 2016.

[3] Parveen Sadotra, Chandrakant Sharma, SQL Injection Impact on Web Server and Their Risk Mitigation Policy Implementation Techniques: An Ultimate solution to Prevent Computer Network from Illegal Intrusion, 2017.

[4] Tejinderdeep Singh Kalsi, Navjot Kaur, Detection and prevention of SQL injection attack using novel method in Web Applications, 2015.

[5] Young-Su Jang, Jin-Young Choi, Detecting SQL injection attack using query result size, 2014.

[6] Khaled Elshazly, Yasser Fouad, Mohamed Saleh, Adel Sewisy, A survey of SQL injection attack detection and prevention, 2014.

[7] SQL injection Attacks: Detection in a Web Application environment, 2016, www.dbnetworks.com

[8] Indrani Balasundaram, E. Ramaraj, An Efficient Technique for Detection and Prevention of SQL Injection Attack using ASCII Based String Matching, 2011.

[9] Manju Kaushik, Gazal Ojha, SQL injection attack detection and prevention methods: A critical review, 2014.

[10] Muhammad Saidu Aliero, Abdulhamid Aliyu Ardo, Imran Ghani, Mustapha Atiku, Classification of SQL injection Detection and prevention measure, 2016.

[11] Yonghee Shin, Laurie Williams, Tao Xie, SQL UnitGen: Test Case Generation for SQL Injection Detection, 2006.

[12] Kanchana Natarajan, Sarala Subramani, Generation of SQL-Injection free secure algorithm to detect and prevent SQL-Injection Attacks, 2011.

[13] XuePing-Chen, SQL Injection attack and guard Technical Research, 2011.

[14] Abdul Bashah Mat Ali, Ala’ Yaseen Ibrahim Shakhatreh, Mohd Syazwan Abdullah, Jasem Alostad, SQL-injection vulnerability scanning tool for automatic creation of SQL-injection attacks, 2010.