Global Scientific Review
A Peer Reviewed, Open Access, International Journal
www.scienticreview.com
Volume 18, August 2023
ISSN (E): 2795-4951

Method and Algorithm for Determining Weaknesses in a Distributed Database

Sadikov Sh.M.
Associate Professor of
Tashkent University of Information Technologies
named after Muhammad al-Khwarizmi

Abstract: The article analyzes the SQL injection attack and its types in the distributed database, the vulnerability search algorithm, the vulnerability detection algorithm by query analysis in the MySQL (SQL) database, linear search algorithm, binary search algorithm, interpolation search algorithms have been developed

Key words: SQL injection, classic and blind SQL-injection, offline injection, search algorithm, linear search, binary search, interpolation search.

SQL injection attacks are typically used by attackers (hackers) to modify, delete, read, and copy data from an organization's database servers. In practice, such types of attacks carried out by attackers are explained by the fact that they pose a great risk to the database. If successful, this attack could have a major impact on all aspects of security, including privacy, integrity, and data availability. SQL (Structured Query Language) is used to send queries to database management systems. There are several scientific works on the detection and prevention of SQL injection attacks, where different protection methods from different fields can be used to improve the detection ability of the attack, and solving this issue in the scientific field is still relevant.

Today, organizations are creating a number of conveniences for users as a result of integrating their websites into web applications. On the other hand, if the database was previously attacked only through the server of the website, now it is possible to carry out these attacks through applications developed for optional mobile phones. The most common database attacks are SQL injection attacks. This attack is based on an injection vulnerability.

There are generally 3 types of SQL injection. These are:

- classic SQL-injection;

- blind SQL-injection;

- injection outside the network (the attack is carried out only by exceeding the size of the session opened between the client and the server.).

In a distributed database, taking into account that data is read, processed and stored from different places, the user can transparently access the data through the application, and also access the transactions through the data stored in different places. The increasing number of distributed databases is greatly helping to store and process video data. Attacks based on SQL injection vulnerabilities rarely fail and succeed in most cases. Because the algorithm implemented on the basis of vulnerability provides full access to the database. The most commonly used type of SQL injection today is Blind SQL Injection. The use of Blind SQL injection method is based on the complexity of injecting syntax one by one to find existing vulnerabilities in a distributed database. The proposed method generates the syntax automatically.

First of all, penetration testing is conducted. This method of testing is a method used to test the security of the system by attacking the system. Penetration Testing has three steps in which the test itself needs to be performed, i.e. gathering information, creating an attack, and analyzing the result. The data collection manager is considered to be the process of collecting data about vulnerabilities with a clear and proven basis and analyzing the objectives to identify additional data. Creating an attack is an attack process that is carried out using special packages based on the information obtained at the previous stage. The next step is to analyze the response, that is, based on the obtained results, to check the attacks, to record information about successful or unsuccessful attacks. In the proposed method, the information gathering step, i.e., the first step, uses the localhost website and chooses the attack position. A search algorithm is used to select a position. A search algorithm is an algorithm used to solve problems by retrieving certain stored information in a dataset. The proposed search algorithm uses a small adaptive intersection algorithm in the second step. The optimal results obtained using binary search are implemented using interpolation search.

Table 1

Search algorithm type and description

№	Algorithm type	Explanation
1.	Linear search	Results are searched in the order in which the data was generated.
2.	Binary search	The data is split into two segments, then the results are compared to see if they are above or below the previous segment, and then continue to split them until the requested data is the same as the results.
3.	Interpolation search	Finds the requested data by guessing the location of the data using key values.

The data used in this method is used from the localhost connected to the MySQL (SQL) database. The lookup data uses printable hex numbers in the range 0x20 to 0x7f. To measure the speed of the proposed method, the search time of each query from each algorithm is compared with the search time of existing methods. Here, T_0 is the start time of request retrieval process, and T_1 is the end time of request retrieval. The time efficiency comes from the following formula:

$$\Delta T = T_1 - T_0$$

Now the following sequences are performed to implement the proposed method. This sequence helps identify any SQL injection vulnerabilities that exist on the system.

1. A type of logical malformed query attack is selected.
2. The necessary tables are attached to exploit syntax errors or logical errors so that the attacking website application returns an error page.
3. A SQL injection vulnerability exists in the system if the injection is passed through a website page obtained from a login form.
4. In the next step, the query extension is checked using SQL elements in the browser being used.
5. After checking these elements, the automation application will call it back using the library queries in the Python (Php...) library. This is because the MBBT MySQL (SQL) query function is a post type, because the system operation principle is designed to send via a query. based on
6. After that, if there is an error in the function, MBsi will allow you to access the website through the login page.
7. And through the request created by the application, it allows to find the username and password in the database.
8. Injection is done using the substring() function, which takes three parameters, column_name, first_index, and an array of characters.
9. The injection request matches the main request of the space in the login form, ensuring that the main request does not work. At this point, the system cannot replace with a valid injection request.
10. The performed requests are automated according to the algorithms in the table above. The first thing to look for is the database name. It will then start searching for a list of tables from that name.
11. Once the table name is obtained, the user is authorized to access the tables containing the list of usernames and passwords.
12. The algorithm of this method is performed individually according to the algorithms (Linear search, Binary search, Interpolation search) in the table above in step 10. Their block diagrams look like this.

Algoritm ma’lumotlar bazasida har bir to‘g‘ri harfni qidiradi va keyin uni o‘n besh marta takrorlaydi. O‘n besh marta takrorlash - bu har safar dastur takrorlanganda va javob to‘g‘ri bo‘lishi uchun jumlaga joylashtirilgan belgi uzunligini bashorat qilishni anglatadi. Keyin izlayotgan ma’lumot xabar ekanligini ko‘rsatadigan ma’lumotni chiqaradi.

Qidiruv 0x20 dan 0x7f gacha bo‘lgan 16 lik sanoq tizimidagi ma’lumotlarini ketma-ket ishlatadi. Shakl va javob funksiyasi ilovalarni veb-saytdagi login formasiga yuboriladigan so‘rov natijalarini taqdim etishi va ma‘lumotlar bazasiga kirishi uchun ilovalarni internetdagi tizim bilan bog‘lashdan iborat bo‘ladi.

Keyingi ikkilik qidiruv algoritmi ma’lumotlarni ikkiga bo‘lish orqali ma’lumotlardagi har bir harfni qidiradi. Keyin ma'lumotlar natijalar yuqorida yoki pastda bo‘ladimi, u har bir harfning barcha natijalarini so‘z bilan tartibga solguncha taqqoslanadi. Shakl va javob chiziqli qidiruv algoritmidagi kabi bir xil funktsiyaga ega bo‘ladi.

The algorithm searches for results by guessing the location of the data, so that the initialization process is not always like a binary search from the middle, but starts with the data closest to the result. The title is also sometimes used to identify the location of the information being searched for, whether it returned true or false results.

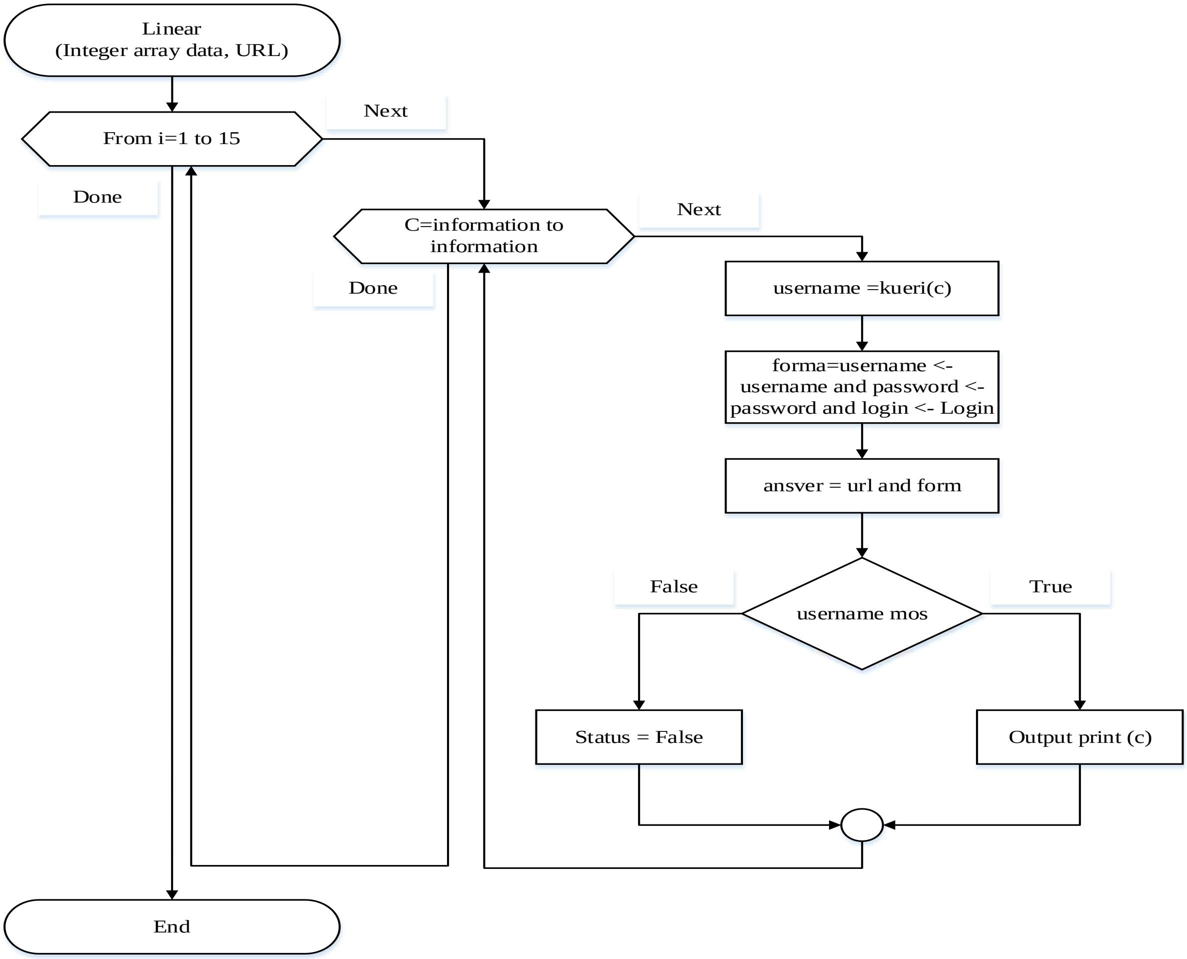

Figure 1. Block diagram of linear search algorithm

When conducting verification tests, it is advisable to conduct at least ten tests for each algorithm. The test is based on the search time for each letter. In order for the search to be balanced, each algorithm looks for the same target, which is a vulnerability in the database. Each letter can be viewed in the attachment section for search information. The test is performed in two forms, the first test form is linear-binary-interpolation and the second is linear-interpolation-binary. The purpose of implementing these two formulations is to clearly determine the performanceof each algorithm.

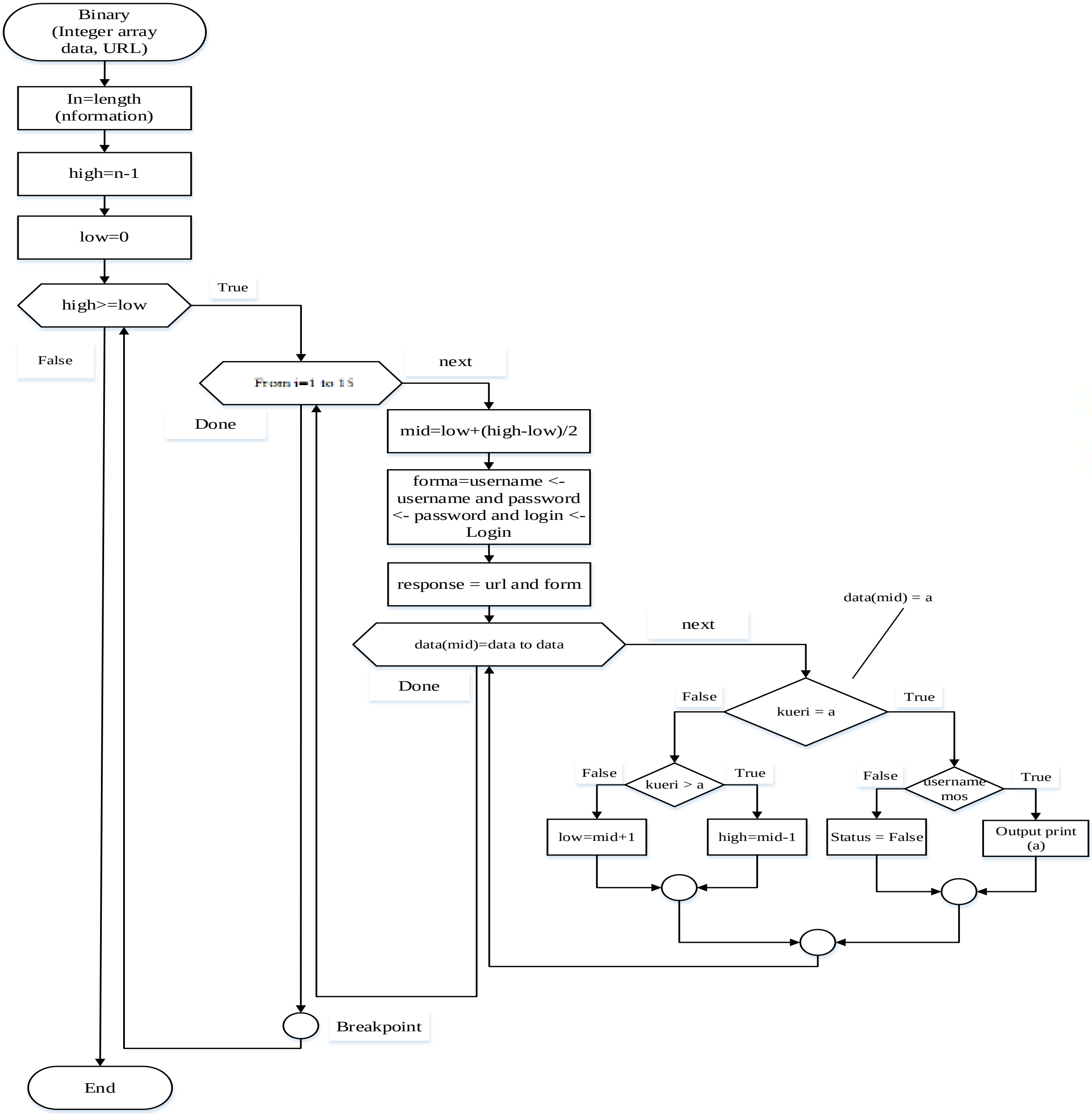

Figure 2. Block diagram of binary search algorithm

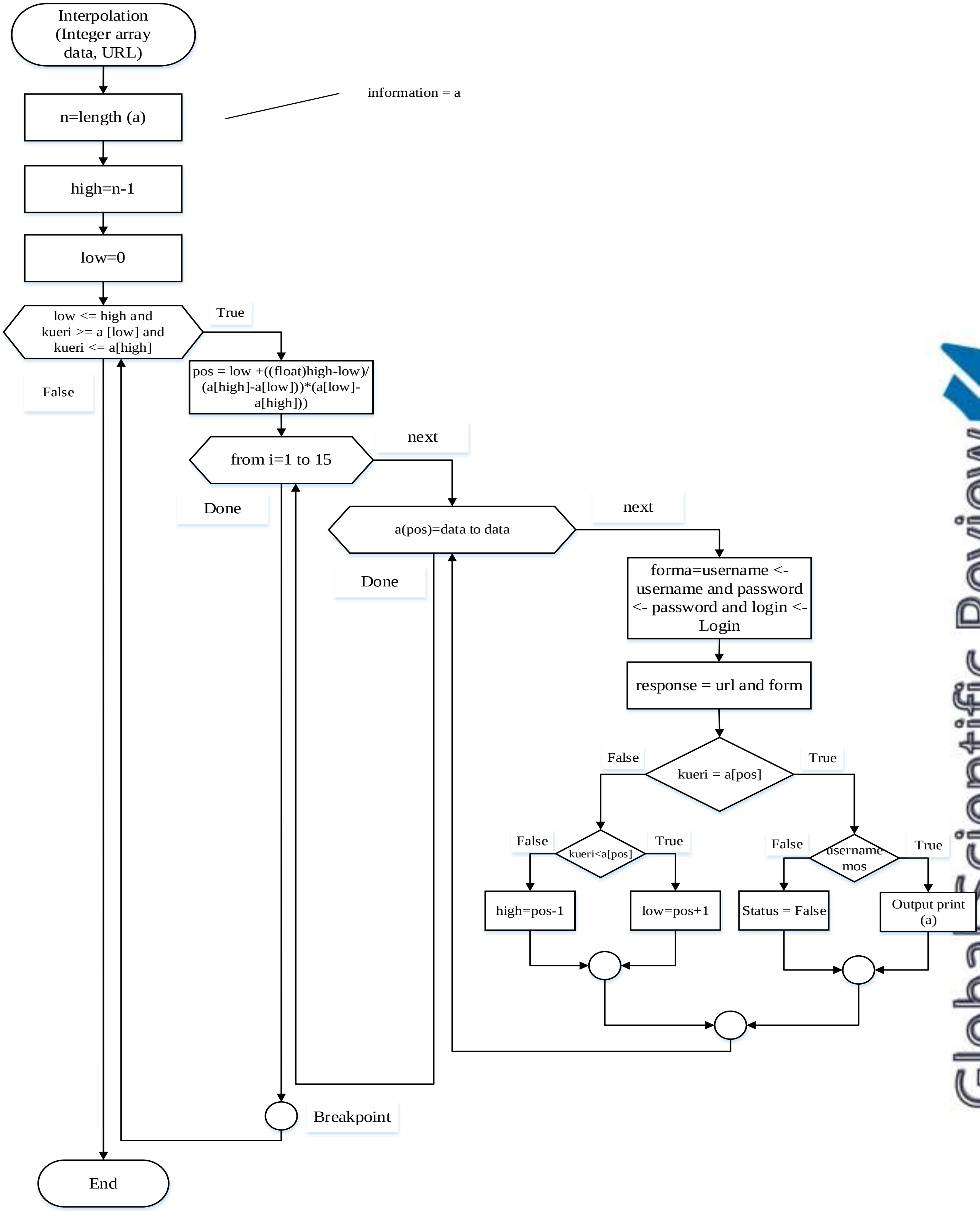

Figure 3. Block diagram of the interpolation search algorithm

Based on the above method, it will be possible to identify vulnerabilities in the distributed database, but even these methods are unlikely to identify all system vulnerabilities. Because the origin of vulnerabilities depends on various factors, it is impossible to determine them 100 percent. therefore, as much as possible, it is advisable to follow the following recommendations for identifying vulnerabilities and eliminating them in the process of ensuring the security of the distributed database of corporate network users.

A distributed database has the same basic SQL flaws as a shared database, and queries are executed the same way in both cases. In this way, identifying SQL injection vulnerabilities in a distributed database is slightly different than identifying vulnerabilities in a shared database. Because tables in a distributed database may be located in different locations, a vulnerability may exist in one part of a distributed database and not in another. A vulnerability in one part of a distributed database does not mean that there are no vulnerabilities in the whole.

The following methods exist for detecting and remediating SQL injection, and these methods vary by platform. These are:

- Syntax method for combining strings;

- method of comments;

- method of batch (or aggregate) requests;

- method of choosing platform-specific APIs

- method of sorting error messages.

In addition, in many cases, SQL injection prevention uses defined, separated, and parameterized SQL queries instead of concatenating strings in the SQL query.

Parameterized queries are queries that can be used in all situations, including WHERE and values in INSERT or UPDATE statements, using SQL queries in a distributed database as input. Note that they cannot be used in other parts of the request. Examples of this include table or column names, or processing data in a distributed database in an ORDER BY section.

In distributed database management systems, these parts of the query can include an additional module that places the data and whitelists new values or requires the use of other logic to perform the desired task.

List of used literature:

1. Yong Wang, Jinsong Xi, Tong Cheng "The Overview of Database Security Threats' Solutions: Traditional and Machine Learning" Journal of Information Security, Vol.12 No.1, January 2021.
2. Chandel, S., Ni, T.-Y. and Yang, G. (2018) Enterprise Cloud: Its Growth & Security Challenges in China. 2018 5th IEEE International Conference on Cyber Security and Cloud Computing, Shanghai, 22-24 June 2018, 144-152. https://doi.org/10.1109/CSCloud/EdgeCom.2018.00034
3. Sh.M.Sadikov "Ptotection of databases corporate information systems" Academic international conference on Multi-disciplinary studies and education, USA 2023.

4. Sh.M.Sadikov "Classification of information security thereats in the database" Innovate research in modern education, Canada 2023.
5. Sushil Jajodia and Bhava "Database Security: Status and Prospects" 2002
6. Alton Chung and Sheng-Uei Guan "Database Security: From Legacy Systems to Blockchain Technology" 2021
7. Charlie Kaufman, Radia Perlman, and Mike Speciner "Network Security: Private Communication in a Public World" 2013
8. Ross Anderson "Security Engineering: A Guide to Building Dependable Distributed Systems" 2014