VOL 2 (2018) NO 3 - 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Review of SQL Injection : Problems and Prevention

Mohd Amin Mohd Yunus[#], Muhammad Zainulariff Brohan[#], Nazri Mohd Nawi [#], Ely Salwana Mat Surin*, Nurhakimah Azwani Md Najib[#], Chan Wei Liang[#]

[#] Faculty of Science Computer and Information Technology, Universiti Tun Hussein Onn Malaysia, Malaysia

**Institute of Visual Informatic, Universiti Kebangsaaan Malaysia*

E-mail: aminy@uthm.edu.my, zainulariff96@gmail.com, nazri@uthm.edu.my, elysalwana@ukm.edu.my, nurhakimahazwani95@gmail.com, weiliang246@gmail.com

***Abstract*— SQL injection happened in electronic records in database and it is still exist even after two decades since it first happened. Most of the web-based applications are still vulnerable to the SQL injection attacks. Although technology had improved a lot during these past years, but, hackers still can find holes to perform the SQL injection. There are many methods for this SQL injection to be performed by the hackers and there is also plenty of prevention for the SQL injection to be happened. The vulnerability to SQL injection is very big and this is definitely a huge threat to the web based application as the hackers can easily hacked their system and obtains any data and information that they wanted anytime and anywhere. This paper can conclude that several proposed techniques from existing journal papers used for preventing SQL injection. Then, it comes out with Blockchain concept to prevent SQL injection attacks on database management system (DBMS) via IP.**

***Keywords*— Database, DBMS, SQL Injection**

I. Introduction

SQL is the short form of Structured Query Language. The usage of SQL is to interact with a database and it can manipulate the data which is stored in the database. Database normally contains data definition language and data manipulation language for allowing result retrieval. Meanwhile, Injection is an action of injecting something into an organism. SQL injection is a technique for hackers to execute malicious SQL queries on the database server. It can be executed over a web-based application to access over the databases that contain sensitive information. According to National Security Agency (NSA), SQL injection is the most typically ways used by hackers, even the famous database organization MYSQL was hacked by this techniques on electronic records [11],[12]. There is some vulnerability that will cause data leakage in MySQL because of the attackers accessing to the database and exposure the information or alter it. One of the vulnerability of it is privilege escalation or called it race condition bug. This bug allows the local system users access to the database and upgrade their privileges like change their id to 1 which can be an admin and alter or execute the information as their like. This will give an opportunity to an attacker access to the entire database server. The attacker might get fully compromise the target server.

Besides that, there is another vulnerability which is root privilege escalation bug. This bug works with the previous vulnerability. Since the previous bug the attackers gain the privilege to access to the server and get upgrade user to administrator, the attacker can change a certain system file to a random file. Due to the present bug, it will cause the tied to an unsafe file. That’s why, the attack can change the file easily because the bug is open a backdoor for the attacker to alter the file.

Normally, the most common attack that will happen and threat the database system is the login system. For the login page, most of the attack will try using brute force with mean that guessing the password by trying every possibility like dictionary attack is consider as a type of brute force. Another attack is very common and use widely for attackers which is SQL injection. SQL injection is putting **'1' OR '1' = '1'** into username and password. If the system does not have any SQL injection prevention, if the attacker enter this code inside, the attacker can access to the system will authorization [1]-[4].

The bad consequences of this SQL injection is hacker can gain access on the database information easily. However, this SQL Injection can be prevented by few ways. The first approach is by using the SQL Injection Sanitizers which is used in the Directory of Useful Decoy (DUD) to detect the intervention in the web based application. For the second approach, firewall should be provided for the SQL server. In completing this review paper, thirteen interesting journal papers regarding SQL injection were reviewed comprehensively. Study by [1], they define SQL injection as the method for hackers executes malicious SQL queries on the database server via a web based application. They also explain about the strategy on how to fight SQL injection in the journal and the solution in fighting SQL injection. In [2], they explained about how SQL injection works and the defensive mechanism against these threats. As for the studies in [3] and [4], they explained about how to prevent SQL Injection on Server-Side Scripting and how to detect SQL injection attack respectively. In [5], they explained also about the prevention of SQL injection.

Database is a set of data and information which is organized so that it can be accessed, easily, handle and updated. The data is organized into rows, column and tables and it is indexed to make it accessible to find the related data and information. The data will get updated, enlarge and deleted as new data and information is added. Databases process workloads to create and update itself, inquiry the data they contain and running the application against it. With the increase in usage of the database, the regularity of attacks against those databases also increased. Data crack are threats to every organization. Crack damage goes beyond the actual loss of sensitive and personal information. The risk of sensitive organizations must always step ahead in their database security to protect and secure their data and information from the attackers. Database attacks are increasing trends nowadays. One of the reasons is the increment of accessing the data and information which is stored in databases. When the data had been accessed by a lot of anonymous people, the chances of the data threats is increases. Furthermore, the database attacks are to make a lot of money by selling the sensitive information such as credit card numbers in illegal ways. Based on my first journal [6], the journal explained about the lack awareness regarding the database security which can lead to a lot of database threats such loss of the integrity, confidentiality and availability of the data and information of the companies and etc. From the [7], to reduce the percentage of database threats, this journal has proposed some techniques to overcome this problem such as improving the existing security system of the database. Furthermore, in [8], the journal discussed about a detection system which is anomaly detection (AD) to detect any insiders attacks of the database which is far more dangerous from the outsider attacks. Moreover, from [9], there are various categories of attacker such as intruder, insider, and administrator. Besides, the journal also discuss about the type of attacks which is direct attacks, indirect attacks, passive attack and active attack. From the last journal [10], it is discussed about the database security threats in mobile and how overcome this problem. In the database system it is compulsory to have support. The security of the database system in mobile is much more important. Thus, next section discusses material and method or algorithm for comparing methods according to each author. Then, result and discussion. Last section is conclusion for summarizing this paper.

II. The Material and Method / Algorithm

The definition of the literature is the report of the information which is evaluative that found in the literature relevant to our elected area of the study. The review should be specify, summarize, classify and interpret the literature. The review should provide the theoretical, analytical base for the research. Database is depository of the most significant and valuable data and information in the company. In the database there different of security layers which is the security officers, system administrator, database administrator, the employees and the developers. The attacker can crack this security layers. Some reviewed papers were studied for avoiding the attacker can crack this security layers in Table I.

TABLE I
Methods Comparison based on Each Authors

Reference Number	Author	Method	Drawback
[1]	S. Nanhay, D. Mohit, R.S. Raw, and K. Suresh	Minimize the privileges, Implementation of consistent coding standards and SQL server firewalling	It does not have node to node verified signature
[2]	K.G. Vamshi, V. Trinadh, S. Soundabaya, and A. Omar	Processing input, Sp_executesql replace with QUOTENAME, Managing Permissions, Tools to detect SQL injection queries	It does not have node to node verified signature
[3]	K. Krit and S. Chitsutha	SQL injection commands datasets extraction, pre-processing, machine learning model analysis for SQL injection prediction and detection, testing and training,	It does not have node to node verified signature
[4]	P.K. Raja and Z. Bing,	Entirely dependent on user-defined approach (DUD) Threshold value	It does not have node to node verified signature
[5]	D. Rhythm and G. Himanshu	Filtering sending and receiving mechanism	It does not have node to node verified signature
[6]	A.A. Nedhal and A. Dana	Web application firewall	It does not have node to node verified signature

[7]	A.S. Aditya and P.N Chatur	Security check model based on safety rule base	It does not have node to node verified signature
[8]	S.P. Ganesh and G. Anandhi	Access control, inference policy, user identification and authentication, accountability and auditing, encryption consideration	It does not have node to node verified signature
[9]	Parviz Ghorbanzadeh, Aytak Shaddeli, Roghieh Malekzadeh, Zoleikha Jahanbakhsh,	security products such as firewalls, virtual private networks (VPNs) and intrusion detection and prevention (IDP) systems	It does not have node to node verified signature
[10]	Asmaa Sallam, Qian Xiao, Daren Fadolalkarim, Elisa Bertino	Role-Based Anomaly Detection approach	It does not have node to node verified signature

Based on [9], the attackers can be divided in some categories which are intruder, insider and administrator. The meaning of an intruder is an anonymous people that have no rule to accessing a computer system in an illegal way and to get some rare data and information that stored in the database. For the insider is not an empower people but a representative of group of trusted users and cause the violet empower people privileges and tried to get the data and information without user's own access permissions. An authorize people that has fully domination over the computer system, but he uses privileges of administration in illegal way to get the information of the system is an administrator. Besides in [9] also discuss about the different types of attacks which is direct attacks, indirect attacks, passive attack and active attack. Most of the web based applications belongs to organization, universities, schools and others. Commonly, all these web based application provide a form for the users to login into the application. The data which the users input can easily be exploited through SQL injection. For example, when a teacher wants to login the school portal she first need to login to access into the school portal as in Fig. 1. But, when she inputs the username and password and the web form is not securely coded as in Fig. 2, hackers can easily gain the data that the user inputs it by using a set of SQL queries as shown in Fig. 3. So, this is basically how SQL injection works.

Attack which is achieved by the direct hitting is the direct attack. If the database is does not contain any security system, the attack is successful. If the attackers change to the next attacks that means the attacks are failed. The meaning of the indirect attack is not directly executed on the objective but the information and data from the objective can be collected through other transitional object for the security system to be trick. The indirect attack is difficult to be track. For the further types of attacks are passive attack and the active attack. For passive attack, clear text passwords and important data and information which can be used in other types of attack and it is also unencrypted traffic to be guide. It is also display of information and data to the attackers beyond the permissions of the users. The active attack is the attackers had performed many attempts to breach the secured system to get the information and data which is stored in the database. The attack can be completed through many ways such as viruses, worm, stealth and others. The information can be accomplished in electronically attack illegal beyond user knowledge.

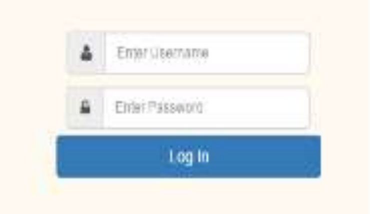
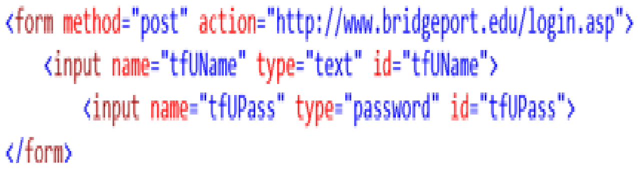
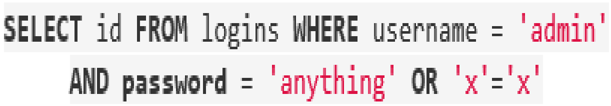


Fig 1. Login form



```
<form method="post" action="http://www.bridgeport.edu/login.asp">
    <input name="tfUName" type="text" id="tfUName">
        <input name="tfUPass" type="password" id="tfUPass">
</form>
```

Fig 2. HTML codes for the input fields [2]



```
SELECT id FROM logins WHERE username = 'admin'
AND password = 'anything' OR 'x'='x'
```

Fig 3. SQL injection query [2]

Based on [1], there are few ways in preventing SQL injection which is minimizing the privileges, implementation of consistent coding standards and SQL server firewalling. Decreasing the privileges is by giving priority to security aspects and suitable steps need to be taken during the development stage. Implementation of consistent coding standards means that the developers need to set some coding policies to ensure that the input validations checks are performed on the server so that it will be more secured. SQL firewall is important so that only the trusted clients can be contacted. The firewall should reject all the untrusted. In [2], there are three prevention methodologies stated. The first method is known as processing inputs. In order to executes SQL injection, keywords such as 'FROM', 'WHERE' and 'SELECT' are used. So, if the keywords are not accepted in the input fields, this problem can be solved. The second method is managing permissions which only allow people with the authorization of the database can access the data. Meanwhile in [3], the vulnerability of SQL injection and they had proposed a framework which is known as "PhpMinerl" for SQL injection. Furthermore, a novel method for detecting SQL injection attack based on removing the SQL queries attributes values. They had planned a way to remove the attributes of SQL queries. Nonetheless, this method cannot justify the SQL syntax before detecting the SQL injection. Besides, in this journal the also explain about Microsoft Azure Machine Language which is a cloud based predictive service that provides a full managed model predictive analytics and predictive models. In [4], DUD approach is used to detect SQL injection. DUD approach is a post generated approach that depends on query classification. This approach is fully depending on user, which needs to be defined prior to the execution of the algorithm. This DUD approach is then improved by using SQLI sanitizers to verify the attacks by comparing the run time of SQL statements with the sanitizers. Moreover, in [5] there are more prevention techniques in order to prevent SQL injection attacks such as black box testing. Black box testing boost the testing system that is infiltrated by the utilization of machine learning approaches. Besides black box testing, they also proposed proxy filters and intrusion detection system [6]-[9].

Nowadays, the security of a web based application can be breached easily by everybody and anytime especially by hackers. Although almost all web based application has their own security system, but not all security system is secured from SQL injection. So, to ensure the security of the database, detection of SQL injection is very crucial because SQL injection is very popular among hackers nowadays and the security of the database can be breached anytime [13]-[15]. As the wording said, prevention is better than cure. The approach of SQL injection can be categorized as pre-generated and post- generated.

In SQL Injection attacks, these are some of the methods of SQL injection attacks such as Using Unauthorized Queries, Stored Procedures, UNION Query and Bypassing Web-based Application. Firstly, the purpose of hackers use Unauthorized Queries technique is because of they want to know the structure of the table. They first input the illegal queries to the web based application. Then, the web based application will detect the error and display the error. From the errors, hackers can know a little bit about the structure of the table. After they had known the structure of the table, they can attack the web based application by SQL injection. Secondly, in Stored Procedures, most of the web based application saved the stored procedures and use it for data transmission. As the developers, they thought that by saving the stored procedures, it will prevent SQL attacks. Unfortunately, the stored procedures will make the web based application be more exposed to SQL injection attacks. Thirdly, for UNION Query, The objective of the attacker is to obtain the data and information from the database. This process is successful until there are no DBMS error messages. Lastly, bypassing Web-based Application, Breaching the web based application is the common method of attacks used by the hackers. This method is easy for the hackers as they had bypassed the web application, they just need to input a certain query. SQL injection is first applied during 1998 and had cause many problem for the web developers. Because of these immoral activities by the hackers, the web based application is getting busy to find the solution in order to prevent this SQL injection from happening and cause a lot of problem for them.

As a result from this SQL injection problem, some methods of prevention of SQL injection have been proposed such as Minimizing Privileges, Implementation of Consistent Coding Standards and SQL Firewalling. Firstly, in Minimizing Privileges, the developers of a web based application need to put number one priority on their securities. To avoid such things from happening, it is important to create a low privilege account. Secondly, Implementation of Consistent Coding Standards is to ensure that our web based application is hard to be hacked; developers need to set a consistent coding standard especially in the input validation form because the hackers usually breached the security of a web based application from the log in system of the web based application. Lastly, any SQL server must be firewalled to give access only to the trusted clients. The firewall will reject any unwanted such as escape sequences, binary data and comment characters.

Based on the reviewed papers, the authors never mentioned about Blockchain concept[16] as it detect verified nodes that may access web server and database for manipulation based on allowed Internet Protocol (IP) access. However, those unallowable nodes only do legal transactions without manipulating or injecting database. It is therefore, Fig. 4 shows that the adaption of Blockchain concept to avoid the SQL injection attack where each node requested access another node's database, the node requested is verified by the node who accepted the request. If not accepted, the request is rejected for security purpose. The concept will be applied to all nodes. A node could be a server, computer etcetera on computer system networking.

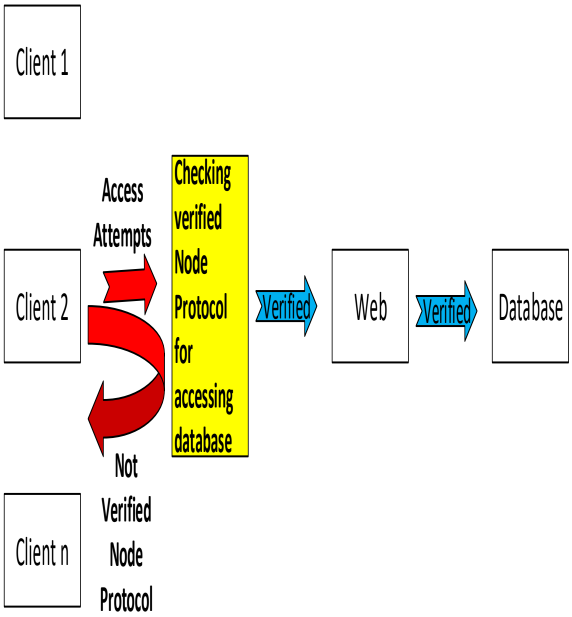

Client 1
Access Attempts
Checking verified Node Protocol for accessing database
Client 2
Verified
Web
Verified
Database
Not Verified Node Protocol
Client n

Fig 4. Proposed Method for Avoiding SQL Injection based on Blockchain Concept based on [16]

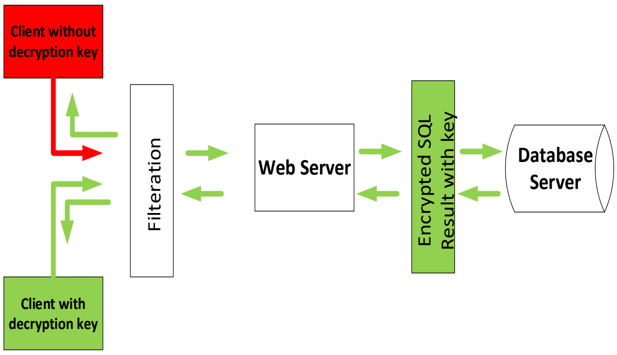

Client without decryption key
Filteration
Web Server
Encrypted SQL Result with key
Database Server
Client with decryption key

Fig 5. SQL injection query prevention approach

Fig. 5 shows the prevention from SQL injection problem happening. There would be two clients with different permission. A red client is without decryption key where as a green is having decryption key for SQL injection result. A red client may not decrypt the result as not a green client even though he or she has the result. Therefore, the result is safe without revealing to unauthorized client as indicated in red colour.

III. Results and Discussion

In this study, SQL injection is one of the most serious cases about data stealing from the database which associate with a web based application. This SQL injection is frequently happen because of the vulnerability of the web based application and the lack of awareness regarding the security of the database. There are a lot of ways for the SQL injection to be performed by the hackers outside there. So, to prevent this from happening, as a developer of a web based application, Blockchain [16] must be put an important priority to the security of web based application to ensure that all of the data in the database is kept safe and sound. The security of the web based application should be tested to check the either the security is vulnerable to SQL injection or not. This is to ensure that nobody can breach into the security of the database of the web based application. Based on my research, I had found that there are so many types of the database security threats which include insiders attack, internal attack, and external attack etcetera. But when there is a problem, there will be a solution. Same cases with threats in database security, there are a lot of problems occurs and in the same time, there are also have some solutions for the problem such as access control, inference policy, user authentication, data encrypted etcetera.

IV. Conclusions

Precisely, the main objective of this research is to study more about the techniques for hackers to execute malicious SQL queries on the database server which is called SQL injection. It is the most popular technique among the hackers to gain data and information about something that is stored in a database of a web based application. The major objective of this research is to figure out about what is the database threats which is define as an immoral activity which is performed by some hackers to steal the data and information in illegal ways. The second objective is about the example of database threats such as excessive privilege abuse, legitimate privileges abuse, privileges elevation and the platform vulnerabilities and how to overcome this problem. Thus, Blockchain concept is introduced for overcoming the SQL injection via Nodes Verfication with IP. For the future work, SQL injection prevention will be executed using Blockchain and Augmented Reality (AR). It might be an approach to view SQL injection attempts using AR that improve the potential injection attack.

Acknowledgment

This project is indirectly sponsored also by Universiti Tun Hussein Onn Malaysia. This research also supported by Research GATES IT Solution Sdn. Bhd. under its publication scheme.

References

[1] S. Nanhay, D. Mohit, R.S. Raw, and K. Suresh, “SQL Injection: Types, Methodology, Attack Queries and Prevention”, in 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, p. 2872 – 2876.

[2] K.G. Vamshi, V. Trinadh, S. Soundabaya, and A. Omar, “Advanced Automated SQL Injection Attacks and Defensive Mechanisms”, in Annual Connecticut Conference on Industrial Electronics, Technology & Automation (CT-IETA), 2016, p. 1-6.

[3] K. Krit and S. Chitsutha, “Machine Learning for SQL Injection Prevention on Server- Side Scripting”, in International Computer Science and Engineering Conference (ICSEC), 2016, p. 1-6.

[4] P.K. Raja and Z. Bing, “Enhanced Approach to Detection of SQL Injection Attack”, in 15th IEEE International Conference on Machine Learning and Applications (ICMLA), 2016, p. 466 – 469.

[5] D. Rhythm and G. Himanshu, “SQL Filtering: An Effective Technique to prevent SQL Injection Attack”, in International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2016, p. 312 – 317.

[6] A.A. Nedhal and A. Dana, “Database Security Threats: A Survey Study”, in 5th International Conference on Computer Science and Information Technology, 2013, p. 60 – 64.

[7] A.S. Aditya and P.N Chatur, “Efficient and Effective Security Model for Database Specially Designed to Avoid Internal Threats”, in International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015, p. 165 – 167.

[8] S.P. Ganesh and G. Anandhi, “Database Security: A Study on Threats And Attacks”, *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 4(6), pp. 512-513, 2015.

[9] Parviz Ghorbanzadeh, Aytak Shaddeli, Roghieh Malekzadeh, Zoleikha Jahanbakhsh, “ A Survey of Mobile Database Security Threats and Solutions for it”, in the 3rd International Conference on Information Sciences and Interaction Sciences, 2007, p. 676 – 682.

[10] Asmaa Sallam, Qian Xiao, Daren Fadolalkarim, Elisa Bertino, “Anomaly Detection Techniques for Database Protection Against Insider Threats”, in 17th International Conference on Information Reuse and Integration (IRI), 2016, p. 20 – 29.

[11] L. Zhang, C. Tan, and F. Yu, “An Improved Rainbow Table Attack for Long Passwords,” *Procedia Computer Science*, vol. 107, pp. 47–52. 2017.

[12] Deniz Gurkan and Fatima Merchant “Interoperable Medical Instrument Networking and Access System with Security Considerations for Critical Care”, *Journal of Healthcare Engineering*, vol. 1(4), pp. 637-654, 2010.

[13] M. A. Halcrow and N. Ferguson, “A Second Pre-image Attack Against Elliptic Curve Only Hash (ECOH),” in IACR Cryptol. ePrint Arch., vol. 2009, p. 168, 2009.

[14] A.K. Kyaw, F. Sioquim, and J. Joseph, “Dictionary attack on Wordpress: Security and forensic analysis,” in 2015 2nd International Conference on Information Security and Cyber Forensics, InfoSec 2015, 2016, p. 158–164.

[15] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, “Social engineering attack framework,” in Proceedings of the ISSA, 2014.

[16] Hilarie Orman, “Blockchain: the Emperors New PKI?”, *IEEE Internet Computing*, vol. 22(2), pp. 23-28, 2018.