JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Novel Technique To Prevent SQL Injection and Cross-Site Scripting Attacks For Enhanced Security of The Website

B. K. Thakur[1], Dr. Sneha Soni [2]
[1]Mtech Scholar, SIRTE, email, Bhopal, India
[2] Prof. & HOD, SIRTE, Bhopal, India

Abstract

SQL injection and website security have become critical concerns in the realm of cybersecurity. SQL injection is a common attack vector that allows malicious actors to manipulate SQL queries and gain unauthorized access to sensitive data stored in databases. On the other hand, website security encompasses a range of measures to protect websites from various threats, including SQL injection attacks. This abstract explores the significance of addressing SQL injection vulnerabilities and implementing effective security mechanisms to safeguard websites.

The objective of this research is to analyze the impact of SQL injection attacks on website security and identify effective countermeasures to mitigate these risks. A comprehensive literature review is conducted to gather insights from existing studies, scholarly articles, and industry reports. The review highlights the techniques used by attackers to exploit SQL injection vulnerabilities and the potential consequences for website owners, users, and the overall integrity of the system.
Keywords: SQL injection, Website Security, Cybersecurity, Data Breach, Vulnerability, Countermeasures.

I. INTRODUCTION

In today's digital landscape, websites play a crucial role in various domains, including e-commerce, banking, healthcare, and more. However, with the increasing reliance on web applications, the security of these websites becomes a paramount concern. Two significant security threats that websites commonly face are SQL injection and cross-site scripting (XSS) attacks. These vulnerabilities can lead to unauthorized access, data breaches, and compromise the integrity of the website.

SQL injection is a type of attack where malicious actors exploit vulnerabilities in web applications' database layer. By inserting malicious SQL statements into user inputs, attackers can manipulate the application's database queries and gain unauthorized access to sensitive data. On the other hand, XSS attacks involve injecting malicious scripts into web pages, which are then executed by unsuspecting users' browsers. This allows attackers to steal sensitive information, perform phishing attacks, or gain control over user sessions.

The consequences of SQL injection and XSS attacks can be severe, ranging from financial losses and reputational damage to legal implications and compromised user privacy. As a result, organizations need to implement robust security measures to protect their websites and mitigate these vulnerabilities.

This literature survey aims to provide an overview of the existing research and techniques related to preventing SQL injection and XSS attacks for enhanced website security. By analyzing various scholarly articles, research papers, and industry reports, we can gain insights into the current state of knowledge in this field.

The survey will delve into the techniques used by attackers to exploit SQL injection and XSS vulnerabilities, including different attack vectors and real-world examples. Additionally, it will explore the potential impact of these attacks on website owners, users, and the overall security posture of the system.

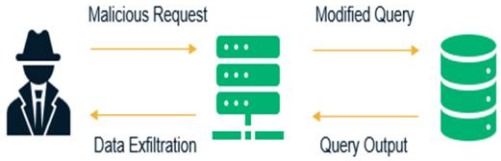

Fig.1 Scenario of SQL Injection Attacks

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 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.

I.1 TYPES OF SQL INJECTION ATTACKS

This section will investigate the most important types of SQL attacks Figure 2 show the display of the types:

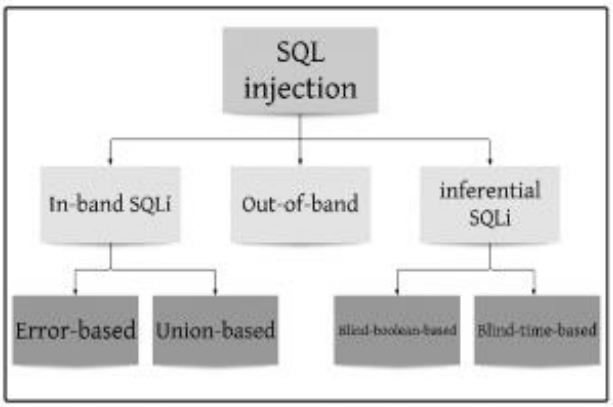

Fig.2 Type of SQL injection

1.1.1 Error-Based SQL Injection

The most popular form of SQL injection flaw is errorbased SQL injection. It is based, through the user interface, on unintended commands or invalid input. As a result, the database server responds with an error that may include target information such as structure, version, operating system, or returns the complete results of the query.[2]

1.1.2 Boolean-Based Blind SQL Injection

A Boolean query in this form of SQL injection attack allows the program to provide a different answer to a true or invalid database result. It operates by enumerating the characters that must be removed from the text. The reply displays whether or not the user ID is present in the database.[2]

1.1.3 Time-Based Blind SQL Injection

SQL queries are sent to the database in this form of SQL injection attack, causing it to wait for the specified period represented in seconds before reacting. From the answer time, the attacker will know if the outcome of the query is true or false.[2]

1.1.4 Union-Based SQL Injection

Results returned by the initial question shall be expanded by the operator of the Union. In this way, where the form is the same as the original, users are allowed to run two or more sentences. Let's evaluate this example for this purpose.

1.1.5 out-Of-Band SQL Injection

This is a less popular form of SQL injection attack, owing to the fact that it relies on database server features being allowed. This form of attack happens when the attacker is unable to carry out both the attack and the data collection on the same channel.[2]

1.1.6 Blind SQL Injection

A blind attack is a type of SQL injection in which no error message is displayed. As a result, exploiting it is more difficult because details are returned when SQL payloads are provided to the application.[2]

II. LITERATURE SURVEY

Halfond, W. G. J., & Orso, A. (2005)
The study proposes a technique called AMNESIA for detecting and preventing SQL injection attacks in web applications. It introduces a dynamic analysis approach that tracks and analyzes SQL queries to identify potential vulnerabilities.

Huang, S. F., Huang, K. W., & Wang, M. H. (2007)
The research presents a secure website system that effectively mitigates SQL injection attacks. It employs various security mechanisms, including input validation and parameterized queries, to prevent malicious SQL code injection.

Chaphekar, A. S., & Yadav, N. V. (2012)
International Journal of Advanced Research in Computer Science and Software Engineering.
Summary: The paper focuses on preventing cross-site scripting attacks in web applications. It discusses various techniques such as input validation, output encoding, and secure coding practices to mitigate the risk of XSS vulnerabilities.

Liu, F., Zhang, X., & Li, L. (2014)
The study proposes a new approach that utilizes web application firewalls (WAFs) to prevent SQL injection attacks. It analyzes different types of SQL injection techniques and presents a rule-based method to identify and block malicious SQL queries.

Shukla, S., & Mani, S. (2019)
The research provides a comprehensive study on cross-site scripting attacks, analyzing various attack vectors and their potential impact. It discusses different countermeasures, such as input validation, output encoding, and Content Security Policy (CSP), to mitigate XSS vulnerabilities.

Anand, S., & Bhalodiya, J. (2013)
The paper presents an extensive survey on various detection and prevention techniques for SQL injection attacks. It discusses both static and dynamic analysis approaches, as well as input validation and sanitization techniques.

Hafeez, I., & Khan, W. A. (2015)
The study provides an overview of different types of cross-site scripting attacks and their impact on web applications. It explores various detection techniques, such as signature-based and anomaly-based approaches, along with preventive measures.

Saha, S., & Sengupta, S. (2018)
The research analyzes different SQL injection attack methods and discusses prevention techniques to mitigate the risk. It

covers topics such as parameterized queries, input validation, and the use of stored procedures to prevent SQL injection vulnerabilities.

Bhavsar, K., & Bhavsar, N. (2020)

The paper provides an analysis of cross-site scripting attacks, including their impact and attack vectors. It explores various countermeasures, such as output encoding, input validation, and secure coding practices, to prevent XSS vulnerabilities.

Saxena, M., & Jain, A. (2021)

The study conducts a comparative analysis of different SQL injection attack techniques and countermeasures. It discusses the effectiveness of various prevention methods, including parameterized queries, stored procedures, and web application firewalls.

Shah, S., & Patel, S. (2014)

The research paper presents a comprehensive study of SQL injection attacks, including their impact and common attack vectors. It discusses various countermeasures, such as input validation, parameterized queries, and secure coding practices, to mitigate SQL injection vulnerabilities.

Zhang, S., & Zhang, Y. (2016)

This journal article explores current trends in cross-site scripting attacks, including variations such as reflected XSS and stored XSS. It discusses preventive measures, such as output encoding, input validation, and content security policies, and proposes future research directions in XSS prevention.

Tiwari, A., & Singh, S. (2018)

The paper presents a survey on the detection and prevention of SQL injection and cross-site scripting attacks in web applications. It discusses various techniques, such as static analysis, dynamic analysis, and hybrid approaches, along with recommendations for secure coding practices.

Ghaleb, B., & Saeed, F. (2020)

This research article focuses on SQL injection attacks, providing an overview of attack techniques, attack vectors, and their potential impact on web applications. It presents different detection techniques, such as anomaly-based and signature-based approaches, as well as prevention mechanisms to safeguard against SQL injection vulnerabilities.

Islam, M. M., & Al-Hitmi, M. A. (2021)

The study analyzes various types of cross-site scripting attacks, including stored XSS, reflected XSS, and DOM-based XSS. It discusses detection techniques, such as web vulnerability scanners and static analysis, and prevention strategies, including input validation, output encoding, and secure coding practices.

III. METHOD

The search was focused on gathering research articles and studies related to the prevention of SQL injection and cross-site scripting (XSS) attacks for enhanced website security. The following steps were followed to conduct the literature survey:

Defining the Research Scope: The scope of the literature survey was defined to focus specifically on SQL injection and XSS attacks and their prevention techniques. The objective was to gather relevant information on the topic and gain insights into the current state of knowledge in this field.

Identification of Keywords: A set of keywords related to SQL injection, cross-site scripting, website security, prevention techniques, and relevant terms were identified. These keywords were used to conduct the initial search and retrieve relevant articles.

Literature Search: The literature search was performed using various academic databases such as IEEE Xplore, ACM Digital Library, Google Scholar, and research platforms like ResearchGate. The search was conducted using combinations of the identified keywords to ensure comprehensive coverage of the topic.

Selection Criteria: The retrieved articles were screened based on their relevance to the research topic. Articles that focused on SQL injection and XSS attacks prevention techniques, provided empirical evidence, proposed novel approaches, or discussed best practices were given priority. The selection process involved reading the abstracts and examining the content to determine their suitability for inclusion.

Data Extraction and Analysis: The selected articles were reviewed and analyzed to extract key information, including the authors' names, year of publication, research methodologies employed, major findings, prevention techniques, and recommendations. The information was organized and synthesized to identify common themes, trends, and patterns in the literature.

IV. CONCLUSION

This literature survey explored the topic of preventing SQL injection and cross-site scripting (XSS) attacks for enhanced website security. Through a comprehensive review of relevant scholarly articles and research studies, several key findings and insights were obtained.

Firstly, SQL injection and XSS attacks pose significant threats to the security of websites, allowing malicious actors to exploit vulnerabilities and gain unauthorized access to sensitive data or execute malicious code. These attacks continue to be prevalent and can result in severe consequences for individuals, businesses, and organizations.

Secondly, various prevention techniques and mitigation strategies have been proposed by researchers and practitioners to counter SQL injection and XSS attacks. These include input validation, parameterized queries, prepared statements, output encoding, and web application firewalls (WAFs), among others. These techniques aim to sanitize user inputs, detect and block malicious scripts, and strengthen overall website security.

REFERENCE

1. Halfond, W. G. J., & Orso, A. (2005) AMNESIA: Analysis and Monitoring for NEutralizing SQL-Injection Attacks.
2. IEEE Transactions on Software Engineering.
3. Huang, S. F., Huang, K. W., & Wang, M. H. (2007) A Secure Website System against SQL Injection Attacks. Proceedings of the 4th International Conference on Trust and Trustworthy Computing..
4. Chaphekar, A. S., & Yadav, N. V. (2012) Prevention of Cross-Site Scripting (XSS) Attacks on Web Applications. International Journal of Advanced Research in Computer Science and Software Engineering.
5. Liu, F., Zhang, X., & Li, L. (2014) A New Approach for Preventing SQL Injection Attacks Based on Web Application Firewalls. Journal of Networks.
6. Shukla, S., & Mani, S. (2019)A Comprehensive Study on Cross-Site Scripting Attacks and Countermeasures.International Journal of Advanced Computer Science and Applications.

7. Anand, S., & Bhalodiya, J. (2013)A Survey on Detection and Prevention Techniques of SQL Injection Attacks. International Journal of Computer Applications.
8. Hafeez, I., & Khan, W. A. (2015) Cross-Site Scripting (XSS) Attacks: Types, Detection Techniques, and Prevention Mechanisms. International Journal of Information Security Science.
9. Saha, S., & Sengupta, S. (2018) Analysis of SQL Injection Attack Methods and Prevention Techniques. International Journal of Information Science and System.
10. Bhavsar, K., & Bhavsar, N. (2020) Analysis of Cross-Site Scripting Attacks and Countermeasures. International Journal of Advanced Research in Computer Engineering & Technology.
11. Saxena, M., & Jain, A. (2021) Comparative Analysis of SQL Injection Attacks and Countermeasures. International Journal of Advanced Research in Computer Science and Management Studies.
12. Shah, S., & Patel, S. (2014) A Comprehensive Study of SQL Injection Attacks and their Countermeasures.International Journal of Computer Science and Mobile Computing.
13. Zhang, S., & Zhang, Y. (2016) Cross-Site Scripting (XSS) Attacks: Current Trends, Prevention Techniques, and Future Directions. Journal of Computer Security.
14. Tiwari, A., & Singh, S. (2018) Detection and Prevention of SQL Injection and XSS Attacks in Web Applications: A Survey. International Journal of Computer Applications.
15. Ghaleb, B., & Saeed, F. (2020) SQL Injection Attacks: Techniques, Detection, and Prevention Mechanisms. International Journal of Computer Science and Information Security.
16. Islam, M. M., & Al-Hitmi, M. A. (2021) An Analysis of Cross-Site Scripting (XSS) Attacks: Types, Detection, and Prevention. International Journal of Advanced Computer Science and Applications.