SQL Injection and its Prevention

Diana Jean Tuquib
(tuqu0002@algonquinlive.com)

Zixuan Lou
(lou00019@algonquinlive.com)

Soha Alsafadi
(alsa0231@algonquinlive.com)

Wai Chun (Daniel) Kwan
(kwan0042@algonquinlive.com)

Table of Contents

Introduction

Topic Description

SQL Injection is a cyber attack that targets web applications that rely on SQL databases. This attack involves inserting malicious code into a SQL statement [1]through an input field on a website. The goal of the attacker is to manipulate or access sensitive data that the application has access to. SQL Injection attacks can have severe consequences, from data breaches and loss of sensitive information to complete system compromise.

Preventing SQL Injection attacks is crucial for any web application that uses SQL databases for data storage. This involves implementing security measures such as input validation and parameterized queries to ensure that all user input is properly sanitized and validated before being passed to the SQL engine. Regular security audits and vulnerability assessments should also be conducted to identify and mitigate any potential weaknesses in the application's security defences.

Our report will provide a comprehensive overview of SQL Injection attacks and their potential impact. We will also discuss various techniques and best practices for preventing and mitigating these types of attacks. We will explore some of the common tools and techniques used by attackers and provide practical examples and code snippets to help developers better understand and implement effective SQL Injection prevention strategies. By following these best practices, web application developers can protect their users' sensitive data from SQL Injection attacks.

Reason for Choosing SQL Injection and its Prevention

We have chosen "SQL Injection and its Prevention" as the topic of this project because SQL Injection attacks are a prevalent type of cyber attack that can have severe consequences for individuals and organizations. As more and more applications rely on SQL databases for data storage, the risk of SQL Injection attacks has grown.

Therefore, it is important for developers to understand the risks associated with SQL Injection attacks and know how to prevent them. By educating ourselves on SQL Injection attacks and their prevention, we can better secure our web applications and protect our users' sensitive information.

Furthermore, understanding SQL Injection attacks and their prevention is essential for anyone interested in cybersecurity or web application development. It is a fundamental component of secure coding practices, and knowledge of SQL Injection attacks and prevention techniques can help developers build more secure applications.

Overall, the topic of SQL Injection attacks and prevention is both important and relevant in today's technology landscape, making it an excellent choice for this project.

Problem Description

Who: Who cares and who does it affect

With the digital world getting bigger each day and more people using the internet, more people are at risk of cyber-attacks. SQL Injection concerns everyone who uses any web or mobile application that involves databases, including users, web developers, database administrators, and other stakeholders. Targets of these attacks include financial institutions, database content management systems, e-commerce platforms, and many more.

What: What is it

SQL Injection is a cyber-attack that exploits vulnerabilities in the input fields of applications. Attackers inject SQL statements to view, create, delete, or modify databases. After a successful attack, they can have access to confidential and sensitive information and use it for other purposes other than its intended use.

Where: Where the problem is—client- or server-side

SQL Injection typically occurs on the server-side of the web or mobile applications. It arises due to inadequate or lack of input validation and sanitation and due to insecure coding practices. [2]

When: Timing aspects

Injection attacks can happen any time an application is insecure. Attackers attempt to exploit insecure applications. A lot of SQL injection attacks increase when there is a known vulnerability or data breach.

Attackers get smarter and their techniques become more sophisticated. Nowadays, they can create bots that automatically attack each time there is an open window of vulnerability. [3]

Why: Laws, regulations, other constraints

SQL injections present significant legal and compliance risks. Organizations who do not secure their applications properly may face major consequences. It usually results in financial losses, legal issues, and damage to their reputation.

The government of Canada has provided a guideline on things to consider for websites. It includes information on how to prevent SQL Injection attacks. [4]

How: How issues happen and get solved

SQL Injection occurs when the application is insecure and fails to properly validate user inputs. Attackers exploit this vulnerability by injecting malicious SQL codes into the input field. Developers should adhere to industry-standard coding practices to prevent this attack and implement secure input fields. [4]

The Canadian Centre for Cyber Security recommends input validation in the areas of the application, including user browser, web application firewall, web server, application business logic, and database. [4]

Solution Description and Results

We will create two basic web applications highlighting the difference between a secure and insecure application. One website will not have input validation and other will make use of one SQL prevention technique. During our presentation, we will demonstrate how an insecure web application can damage a database and how a secure web application can prevent it.

Work Plan

Our tentative work plan for the final report and presentation includes the following component and deliverables:

Component/Deliverable	**Hours per Person**	**Group Member**
Presentation slides	TBD	Diana
Presentation script	TBD	Diana & Daniel
Introduction	TBD	Daniel
Problem Description	TBD	Zixuan
Solution Description	TBD	Soha
Demo	TBD	Daniel
Conclusion	TBD	Diana
Insecure website	TBD	Zixuan
Secure website	TBD	Soha
Database	TBD	Zixuan and Soha
References	TBD	Zixuan
Lessons learned	TBD	Soha
Proofreading	TBD	Diana

Note: The hours per person will still be determined due to potential scheduling changes after the reading week.

References

[1] OWASP, "SQL Injection Prevention Cheat Sheet," [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html. [Accessed 23 June 2023].

[2] S. Srivastava, "A Survey On: Attacks due to SQL injection and their prevention method for web application," *IJCSIT International Journal of Computer Science and IT*, vol. 3, no. 1, 2012.

[3] V. Sundar, "Prevention against Bot-Driven SQL Injection Attacks," Express Computer, 6 December 2022. [Online]. Available: https://www.expresscomputer.in/guest-blogs/prevention-against-bot-driven-sql-injection-attacks/92517/. [Accessed 23 June 2023].

[4] Canadian Centre for Cyber Security, "Security considerations for your website (ITSM.60.005)," 6 October 2021. [Online]. Available: https://www.cyber.gc.ca/en/guidance/security-considerations-your-website-itsm60005. [Accessed 23 June 2023].

[5] Imperva, "SQL Injection Prevention," [Online]. Available: https://www.imperva.com/learn/application-security/sql-injection-prevention. [Accessed 23 June 2023].

[6] Varonis, "SQL Injection: A beginner's guide to understanding and prevention," [Online]. Available: https://www.varonis.com/blog/sql-injection-prevention/. [Accessed 23 June 2023].

[7] Acunetix, "SQL Injection Prevention Techniques," [Online]. Available: https://www.acunetix.com/websitesecurity/sql-injection-prevention-techniques/. [Accessed 23 June 2023].