SQL Injection and its Prevention

**Diana Jean** **Tuquib**

([tuqu0002@algonquinlive.com](mailto:tuqu0002@algonquinlive.com))

**Zixuan Lou**

([lou00019@algonquinlive.com](mailto:lou00019@algonquinlive.com))

**Soha Alsafadi**

([alsa0231@algonquinlive.com](mailto:alsa0231@algonquinlive.com))

**Wai Chun (Daniel) Kwan**

([kwan0042@algonquinlive.com](mailto:kwan0042@algonquinlive.com))

**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 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.

**The reason we chose this topic**

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.

We propose to outline our discussion as follows:

1. SQL Injection Introduction
   1. Definition
   2. Importance of Awareness
2. How it Works
   1. SQL Queries Overview
   2. Different SQL Injection Techniques
   3. Example of Scripts Used in SQL Attacks
3. Risks and Consequences
   1. Access to Private/Confidential Data
   2. Data Breach
   3. Real-life Example
4. Prevention
   1. Validation
   2. Access Control and User Privileges
   3. Firewall
   4. Regular Screening and Testing
   5. Regular Updating of Software and Framework
   6. Following Industry-Standard Practices
   7. User and Developer Training
5. Conclusion
   1. Recap of Definition
   2. Recap of How it Works
   3. Recap of Risks and Consequences
   4. Summary of Prevention Techniques

We will divide the tasks as follows:

|  |  |
| --- | --- |
| **Name** | **Topic** |
| Diana Jean Tuquib | Introduction Conclusion |
| Zixuan Lou | How it Works |
| Soha Alsafadi | Risks and Consequences |
| Wai Chun Kwan (Daniel) | Prevention |

**Reference:**

1. OWASP. "SQL Injection Prevention Cheat Sheet." OWASP Cheat Sheet Series. Accessed May 23, 2023. <https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html>.
2. Imperva. "SQL Injection Prevention." Accessed May 23, 2023. https://www.imperva.com/learn/application-security/sql-injection-prevention/.
3. Varonis. "SQL Injection: A Beginner’s Guide to Understanding and Prevention." Accessed May 23, 2023. https://www.varonis.com/blog/sql-injection-prevention/.
4. Acunetix. "SQL Injection Prevention Techniques." Accessed May 23, 2023. https://www.acunetix.com/websitesecurity/sql-injection-prevention-techniques/.