# Chapter 4. DATABASE ATTACKS AND SECURITY

- MySQL
  - A popular and open database management system.
  - Use SQL query language to perform operations.
- Oracle Database
  - Powerful database management systems are often used for large enterprise applications.
  - Supports many advanced features and technologies.

- Microsoft SQL Server
  - Developed by Microsoft, suitable for Windows environment.
  - Supports tight integration with other Microsoft products.
- PostgreSQL
  - A powerful open source database management system with advanced features.
  - Multi-user support and good scalability.

- MongoDB
  - A database management system that uses no structure (NoSQL) primarily for JSON-like data.
  - Suitable for applications that require flexibility with irregular data.
- SQLite
  - A database management system that is lightweight, embedded and requires no server.
  - Popular in mobile and embedded apps.

# 4.2. Common Types of Database Attacks

- SQL Injection: Attack technique where attackers insert malicious SQL code snippets into SQL queries being processed by the database.
- Cross-Site Scripting (XSS): An attack where an attacker injects malicious JavaScript code into a website or app, which can affect users when they visit that page.
- Brute Force Attacks: An attack where an attacker tries to log in by repeatedly trying different combinations of username and password to infiltrate the system.

- Denial of Service (DoS) and Distributed Denial of Service (DDoS)
  - Denial of Service (DoS) và Distributed Denial of Service (DDoS): The attack aims to make the database service unavailable by overloading the system or network.
  - Phishing Attacks: Phishing techniques where attackers spoof trusted websites or apps to collect credentials from users.
  - Privilege Escalation: Attacks where the attacker tries to elevate his privileges in the database system to gain greater access and control.

- Data Exfiltration
  - Data Exfiltration: The act of taking unauthorized data from the database and transferring it out of the system without permission.
  - Man-in-the-Middle (MitM): The attack technique is when an attacker places himself between two sides of communication to monitor and even modify the transmitted data.
  - Buffer Overflow Attacks: An attack technique in which an attacker tries to insert malicious code into the memory allocated to an application, usually results in control of a server or system.

- Union-Based SQL Injection
  - Union-Based SQL Injection: An attacker injects a SQL UNION statement to combine the result of the current query with the result of another query. This helps them gather information from different tables in the database.
  - Time-Based Blind SQL Injection: An attacker inserts an SQL statement that creates a delay in the query. By examining the response time from the database, they can determine if their condition is true.
  - Error-Based SQL Injection: An attacker takes advantage of an error that appears when executing invalid SQL queries. Through these errors, they can gather information about the structure of the database.

- UNION-SELECT Payloads
  - UNION-SELECT Payloads: Attackers use UNION-SELECT strings to bind queries and collect data from different tables.
  - Boolean-Based Blind SQL Injection: An attacker inserts Boolean conditions into SQL statements to check whether the conditions are true or false, thereby inferring information.
  - Out-of-Band SQL Injection: Attackers take advantage of techniques that send information over different channels in addition to the usual one, such as DNS or HTTP requests.

- Second-Order SQL Injection
  - Second-Order SQL Injection: This type of attack occurs when data is inserted into a database, which is then used in another query that is not handled properly.
  - Time-Based Blind SQL Injection Using Conditional Responses: An attacker uses latency and conditions to determine the correct value of a query.

# 4.4. SQL Injection Attack Tool

- SQLMap
- Havij
- SQLNinja
- BSQL Hacker
- NoSQLMap
- Sqlninja
- Automated SQL Injection Tool (A-SQL)
- BBSQL

- SQLMap
  - SQLMap: The tool automates SQL Injection attacks, supports many mining techniques and provides automatic detection capabilities.
  - Havij: An easy-to-use SQL Injection attack tool with a graphical user interface.
  - SQLNinja: Powerful tool for security testers, supporting multiple attack techniques.

- BSQL Hacker
  - BSQL Hacker: Versatile tool for database security testing, supporting many types of SQL Injection attacks.
  - NoSQLMap: Similar to SQLMap, but specifically designed to attack NoSQL databases.
  - Sqlninja: Professional SQL Injection attack tool, supports many types of attacks and has the ability to extract data.

- Automated SQL Injection Tool (A-SQL)
  - Automated SQL Injection Tool (A-SQL): Tool for beginners, automating SQL Injection attack steps.
  - BBSQL: Open-source, easy-to-use SQL Injection attack tool with a graphical interface.

# 4.5. Preventive measures

- Use Secure Coding Practices
- Input Validation and Sanitization
- Use a secure database manipulation library
- Least Privilege Principle
- Access Control
- Firewall và Web Application Firewall (WAF)
- Logging and Monitoring
- System and Application Updates

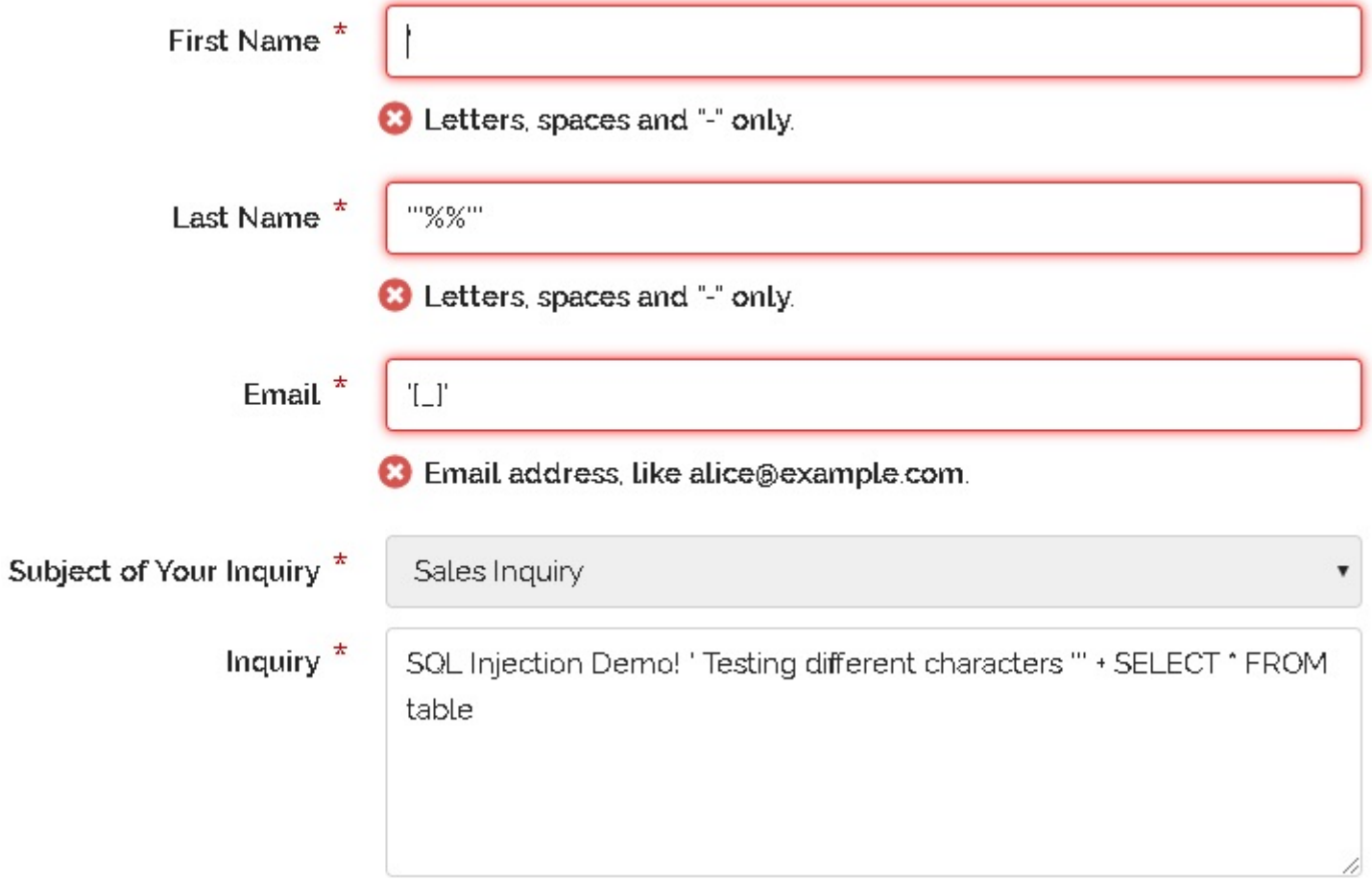
- Use Secure Coding Practices
  - Use Secure Coding Practices: Application development with the use of safe programming procedures, such as the use of parameterized execution statements, avoids the use of query strings built from user data that are not processed.
  - Input Validation and Sanitization: Check and handle user input carefully. Filter and remove special characters that can be used in SQL Injection attacks.
  - Use a secure database manipulation library: Using secure database manipulation libraries or frameworks, they can automatically protect against types of attacks such as SQL Injection.

- Least Privilege Principle
  - Least Privilege Principle: Assign database access permissions with a mini-archetype principle, which means providing only the necessary permissions to the user or application. Avoid over-assigning permissions.
  - Access Control: Use access controls to ensure that only users with the necessary permissions can access and execute queries on the database.
  - Firewall và Web Application Firewall (WAF): Use firewalls and WAFs to filter and block malicious queries before they reach the database.

- Logging and Monitoring
  - Logging and Monitoring: Set up a logging system to monitor database access activities and monitor manifestations of various types of SQL Injection attacks.
  - System and Application Updates: Always keep your system and applications up to date with the latest version to protect against known security vulnerabilities.

# 4.6. Look for websites with SQL Injection errors

- Search for websites with SQL Injection errors



# 4.7. Exploit SQL Injection error detection tools

- Sqlmap
  - sqlmap is a popular open-source SQL injection detection tool that is widely used by security professionals and penetration testers. It can detect and exploit SQL injection vulnerabilities in databases and web applications. sqlmap has a powerful detection engine that can automatically detect and exploit SQL injection vulnerabilities. It can also perform various tests, such as fingerprinting the database management system, retrieving data from the database, and executing arbitrary commands.

# 4.7. Exploit SQL Injection error detection tools

- Pros of using sqlmap:
  - Open-source and free to use
  - Can detect and exploit SQL injection vulnerabilities automatically
  - Supports various database management systems and web applications
  - Can perform a wide range of tests
- Cons of using sqlmap:
  - Steep learning curve
  - Can generate false positives
  - Can be blocked by web application firewalls

- Invicti
  - Invicti is a cloud-based application security platform that provides comprehensive web application security testing, including SQL injection detection. It uses a combination of manual testing and automated scanning to detect SQL injection vulnerabilities. Invicti has a user-friendly interface allows security professionals and developers to manage and track vulnerabilities easily. It also provides detailed reports and remediation advice to help fix vulnerabilities.

.

# 4.7. Exploit SQL Injection error detection tools

- Pros of using Invicti:
  - User-friendly interface
  - Comprehensive web application security testing
  - Detailed reports and remediation advice
  - Cloud-based platform
- Cons of using Invicti:
  - Expensive compared to other SQL injection detection tools
  - Limited customization options

- Burp Scanner
  - Burp Scanner is a web application security testing tool that includes SQL injection detection capabilities. It can detect various SQL injection vulnerabilities, including blind and time-based SQL injection. Burp Scanner has a comprehensive database of attack payloads that can be used to test for SQL injection vulnerabilities. It also has a user-friendly interface that allows users to manage and track vulnerabilities.

# 4.7. Exploit SQL Injection error detection tools

- Pros of using Burp Scanner:
  - A comprehensive database of attack payloads
  - User-friendly interface
  - Can detect various types of SQL injection vulnerabilities
- Cons of using Burp Scanner:
  - Expensive compared to other SQL injection detection tools
  - Requires a good understanding of web application security testing

- jSQL Injection
  - jSQL Injection is a lightweight and easy-to-use SQL injection detection tool that is suitable for beginners. It can detect various types of SQL injection vulnerabilities, including error-based, time-based, and blind SQL injection. jSQL Injection has a user-friendly interface that allows users to scan web applications for vulnerabilities easily. It also provides detailed reports and suggestions for remediation.

# 4.7. Exploit SQL Injection error detection tools

- Pros of using jSQL Injection:
  - Lightweight and easy-to-use
  - Can detect various types of SQL injection vulnerabilities
  - User-friendly interface
  - Provides detailed reports and remediation suggestions
- Cons of using jSQL Injection:
  - Limited customization options
  - Not suitable for advanced security testing

- AppSpider
  - AppSpider is a comprehensive web application security testing tool that includes SQL injection detection capabilities. It can detect various SQL injection vulnerabilities, including blind SQL injection. AppSpider has a user-friendly interface that allows users to manage and track vulnerabilities. It also provides detailed reports and suggestions for remediation.

# 4.7. Exploit SQL Injection error detection tools

- Pros of using AppSpider:
  - Comprehensive web application security testing
  - Can detect various types of SQL injection vulnerabilities
  - User-friendly interface
  - Provides detailed reports and remediation suggestions
- Cons of using AppSpider:
  - Expensive compared to other SQL injection detection tools
  - Requires a good understanding of web application security testing

- Acunetix
  - Acunetix is a comprehensive web application security testing tool that includes SQL injection detection capabilities. It can detect various SQL injection vulnerabilities, including blind SQL injection. Acunetix has a user-friendly interface that allows users to manage and track vulnerabilities. It also provides detailed reports and suggestions for remediation.

# 4.7. Exploit SQL Injection error detection tools

- Pros of using Acunetix:
  - Comprehensive web application security testing
  - Can detect various types of SQL injection vulnerabilities
  - User-friendly interface
  - Provides detailed reports and remediation suggestions
- Cons of using Acunetix:
  - Expensive compared to other SQL injection detection tools
  - Requires a good understanding of web application security testing

- SQL Injection Vulnerability Identification
  - SQL Injection Vulnerability Identification: Find and identify weaknesses in web applications that can be attacked by SQL Injection.
  - Check the database version: Identify the specific version of the database management system (e.g. MySQL, SQL Server, PostgreSQL) to prepare for appropriate attacks.
  - Execute the SQL Injection statement: Insert SQL Injection statements into the input cells of the application to see if data can be accessed and extracted from the database.

- Perform attack techniques
  - Perform attack techniques: Use techniques such as Union-Based SQL Injection, Time-Based Blind SQL Injection, Error-Based SQL Injection to extract data from databases.
  - Information Collection and System Control: Gather information about database structures, tables, and try to control the system through SQL Injection attacks.

- Take measures to prevent SQL Injection

# Enjoy the Course…!