

# **DB Connectivity Web Technology**



# Where Are We

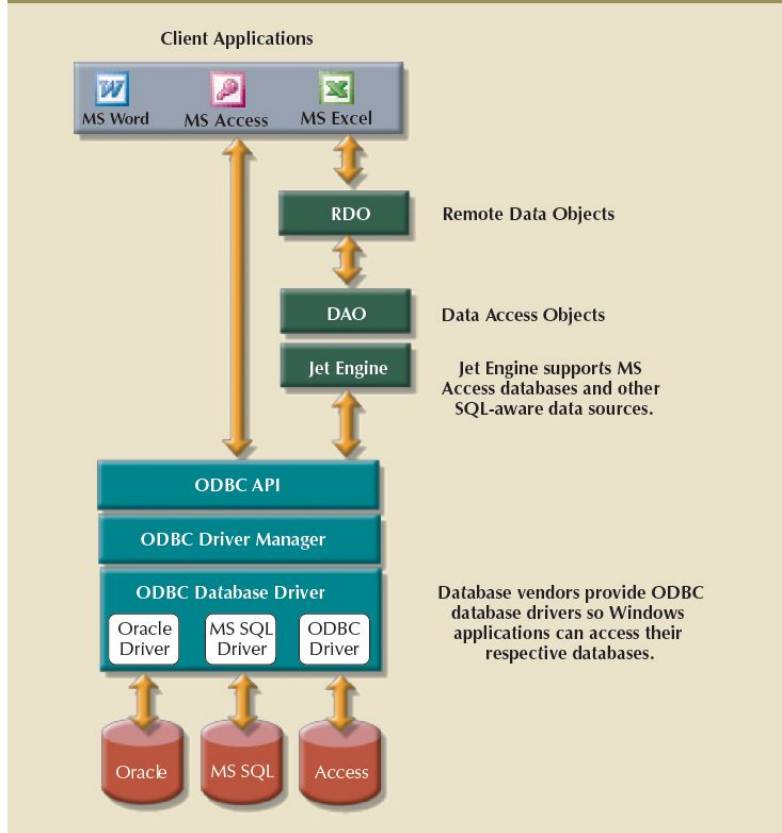
- Through this unit we have looked at:
  - The fundamental principles on which relational databases are built
  - Designing a relational database and
  - Implementing a relational database and manipulating its data via SQL
- In practice the database you create & populate will be used by *normal users* not database professionals
  - set of tables/views created under one account
  - control access to this accounts objects

# Database connectivity

# Database Connectivity

- The DATA LAYER – your data management application (DBMS)
- The DATABASE MIDDLEWARE – manages connectivity and data transformation issues. Many options available such as:
  - Native SQL Connectivity
    - Vendor provided eg. Oracle SQL\*Net
  - Microsoft ODBC, DAO, RDO; OLE-DB and ADO.NET
  - Java Database Connectivity (JDBC)
- The APPLICATION – the external interface, mostly in the form of an Application Programming Interface (API)

FIGURE 15.2 USING ODBC, DAO, AND RDO TO ACCESS DATABASES



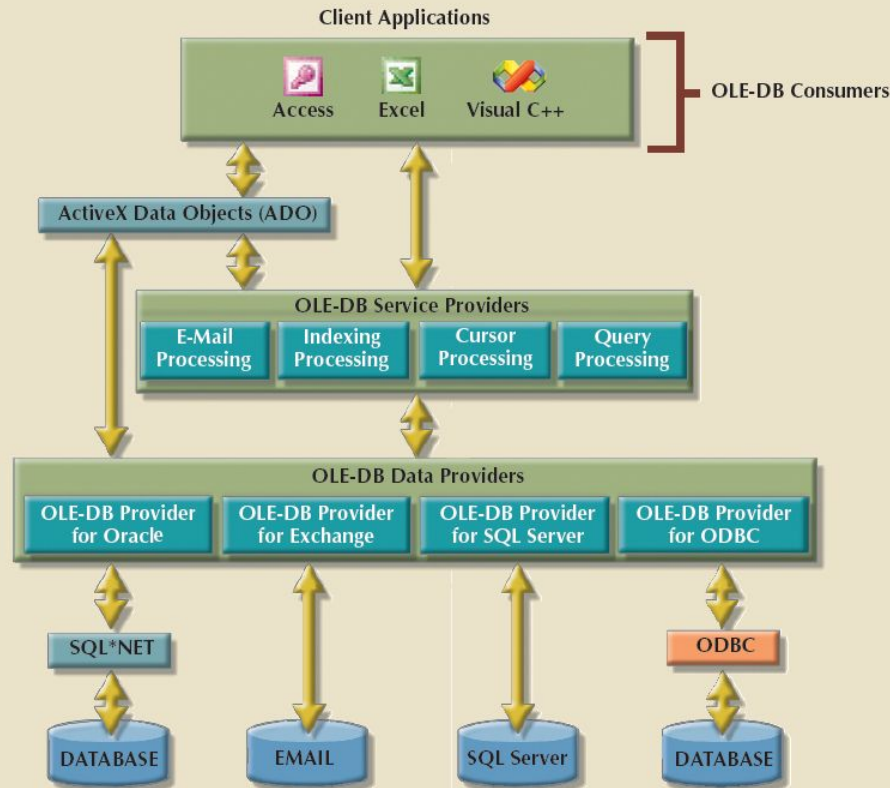
Coronel & Morris  
Fig 15.2 Ed 13



*iODBC.org*

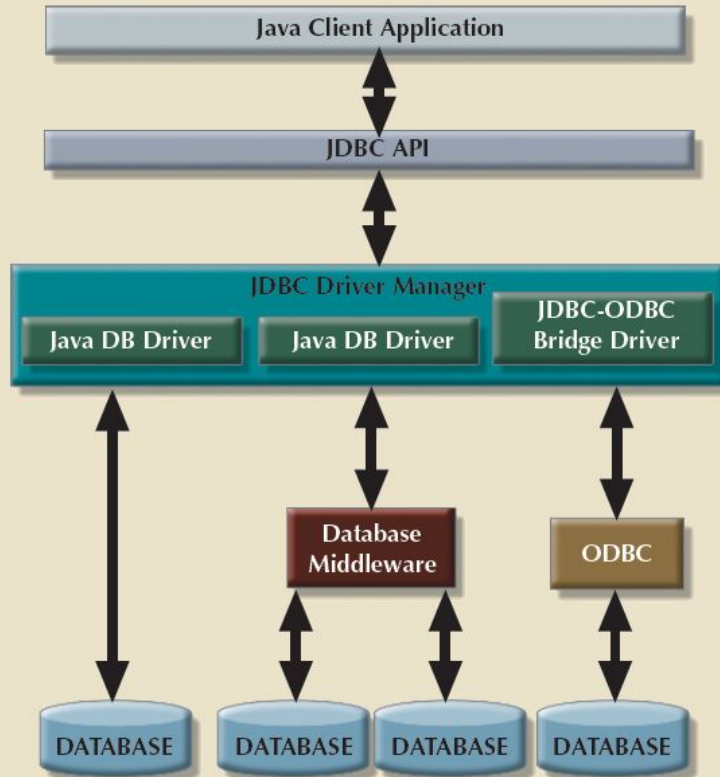
Independent Open DataBase Connectivity for Linux, MacOS X and Unix systems

FIGURE 15.5 OLE-DB ARCHITECTURE



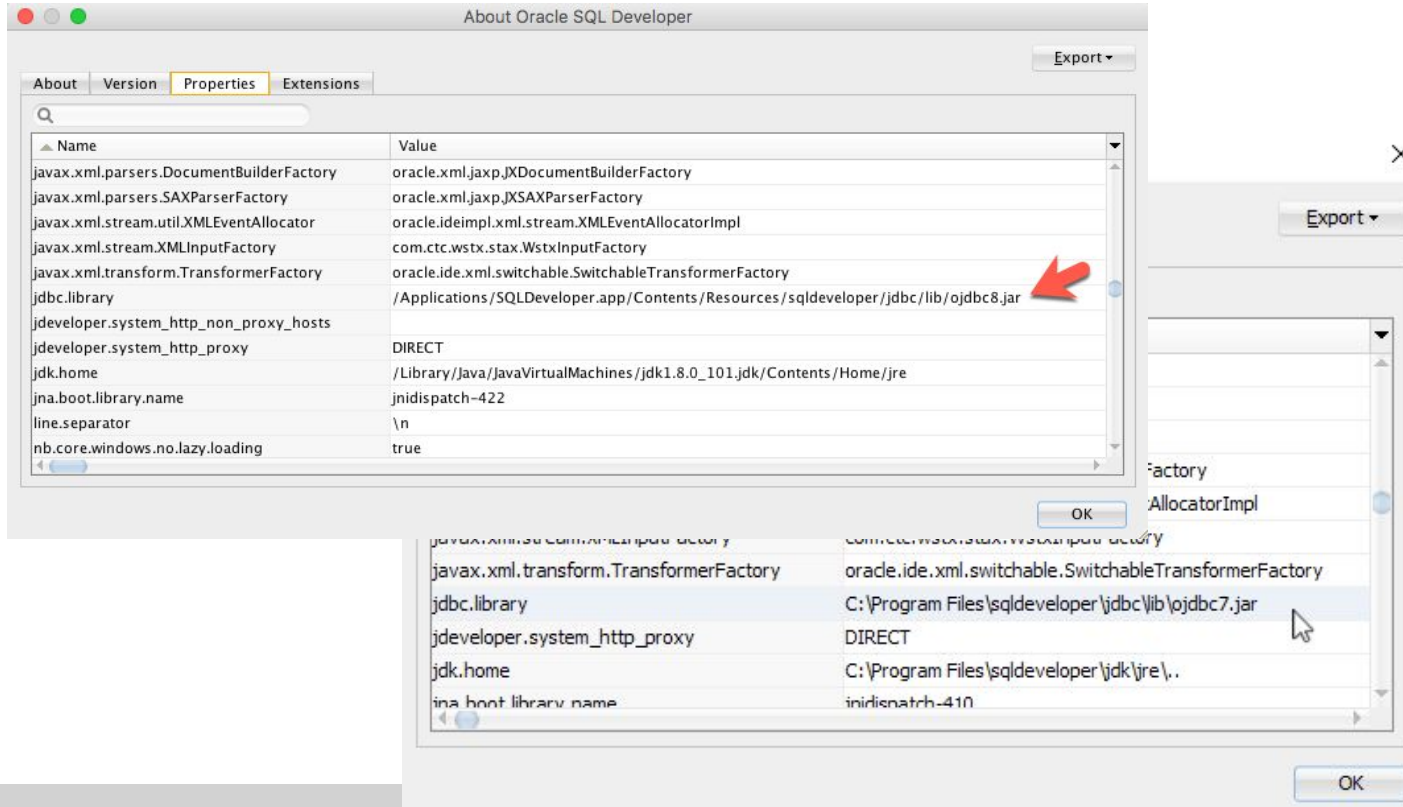
Coronel & Morris  
Fig 15.5 Ed 13

FIGURE 15.7 JDBC ARCHITECTURE



Coronel & Morris  
Fig 15.7 Ed 13

# SQLDeveloper - JDBC





# Sample JDBC code snippet

```
public static void viewTable(Connection con, String dbName)
    throws SQLException {

    Statement stmt = null;
    String query = "select COF_NAME, SUP_ID, PRICE, " +
        "SALES, TOTAL " +
        "from " + dbName + ".COFFEES";

    try {
        stmt = con.createStatement();
        ResultSet rs = stmt.executeQuery(query);
        while (rs.next()) {
            String coffeeName = rs.getString("COF_NAME");
            int supplierID = rs.getInt("SUP_ID");
            float price = rs.getFloat("PRICE");
            int sales = rs.getInt("SALES");
            int total = rs.getInt("TOTAL");
            System.out.println(coffeeName + "\t" + supplierID +
                "\t" + price + "\t" + sales +
                "\t" + total);
        }
    } catch (SQLException e) {
        JBDBCTutorialUtilities.printSQLException(e);
    } finally {
        if (stmt != null) { stmt.close(); }
    }
}
```

Oracle JDBC Tutorial  
<https://goo.gl/p1bl2b>

Oracle Python Tutorial  
<https://goo.gl/8l8R>

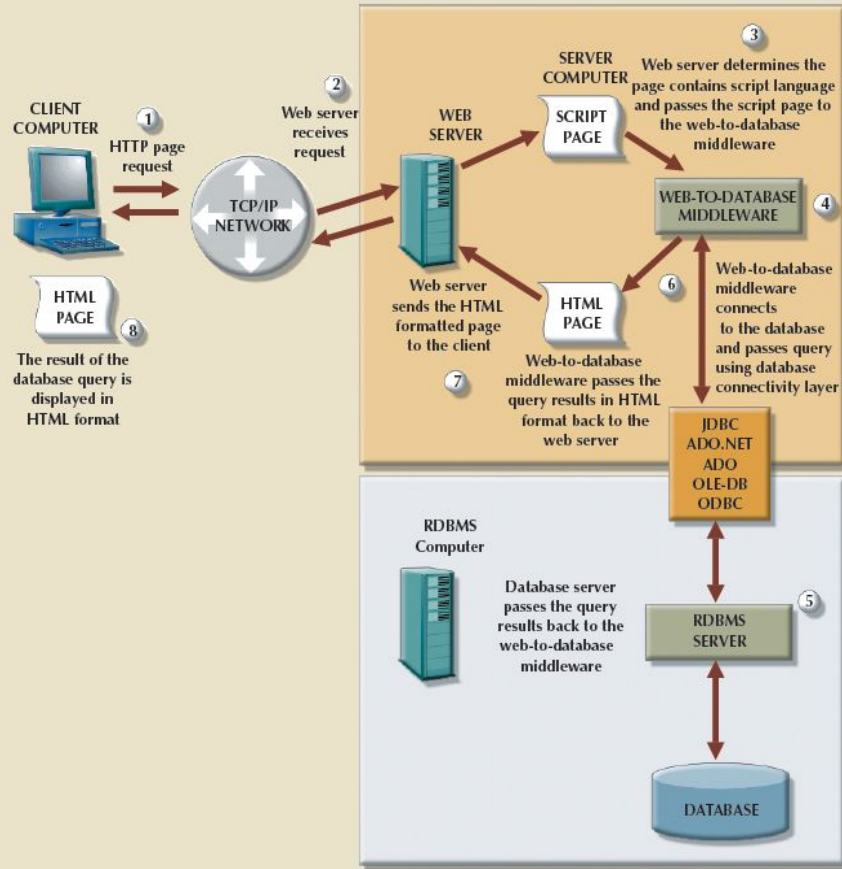
# Placing application logic in the backend

- In this approach we code database objects which "black box" the logic and store them in the database
- Procedures and Packages
  - written using PL/SQL a mixture of a procedural language and SQL
  - called by invoking package name and handing parameters
  - add\_booking (.....)

```
173 -- Procedure to add a new booking for a tour
174 PROCEDURE add_booking
175 (
176     arg_cust_no      IN book.cust_no%type,
177     arg_tour_no      IN book.tour_no%type,
178     arg_book_no_adults IN book.book_no_adults%type,
179     arg_book_no_children IN book.book_no_children%type,
180     arg_booking_success OUT CHAR
181 )
182 AS
183
184     no_participants EXCEPTION;
185     already_booked   EXCEPTION;
186     tour_expired     EXCEPTION;
187     tour_no_space    EXCEPTION;
188
189     tourdatepart      DATE;
190     tourmaxpartic     NUMBER;
191     totalchildren     NUMBER;
192     totaladults       NUMBER;
193     tourchildcost     NUMBER;
194     touradultcost     NUMBER;
195     tourbookcost      NUMBER;
196
197 BEGIN
198     arg_booking_success := '';
199
200     -- Check that some participants have been handed in for this booking
201     IF (arg_book_no_adults = 0) AND ( arg_book_no_children = 0) THEN
202         raise no_participants;
203     END IF;
204
205     -- Check customer, tour and booking validity
206
207     -- check_cust and tour are valid;
208     IF NOT valid_customer (arg_cust_no) THEN
209         raise invalid_customer;
```

# Database connectivity - web technology

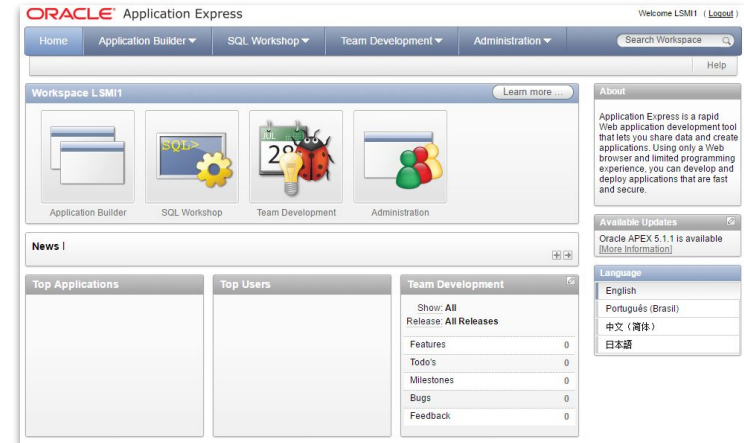
FIGURE 15.8 WEB-TO-DATABASE MIDDLEWARE



Coronel & Morris  
Fig 15.8 Ed 13

# Web Database Development

- Creating web pages which access data in a database. Many options available, including
  - ColdFusion Uses CFML - <https://goo.gl/7FnYgi> or <http://openbd.org/>
  - PHP - <http://php.net/>
  - Oracle Application Express (Apex)



# TIOBE Index for May 2020

May 2020	May 2019	Change	Programming Language	Ratings	Change
1	2	⬆	C	17.07%	+2.82%
2	1	⬇	Java	16.28%	+0.28%
3	4	⬆	Python	9.12%	+1.29%
4	3	⬇	C++	6.13%	-1.97%
5	6	⬆	C#	4.29%	+0.30%
6	5	⬇	Visual Basic	4.18%	-1.01%
7	7		JavaScript	2.68%	-0.01%
8	9	⬆	PHP	2.49%	-0.00%
9	8	⬇	SQL	2.09%	-0.47%
10	21	⬆	R	1.85%	+0.90%
11	18	⬆	Swift	1.79%	+0.64%
12	19	⬆	Go	1.27%	+0.15%
13	14	⬆	MATLAB	1.17%	-0.20%
14	10	⬇	Assembly language	1.12%	-0.69%
15	15		Ruby	1.02%	-0.32%
16	20	⬆	PL/SQL	0.99%	-0.03%
17	16	⬇	Classic Visual Basic	0.89%	-0.43%

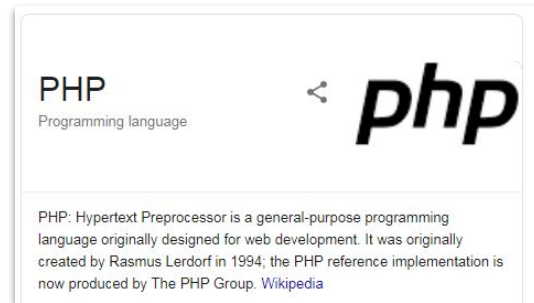
<https://www.tiobe.com/tiobe-index/>



# PHP Basic

# PHP Basic Case Study

- PHP language - server-side
  - ‘PHP-enabled web pages’ - <https://www.php.net/manual/en/tutorial.php>
  - Commonly used in combination / part of frameworks (more later)
- PHP software needs to be alongside web server software
  - e.g. besides Apache in LAMP stacks [https://en.wikipedia.org/wiki/LAMP\\_\(software\\_bundle\)](https://en.wikipedia.org/wiki/LAMP_(software_bundle));
  - or PHP on IIS <https://php.iis.net/>
- **Further reading on PHP - “What can PHP do?”**
  - <https://www.php.net/manual/en/intro-whatcando.php>





# PHP Basic Case Study

- Quick synopsis
  - When a PHP page is accessed, PHP interpreter living in the server produces output, which is served to the user (commonly interpreted in the user's browser as HTML). Users don't see the raw PHP code.
- “... when PHP is installed, the web server is configured to expect certain file extensions to contain PHP language statements. ... **When the web server gets a request for a file with the designated extension, it sends the HTML statements as is, but PHP statements are processed by the PHP software before they're sent to the requester...** When PHP language statements are processed, **only the output, or anything printed to the screen is sent by the web server to the web browser.**”
  - Source: Suehring & Valade. Read the full article:  
<https://www.dummies.com/programming/php/how-php-works/>



# Example: Web Server and PHP

PHP Version 5.4.16



System	Linux [REDACTED] 3.10.0-862.el7.x86_64 #1 SMP Wed Mar 21 18:14:51 EDT 2018 x86_64
Build Date	Jan 23 2018 07:27:50
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d

## oci8

OCI8 Support	enabled
OCI8 DTrace Support	disabled
OCI8 Version	2.0.12
Revision	\$Id: 020312b6429ebb9d6272ac9bc28f6dce529434b6 \$
Oracle Run-time Client Library Version	12.1.0.2.0
Oracle Compile-time Instant Client Version	12.1

Directive	Local Value	Master Value
oci8.connection_class	no value	no value
oci8.default_prefetch	100	100
oci8.events	Off	Off
oci8.max_persistent	-1	-1
oci8.old_oci_close_semantics	Off	Off
oci8.persistent_timeout	-1	-1
oci8.ping_interval	60	60
oci8.privileged_connect	Off	Off
oci8.statement_cache_size	20	20



# PHP Database Access

- PHP interacts with Oracle.
- Interaction via Oracle OCI 8 functions
  - Recommended reading: <https://php.net/manual/en/book.oci8.php>
  - Other RDBMS examples: PHP interacts with MySQL/MariaDB with **mysql\_connect()**  
[https://www.tutorialspoint.com/mariadb/mariadb\\_connection.htm](https://www.tutorialspoint.com/mariadb/mariadb_connection.htm)
- Definition: “**OCI8 is the PHP extension for connecting to Oracle Database.** OCI8 is open source and included with PHP. The name is derived from Oracle's C "call interface" API first introduced in version 8 of Oracle Database. OCI8 links with Oracle client libraries, such as Oracle Instant Client.”
  - <https://www.oracle.com/technetwork/articles/technote-php-instant-084410.html>



# Practical considerations and security

# Use of Frameworks

- Earlier we discussed the fact that PHP is used within many frameworks
  - So what are frameworks?
- “A web framework (WF)... is a software framework that is designed to support the development of web applications ...
  - “[they] provide a standard way to build and deploy web applications on the World Wide Web... automate the overhead associated with common activities performed in web development. ...
  - “[e.g.] provide libraries for database access”
- Trends in 2020 - see e.g.
  - <https://hackr.io/blog/top-10-web-development-frameworks-in-2020>

[https://en.wikipedia.org/wiki/Web\\_framework](https://en.wikipedia.org/wiki/Web_framework)



# Frameworks, Oracle Support, ORM

- Many frameworks support Oracle connectivity.
- Examples:
  - Django <https://docs.djangoproject.com/en/2.2/ref/databases/>
  - Node.js <https://www.oracle.com/au/database/technologies/appdev/nodejs.html>
  - CakePHP <https://github.com/CakeDC/cakephp-oracle-driver>
  - Symfony <https://symfony.com/doc/current/doctrine.html>
- Object-Relational Mapping (ORM) helps make it easy to write code ...
  - A short definition: “Object-Relational Mapping is a technique that lets you query and manipulate... data from a database using an object-oriented paradigm.”  
Reference: <https://blog.yellowant.com/orm-rethinking-data-as-objects-8ddaa43b1410>
  - Shorter example: CakePHP’s ORM maps a DB row to an object in your programming language of choice (e.g. **\$article** in CakePHP)...
    - so you can use the object directly to access its attributes e.g.  
**\$article->title**

# SQL Injection - Example

SQL Injection demo

# Security Considerations

- Databases, especially when they are user-facing (web apps etc), are at risk of attacks over the web...
  - **OWASP's Top 10 list since 2010 to 2017 -- #1 is "Injection"**
  - Read [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)
- SQL injection is very common! Definition: quoted verbatim (OWASP)
  - “A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.” [https://www.owasp.org/index.php/SQL\\_Injection](https://www.owasp.org/index.php/SQL_Injection)
  - (OWASP: Open Web Application Security Project)



# Security Considerations

- Examples -
  - simple ones illustrated in [https://www.w3schools.com/sql/sql\\_injection.asp](https://www.w3schools.com/sql/sql_injection.asp)
- Lessons:
  - Sanitise and check your input!
  - Configure your database to minimise the damage
    - restricted user - least privileges
    - using views (Workshop 10)
  - Follow security best practices
    - e.g. OWASP  
[https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet.md](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.md)
    - e.g. for Oracle -
      - Oracle Blog <https://blogs.oracle.com/sql/what-is-sql-injection-and-how-to-stop-it>
      - 67-page whitepaper  
<https://www.oracle.com/assets/how-to-write-injection-proof-plsql-1-129572.pdf>