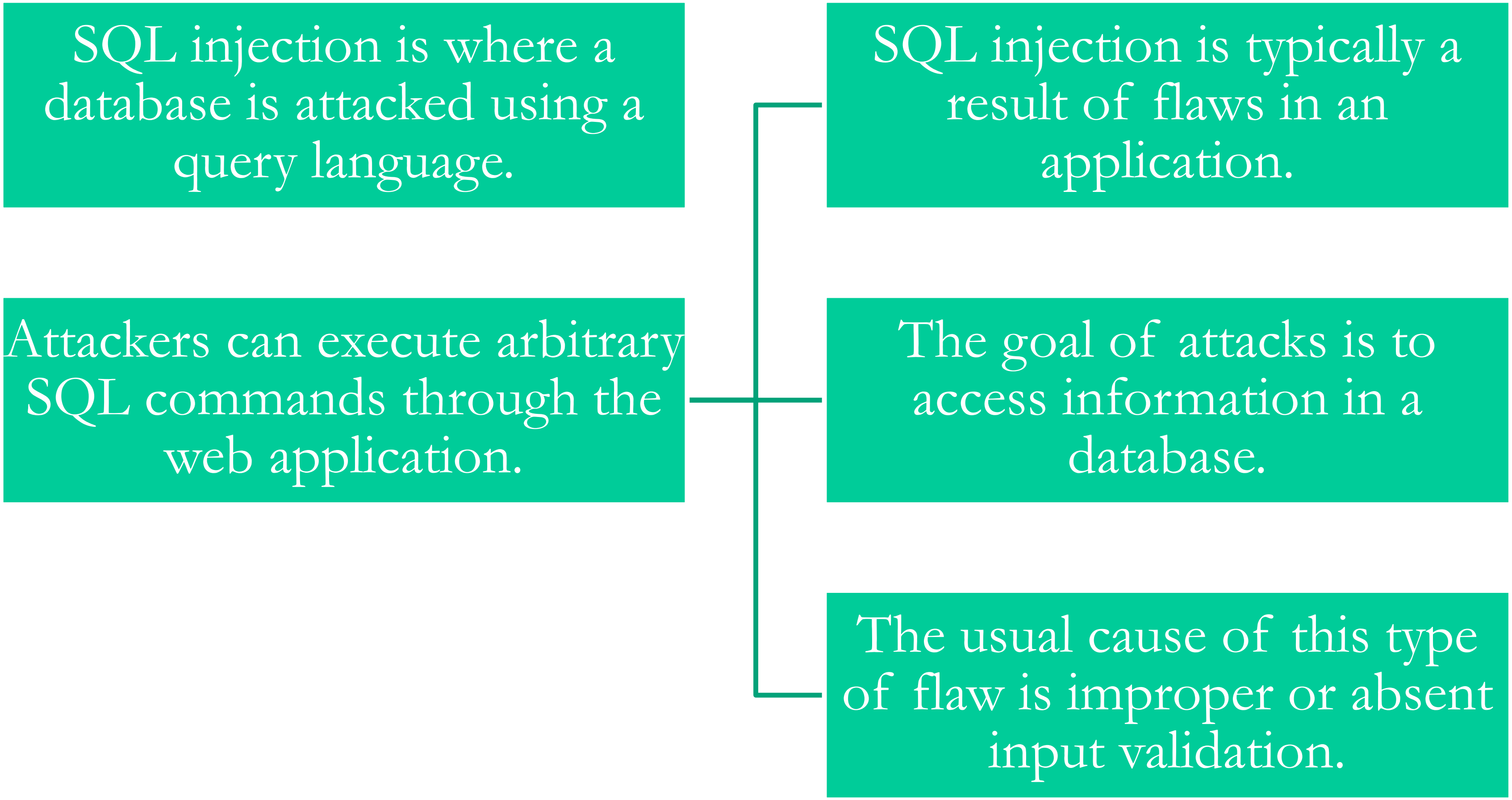
SQL Injection

Chapter 14

What Is SQL Injection?



SQL injection is where a database is attacked using a query language.

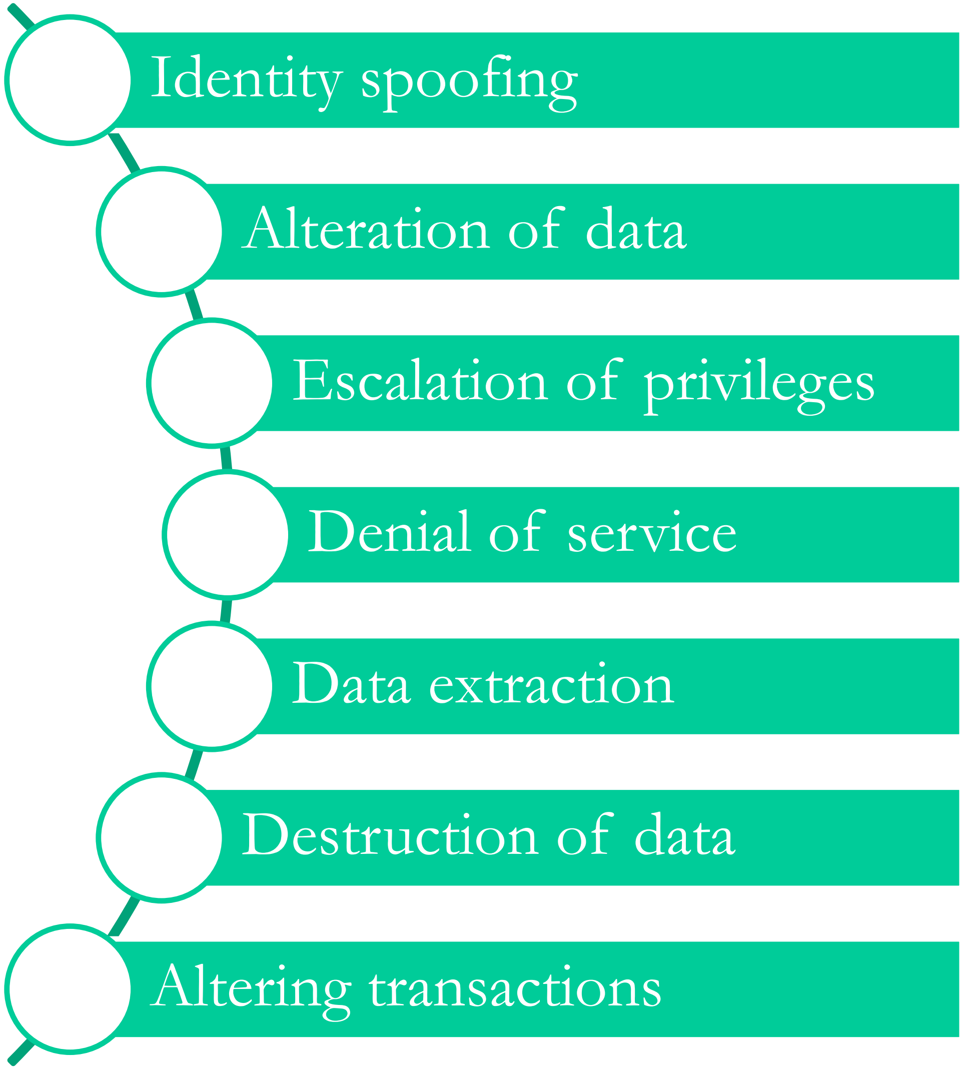
Attackers can execute arbitrary SQL commands through the web application.

SQL injection is typically a result of flaws in an application.

The goal of attacks is to access information in a database.

The usual cause of this type of flaw is improper or absent input validation.

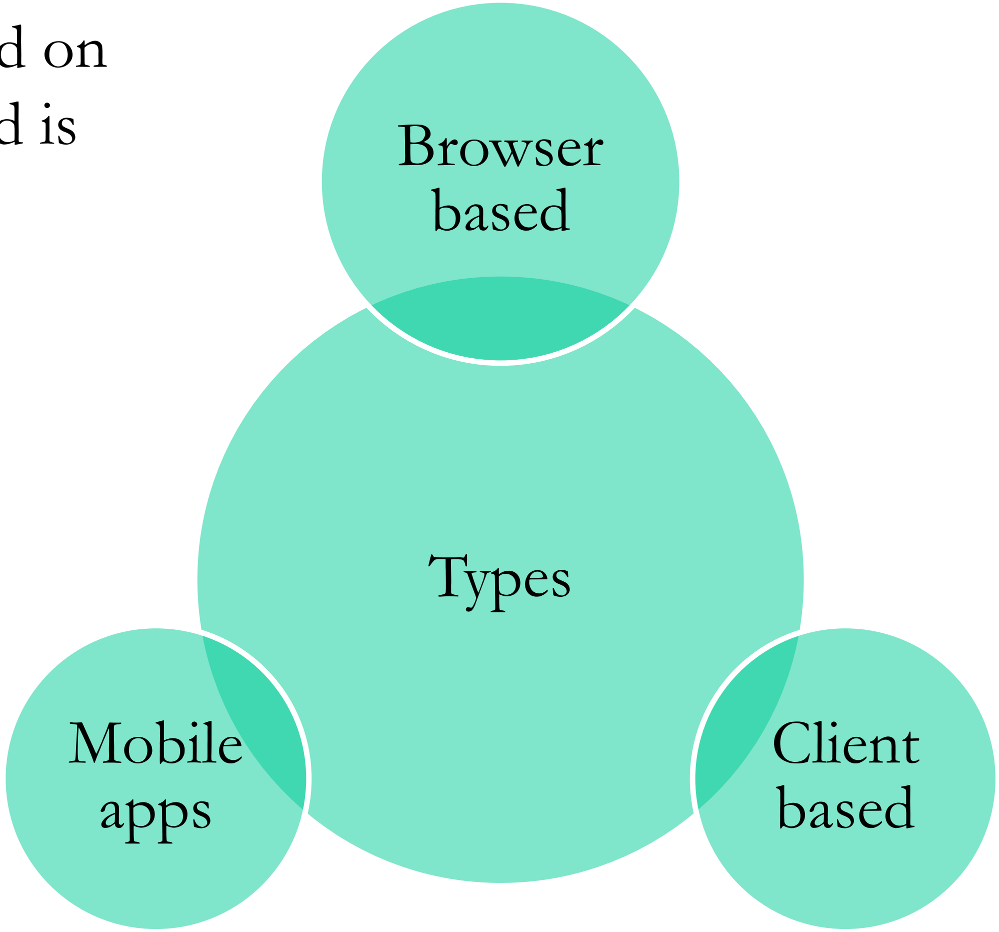
Results of SQL Injections



- Identity spoofing
- Alteration of data
- Escalation of privileges
- Denial of service
- Data extraction
- Destruction of data
- Altering transactions

Web Applications

A web application is software that is installed on top of a web server and is designed to respond to requests, process information, and store information.



Client and Server Web Applications

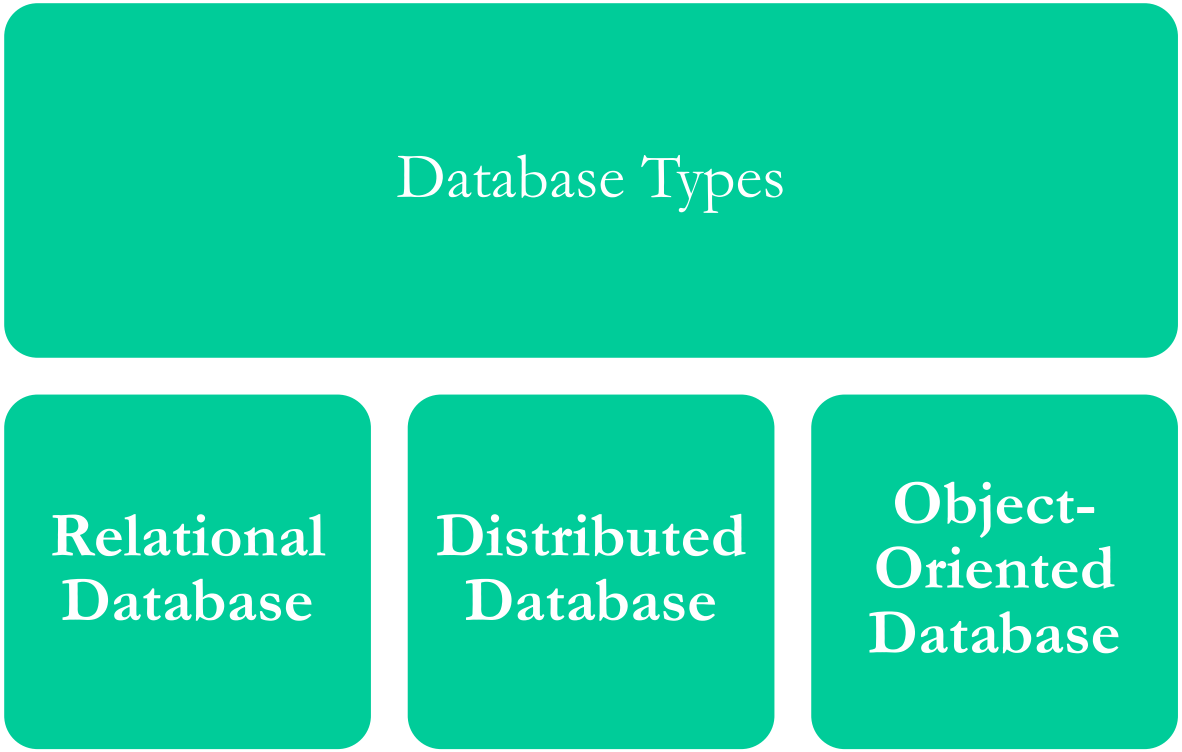
A server application is hosted on a web server and is designed to be accessed remotely via a web browser or web-enabled application.

- The server application is on the web server.
- The client is a web browser or web-enabled application.
- Information is stored on the server.
- Processing is done on the server.
- The end result is delivered to the user.
- Applications can be made for one platform.

Server-Side vs. Client-Side Technology

- **Database**
  - Oracle
  - SQL Server
  - IBM DB2
  - MySQL
- **Development Languages**
  - ASP
  - ASP.NET
  - PHP
  - JSP
  - Ruby on Rails

The Shape of Databases



Database Types

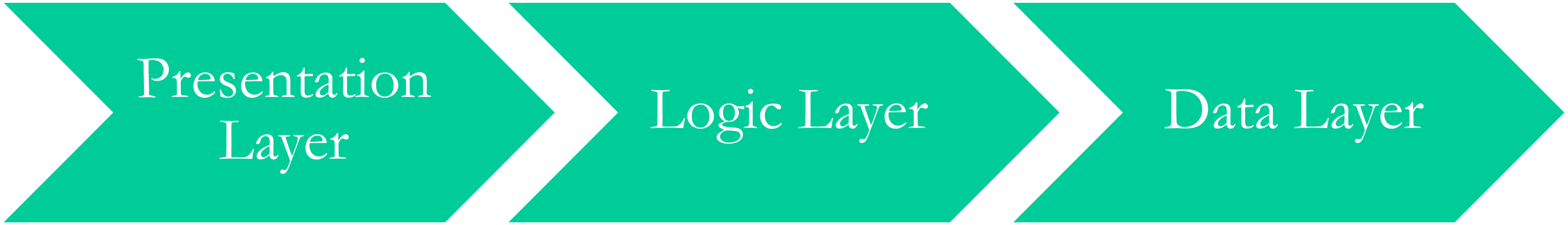
Relational Database

Distributed Database

Object-Oriented Database

For all of its complexities, a database can be described as simply a hierarchical, structured format for storing information for later retrieval, modification, management, and other purposes.

The Structure of Web Applications



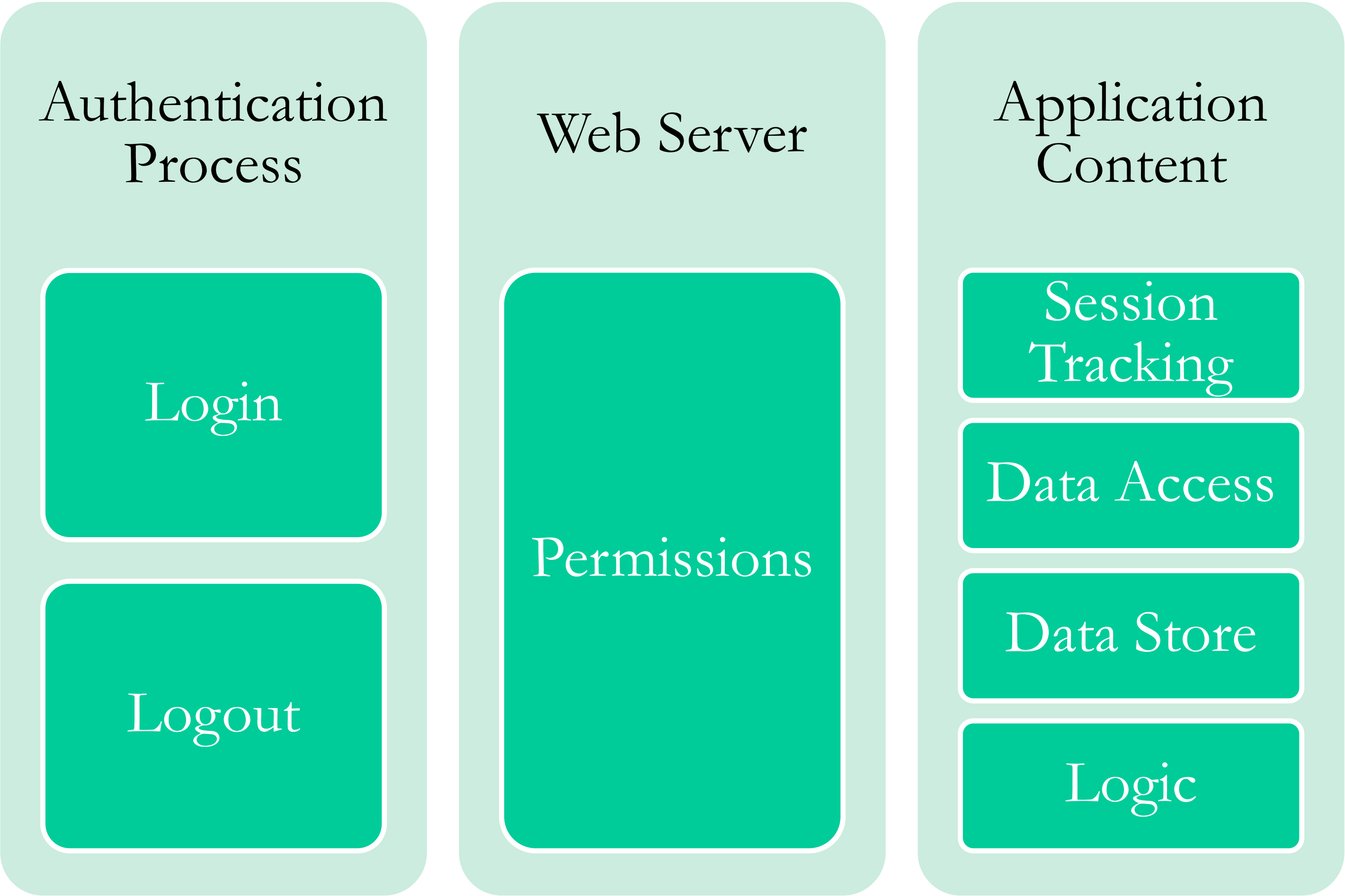
Presentation Layer

Logic Layer

Data Layer

All of these layers depend on the technology brought to the table in the form of the World Wide Web, HTML, and HTTP.

Pieces of the Web Application Puzzle



Authentication Process

Login

Logout

Web Server

Permissions

Application Content

Session Tracking

Data Access

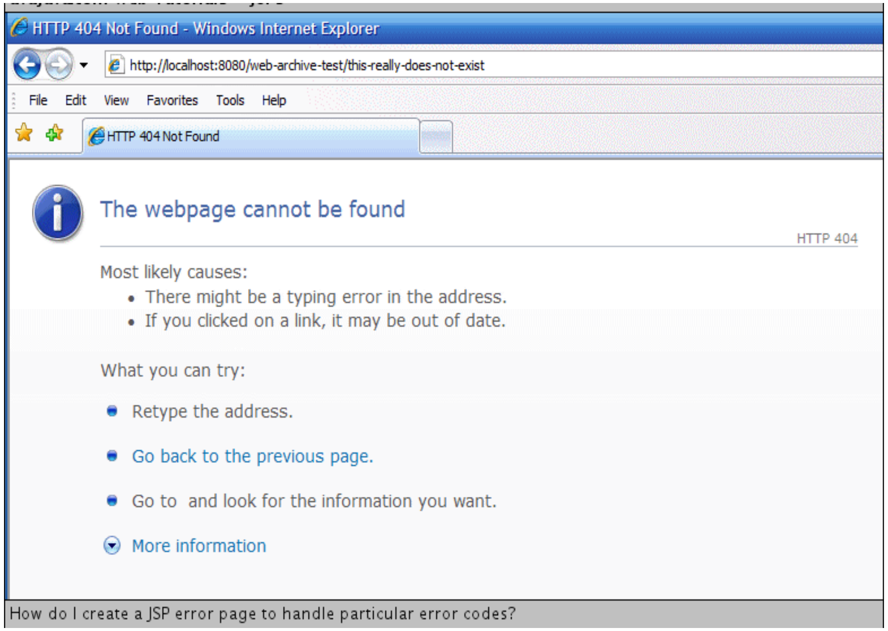
Data Store

Logic

Common Problems with Web Applications

- **Flawed Web Design**
  - Too much revealed in code
  - Presence of server information
  - Presence of connection information
- **Buffer Overflow**
  - Software-based issue
  - Common vulnerability
  - Can cause numerous issues

Error Messages



HTTP 404 Not Found - Windows Internet Explorer
http://localhost:8080/web-archive-test/this-really-does-not-exist
File Edit View Favorites Tools Help
HTTP 404 Not Found

The webpage cannot be found

HTTP 404

Most likely causes:

- There might be a typing error in the address.
- If you clicked on a link, it may be out of date.

What you can try:

- Retype the address.
- Go back to the previous page.
- Go to and look for the information you want.
- More information

How do I create a JSP error page to handle particular error codes?

May reveal too much information

Should be suppressed or sanitized

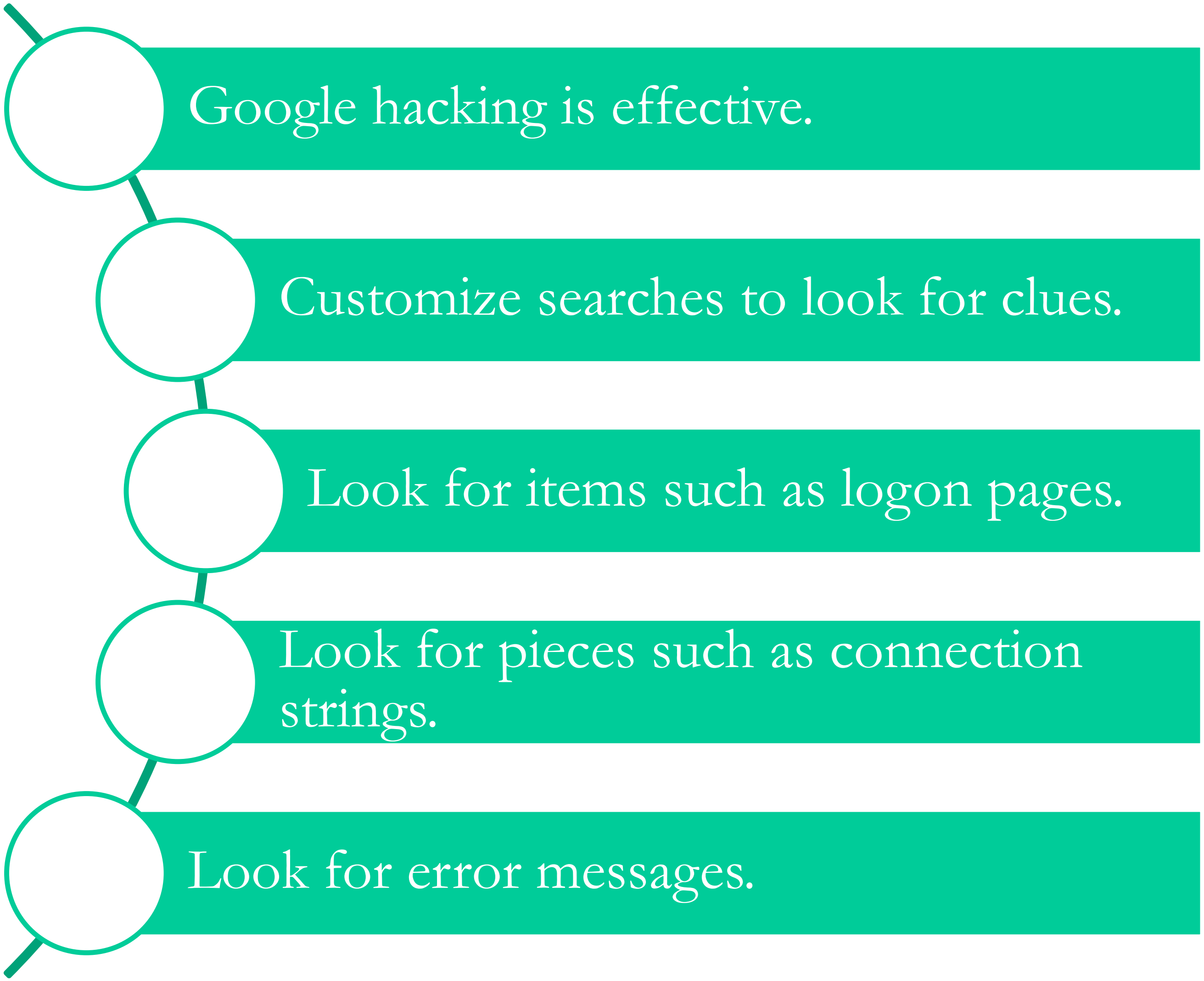
Detailed messages should be accessible only in development

Custom error message pages may be a solution

Common Flaws and Attack Messages

- **Misconfiguration**
  - May be caused by inexperience
- **Input validation**
  - Database manipulation
  - Database corruption
  - Buffer overflows
  - Inconsistent data

Locating a Target



- Google hacking is effective.
- Customize searches to look for clues.
- Look for items such as logon pages.
- Look for pieces such as connection strings.
- Look for error messages.

SQL Injection Countermeasures

- Avoid the use of dynamic SQL.
- Perform maintenance on the server regularly.
- Deploy intrusion detection systems.
- Harden a system to include the OS and database.
- Exercise least privilege.
- Ensure that applications are well-tested.
- Avoid default configurations and passwords.
- Disable error messages in production.

Summary

- SQL injection
- Steps for performing SQL injection
- SQL injection techniques
- SQL injection in Oracle
- SQL injection in MySql
- Attacking SQL servers
- Automated tools for SQL injection
- Countermeasures to SQL injection