## Course Description

This course is a one day class run on your site or at a public venue or can be arranged on-line that teaches the delegates about the common security issues often located in PL/SQL code and created by developers without an experience of database security. The course first places PL/SQL into the context of the problem of securing data and then looks at all of the common types of issues that make PL/SQL code vulnerable. Each type of PL/SQL coding issue is demonstrated so that the delegates can appreciate what vulnerable code looks like and then sample exploitations are demonstrated to show how the code is actually exploited by an attacker. Then for each example the code is re-written to show how it can be made secure. Common issues include SQL and PL/SQL injection and design issues that allow this to happen.

The course also includes a look at other issues such as encryption, leakage of critical data, dangerous functions and use of incorrect privileges. The class also considers how to protect your PL/SQL code to make it harder for an attacker to steal or run code out of context

## Course Goals

The aim of the course is for the students to get an appreciation of how insecure PL/SQL coding can allow an attacker to steal data or abuse privilege.

## Course Duration

The class is One Day 9am to 5pm and is instructor lead with demonstrations

## Course Location

The course can be held at your site or students can attend a public class. No public classes are scheduled at present. Details of on-site requirements are provided during the booking process

## Course Pre-Requisites

The delegates must have a good working knowledge of PL/SQL ideally as a Developer or DBA to appreciate the content.

The class is intended for DBA's and developers who can write PL/SQL and is of an intermediate level when vulnerabilities are explained but a developer who can write PL/SQL can understand the secure coding practices

## Course Material

The student will receive a URL to download a zip file that includes:

- The course notes as PDF files
- Free PL/SQL tools and scripts
- All of the examples used as SQL and PL/SQL scripts

 

## Course Outline

The course outline is as follows

- Data Theft
  - This lesson covers why data can be stolen or privilege escalated in a database focusing on issues related to privileges assigned to PL/SQL, bad programming practices and leakage of data.
  - This section is an overview to allow the student to see how PL/SQL fits into the security model intended to protect Data
- Permissions
  - We cover permissions of packages and procedures
  - Design decisions that affect security
  - PL/SQL used as part of a security solution such as VPD or encryption
- Coding Errors
  - This section introduces common PL/SQL Security programming issues and for each shows the issue in code form and exploitation and then also in terms of secure coding and solution. These include:
    - Input validation
    - Object validation
    - Open interfaces
    - SQL and PL/SQL and Other Injection issues
    - File and external access
    - Operating system commands
    - Vulnerable and dangerous package use
    - More
- Dynamic SQL best practices
- Encryption
  - Discusses encryption in the database and show examples of weakness in code design, encryption keys and more
  - Also highlights methods attackers can use to steal encrypted data or decrypt it in situ
- Protecting PL/SQL
  - This section discusses techniques to lock down PL/SQL in terms of
    - Preventing IPR loss
    - Prevent unauthorised execution both in the host database or if the code is removed
    - License type features
    - Wrapping and unwrapping

This course is fast paced and very interesting and is delivered by one of the most well known experts in database security. Pete Finnigan created the SANS Oracle security step-by-step guide and the CIS Oracle benchmark used by NIST, USA DoD and more is a reference to secure Oracle databases. Pete worked out the mechanisms that Oracle used to protect PL/SQL and showed how they can be easily defeated at the Black Hat conference in Las Vegas in 2006. Pete has published multiple books on databases security and speaks and publishes papers regularly. His company also produces the tool PFCLObfuscate used to protect IPR in PL/SQL.

 