Database Security Testing

Introduction

- Why Care About Database Security?
- Which Database Is the Most Secure?
- The State of Database Security Research
- Classes of Database Security Flaws
- Finding Flaws in Your Database Server

Oracle

- The Oracle Architecture
- Attacking Oracle
- Examining the Oracle Architecture
- Oracle: Moving Further into the Network
- Securing Oracle
- Oracle Processes and Oracle on the Network
- The Oracle TNS Listener
- The Oracle RDBMS
- Oracle Authentication and Authorization
- The Oracle Intelligent Agent
- Database Authentication
- Oracle Auditing
- Scanning for Oracle Servers
- Oracle's PL/SQL
- PL/SQL Injection
- Injecting into Anonymous PL/SQL Blocks
- Executing User-Supplied Queries with DBMS_SQL
- PL/SQL Injection and Database Triggers
- PL/SQL and Oracle Application Server
- Running OS Commands with PL/SQL
- Accessing the File System
- Accessing the Network
- PL/SQL and the Network
- Oracle Security Recommendations

DB2

- IBM DB2 Universal Database
- DB2 on the Network
- DB2 Processes
- DB2 Physical Database Layout
- DB2 on Windows
- DB2 on Linux
- DB2 Logical Database Layout
- DB2 Authentication and Authorization
- Authorization
- The DBAUTH View
- The TABAUTH View
- The ROUTINEAUTH View
- DB2: Discovery, Attack, and Defense
- Finding DB2 on the Network
- Buffer Overflows in DB2 Procedures and Functions
- Other Overflows in DB2
- DB2 Remote Command Server
- Running Commands Through DB2
- Gaining Access to the Filesystem Through DB2
- Local Attacks Against DB2
- Attacking DB2
- Securing DB2

Informix

- The Informix Architecture
- Examining the Informix Architecture
- Informix on the Network
- Connecting to a Remote Informix Server
- The Informix Logical Layout
- Understanding Authentication and Authorization
- Attacking and Defending Informix
- Attacking Informix with Stored Procedural Language (SPL)
- Running Arbitrary Commands with SPL
- SQL Buffer Overflows in Informix

- Local Attacks Against Informix Running on Unix Platforms
- Informix: Discovery, Attack, and Defense
- Securing Informix

Sybase ASE

- Sybase Architecture
- Introduction
- History
- Stand-Out Features
- Finding Targets
- Attacking Sybase
- MS SQL Server Injection Techniques in Sybase
- External Filesystem Access
- Defending Against Attacks
- Older Known Sybase ASE Security Bugs
- Sybase Version Tool
- Connecting to Other Servers with Sybase
- Java in SQL
- Trojanning Sybase
- Sybase: Discovery, Attack, and Defense
- Sybase: Moving Further into the Network
- Securing Sybase

MySQL

- MySQL Architecture
- MySQL: Discovery, Attack, and Defense
- MySQL: Moving Further into the Network
- Securing MySQL
- MySQL Client Hash Authentication Patch
- Running External Programs: User-Defined Functions
- User-Defined Functions in Windows
- MySQL Security Checklist

SQL Server

- Microsoft SQL Server Architecture
- SQL Server: Exploitation, Attack, and Defense
- Securing SQL Server

PostgreSQL

- The PostgreSQL Architecture
- PostgreSQL: Discovery and Attack
- Securing PostgreSQL