

1-800-ROI-9877

www.trainingbyROI.com

Course 519: MS SQL Server –Analysis, Coding, and Development for Secure Applications (5 days)

Course Description...

Microsoft SQL Server functions as the backend to a vast number of web-based applications. The ease and speed with which servers can be installed and deployed, and the powerful scripting languages available to rapidly create web applications has led to record numbers of publicly-accessible web sites exhibiting varying degrees of vulnerability to attack.

Minimizing vulnerability through server installation and configuration and via design and coding practices is crucially important. In addition, detecting and responding to attacks, both successful and unsuccessful, is vital to maintaining site integrity and protecting confidential data. This course covers current vulnerabilities, the methods by which they are exploited, and the means by which these vulnerabilities can be minimized.

Who should attend...

This course is targeted to database administrators, project managers, and developers working with Microsoft SQL Server. This is a *hands-on* course, with demonstrations and labs demonstrating weaknesses, coding techniques, and how to use tools described in the course.

Prerequisites...

Experience with SQL, Transact SQL, Microsoft SQL Server, HTML coding, and web application scripting languages such as vbscript and javascript is assumed. Familiarity with Microsoft.NET is not required – aspects of .NET pertinent to this course are introduced within the course.

See next page for a detailed course outline....



Course Outline:

- Learn about current trends in application penetrations and attacks – methods, perpetrators, intentions, extent of threats, and consequences
- Install and Configure MS SQL Server to minimize attack opportunities
 - Best practices for SQL Server Account
 - Best practices for authentication method
 - Minimizing Attack Surface
 - Disabling Unused or Exploitable Accounts
 - Disabling Exploitable Stored Procedures
 - Removing Unused/Sample Databases
 - Ensuring that SA password in cleartext is removed after installs/updates
 - Disabling unused protocols
 - “Lockdown” scripts
- Understand how to grant MS SQL Server Rights, and Permissions, and how to manage logins, accounts, and roles.
- Use Logging and Log Analysis to detect attacks
- Learn to recognize and avoid coding practices that increase application vulnerability, by understanding attack methods
 - SQL Injection
 - Exploitation of Improper Error Handling and Reporting
 - Cross Site Scripting
 - Script Injection: Dynamic Execution in scripting languages
- Best Practices
 - Validating User Input
 - Parameterizing queries
 - Eliminating dynamic SQL
 - “Blacklist” user input filtering
 - Suppressing/Replacing “overly informative” error messages
 - Minimizing/Eliminating use of eval()
- Explore manual and automated methods for analyzing existing applications for vulnerabilities, using both free and commercial tools
 - Microsoft Source Code Analyzer
 - URLScan
 - Scrawlr
 - Acunetix
 - WebInspect
 - Others
- Understand new capabilities and weaknesses and dangers introduced with ASP.NET and MS SQL Server
 - CLR Integration
 - Code Access Security
 - Deployment of CLR-based procedures, functions, triggers

This course can be tailored to meet your specific requirements!!