Training Course on Database Forensics and SQL Injection Aftermath

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

Databases are the crown jewels of any organization, housing sensitive customer data, intellectual property, and critical operational information. Consequently, they are prime targets for cyberattacks, with SQL Injection (SQLi) remaining a persistent and devastating vector for data breaches and unauthorized access. Training Course on Database Forensics and SQL Injection Aftermath is meticulously designed to equip digital forensic investigators, incident responders, and database administrators with the deep technical expertise required to effectively conduct database forensics and respond to the aftermath of SQL Injection attacks. Participants will learn to identify indicators of compromise, reconstruct attack methodologies, recover stolen data, and build irrefutable digital evidence from compromised database systems.

This intensive program delves beyond basic log analysis, focusing on the intricate forensic analysis of database artifacts, memory, and network traffic to uncover stealthy SQLi exploits, privilege escalation, and data exfiltration techniques. Through hands-on labs with real-world attack scenarios (including live SQLi attacks against vulnerable databases), attendees will master the nuances of popular database systems (SQL Server, MySQL, PostgreSQL, Oracle), understand how to correlate diverse data sources, and develop strategies for proactive defense. Elevate your investigative capabilities to effectively respond to complex database breach investigations and safeguard your organization's most valuable digital assets from the persistent threat of SQL Injection.

Programme Curriculum

Training Course on Database Forensics and SQL Injection Aftermath

Introduction

Databases are the crown jewels of any organization, housing sensitive customer data, intellectual property, and critical operational information. Consequently, they are prime targets for cyberattacks, with SQL Injection (SQLi) remaining a persistent and devastating vector for data breaches and unauthorized access. Training Course on Database Forensics and SQL Injection Aftermath is meticulously designed to equip digital forensic investigators, incident responders, and database administrators with the deep technical expertise required to effectively conduct database forensics and respond to the aftermath of SQL Injection attacks. Participants will learn to identify indicators of compromise, reconstruct attack methodologies, recover stolen data, and build irrefutable digital evidence from compromised database systems.

This intensive program delves beyond basic log analysis, focusing on the intricate forensic analysis of database artifacts, memory, and network traffic to uncover stealthy SQLi exploits, privilege escalation, and data exfiltration techniques. Through hands-on labs with real-world attack scenarios (including live SQLi attacks against vulnerable databases), attendees will master the nuances of popular database systems (SQL Server, MySQL, PostgreSQL, Oracle), understand how to correlate diverse data sources, and develop strategies for proactive defense. Elevate your investigative capabilities to effectively respond to complex database breach investigations and safeguard your organization's most valuable digital assets from the persistent threat of SQL Injection.

Course Duration

5 Days

Course Objectives

1. Understand Database Architectures: Comprehend the internal structures, components, and data storage mechanisms of leading relational databases (SQL Server, MySQL, PostgreSQL, Oracle).
2. Master SQL Injection Attack Vectors: Analyze various SQL Injection techniques (e.g., Union-based, Error-based, Blind SQLi, Time-based, Out-of-band) and their forensic artifacts.
3. Conduct Forensically Sound Database Acquisition: Safely acquire database files, logs, and memory from live and dead database servers.
4. Perform Database Log Analysis: Deeply analyze database-specific logs (e.g., transaction logs, audit logs, error logs) for signs of compromise and malicious queries.
5. Investigate Web Server Logs for SQLi: Correlate web server access logs (IIS, Apache, Nginx) with database activity to pinpoint initial injection points.
6. Analyze Database Memory Forensics: Extract and interpret volatile data from database server memory dumps to identify active attacks, processes, and network connections.

7. Recover Deleted or Modified Data: Utilize advanced techniques to recover tampered, deleted, or exfiltrated data from database files.
8. Trace Data Exfiltration Paths: Identify how stolen data was extracted from the database, including methods like web shells, remote command execution, and direct database connections.
9. Detect Privilege Escalation in Databases: Uncover evidence of elevated privileges gained by attackers within the database system.
10. Analyze Database Backups & Snapshots: Forensically examine database backups and snapshots for evidence of compromise or data changes.
11. Leverage Specialized Database Forensic Tools: Proficiency in using commercial and open-source tools for database parsing, recovery, and analysis.
12. Develop Post-SQLi Remediation Strategies: Formulate and implement effective steps for database hardening, patch management, and re-securing compromised systems.
13. Generate Comprehensive Forensic Reports: Produce detailed, technical, and legally defensible reports on database breach investigations and SQLi aftermath.

Organizational Benefits

1. Accelerated Breach Response: Rapidly identify, contain, and remediate data breaches originating from database compromises.
2. Minimized Data Loss & Downtime: Reduce the impact of database attacks through efficient forensic investigation and recovery.
3. Enhanced Data Security Posture: Proactive identification of vulnerabilities and weaknesses in database configurations.
4. Improved Compliance & Audit Readiness: Demonstrate robust investigative capabilities for data breach reporting and regulatory adherence (e.g., GDPR, PCI DSS).
5. Stronger Insider Threat Detection: Uncover malicious activity or data misuse by internal actors within database systems.
6. Better Root Cause Analysis: Pinpoint the exact SQL Injection vector, attack methodology, and exploited vulnerabilities.
7. Reduced Litigation Risk: Produce high-quality, admissible digital evidence for legal proceedings stemming from database breaches.
8. Optimized Security Investments: Maximize the effectiveness of existing security controls by understanding database attack patterns.
9. Skilled Internal Workforce: Develop in-house expertise to handle complex database-centric investigations independently.
10. Protection of Critical Business Data: Safeguard sensitive customer, financial, and proprietary information stored in databases.

Target Participants

- Digital Forensic Investigators
- Incident Response Team Leads & Members
- Database Administrators (DBAs)
- Application Security Engineers
- Cybersecurity Analysts (SOC Tier 2/3)
- Penetration Testers (interested in post-exploitation)
- IT Auditors
- Software Developers (focused on secure coding)
- Threat Hunters
- Compliance Officers

Course Outline

Module 1: Database Fundamentals & Forensic Acquisition

- **Database Types & Architectures:** Relational vs. NoSQL, common RDBMS (SQL Server, MySQL, PostgreSQL, Oracle).
- **Database Components:** Instances, schemas, tables, indexes, logs, and their forensic relevance.
- **Forensically Sound Acquisition:** Live vs. dead acquisition of database files, log files, and memory dumps.
- **Tools for Database Acquisition:** Native database tools, specialized forensic tools.
- **Case Study: Initial Triage of a Potentially Compromised SQL Server**

Module 2: Understanding SQL Injection & Attack Vectors

- **Introduction to SQL Injection:** How it works, common vulnerable inputs, and impact.
- **Types of SQLi Attacks:** In-band (Union, Error-based), Inferential (Blind, Time-based), Out-of-band.
- **SQLi Payloads & Techniques:** Data extraction, command execution, database schema enumeration.
- **SQLi Detection Mechanisms:** Signatures, anomalies, web application firewalls (WAFs).
- **Case Study: Analyzing a Web Application Log for SQL Injection Attempts**

Module 3: Database Log Analysis for Compromise Detection

- **SQL Server Log Analysis:** Error logs, audit logs, SQL Server Agent logs, default traces.
- **MySQL/MariaDB Log Analysis:** Error logs, general query logs, slow query logs, binary logs.
- **PostgreSQL Log Analysis:** Standard logs, connection logs, statement logging.
- **Oracle Database Log Analysis:** Audit logs (DBA_AUDIT_TRAIL), listener logs, alert logs, redo logs.
- **Case Study: Identifying Malicious Queries and Unauthorized Access in Database Logs**

Module 4: Web Server & Application Logs Correlation

- **IIS Web Server Logs:** Analyzing access logs for suspicious SQLi parameters and error codes.
- **Apache/Nginx Web Server Logs:** Understanding access.log and error.log in relation to SQLi.
- **Application Logs:** Interpreting custom application logs for database interaction and errors.

- **Correlating Web Server & Database Logs:** Building a unified timeline of the attack chain.
- **Case Study: Tracing an SQLi Attack from the Web Front-End to Database Activity**

Module 5: Database File & Data Artifact Analysis

- **Database File Structures:** Deep dive into MDF/LDF (SQL Server), .ibd/.frm (MySQL), pg_data (PostgreSQL), datafiles (Oracle).
- **Recovering Deleted/Modified Data:** Techniques for undeleting records, analyzing transaction logs for data manipulation.
- **Identifying Database Objects:** Enumerating tables, columns, stored procedures, functions created by attackers.
- **Extracting User & Permission Data:** Analyzing database roles, users, and assigned privileges.
- **Case Study: Recovering Stolen Customer Records from a Compromised Database**

Module 6: Database Memory Forensics & Live Analysis

- **Acquiring Database Server Memory:** Challenges and tools for large memory dumps.
- **Analyzing Memory Dumps:** Identifying active connections, processes, loaded modules, and query buffers in memory.
- **Extracting Database Credentials from Memory:** Locating cached passwords or connection strings.
- **Detecting In-Memory SQLi Payloads:** Identifying dynamically loaded malicious code.
- **Case Study: Analyzing a Live Database Server Memory Dump for Active SQLi Attacks**

Module 7: Data Exfiltration & Post-Exploitation Forensics

- **Common Data Exfiltration Methods:** Out-of-band channels, DNS exfiltration, direct network connections, web shells.
- **Identifying Malicious User-Defined Functions (UDFs) & Stored Procedures:** Backdoors created for data exfiltration.
- **Analyzing Database Backups & Snapshots:** Forensic value of backups for historical context and data recovery.
- **Detecting Privilege Escalation within the Database:** From low-privilege user to DBA, or OS command execution.
- **Case Study: Tracing Data Exfiltration After a Successful SQL Injection**

Module 8: Remediation, Reporting & Proactive Defense

- **Post-Breach Hardening:** Patching, secure configurations, least privilege, input validation.
- **Database Monitoring & Auditing:** Implementing robust logging and real-time alerts.
- **Crafting a Database Forensic Report:** Structure, content, and legal considerations.
- **Presenting Findings & Recommendations:** Communicating technical details to stakeholders.
- **Case Study: Full Incident Response and Remediation Plan for a SQLi-Induced Data Breach**

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.

- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com