EMA SECURITY

Veritabanı Saldırı ve Savunma Eğitimi

AI-Powered Offensive Services

İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

Veritabanı Saldırı ve Savunma Eğitimi

Eğitim Açıklaması

Veritabanı Saldırı ve Savunma Eğitimi, veritabanı güvenliğini sağlamak ve saldırılara karşı koruma sağlamak için gerekli olan bilgileri sunar. Katılımcılar, veritabanı saldırı teknikleri ve bu saldırılara karşı savunma yöntemlerini öğrenirler. Eğitimde, veritabanlarının nasıl güvence altına alınacağı, zayıf noktaların nasıl tespit edileceği ve olası tehditlere karşı nasıl etkin savunma yapılacağı ele alınacaktır.

Eğitim Yeri

- Online
- Fiziksel

Eğitim Süresi

- 5 Gün

Eğitim Seviyesi

- Başlangıç
- Orta

Eğitim İçin Ön Gereksinimler

- Temel veritabanı yönetim sistemleri bilgisi (MySQL, PostgreSQL, vb.)
- SQL sorgulama dili bilgisi
- Temel ağ ve sistem güvenliği bilgisi
- Web uygulamaları ve veritabanı arasındaki etkileşim hakkında genel bilgi

Eğitimi Kimler Katılmalı?

- Veritabanı yöneticileri ve güvenlik uzmanları
- SQL enjeksiyonu gibi saldırılara karşı savunma tekniklerini öğrenmek isteyenler
- Veritabanı ve web uygulama güvenliği konusunda bilgi sahibi olmak isteyen IT profesyonelleri

Eğitim Sonunda Katılımcılar Ne Öğrenmiş Olacak?

- Katılımcılar, veritabanı güvenliği tehditlerini tanır ve bu tehditlere karşı etkili savunma stratejileri geliştirirler.

Eğitim İçeriği

- Veritabanı Zafiyetleri ve Saldırı Yüzeyleri
- Saldırıya Açık Komponentler
- Network exposure (açık portlar: 1433, 3306, 5432, 1521)
- Varsayılan kullanıcılar ve şifreler
- Güvensiz yapılandırmalar (örnek: xp_cmdshell, LOAD_FILE, COPY TO)
- Güvenlik Zafiyetleri
- OWASP Top 10 – Injection (A01:2021)
- Unpatched RCE zafiyetleri (MySQL CVE-2021-27928, Oracle RCE'ler)
- SQL sunucularında dosya sistemine erişim
- SQL Enjeksiyon ve Sızma Teknikleri
- SQL Injection (SQLi) Türleri
- Classic SQLi (1=1), Blind SQLi, Time-based SQLi, Error-based SQLi
- Out-of-band (OOB) SQLi ile DNS üzerinden veri sızdırma
- SQLMap ve manuel exploitation örnekleri
- Platforma Özel Enjeksiyonlar
- SQL Server: xp_cmdshell, OPENROWSET, linked server istismarı
- MySQL: LOAD_FILE(), INTO OUTFILE, UDF shell açma
- PostgreSQL: COPY TO, lo_export, COPY PROGRAM
- Oracle: DBMS_SQL, Java Stored Procedure saldırıları
- Kimlik Bilgisi Elde Etme ve Lateral Movement
- Kimlik Bilgisi Toplama
- mysql.user, pg_shadow, sys.sql_logins tablolarından hash çekme
- Memory scraping (Metasploit mssql_enum, hashdump)
- Sniffing ile bağlantı üzerindeki şifreleri toplama
- Parola Kırma ve Lateral Movement
- Hash formatları: MySQL (SHA1), SQL Server (NTLM), PostgreSQL (MD5)
- Cracking araçları: Hashcat, John the Ripper
- Database linked connections ile ağ içinde zıplama

Eğitim İçeriği

- Yetki Yükseltme ve Kalıcılık
- Yetki Yükseltme Yolları
- Misconfigured roles: db_owner, sysadmin, superuser
- xp_cmdshell ve sp_configure ile OS seviyesine geçiş
- Scheduled job abuse, trigger persistence
- Kalıcılık Yöntemleri
- Malicious stored procedures
- Backdoor view veya trigger tanımlamaları
- SYSLOG manipülasyonu (PostgreSQL)
- Loglama, İzleme ve Olay Tespiti
- Veritabanı Loglama Yapıları
- SQL Server: SQL Audit, Server Audit Specification
- MySQL: general_log, audit_log plugin
- PostgreSQL: log_statement, log_connections, pg_audit
- Oracle: Unified Audit Trail
- Tespit Edilmesi Gereken Aksiyonlar
- Şüpheli sorgular: UNION, SELECT * FROM information_schema
- Privilege escalation girişimleri
- Dosya sistemine erişim denemeleri
- Anormal saatlerde admin erişimleri
- Sıkılaştırma ve Güvenlik Kontrolleri
- En İyi Güvenlik Uygulamaları
- Minimum yetki prensibi: Role-based access control (RBAC)
- DB firewall ve SQL injection WAF
- Şifre politikaları ve MFA entegrasyonu
- CIS Benchmarks ve Kontroller
- Secure configuration checklist (port kapatma, TLS)
- Audit log retention & alerting

Eğitim İçeriği

- Erişim sınırlama: IP, subnet bazlı whitelist
- Olay Müdahalesi ve Post-Saldırı Analizi
- Hacklenmiş Veritabanı Analizi
- Log analizi: Sorgu geçmişi, login kaynakları
- Dump alınan veriler, veri sızıntısı izleri
- Persistence bileşenleri tespiti: job, trigger, backdoor
- MITRE ATT&CK DB-Mapped Teknikler
- T1059 (Command Execution), T1003 (Credential Dumping)
- T1078 (Valid Accounts), T1086 (PowerShell)
- T1021.002 (SQL)
- Uygulamalı Senaryolar ve Simülasyonlar
- SQLi üzerinden shell alma (SQLMap + Netcat)
- Veritabanından parola hash'lerinin çekilmesi ve kırılması
- Linked SQL sunucular arasında lateral movement
- MySQL'de OUTFILE ile webshell bırakma
- PostgreSQL'de COPY TO ile dosya dışa aktarımı
- Syslog ve log analiziyle saldırı tespiti

Sıkça Sorulan Sorular

Veritabanı saldırıları hangi tekniklerle gerçekleştirilir?

- SQL injection, credential stuffing ve veri sızıntıları gibi saldırı teknikleri üzerinden pratik yapılacaktır.

Veritabanı güvenliğini artırmak için hangi adımlar atılmalıdır?

- Güçlü parola politikaları, encryption, güvenlik duvarı kullanımı, erişim kontrol listeleri (ACL) gibi önlemler alınmalıdır.

Eğitimde hangi veritabanı yönetim sistemleri üzerinde çalışılacak?

- MsSQL, MySQL, PostgreSQL ve Oracle gibi yaygın kullanılan veritabanı yönetim sistemleri üzerinde saldırı ve savunma teknikleri öğretilmektedir.