Java Security Eğitimi

Açıklama

Bu eğitim, katılımcıların birçok zorlukların ve farklı tekniklerin bulunduğu Java güvenliği hakkında bilgi sahibi olmalarını sağlar. Java'da güvenli kod yazma uygulaması, Java SE ve Java EE'deki çeşitli teknikleri kullanır. Ayrıca her geçen gün daha fazla sayıda EE uygulamaları politika dosyaları ve JAAS kimlik doğrulama gibi SE tekniklerini kullanmaya başlıyor. Bu eğitimde tüm platformlar üzerinde belirli sürelerle duruluyor. Bu sayede katılımcılar erişim denetleyicileri, izinler ve politikalar gibi çeşitli temel SE konuları hakkında bilgi sahibi olurken, Web güvenliği bildirimleri ve EJB yetkilendirme modeli gibi geleneksel EE tekniklerini de öğreniyorlar. En iyi uygulamaların ele alındığı bölümler her bir platformun kapsamını genişletiyor.

Uygulamalı derslerin ağırlıklı olduğu eğitimde, katılımcılar vakitlerinin büyük bölümünü güvenlikle ilgili sorunları çözmeyle geçiriyorlar. Laboratuvar çalışmalarının büyük bölümü mümkün olduğunca mevcut yazılımlardaki güvenlik açıklarını yansıtan senaryolar şeklinde düzenlenmiş. Bu sayede katılımcılar bir şekilde sistemleri kırmaya (hacking) başlıyorlar. Sonrasında laboratuvar çalışması tehditlerin ortadan kaldırılması için yazılımı daha sıkı bir hale getirme şeklinde devam eder: Güvenlik politikası oluşturma, dosya imzalama, API'nin çok aşırı şekilde gösterilmiş bölümlerini temizleme ve kullanıcı girişi gerektirme ve diğerleri.

Bu eğitimde neler öğreneceksiniz?

- Java uygulamaları, sunucular ve bileşenler için güvenlik politikaları tasarlama ve uygulama
- Java uygulaması için sertifikaları ve anahtarları yönetme, gerektiğinde kod kaynaklarını imzalama
- Güvenli tasarlama ve kodlama uygulama, UI ve API'de güvenlik ve kullanılabilirlik arasında denge kurma
- Uygulama verileri ve mesajlarını JCA kullanarak imzalama ve doğrulama, bu

verileri mesajları JCE kullanarak şifreleme ve şifreyi çözme
- Uygulamaya JAAS kimlik doğrulaması ekleme
- Uygulama verilerine bağlanmak için JAAS LoginModule kullanma
- URL ve rol ile Java EE uygulamalarını güvenli hale getirme ve JAAS kimlik doğrulamayı ekleme
- SQL enjeksiyonu ve siteler arası komut dosyası saldırıları gibi Java Web uygulamalarında çok sık karşılaşılan durumlardan kaçınma

---

Eğitim İçeriği

Java SE Security

- Holistic Security Practices
- Threats to the User
- The Class Loader and Bytecode Verifier
- System Classes and the Core API
- SecurityManager and AccessController
- Permissions
- Implication
- CodeSources
- Policies
- Configuring Java SE Security
- Dynamic Policies
- Privileged Actions

Code Signature and Key Management

- Encryption and Digital Signature
- Keystores
- Keys and Certificates
- Certificate Authorities
- The KeyStore API
- Signing JARs

- Signed CodeSources
- Additional Policy Semantics

Secure Development Practices: Java SE

- Code Injection
- Final Classes and Methods
- Singletons, Factories, and Flyweights
- Methods, Collections, and Data Hiding
- Sealing JARs
- Code Obfuscation
- Object Serialization

Cryptography

- Threats to Identity and Privacy
- The Java Cryptography Extensions
- The Signature Class
- SignedObjects
- The Java Cryptography Extensions
- SecretKeys and KeyGenerator
- The Cipher Class
- Dangerous Practices
- HTTP and JSSE

JAAS

- Pluggable Authentication Logic
- JAAS
- Packages and Interfaces
- Subjects and Principals
- ANDs and ORs
- Impersonation Methods
- Permissions for JAAS Use
- LoginContext and LoginModule
- Configuring JAAS
- CallbackHandler and Callbacks
- Implementing a JAAS Client
- Implementing a LoginModule

Java EE Security

- Java EE Servers as Code Hosts
- Tomcat Security Configuration
- Declaring Roles
- Securing URLs
- HTTP Authentication Schemes
- Securing EJBs
- Programmatic Security
- JAAS in Java EE
- Realms and LoginModules
- JAAS in Tomcat
- JACC
- Certifying a Java EE Application
- HTTPS Configuration

Secure Development Practices: Java EE

- Presentation-Tier Vulnerabilities
- User Accounts
- MVC and Security
- Validating User Input
- SQL Injection
- Cross-Site Scripting
- Reflected XSS
- Defeating XSS
- OWASP
- Penetration Testing
- Error Handling and Information Leakage
- Logging and Auditing