Güvenli Java EE Geliştirme Eğitimi

Eğitim Hakkında

Digital Vizyon Akademi'nin Güvenli Java EE Geliştirme kursu, Java EE uygulamalarının ve hizmetlerinin deneyimli geliştiricilerine, maksimum güvenlik için yeni kod yazmayı ve mevcut kodu nasıl yükselteceklerini gösterir.

Neler Öğreneceksiniz

Güvenli Java web uygulamaları ve hizmetleri geliştirin veya gerektiğinde yeniden düzenleme yaparak mevcut uygulamaları ve hizmetleri güvence altına almayı,
Web kapsayıcısına kimlik doğrulama ve yetkilendirme politikalarını uygulama talimatı veren güvenlik kısıtlamalarını ve oturum açma yapılandırmalarını,
XSS, CSRF ve SQL enjeksiyonu dahil olmak üzere yaygın web saldırılarına karşı koruma sağlamayı,
Genel uygulama sağlığı için ve özellikle enjeksiyon ve XSS saldırılarını engellemek için kullanıcı girişini agresif bir şekilde doğrulamayı,
Tek yönlü veya iki yönlü HTTPS kullanmak için bir sunucu ve / veya uygulamayı yapılandırmayı,
Gerektiğinde uygulama düzeyinde şifreleme uygulamayı,
Özellikle hassas bilgiler veya eylemler için günlük dosyalarını güvenli hale getirin ve denetim izleri oluşturmayı,
RESTful web hizmetlerinde uygun şekilde HMAC güvenliğini kullanımayı,
SAML SSO sistemlerine katılın ve tek oturum açma ile ilgili güvenlik endişelerinin farkında olmayı,
Kaynaklara güvenli bir şekilde üçüncü taraf yetkilendirme sağlamak için OAuth-2.0 ilk akışının sunucu ve istemci taraflarını uygulamayı öğrenebilirsiniz.

Eğitim İçeriği

Güvenli Web Uygulamaları
Tehditler ve Saldırı Vektörleri
Sunucu, Ağ ve Tarayıcı Güvenlik Açıkları
Güvenli Tasarım İlkeleri
GET ve POST karşılaştırması
Kapsayıcı Kimlik Doğrulaması ve Yetkilendirmesi
HTML Formları
Gizlilik / WEB-INF
HTTP ve HTTPS
Diğer Kriptografik Uygulamalar
SOA ve Web Hizmetleri
OWASP İlk 10

Kimlik doğrulama ve yetkilendirme
HTTP TEMEL ve DIGEST Kimlik Doğrulama Şemaları
Güvenlik Kısıtlamalarının Bildirilmesi

Kullanıcı hesapları
Geçiş Sırasında Kimlik Bilgilerinin Korunması
Saldırıları Tekrar Oynatma
URL Kalıpları Üzerinden Yetkilendirme
Roller
FORM Kimlik Doğrulaması
Login Form Tasarımı
EJB Yetkilendirmesi
Programatik Güvenlik
JSF'de Programatik Güvenlik

Yaygın Web Saldırıları
Tek Karar Noktaları
Siteler Arası Komut Dosyası
Doğrulama ve Çıkıştan Kaçma
Güçlü Tarama
Siteler Arası İstek Sahteciliği
Jeton İste
Enjeksiyon Saldırıları
JDBC ve JPA'daki korumalar
Oturum Yönetimi
Tanımlama Bilgilerinin Bakımı

Giriş Doğrulama
Kullanıcı Girişini Doğrulama
Doğrulama Uygulamaları
Düzenli ifadeler
JSF Doğrulaması
Bean Doğrulaması (a / k / a JSR-303)
Kısıtlama Ek Açıklamaları
Alanlar Arası Doğrulama
Java EE'de Yerleşik Destek
Doğrulayıcı kullanmak
Hata Yanıtları Üretme

HTTPS ve Sertifikalar
Dijital Kriptografi
Şifreleme
SSL ve Güvenli Anahtar Değişimi
Hashing
İmza
Anahtar mağazaları
Önemli araç
Anahtarlar Neden Yeterli Değil?
X.509 Sertifikaları
Sertifika Yetkilileri

İmzalı bir Sertifika Alma
HTTPS'yi Yapılandırma
İstemci Tarafı Sertifikaları ve İki Yönlü SSL
PKCS # 12 ve Güven Mağazaları
İSTEMCİ-CERT Kimlik Doğrulaması

Uygulama Düzeyinde Şifreleme
Java Şifreleme Mimarisi
Güvenli Rastgele Sayı Üretimi
KeyStore API
Elektronik imza
Hashing
Parola Karıştırma
Hashing Neden Yeterli Değil
Tuzlar
Yavaş Algoritmalar
Anahtar Uzatma ve Anahtar Güçlendirme
Java Şifreleme Uzantıları
SecretKey ve KeyGenerator Türleri
Simetrik Şifreleme
Algoritmaları ve Anahtar Boyutlarını Seçme
Tehlikeli Uygulamalar

Güvenli Geliştirme Uygulamaları
Güvenli Geliştirme Döngüsü
Hata İşleme ve Bilgi Sızıntısı
Güvenli Modda Başarısızlık
Günlük Kaydı Uygulamaları
Günlükler için Uygun İçerik
Denetleme
Stratejiler: Filtreler, Durdurucular ve Komut Zincirleri
Penetrasyon testi
Arka Kapılar
Güvenli Kod İncelemesi

REST Güvenlik Temelleri
REST Hizmetleri için Güvenlik Kaygıları
HTTPS
HTTP TEMEL ve ÖZET
URL Modeli ile Yetkilendirme
Siteler Arası Komut Dosyası
Enjeksiyon Saldırıları
Siteler Arası İstek Sahteciliği
Yaygın Karşı Tedbirler

HMAC Güvenliği

Kullanım Örneği: Mesaj Kimlik Doğrulaması
Elektronik imza
İmza Olarak Hashing: HMAC
Uygun Tuzlar
Kanonikleştirme
Amazon S3
Zaman damgaları
Mesajları İmzalama ve Doğrulama
XML Şifreleme ve Kanonikleştirme
JSON'u kanonikleştirme

SAML SSO
Kullanım Örneği: Tek Oturum Açma
SAML Yönlendirmesi
SAML İddiaları
SAML Protokolü
HTTP Bağlamaları
Tarayıcı Üzerinden "Konuşma"
Artefakt ve SOAP Bağlamaları
SAML Özellikleri
SAML SSO
Federe Kimlik
Kimlik Sağlayıcılar ve Hizmet Sağlayıcılar
Meta veriler
OpenID
Evrensel Kimlik
SSO Sistemlerinde Güvenlik Kaygıları

OAuth
Kullanım Örneği: Üçüncü Taraf Yetkilendirme
OAuth
İlk Akış
Hibe Türleri
Erişim Belirteçleri
Google OAuth API
Yetkilendirme ve Kaynak Sunucularını Uygulama
İstemcileri Uygulama
OAuth ile Güvenlik Sorunları