

Java and Web Application Security Eğitimi

Eğitim Hakkında

Java Eğitiminde Güvenli Kodlaması, geliştiricilere Java uygulamalarındaki yaygın güvenlik açıklarını ve sağlamlaştırılmış, daha güvenli kod yazmayı öğretir. Katılımcılar, bu sorunların tüm yığın genelinde Java web uygulamalarını nasıl etkilediğine odaklanarak OWASP İlk On'u ve tipik Web güvenlik açıklarını öğrenirler.

Neler Öğreneceksiniz

Web uygulaması güvenlik sorunlarını anlamayı,
PCI-DSS gereksinimlerini ve güvenli kodlamayı öğrenmeyi,
OWASP İlk On Unsurlarını Analiz Etmeyi,
Web uygulama güvenliğini Java bağlamına yerleştirmeyi,
Düşük asılı meyvelerin ötesine geçmeyi,
Java kodunuzdaki güvenlik zorluklarının üstesinden gelmeyi.

Eğitim İçeriği

Siber Güvenlikle İlgili Temel Bilgiler

Güvenlik nedir?
Tehdit ve risk
Siber güvenlik tehdit türleri
Güvensiz yazılımın sonuçları
Kısıtlamalar ve pazar
Karanlık taraf

Finans sektöründe siber güvenlik

Finans dünyasında yazılım güvenliği
Fintech'teki tehditler ve eğilimler

PCI-DSS (isteğe bağlı)

PCI-DSS'ye genel bakış
PCI-DSS varlıkları
PCI-DSS gereksinimleri ve güvenli kodlama
Güvenli sistemler ve uygulamalar geliştirin ve sürdürün
Yaygın kodlama güvenlik açıklarını ele alın

OWASP İlk On (1. Bölüm)

OWASP İlk 10 - 2017

Bozuk kimlik doğrulama

Kimlik doğrulama temelleri

Kimlik doğrulama zayıflıkları

Örnek olay - Equifax Arjantin

Web'de sahtecilik

Örnek olay - PayPal 2FA atlama

Kullanıcı arayüzü en iyi uygulamaları

Örnek olay - Android için Basit Bankacılıkta bilgilerin ifşası

Parola yönetimi

Hassas Verilerin Ifşası

Bilgi maruziyeti

Çıkarılan veriler ve toplama yoluyla maruz kalma

Örnek olay - Strava fitness uygulaması verilerinin teşhiri

Sistem bilgisi sızıntısı

Bilgiye maruz kalma en iyi uygulamaları

Bilinen Güvenlik Açıklarına Sahip Bileşenleri Kullanma

Savunmasız bileşenleri kullanma

Çevreyi değerlendirmek

Sertleştirme

Güvenilmeyen işlevselliği içe aktarma

JavaScript'i içe Aktarma

Örnek olay - British Airways veri ihlali

Örnek olay - Equifax veri ihlali

Güvenlik açığı yönetimi

OWASP İlk On (Bölüm II)

Injection

Injection prensipleri

Injection saldırıları

SQL Injection

En iyi SQL Injection uygulamaları

Kod yerleştirme

OS komut Injection için en iyi uygulama

Runtime.exec () kullanma

ProcessBuilder'ı kullanma

Örnek olay - Shellshock

Örnek olay - Shopify'da RCE'ye giden şablon yerleştirme

En iyi Injection uygulamaları

Bozuk Kimlik Doğrulama

Oturum yönetimi

CSRF en iyi uygulamaları

XML Harici Varlıkları (XXE)

DTD ve varlıklar

Varlık genişletme

Harici Varlık Saldırısı (XXE)

Siteler Arası Komut Dosyası (XSS)

Siteler arası komut dosyası yazmanın temelleri

Siteler arası komut dosyası türleri

Örnek olay - Fortnite hesaplarında XSS

XSS koruması en iyi uygulamaları

İlk 10'un Ötesinde Web Uygulama Güvenliği

İstemci tarafı güvenliği

Tabnabbing

Çerçeve korumalı alanı

Yaygın Yazılım Güvenliği Zayıf Yönleri

Giriş doğrulama

Giriş doğrulama ilkeleri

Tamsayı işleme sorunları

İmzalı numaraları temsil etmek

Tamsayı görselleştirme

Tamsayı taşması

Lab - Tamsayı taşması

Java'da imzalı / imzasız kafa karışıklığı

Tamsayı kesme

En iyi uygulamalar

Diğer sayısal problemler

Sıfıra bölüm

Kayan noktalı sayılarla çalışma

Güvenli olmayan yansıma

Doğrulamadan yansıtma

Güvenli olmayan yerel kod

Yerel kod bağımlılığı

Yerel kodla başa çıkmak için en iyi uygulamalar

Güvenlik özellikleri

Java platform güvenliği

Java programlama dili ve çalışma zamanı ortamı

Güvenlik ve güvenlik yazın

JRE'nin güvenlik özellikleri

ClassLoader ve BytecodeVerifier

Java'da uygulama düzeyinde erişim denetimi

Rol tabanlı erişim kontrolü

Java kodunu ve uygulamalarını koruma

Kod kalitesi

Yapıcılar ve yıkıcılar

Sınıf başlatma döngüleri

Lab - Başlatma döngüleri

Yayınlanmamış kaynak

Finalize () yöntemi - en iyi uygulamalar

Nesne yönelimli programlama güçlükleri

Serileştirme

Hassas verileri seri hale getirme
Serileştirme en iyi uygulamaları
Güvenilmeyen akışların serisini kaldırma
En iyi uygulamaları seriyi kaldırma
ReadObject'i kullanma
Mühürlü nesneler
Seri durumdan arındırmaya bak
Mülkiyet Odaklı Programlama (POP)

Güvenli kodlama ilkeleri

Matt Bishop'tan sağlam programlamanın ilkeleri
Saltzer ve Schröder'in güvenli tasarım ilkeleri

Diğer kaynaklar ve okumalar

Java kaynakları