

Security Testing Java Web Applications Eğitimi

Eğitim Hakkında

Güvenlik Testi Java Web Uygulamaları eğitimi, katılımcılara Java kodunda bulunan web uygulaması güvenlik sorunlarını nasıl belirleyeceklerini ve düzelteceklerini öğretir. Katılımcıların, test sırasında olası sorunları nasıl bulacaklarını ve güvenlik testi metodolojisini, tekniklerini ve araçlarını Java programlarına nasıl uygulayacaklarını öğrenirler. Ana hattaki A1, A2 vb. Referanslar, OWASP İlk 10'daki belirli güvenlik açıklarına atıfta bulunur .

Neler Öğreneceksiniz

Temel siber güvenlik kavramlarına aşina olmayı,

Web uygulaması güvenlik sorunlarını anlamayı,

OWASP İlk On Unsurunu Analiz Etmeyi,

Web uygulama güvenliğini Java bağlamına yerleştirmeyi,

Güvenlik testi metodolojisini ve yaklaşımlarını anlamayı,

Yaygın güvenlik testi tekniklerine ve araçlarına aşina olmayı.

Eğitim İçeriği

Siber Güvenlik Temelleri

Güvenlik nedir?

Tehdit ve risk

Siber güvenlik tehdit türleri

Güvensiz yazılımın sonuçları

OWASP İlk 10 (Bölüm 1)

A1: Injection

Injection prensipleri

Injection saldırıları

SQL Injection

En iyi SQL Injection uygulamaları

Kod yerleştirme

En iyi Injection uygulamaları

A2: Bozuk Kimlik Doğrulama

Kimlik doğrulama temelleri

Kimlik doğrulama zayıflıkları
Web'de sahtecilik
Zayıf kimlik doğrulama testi
Örnek olay - PayPal 2FA atlama
Parola yönetimi
Güvenlik Testi
Güvenlik testi ile işlevsel test karşılaştırması
Manuel ve otomatik yöntemler
Güvenlik testi metodolojisi
Güvenlik testi - hedefler ve metodolojiler
Güvenlik testi süreçlerine genel bakış
Varlıkları tanımlama ve derecelendirme
Tehdit modelleme
Güvenlik testi yaklaşımları
OWASP İlk 10 (Bölüm 2)

A3: Hassas Verilerin İfşası

Bilgi maruziyeti
Çıkarılan veriler ve toplama yoluyla maruz kalma
Örnek olay - Strava verilerinin açığa çıkması

A4: XML Harici Varlıklar (XXE)

DTD ve varlıklar
Varlık genişletme
Harici Varlık Saldırısı (XXE)

A5: Bozuk Erişim Kontrolü

Erişim kontrolünün temelleri
URL erişimini kısıtlayamama
Yetkilendirme sorunları için test etme
Dosya yükleme

A6: Yanlış Güvenlik Yapılandırması

Yapılandırma ilkeleri
Konfigürasyon yönetimi
Java ile ilgili bileşenler - en iyi uygulamalar

A7: Siteler Arası Komut Dosyası (XSS)

Siteler arası komut dosyası yazmanın temelleri
Siteler arası komut dosyası türleri
XSS koruması en iyi uygulamaları

A8: Güvensiz Seri Durumdan Çıkarma

Serileştirme ve seriyi kaldırma zorlukları
Güvenilmeyen akışların serisini kaldırma
Seri kaldırma en iyi uygulamaları
ReadObject'i kullanma
Mühürlü nesneler
Seri durumdan arındırmaya bak
Güvenli olmayan seriyi kaldırma testi

Mülkiyet Odaklı Programlama (POP)

Y9: Bilinen Güvenlik Açıklarına Sahip Bileşenleri Kullanma

Savunmasız bileşenleri kullanma
Güvenilmeyen işlevselliği içe aktarma
JavaScript'i içe Aktarma
Örnek olay - British Airways veri ihlali
Güvenlik açığı yönetimi

A10: Yetersiz Günlük Kaydı ve İzleme

Günlük kaydı ve izleme ilkeleri
Yetersiz günlük kaydı
Facebook'ta düz metin parolalar
En iyi uygulamaları günlüğe kaydetme
Java için OWASP güvenlik günlük kaydı kitaplığı

İlk 10'un Ötesinde Web Uygulama Güvenliği

İstemci tarafı güvenliği
Tabnabbing
Ters sekme
Çerçeve korumalı alanı
Çapraz Çerçeve Komut Dosyası (XFS) saldırısı
Clickjacking
Bir tıklamayı ele geçirmenin ötesinde tıklama hırsızlığı
Clickjacking koruması için en iyi uygulamalar
Tıklama korsanlığını önlemek için CSP kullanma

Güvenlik Test Teknikleri ve Araçları

Kod analizi
Kod incelemesinin güvenlik yönleri
Statik Uygulama Güvenliği Testi (SAST)
Statik analiz araçlarını kullanma
Dinamik analiz
Çalışma zamanında güvenlik testi
Penetrasyon testi
Stres testi
Dinamik analiz araçları
Dinamik Uygulama Güvenliği Testi (DAST)
Web güvenlik açığı tarayıcıları
SQL Injection araçları
Proxy sunucuları

Yaygın yazılım güvenliği zayıflıkları

Giriş doğrulama
Kara listeler ve beyaz listeler
Veri doğrulama teknikleri
Ne doğrulanmalı - saldırı yüzeyi
Nerede doğrulanmalı - derinlemesine savunma
Doğrulama - doğrulama ve dönüşümler
Çıktı temizleme

Kodlama zorlukları
Normal ifade ile doğrulama
Güvenli olmayan yansıma
Doğrulamadan yansıma

Güvenli kodlama ilkeleri

Matt Bishop'tan sağlam programlamanın ilkeleri
Saltzer ve Schröder'in güvenli tasarım ilkeleri
Ve şimdi ne olacak?
Yazılım güvenlik kaynakları ve daha fazla okuma
Java kaynakları
Güvenlik testi kaynakları