
.NET Web Uygulama Güvenliđi

.NET Web Uygulama Güvenliđi eđitimi, katılımcılara kötü niyetli bir kullanıcı rolünü oynamalarına izin vererek web uygulama güvenliđinin temellerini öğretir.

Hedefler:

- Web uygulaması güvenlik açıklarından yararlanmak için kullanılan araçlara ve tekniklere aşinalık kazanmayı
- Örnek bir web uygulamasına karşı profil oluşturma görevleri ve sızma testi gerçekleştirmeyi
- Çeşitli girdi ekleme biçimleri ve bunlarla ilişkili karşı önlemler hakkında bilgi edinmeyi
- IIS'yi güvenli ASP.NET web uygulamalarını barındıracak şekilde yapılandırma konusunda uygulamalı deneyim kazanmayı
- Çeşitli şifreleme ve imzalama biçimlerini keşfetmek için .NET Framework'teki şifreleme sınıflarını kullanmayı
- Birkaç farklı kimlik doğrulama yöntemi hakkında bilgi edinin ve bunların avantajlarını ve dezavantajlarını incelemeyi

Topics:

- Giriş
 - Bir Siber Saldırının İş Üzerindeki Etkileri
 - Sektör İstatistikleri
 - Popülerlik Faktörleri
 - Web Uygulaması Zayıf Noktalar
- HTTP İncelemesi

- Giriş
- Başlıklar
- Fiiller
- Durum
- Talepler
- Web Hata Ayıklama Proxy'leri
- Protokol Analizörleri
- OWASP İlk On
 - Giriş
 - Güncel İlk On Liste
- Profil oluşturma
 - Giriş
 - Kurumsal Profil Oluşturma
 - Altyapı Profili Oluşturma
 - Ayak İzi, Tarama ve Parmak İzi
 - Uygulama Profili Oluşturma
 - Anonimlik
 - Karşı önlemler
- Kriptografi
 - Giriş
 - Simetrik Şifreleme

- Asimetrik Şifreleme
- Kriptografik Hash Fonksiyonları
- Anahtarlı Karma Mesaj Kimlik Doğrulama Kodları (HMAC)
- Dijital imzalar
- Dijital Sertifikalar
- SSL, TLS ve HTTPS
- Injection
 - Giriş
 - SQL Enjeksiyonu
 - ASP.NET ViewState
 - Fazla Gönderi
 - Karşı önlemler
- Kimlik Doğrulamanın Temelleri
 - Giriş
 - Kimlik Bilgisi Türleri
 - İki Faktörlü Kimlik Doğrulama
 - IIS Kimlikleri
 - IIS Anonim Kimlik Doğrulaması
- Kimlik Doğrulama Protokolleri
 - HTTP Temel Kimlik Doğrulaması
 - HTTP Özet Kimlik Doğrulaması

- Windows Kimlik Doğrulaması
- İstemci Sertifikası Kimlik Doğrulaması
- Form Kimlik Doğrulaması
- Önceden Paylaşılan Anahtar Kimlik Doğrulaması
- Token Tabanlı Kimlik Doğrulama
- OAuth 2.0
 - Giriş
 - Roller
 - İstemci Türleri
 - Hibe Türleri
 - Erişim Jetonu
 - OpenID Connect
 - IdentityServer
- ASP.NET Kimliği
 - Giriş
 - OWIN
 - Visual Studio Şablonları
- Yetki
 - Giriş
 - NTFS Yetkilendirmesi
 - URL Bazlı Yetkilendirme

- Uygulama Düzeyinde Yetkilendirme
- Uygulama Güvenlik Açıkları
 - Oturum Yönetimi
 - Siteler Arası Komut Dosyası (XSS)
 - Doğrudan Nesne Referansları
 - Hassas Verilerin İfşası
 - İşlev Seviyesi Erişim Kontrolü
 - Siteler Arası İstek Sahteciliği (CSRF)
 - Platform Güvenlik Açıkları
 - Yönlendirmeleri ve Yönlendirmeleri Doğrulama
- IIS Hardening
 - Saldırı Yüzey Alanının Azaltılması
 - En Az Ayrıcalık için Yapılandırma
 - İşleyici Eşlemeleri
 - ISAPI ve CGI
 - MIME Türleri
 - IP Adresi ve Etki Alanı Kısıtlamaları