OWASP Top 10 Güvenlik Zafiyetleri Raporu

A01:2021 – Kırık Erişim Kontrolü (Broken Access Control)

Zafiyet: Kullanıcıların yetkileri dışında işlem yapmasına izin veren güvenlik açığıdır.

Neden Kaynaklanır? Yanlış yapılandırılmış erişim kontrolleri, rol bazlı erişim kontrollerinin yetersiz uygulanması.

Nasıl Önlenir? Güçlü erişim kontrol mekanizmaları, her isteğin yetkilendirilmesi.

A02:2021 – Kriptografik Güvenlik Açıkları (Cryptographic Failures)

Zafiyet: Verilerin güvenli bir şekilde şifrelenmemesi.

Neden Kaynaklanır? Zayıf veya yanlış kriptografik algoritmaların kullanımı.

Nasıl Önlenir? Güçlü şifreleme algoritmalarının kullanılması, doğru anahtar yönetimi.

A03:2021 – Enjeksiyon (Injection)

Zafiyet: Kötü niyetli kodların, veri tabanı sorgularına, işletim sistemi komutlarına veya diğer işlemlere enjekte edilmesi.

Neden Kaynaklanır? Kullanıcı girdilerinin doğru şekilde işlenmemesi.

Nasıl Önlenir? Parametrik sorguların kullanılması, kullanıcı girdilerinin doğru bir şekilde doğrulanması.

A04:2021 – Güvensiz Tasarım (Insecure Design)

Zafiyet: Uygulamanın güvenlik zayıflıkları içerecek şekilde tasarlanması.

Neden Kaynaklanır? Güvenlik gereksinimlerinin doğru belirlenmemesi.

Nasıl Önlenir? Güvenlik tasarım incelemelerinin yapılması, tehdit modelleme.

A05:2021 – Güvensiz Yazılım ve Bileşen Kullanımı (Security Misconfiguration)

Zafiyet: Yanlış yapılandırılmış sunucu, veritabanı veya uygulama.

Neden Kaynaklanır? Varsayılan yapılandırmaların değiştirilmemesi.

Nasıl Önlenir? Güvenli yapılandırma ayarlarının yapılması, düzenli yapılandırma denetimleri.

A06:2021 – Güvensiz Bileşenler Kullanımı (Vulnerable and Outdated Components)

Zafiyet: Güvensiz veya güncel olmayan üçüncü taraf bileşenlerin kullanımı.

Neden Kaynaklanır? Yazılım bileşenlerinin düzenli olarak güncellenmemesi.

Nasıl Önlenir? Güncellemelerin düzenli olarak yapılması, yazılım bileşenlerinin güvenlik açısından değerlendirilmesi.

A07:2021 – Kimlik Doğrulama ve Yetkilendirme Güvenlik Açıkları (Identification and Authentication Failures)

Zafiyet: Kullanıcı kimlik doğrulama süreçlerinin zayıf olması.

Neden Kaynaklanır? Zayıf şifre politikaları, çok faktörlü kimlik doğrulamanın kullanılmaması.

Nasıl Önlenir? Güçlü şifre politikaları, çok faktörlü kimlik doğrulama kullanımı.

A08:2021 – Yazılım ve Veri Bütünlüğü Güvenlik Açıkları (Software and Data Integrity Failures)

Zafiyet: Yazılım veya verilerin yetkisiz kişiler tarafından değiştirilmesi.

Neden Kaynaklanır? Kod bütünlüğü kontrollerinin eksikliği.

Nasıl Önlenir? Kod imzalama, dosya bütünlüğü kontrol mekanizmalarının kullanılması.

A09:2021 – Güvenlik Loglama ve İzleme Eksiklikleri (Security Logging and Monitoring Failures)

Zafiyet: Güvenlik olaylarının yeterince izlenmemesi veya loglanmaması.

Neden Kaynaklanır? Yetersiz loglama ve izleme yapılandırmaları.

Nasıl Önlenir? Detaylı loglama, gerçek zamanlı izleme ve uyarı sistemlerinin kurulması.

A10:2021 – Sunucu Tarafı Talep Sahteciliği (Server-Side Request Forgery - SSRF)

Zafiyet: Uygulamanın, saldırgan tarafından yönlendirilen istekleri sunucu tarafında gerçekleştirmesi.

Neden Kaynaklanır? Kullanıcı tarafından sağlanan URL'lerin güvenli şekilde işlenmemesi.

Nasıl Önlenir? Sunucu tarafında yapılan isteklerin kontrol edilmesi, dış kaynakların erişiminin sınırlandırılması.