- A01: Bozuk Erişim Kontrolleri
- Güvenlik Açığı Nedir?
- Kullanıcıların yetkisiz kaynaklara veya işlemlere erişebildiği bir durum. Bu durum kullanıcıların yetki seviyelerini aşmalarına ve diğer kullanıcıların verilerine veya sistemin hassas bölümlerine erişmelerine neden olabilir.
- Buna ne sebep olur?
    - Yanlış yapılandırılmış veya eksik yetkilendirme politikaları
    - Erişim kontrollerinin düzgün şekilde uygulanmaması
- Türler ve Kısa Açıklamalar:
    - Yatay ayrıcalık yükseltme: Kullanıcıların diğer kullanıcıların verilerine kendi yetki seviyelerinde erişmesi.
    - Dikey ayrıcalık yükseltme: Kullanıcıların kaynaklara kendilerinden daha yüksek yetkilerle erişmesi.
- Örnek:
- Yetkili olmayan bir kullanıcının yönetici paneline doğrudan bir URL aracılığıyla erişmesi.
- e. Nasıl Önlenir?
    - Tüm kaynaklar için sıkı erişim kontrolü politikaları uygulayın.
    - Uygun yetkilendirme ve denetim süreçlerini otomatikleştirin.

- A02: Şifreleme Hataları
- Güvenlik Açığı Nedir?
- Kritik verilerin (şifreler, kredi kartı bilgileri, kişisel veriler vb.) yetersiz veya yanlış şifrelenmesiyle sonuçlanan güvenlik açıklarıdır. Bu, hassas verilerin çalınmasına yol açabilir.
- Buna ne sebep olur?
- Zayıf veya yanlış şifreleme algoritmaları kullanma
    - Verilerin şifrelenmeden saklanması veya iletilmesi
- Türler ve Kısa Açıklamalar:
    - Yanlış SSL/TLS yapılandırması: HTTPS trafiği yeterince güvenli değil.
    - Yanlış veya eksik şifreleme: Kritik verilerin düz metin olarak saklanması veya iletilmesi.
- Örnek:
- Kullanıcı şifrelerinin MD5 gibi güvenli olmayan algoritmalarla karıştırılması.
- e. Nasıl Önlenir?
    - Güçlü, modern şifreleme algoritmaları (AES, RSA) kullanın.
    - Tüm hassas verileri şifreleyin ve güvenli anahtar yönetimi sağlayın.

- A03: Enjeksiyon Güvenlik Açıkları
- Güvenlik Açığı Nedir?
- Bunlar, bir uygulamanın komutlarına kötü amaçlı veriler dahil edilerek sistemin manipüle edilmesine olanak sağlayan güvenlik açıklarıdır. SQL, OS, LDAP, XML enjeksiyonları gibi çeşitli türleri vardır.
- Neden ortaya çıkıyor?
    - Kullanıcı girişinin doğrulanamaması
    - Doğrudan kullanıcıdan alınan girişin komutlara dahil edilmesi
- Türleri ve Kısa Açıklamaları:
    - SQL Enjeksiyonu: SQL sorgularına kötü amaçlı kod ekleyerek veritabanına zarar vermek.
    - İşletim Sistemi Enjeksiyonu: Sistemde komutların yürütülmesine izin veren güvenlik açığı.
- Örnek Kod:
- SELECT * FROM users WHERE id = '1' or'1'='1';
- e. Nasıl Önlenir?
    - Hazırlanmış ifadeleri kullanın.
    - Giriş doğrulama ve temizleme süreçlerini uygulayın.

- A04: Güvenli Olmayan Tasarım
- Güvenlik Açığı Nedir?
- Yazılım güvenlik açısından zayıf bir tasarıma sahiptir ve bu nedenle saldırılara karşı savunmasız hale gelmektedir.
- Neden ortaya çıkıyor?
    - Güvenlik testlerinin eksikliği
    - Güvenlik gereksinimlerinin dikkate alınmaması
- Türleri ve Kısa Açıklamaları:
    - Yetersiz tehdit modellemesi: Uygulama tehditlerinin doğru analiz edilememesi.
    - Kötü mimari kararlar: Güvensiz mimari yapıların kullanılması.
- e. Nasıl Önlenir?
    - Güvenli yazılım geliştirme uygulamalarını hayata geçirin.
    - Yazılım tasarımının ilk aşamalarında güvenlik gereksinimlerini göz önünde bulundurun.

- A05: Güvenlik Yanlış Yapılandırması
- Güvenlik Açığı Nedir?
- Uygulamanın, sunucunun veya veri tabanının yanlış veya yetersiz yapılandırılması nedeniyle ortaya çıkan güvenlik açıkları.
- Buna ne sebep olur?
- •Varsayılan ayarları kullanma
    - Gereksiz özelliklerin etkin bırakılması
- Türler ve Kısa Açıklamalar:
    - Geliştirme ortamının yanlış yapılandırılması: Geliştirme ortamlarının üretim ortamında açık bırakılması.
    - Güvenlik yamalarını güncellememek: Eski veya güncel olmayan sistemleri kullanmak.
- e. Nasıl Önlenir?
    - Güvenli yapılandırma kılavuzlarını izleyin.
    - Tüm sistem ve yazılımlar düzenli olarak güncellenmelidir.

- A06: Hassas Bilgilerin İfşa Edilmesi (Hassas ve Eski Bileşenler)
- Güvenlik Açığı Nedir?
- Uygulamanın eski, savunmasız veya güncelliğini yitirmiş yazılım bileşenlerini kullanması durumu.
- Buna ne sebep olur?
    - Eski sürümleri kullanmaya devam etmek
    - Üçüncü taraf bileşenlerini düzenli olarak güncellememek
- Türler ve Kısa Açıklamalar:
    - Eski kütüphanelerin kullanılması: Güvenlik açıkları içeren eski kütüphanelerin entegrasyonu.
    - Yama uygulamamak: Yazılım bileşenlerine gelen güvenlik yamalarını yüklememek.
- e. Nasıl Önlenir?
    - Düzenli güvenlik taramaları gerçekleştirin ve bileşenleri güncel tutun.
    - Üçüncü taraf yazılımlarını dikkatle izleyin.

- A07: Tanımlama ve Kimlik Doğrulama Hataları
- Güvenlik Açığı Nedir?
- Kullanıcı kimlik doğrulama ve yetkilendirme süreçlerindeki zayıflıklar, saldırganların kimlikleri taklit etmesine veya yetkisiz eylemler gerçekleştirmesine olanak tanıyabilir.
- Buna ne sebep olur?
    - Zayıf şifre politikaları
    - Çok faktörlü kimlik doğrulamanın olmaması
- Türler ve Kısa Açıklamalar:
    - Zayıf şifreleme