OWASP Top 10

Hazırlayan: Yavuz Selim Yılmaz

1- A01:2021 – Broken Access Control

a) Zafiyet Nedir?

Erişim kontrolü kullanıcıların kendi yetki alanları dışındaki eylemleri gerçekleştirmelerini engeller. Erişim kontrolündeki eksiklikler bilgilere izinsiz erişilmesine, verilerin izinsiz şekilde düzenlenmesine veya silinmesine ve kullanıcının normalde yapamaması gereken işlemleri yapması gibi sorunlara yol açar.

b) Neden Kaynaklanır?

• Sadece belirli rollere sahip kullanıcıların(örn: admin) erişebilmesi gereken kaynakların herkese açık olması

• Kullanıcıların URL parametrelerini değiştirerek izinleri olmayan verilere erişebilmeleri

•API tarafında POST, PUT ve DELETE requestleri için erişim kontrolü olmaması

c) Nasıl Önlenir?

• Herkese açık olan kaynaklar dışındaki kaynakları varsayılan olarak erişilemez yapın.

• Erişim kontrolü mekanizmaları geliştirip uygulamanın gerekli kısımlarında kullanın.

• Web sunucusu klasör listelemesini devre dışı bırakın ve önemli dosyaların (örn: .git) web dizininde bulunmadığından emin olun.

2- A02:2021 – Cryptographic Failures

a) Zafiyet Nedir?

Bu güvenlik açığı kriptografi mekanizmalarının yanlış veya eksik kullanımını kapsamaktadır. Kriptografik hatalar, hassas verilerin ifşa olmasına, verilerin bütünlüğünün bozulmasına, ve yetkisiz erişimlere yol açabilir.

b) Neden Kaynaklanır?

• Verilerin şifrelenmeden aktarılması

• Eski veya zayıf şifreleme algoritmalarının kullanılması

• Güvensiz protokollerin kullanılması (örn: https yerine http kullanılması)

c) Nasıl Önlenir?
• Uygulama tarafından verileri sınıflandırın. Hangi verilerin hassas olduğunu belirleyin.

• Hassas verileri kriptografi algoritmaları ile şifreleyin.

• Hassas verileri taşımak için FTP ve SMTP gibi eski protokolleri kullanmayın.

• Şifreleri Argon2, scrypt, bcrypt veya PBKDF2 gibi güçlü kriptografi fonksiyonlarını kullanarak depolayın.

3- A03:2021 – Injection

a) Zafiyet Nedir?
Bu güvenlik açığı saldırgan tarafından web uygulamasına gönderilen zararlı verilerin uygulamada beklenmeyen davranışlara yol açmasıdır.

b) Neden Kaynaklanır?
• Kullanıcı input'unun uygulama tarafından doğrulanmaması, filtrelenmemesi veya temizlenmemesi

•Zararlı verilerin hassas kayıtları ayrıştırmak için ORM(object-relational mapping) arama parametrelerinde kullanılması

c) Türleri
• SQL Injection: Zararlı SQL ifadelerinin filtrelenmeden çalıştırılması durumunda oluşan bu güvenlik açığı veritabanı içeriğinin ifşalanması, veritabanın silinmesi gibi sorunlara yol açabilir.

• NoSQL Injection: Zararlı NoSQL sorgularının filtelenmeden çalıştırılması durumunda oluşur. SQL Injection'un yol açtığı sorunlara benzer sorunlara yol açar.

• OS Command Injection: Saldırganın uygulamayı barındıran sunucuda keyfi komut çalıştırabilmesine izin verir. Sonuç olarak tüm sunucu bilgileri tehlikeye girebilir.

d) Nasıl Önlenir?
• Kullanıcı input'unu filteleyin ve zararlı olabilecek sorgulardan temizleyin

• SQL Injection durumunda kayıtların toplu ifşasını önlemek için LIMIT ve diğer SQL kontrol sorgularını kullanın

• ORM (object-relational mapping) kütüphanelerini kullanarak verileri yönetin

4- A04:2021 – Insecure Design

a) Zafiyet Nedir?
Bu güvenlik açığı web uygulamalarındaki kontrol mekanizmasının eksik veya verimsiz kullanılması sonucu açığa çıkar.

b) Neden Kaynaklanır?

• Uygulama geliştirilirken güvenlik gereksinimlerinin dikkate alınmaması

• Potansiyel tehditlerin yeterince analiz edilmemesi

• Güvenlik açıklarının tespit edilmesi için yeterince test yapılmaması

c) Nasıl Önlenir?
• Güvenlik gereksinimlerinin belirlenmesi ve uygulama geliştirilirken dikkate alınması
• Potansiyel tehditler analiz edilerek tehdit modellemesi oluşturulması
• Penetrasyon testi gibi güvenlik testlerinin düzenli olarak yapılması

5- A05:2021 – Security Misconfiguration

a) Zafiyet Nedir?
Bu güvenlik açığı sistemlerin güvenlik ayarlarının yanlış veya eksik yapılandırılması sonucu ortaya çıkar.

b) Neden kaynaklanır?
• Gereksiz özelliklerin kurulmuş veya aktifleştirilmiş olması (örn: gereksiz portlar, servisler, hesaplar veya yetkiler)

• Şifreleri değiştirilmemiş varsayılan hesapların kullanılması

• Hata mesajlarının sistemle ilgili gizli bilgileri sızdırması

c) Nasıl Önlenir?

• Kullanılmayan özellikleri devre dışı bırakın

• Varsayılan kimlik bilgilerini değiştirin

• Tüm sistemin güvenlik ayarlarını düzenli olarak gözden geçirin

6- A06:2021 – Vulnerable and Outdated Components

a) Zafiyet Nedir?
Bu güvenlik açığı uygulamalarda kullanılan üçüncü parti bileşenlerin güvenlik açıklarına sahip olması veya güncel olmamasıdır.

b) Neden Kaynaklanır?
• Bileşenlerin en son sürümlerinin kullanılmaması

• Üçüncü parti bileşenlerde bilinen güvenlik açıklarının bulunması

• Bileşenlerin yeni sürümlerinin sistemle uyumlu olmaması nedeniyle güncellemelerin yapılamaması

c) Nasıl Önlenir?
• Kullanılan bileşenleri düzenli olarak güncelleyin
• Üçüncü parti bileşenlere düzenli olarak güvenlik taramaları yapın
• Kullanılmayan bileşenleri kaldırın

7- A07:2021 – Identification and Authentication Failures

a) Zafiyet Nedir?
Bu güvenlik açığı uygulamadaki kimlik doğrulama ve kullanıcı tanımlama mekanizmalarındaki zayıflıklardır.

b) Neden Kaynaklanır?
• Zayıf veya bilindik şifrelerin kullanılması (örn: “admin/admin”, “Password1”)
• Çok yönlü kimlik doğrulamanın kullanılmaması
• Kullanıcı oturumlarının düzgün şekilde saklanmaması

c) Nasıl Önlenir?
• Kullanıcılar güçlü şifreler kullanmaya zorlanmalı
• Kimlik doğrulama sürecinde çok yönlü kimlik doğrulama kullanılmalı
• Kullanıcı oturumları düzgün şekilde saklanmalı, gerektiğinde güvenli bir şekilde sonlandırılmalı

8- A08:2021 – Software and Data Integrity Failures

a) Zafiyet Nedir?
Bu güvenlik açığı bütünlük(integrity) ihlallerine karşı koruma sağlayamayan kod ve altyapılar ile ilgilidir.

b) Neden Kaynaklanır?
• Uygulamanın güvenilir olmayan kaynaklardan gelen bileşenlere bağımlı olması
• Yazılım güncellemelerinin güvenilir olmayan kaynaklardan indirilmesi
• Verilerin bütünlüğünün doğrulanamaması

c) Nasıl Önlenir?
• Yazılım veya verilerin beklenen kaynaktan geldiğini ve değiştirilmediğini doğrulamak için dijital imzalar veya benzer mekanizmalar kullanın

• Npm veya Maven gibi kütüphanelerin güvenli depo'ları(repository) kullandığından emin olun

• Verilerin bütünlüğünü doğrulayan mekanizmalar oluşturun

9- A09:2021 – Security Logging and Monitoring Failures

a) Zafiyet Nedir?
Bu güvenlik açığı sistemde yeterli loglama ve monitörleme yapılmadığında oluşur. Sistemde meydana gelen ihlallerin tespit edilememesi ile sonuçlanır.

b) Neden Kaynaklanır?

• Kritik olaylar ve güvenlik ihlalleri ile ilgili logların yeterince tutulmaması

• Şüpheli aktiviteler veya güvenlik ihlalleri durumunda uygun uyarıların oluşturulmaması

c) Nasıl Önlenir?
• Uygulamadaki kritik olaylar ve güvenlik ihlalleri ile ilgili detaylı loglar tutun
• Şüpheli aktiviteleri tespit etmek için logları düzenli olarak inceleyin
• Şüpheli aktiviteler ve güvenlik ihlalleri için uyarı mekanizmaları kurun

10- A10:2021 – Server-Side Request Forgery (SSRF)

a) Zafiyet Nedir?
Bu güvenlik açığı web uygulaması kullanıcıdan gelen URL'yi doğrulamadan dış bir kaynağa istek göndermesi durumunda ortaya çıkar.

b) Neden Kaynaklanır?
• Kullanıcı tarafından girilen URL'lerin yeterince doğrulanmaması veya filtrelenmemesi

• Uygulamanın gönderilen isteklerin hedeflerini veya içeriklerini kontrol etmemesi

c) Nasıl Önlenir?

• Kullanıcıdan gelen girdileri dikkatlice doğrulayın ve filtreleyin

• Sunucunun yalnızca güvenilir kaynaklara istek gönderebilmesini sağlayın

• Sunucunun hassas hizmetlere erişimini sınırlandırın