Broken Access Control

Bir uygulamanın kullanıcıların erişim yetkilerini yanlış şekilde yönetmesine denir. Saldırganın normalde yetkisi olmayan içeriklere veya işlevlere erişmesine olanak tanır.

Neden Kaynaklanır?

Genellikle erişim kontrolü politikalarının eksik ya da hatalı uygulanmasından kaynaklanır.

Cryptographic Failures

Kriptografinin uygulanmasında ki hatalar ile ilgilidir. Güncel olmayan şifreleme algoritmaları kullanımı, yanlış şifreleme anahtarı yönetimi veya hassas veriler için şifreleme eksikliği neden olur. Bununla birlikte verilerin gizliliği sağlanamaz.

Injection

Kullanıcıdan alınan verileri kontrol edilmeden ve önlem almadan kullanılması sonucu komut olarak çalıştırılması yada sorguya dahil edilmesi durumundan ortaya çıkar. eritabanı sorgularının veya uygulama kodlarının mainpule edilmesine neden olur.

-Insecure Design

Güvenlik gereksinimlerinin yeterince dikkate alınmaması nedeni ile olduğunu anladım ama tam olarak çözemedim.

Security Misconfiguration

Yanlış yapılandırmalar veya varsayılan ayarların değiştirilmemesi, güvenlik açıklarına yol açabilir. Bu tür hatalar, uygulamanın veya sistemin gereksiz yere risk altında kalmasına neden olabilir.

Neden Kaynaklanır?

Güvenlik yapılandırmalarının doğru yapılmaması veya güncellemelerin ihmal edilmesi.

Nasıl Önlenir?

Tüm güvenlik ayarları dikkatlice yapılandırılmalı ve düzenli olarak kontrol edilmelidir. Gereksiz özellikler devre dışı bırakılmalı ve sistemler güncel tutulmalıdır

Vulnerable and Outdated Components

Güncellenmemiş veya desteklenmeyen yazılım bileşenlerinin kullanılması, güvenlik açıklarına neden olabilir.

Neden Kaynaklanır?

Yazılım bileşenleri düzenli olarak güncellenmeli ve güvenlik yamaları zamanında uygulanmalıdır.

Identification and Authentication Failures

Kimlik doğrulama ve oturum yönetimi hataları, kullanıcıların kimliklerini çalmasına veya yetkisiz oturumlara erişim sağlamasına neden olabilir.

Zayıf parola politikaları, güvenli olmayan kimlik doğrulama mekanizmaları ve oturum yönetiminde yapılan hatalar bu tür zafiyetlere yol açar.

Güçlü parola politikaları uygulanmalı, çok faktörlü kimlik doğrulama (MFA) kullanılmalı ve oturum yönetimi güvenli bir şekilde yapılmalıdır.

Software and Data Integrity Failures

Yazılım veya veri bütünlüğünün sağlanamaması, kötü amaçlı yazılım yüklenmesi veya verilerin manipüle edilmesiyle sonuçlanabilir.

Yazılım veya veri bütünlüğünün sağlanamaması, kötü amaçlı yazılım yüklenmesi veya verilerin manipüle edilmesiyle sonuçlanabilir.

Verilerin veya yazılımın yetkisiz değişikliklere karşı korunmaması ve kaynak kodlarının güvenliğinin ihmal edilmesi.

Security Logging and Monitoring Failures

Güvenlik olaylarının yeterince izlenmemesi ve kaydedilmemesi, saldırıların fark edilmemesine neden olabilir.

Yetersiz loglama, olay izleme eksiklikleri ve bu logların düzenli olarak incelenmemesi.

Güvenlik olaylarının izlenmesi ve kaydedilmesi için etkili loglama araçları kullanılmalı, loglar düzenli olarak incelenmeli ve anormallikler tespit edilmelidir.

Server-Side Request Forgery

Bu zafiyet, saldırganların, sunucunun diğer sunuculara istek göndermesini manipüle ederek, sunucu üzerinden yetkisiz istekler gönderebilmesine neden olur.

Sunucu tarafında kullanıcıdan gelen isteklerin yeterince doğrulanmaması ve filtrelenmemesi bu zafiyetin temel sebebidir.

Kullanıcıdan gelen istekler dikkatlice doğrulanmalı, filtrelenmeli ve sunucu tarafı istekleri kısıtlanmalıdır.