# JSON Web Token (JWT) Kullanımı Raporu

Bu projede kullanıcı kimlik doğrulama sürecinde **JSON Web Token (JWT)** teknolojisi kullanılmaktadır. JWT, kullanıcı oturumlarını yönetmek ve kimlik doğrulamasını güvenli bir şekilde gerçekleştirmek için modern ve yaygın bir yöntemdir. Bu raporda, projemizde JWT'nin nasıl üretildiği, nasıl saklandığı ve hangi güvenlik önlemleri alındığı açıklanacaktır.

# JWT’nin Kullanım Amacı

* Kullanıcı doğrulaması sonrasında kimlik bilgilerini güvenli bir şekilde temsil etmek.
* Yetkilendirme işlemlerinde (kullanıcıya özel içerek veya API erişimlerinde) kullanılmak üzere istemcinin kimliğini sormak.
* Stateless yapı sayesinde sunucu tarafında oturum bilgisi tutmadan kimlik kontrolü yapılmasını sağlamak.

# JWT Servisi

Projede JwtService sınıfı, IJwtService arayüzünü implemente eden bir servistir. Bu servis, kullanıcı kimliğine göre JWT üretmektedir. Servis yapılandırması:

1. **Token Üretimi**
   * GenerateToken(string userId) metodu ile kullanıcı kimliğine göre token üretilmektedir.
   * Token oluşturulurken aşağıdaki bilgiler (claims) token içine gömülmektedir:
     + NameIdentifier: Kullanıcının benzersiz ID’si.
     + Jti: Token’in benzersiz ID’si.
2. **Güvenlik Detayları**
   * Token HMAC SHA256 algoritmasıyla imzalanır.
   * İmza için kullanılan gizli anahtar Secrets.JwtSecretKey ile erişilmektedir ve UTF8 ile kodlanmaktadır.
   * Token’in geçerlilik süresi, JwtSettings:ExpiryMinutes konfigürasyon ayarından(appsettings.json) alınır ve DateTime.UtcNow.AddMinutes() ile hesaplanır.
   * Issuer ve Audience bilgileri de JwtSettings altındaki konfigürasyonlardan alınır.

# Token Saklama ve Güvenlik

1. **Secure HTTP-Only Cookie**
   * Üretilen JWT, istemciye doğrudan gösterilmez. Bunun yerine, response ile birlikte HTTP-Only ve Secure niteliklerine sahip bir çerez olarak gönderilir. Böylece:
     + Token, tarayıcıda JavaScript ile erişilemez (XSS koruması).
     + Token sadece HTTPS bağlantılarında iletilir (MITM saldırılarına karşı koruma).
   * Bu yapı sayesinde, frontend tarafında tkoen yönetimi yapılmasına gerek kalmadan oturum güvenli bir şekilde sürdürülür.