**GAZİ ÜNİVERSİTESİ TEKNOLOJİ FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

**BMT216 WEB ARAYÜZ GELİŞTİRME DERSİ**

**PROJE RAPORU**

**Proje Başlığı:** Parola Güçlülük Kontolü

**Teslim Tarihi:** 22.05.2025

**Dersi Veren Öğretim Elemanı:** Dr. Esra SÖĞÜT

**Öğrenci Numarası ve Ad Soyad Bilgileri:**

1. Alper Yıldırım: 23181616031
2. Erdem Çakır: 23181616008
3. Yağmur Damla Kara: 23181616056
4. Enes Özmekik: 23181616021
5. **AMAÇ**

Bu projenin temel amacı, kullanıcıların oluşturdukları parolaların güvenlik seviyelerini gerçek zamanlı olarak analiz ederek, onları daha güçlü ve güvenli parolalar oluşturmaya teşvik etmektir. Günümüzde zayıf parolaların birçok güvenlik ihlaline yol açtığı göz önüne alındığında, kullanıcıların parola oluşturma sürecinde rehberlik edilmesi büyük önem taşımaktadır. Bu web uygulaması, kullanıcının girdiği parolanın uzunluğunu, büyük/küçük harf kullanımı, rakam ve özel karakter içerip içermediğini değerlendirerek parola gücünü belirler ve bunu görsel bir şekilde kullanıcıya sunar. Ayrıca, kullanıcı deneyimini artırmak adına karanlık/aydınlık tema seçenekleri ve parola görünürlüğünü değiştirme gibi işlevsel özellikler de sunulmuştur.

Bu proje ile hem kullanıcıların güvenlik farkındalığının artırılması hem de daha güvenli dijital ortamların desteklenmesi hedeflenmektedir.

1. **KULLANILAN TEKNOLOJİLER**

Proje, HTML, CSS, JavaScript ve Bootstrap gibi modern web teknolojileri kullanılarak geliştirilmiştir. Kullanıcı arayüzü responsive yapıda tasarlanmış ve tema desteği (karanlık/açık mod) ile kullanıcı deneyimi artırılmıştır.

1. **ARAYÜZ TASARIMI VE EKRAN GÖRÜNTÜLERİ**

* **Sayfa Yapısı**

Uygulama tek sayfa (single-page) yapıda tasarlanmıştır. Kullanıcı giriş yaptığı anda karşısına çıkan sayfa üzerinden parola analizi işlemleri gerçekleştirilmektedir. Arayüz; giriş kutusu, gerçek zamanlı parola kontrol listesi ve renkli bir güç çubuğundan oluşmaktadır.

* **Renk Seçimi**

Arka plan için mavi, gri ve beyaz tonlar tercih edilerek göz yormayan bir görünüm sağlanmıştır.

Parola gücünü ifade eden çubukta:

* Zayıf parola için kırmızı,
* Orta düzey için turuncu,
* Güçlü parola için yeşil renkler kullanılmıştır.

Gece modu (dark mode) desteği ile kullanıcılar arayüzü tercihlerine göre karanlık temada kullanabilmektedir.

* **Yazı Tipi ve Stilleri**

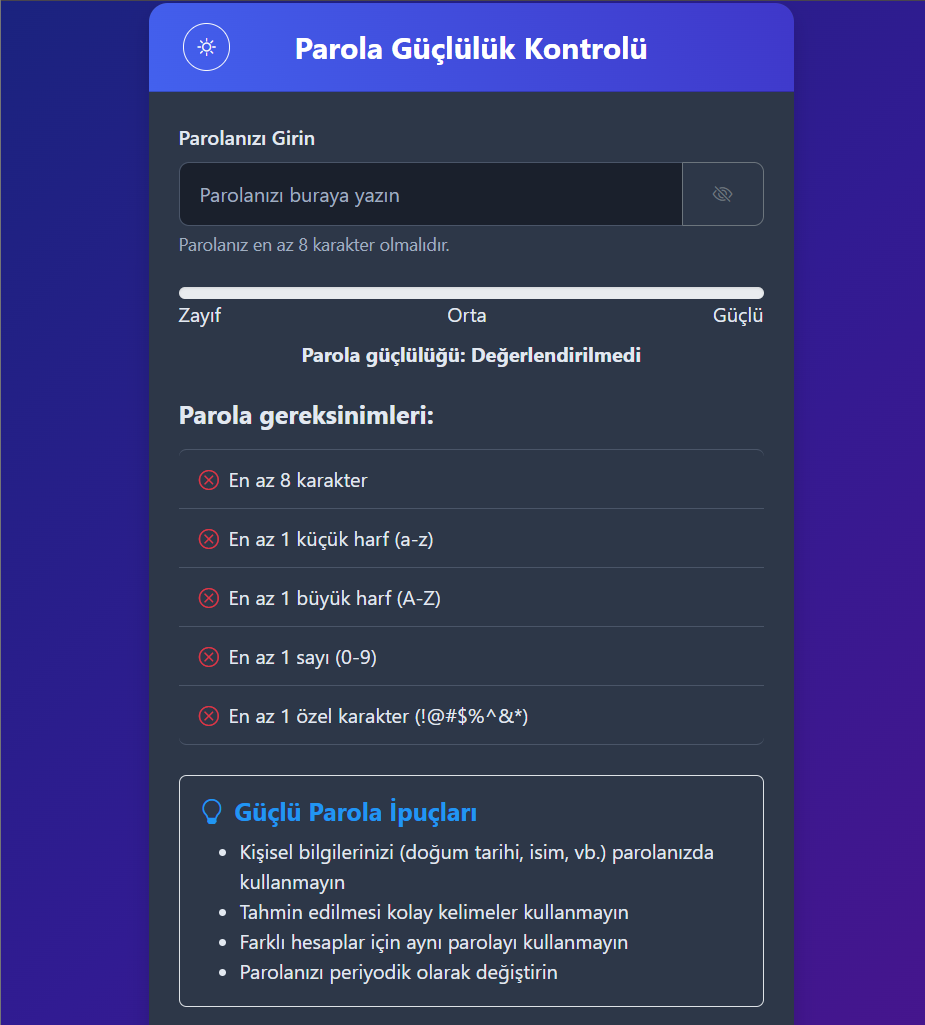
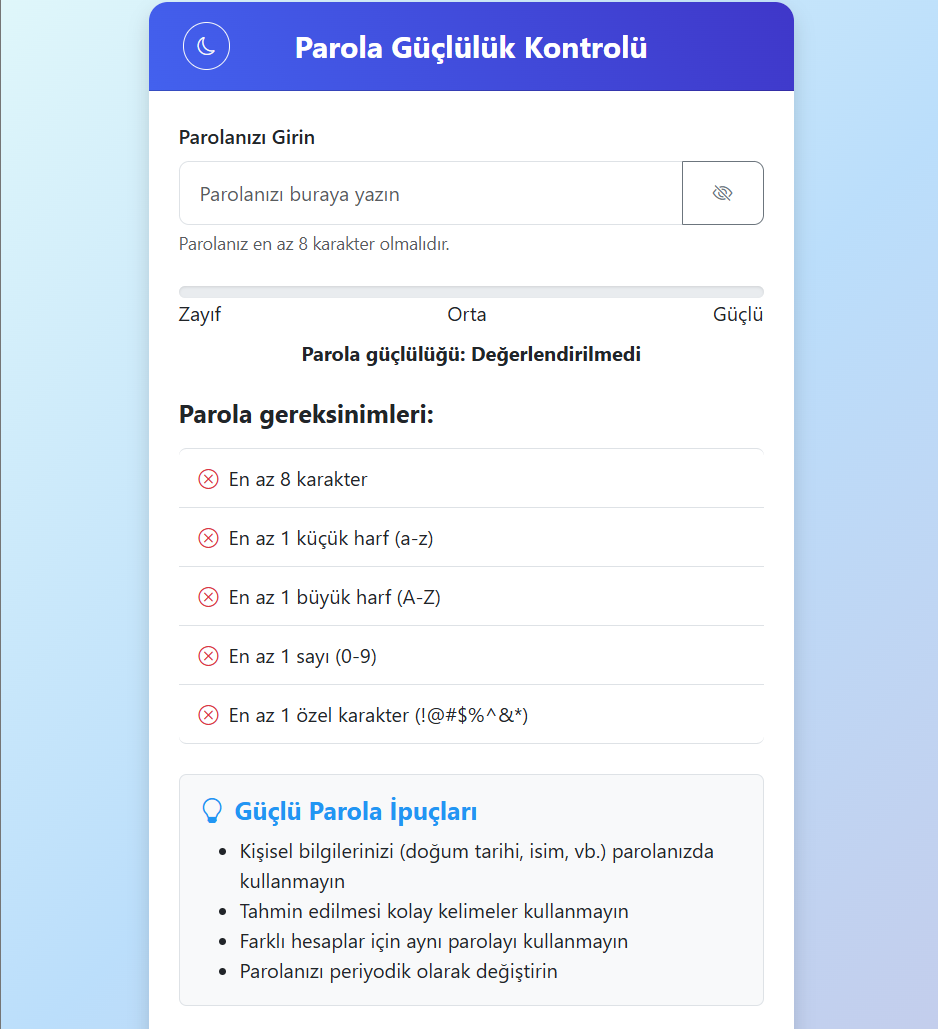
 Yazı tipi olarak modern ve sade bir görünüm sağlayan **Segoe UI** ve **Arial** gibi sistem fontları tercih edilmiştir.

 Bilgilendirici metinlerde daha küçük punto kullanılırken, başlıklar daha büyük ve dikkat çekici şekilde biçimlendirilmiştir.

### Mobil Uyumluluk

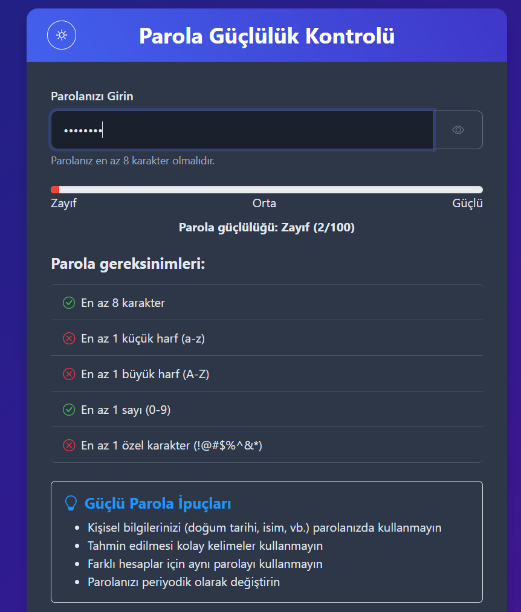
Tasarımda Bootstrap 5 kütüphanesinden yararlanılarak responsive yapı sağlanmıştır. Sayfa tablet ve telefon gibi farklı cihazlarda sorunsuz biçimde çalışmaktadır. Tüm bileşenler mobil ekranlara göre yeniden hizalanmakta ve kullanılabilirlik korunmaktadır.

* **EKRAN GÖRÜNTÜLERİ**

Ana Sayfa Görünümü açık ve koyu modda: 

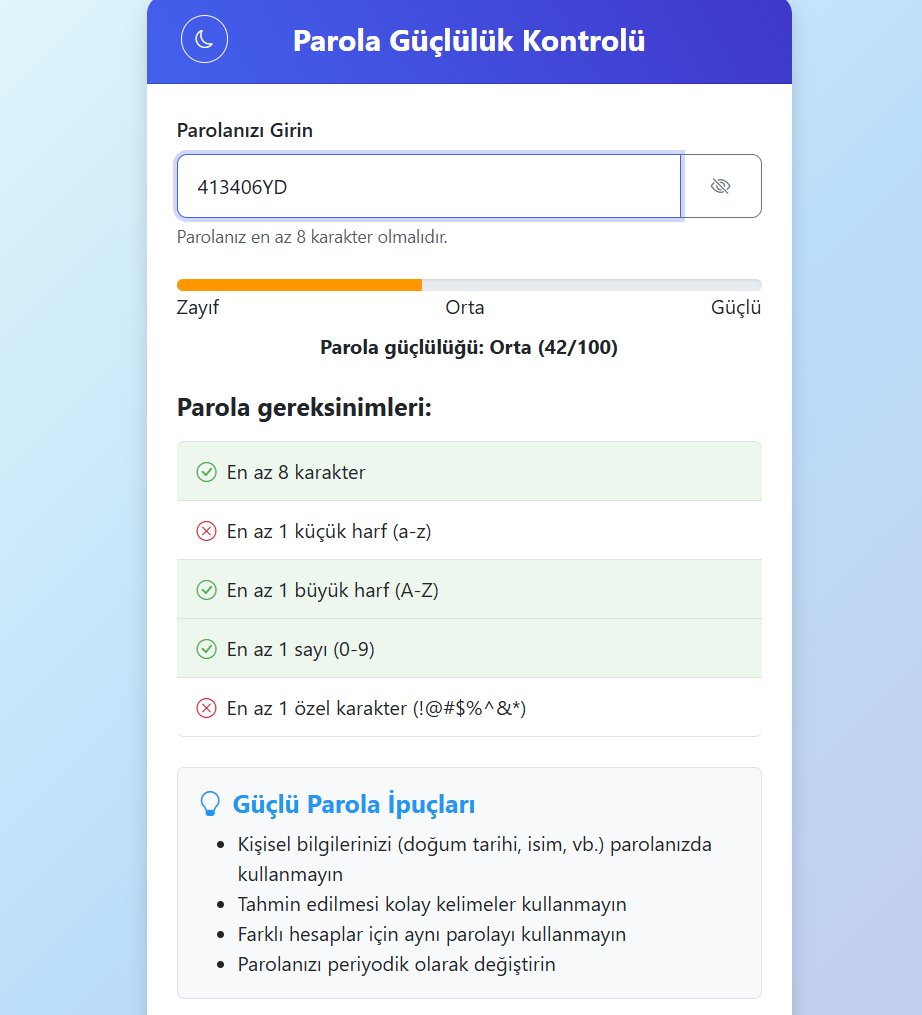
Kullanıcının şifresini girdiği, anlık analiz sonuçlarını görebildiği ana ekrandır. Sağ altta anlık parola gücünü gösteren çubuk, sol altta ise karşılanan gereksinimlerin listesi yer almaktadır.

Zayıf Parola Durumu:



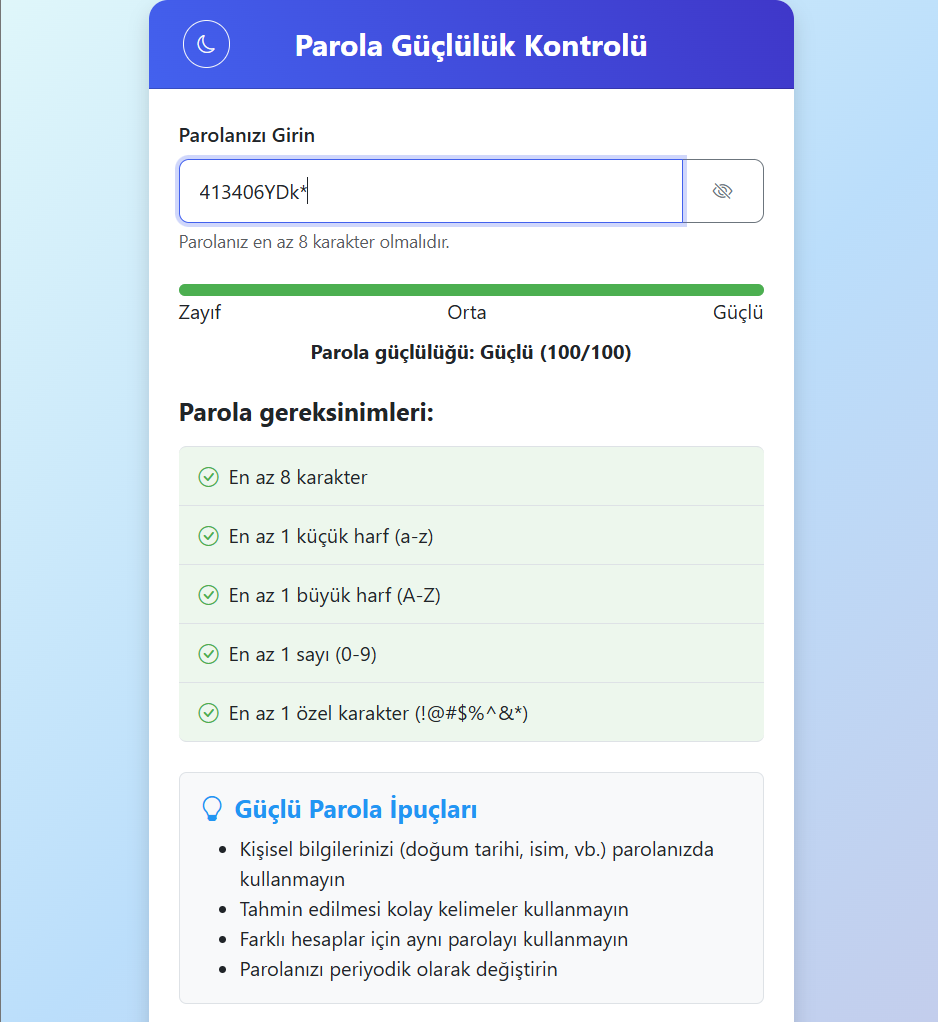
Giriş yapılan parolanın yetersiz olduğu bir senaryoyu göstermektedir. Güç çubuğu kırmızı renkte görünür ve gereksinimlerin çoğu sağlanmamıştır.

Orta Seviye Parola Durumu:



Bazı gereksinimlerin karşılandığı, ancak parolanın hala güvenlik açısından yeterli olmadığı bir durumu temsil eder. Güç çubuğu turuncu renge döner.

Güçlü Parola Durumu:



Tüm güvenlik gereksinimlerinin sağlandığı bir senaryodur. Parola çubuğu yeşil renge ulaşır ve kullanıcıya güçlü bir parola oluşturduğu bilgisi verilir.

1. **PROJE ÖZELLİKLERİ**

Uygulama aşağıdaki işlevsel özellikleri kullanıcıya sunmaktadır:

* **Gerçek Zamanlı Parola Analizi:**  
  Kullanıcı parola girişini yaparken, parola anlık olarak analiz edilir ve güvenlik seviyesi belirlenir.
* **Parola Güç Göstergesi:**  
  Parolanın zayıf, orta veya güçlü olduğunu görsel bir çubuk ile kullanıcıya gösterir.
* **Gereksinim Kontrol Listesi:**  
  Girilen parolanın küçük harf, büyük harf, rakam, özel karakter içerip içermediği ve minimum uzunluk koşullarını sağlama durumu kontrol edilir ve listelenir.
* **Renk Kodlamalı Uyarı Sistemi:**  
  Parola güvenliği seviyesi; kırmızı (zayıf), turuncu (orta), yeşil (güçlü) renkleriyle kullanıcıya net bir şekilde sunulur.
* **Responsive (Mobil Uyumlu) Arayüz:**  
  Uygulama tüm ekran boyutlarında (mobil, tablet, masaüstü) sorunsuz çalışacak şekilde responsive olarak tasarlanmıştır.
* **Karanlık Mod (Dark Mode) Desteği:**  
  Kullanıcılar arayüzü isteğe bağlı olarak açık veya koyu tema arasında geçiş yaparak kullanabilir.
* **Bootstrap Tabanlı Modern Tasarım:**  
  Arayüz, kullanıcı deneyimini artırmak için modern görsel bileşenler ve uyumlu stil yapısıyla Bootstrap 5 kullanılarak tasarlanmıştır.
* **Kullanıcı Hatalarına Karşı Anında Geri Bildirim:**  
  Eksik ya da zayıf parolalar girildiğinde kullanıcıya anında görsel uyarılar sunulur.

1. **KARŞILAŞILAN ZORLUKLAR VE ÇÖZÜMLER**

Proje geliştirme sürecinde karşılaşılan bazı teknik ve tasarımsal sorunlar aşağıda belirtilmiş ve bu sorunlara bulunan çözümler açıklanmıştır:

* **Anlık Parola Analizi Gecikmesi:**  
  Parola yazılırken analiz sonuçlarının gecikmeli olarak güncellenmesi sorunu yaşandı.  
  → Bu sorun input yerine keyup olay dinleyicisi kullanılarak çözüldü. Böylece her tuş basımında analiz işlemi anlık olarak tetiklendi.
* **Parola Güç Göstergesinin Düzensiz Renk Değişimi:**  
  Güç seviyesine göre değişmesi gereken renkli çubuğun her zaman doğru rengi göstermemesi problemi ortaya çıktı.  
  → Durumların sınıflandırılması if-else yapıları ile daha net ayrılarak, her seviyeye özgü sabit renk sınıfları belirlendi ve stil geçişleri düzenlendi.
* **Mobil Uyumluluk Problemleri:**  
  Uygulama küçük ekranlarda taşma ve hizalama sorunları yaşadı.  
  → Bootstrap’ın container, row, col yapıları yeniden düzenlendi, responsive sınıflar (col-md, col-sm) kullanılarak farklı ekran boyutlarına uygun hale getirildi.
* **Minimum Güvenlik Kriterlerinin Net Gösterilememesi:**  
  Kullanıcının hangi güvenlik kriterlerini sağlayıp hangilerini sağlamadığını ayırt etmesi zor oldu.  
  → Her kriterin yanında ✓ veya ✗ işareti gösteren dinamik bir kontrol listesi eklendi. Sağlanan kurallar yeşil, eksik olanlar kırmızı renkte gösterildi.
* **Tema Geçişinde Stil Uyumsuzlukları:**  
  Karanlık ve aydınlık tema arasında geçiş yapılırken bazı metin ve arka plan renkleri uyumsuz kaldı.  
  → CSS değişkenleri (custom properties) tanımlanarak temalar arasında geçişlerde tüm renkler merkezi olarak kontrol edilebilir hale getirildi.
* **Parola Skorunun Gerçekçi Hesaplanmaması:**  
  İlk başta parola güvenliği sadece karakter türü sayısına göre değerlendirilirken gerçekçi bir sonuç vermiyordu.  
  → Skor sistemi geliştirilerek parolanın uzunluğu, karakter çeşitliliği ve özel karakterlerin konumları da skora dahil edildi.

1. **SONUÇ**

Bu proje kapsamında geliştirilen web tabanlı parola güvenliği analiz uygulaması, kullanıcıların parola oluştururken anlık olarak geri bildirim almasını sağlayarak daha güvenli parolalar üretmelerine yardımcı olmayı hedeflemiştir. Uygulama; parola uzunluğu, karakter çeşitliliği (büyük harf, küçük harf, rakam, özel karakter) ve genel yapıya göre analiz yaparak parolayı zayıf, orta veya güçlü olarak sınıflandırmaktadır.

**Başarılı Yönler:**

* Kullanıcı dostu, sade ve anlaşılır bir arayüz tasarlanmıştır.
* Anlık analiz ve görsel geri bildirimlerle kullanıcıya rehberlik sağlanmıştır.
* Kriter bazlı kontrol listesi sayesinde kullanıcı, eksiklerini doğrudan görebilmektedir.
* Temaya uygun renk geçişleri ve mobil uyumluluk sağlanmıştır.

**Geliştirilebilir Yönler:**

* Parola analiz algoritması daha gelişmiş güvenlik metrikleri (örneğin, sözlük tabanlı zayıf parola kontrolü) ile desteklenebilir.
* Şu an sadece istemci taraflı çalışan sistem, sunucu tarafında da kontrol yaparak daha güvenli hale getirilebilir.
* Kullanıcı geçmişine veya önerilen güçlü parolalara dair destek eklenebilir.

**Gelecekte Eklenmesi Planlanan Özellikler:**

* Parola geçmişi saklama ve analiz özeti sunma
* En yaygın kullanılan zayıf parolalarla karşılaştırma
* CAPTCHA ve benzeri güvenlik öğeleriyle bütünleşme
* Çok dilli destek ile farklı kullanıcı gruplarına hitap etme

Sonuç olarak proje, temel hedeflerine ulaşmış ve kullanıcıların parola güvenliği konusunda bilinçlenmesine katkı sağlayacak işlevsel ve etkili bir araç olarak başarıyla tamamlanmıştır.