**Şifre Güvenilirliğini Ölçen ve Rastgele Şifre Üreten Web Sayfası**

**(GitHub)**

**Latife YILMAZ-200106206002**

**Aysu YİĞİT-211106206002**

**GİRİŞ**

Bulut bilişim dersi kapsamında hazırlanan bu proje, kullanıcıların zayıf şifreler kullanması nedeniyle hesaplarının ele geçirilmesine yönelik ciddi bir riski ortadan kaldırmayı hedeflemektedir. Proje kapsamında, kullanıcılara rastgele şifreler üretilip önerilecek ve bu web sayfası GitHub'a yüklenerek bulut ortamına taşınacaktır. Kullanıcıların güçlü ve güvenli şifreler oluşturabilmeleri için rehberlik sağlanacak ve kullanıcı dostu bir arayüz geliştirilecektir. Bu arayüz, şifrelerin uzunluk, büyük-küçük harf, sayı ve sembol gibi faktörlere odaklanarak güçlü şifrelerin oluşturulmasını sağlayacaktır.

Ayrıca, Zxcvbn kütüphanesi kullanılarak girilen şifrelerin güvenilirliği değerlendirilecek ve kullanıcıların şifrelerinin güvenilirlik düzeyini, tahmini şifre kırma süresini hesaplayan bir araç ile değerlendirmeleri sağlanacaktır. Proje, kullanıcıların rastgele şifreler üretmelerini ve alternatif şifreler oluşturmalarını sağlayacak bir sistem sunarak, şifre oluşturma süreçlerini iyileştirmeyi amaçlamaktadır.

Bu proje, bulut tabanlı GitHub ortamında saklanarak depolanacak ve böylece kullanıcılara her yerden erişim imkanı sağlanacaktır. Bu şekilde, kullanıcıların dijital güvenliklerini artırmaları ve potansiyel risklere karşı bilinçlenmeleri sağlanacaktır.

**Projenin Aşamaları:**

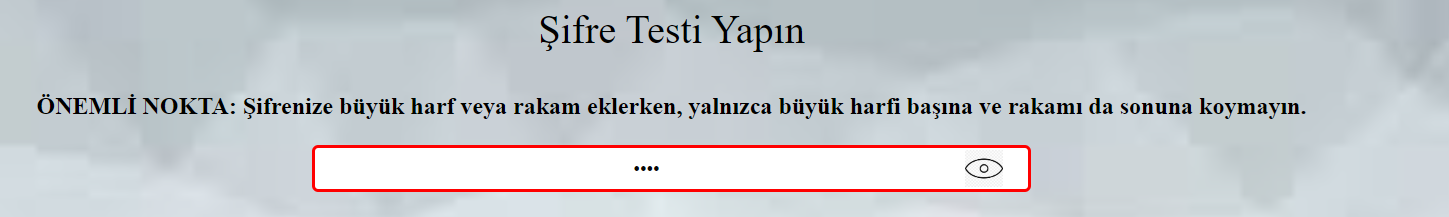
**1.Adım: Şifre Gösterme/Gizleme:**

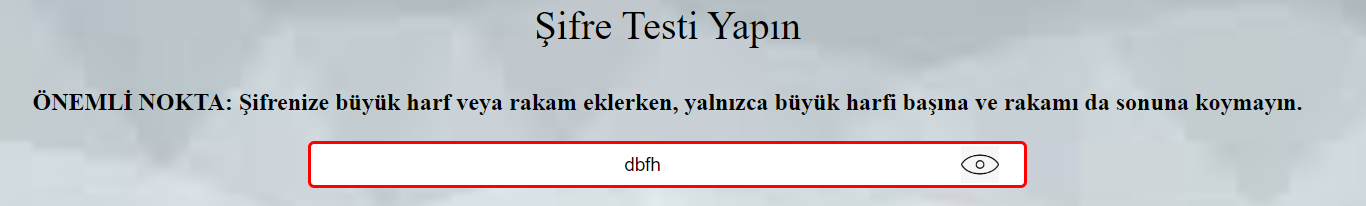
toogle() fonksiyonu, kullanıcının şifreyi gösterip gizlemesini sağlar. Kullanıcı, göz simgesine tıkladığında şifrenin görünürlüğü değişir. Bu işlev, kullanıcının şifresini yazarken yanlışlıkla hatalı karakterler eklemesini önlemek için tasarlanmıştır. Ayrıca, kullanıcıların şifrelerini hatırlamalarına yardımcı olur ve doğru girişi sağlamalarına yardımcı olur.

**Kod Yapısı:**



**Web Kısmı:**





**2.Adım: Şifre Uyarıları ve Şifre Güvenilirliği Değerlendirme Mekanizması:**

Bu arayüz, bir kullanıcının girdiği şifrenin güvenlik seviyesini kontrol eden bir mekanizmayı uygular. Kullanıcının girdiği şifre, büyük harf, küçük harf, rakam ve sembol içeriyorsa, bu kriterleri karşıladığına dair renkli göstergeler verilir. Her bir şart için ayrı bir kontrol yapılır.

**Büyük ve Küçük Harf Kontrolü:** Girilen şifrede hem büyük hem de küçük harf bulunup bulunmadığı kontrol edilir. Eğer şifre hem büyük hem de küçük harf içeriyorsa, ilgili alanların (HTML'de muhtemelen metin veya giriş kutuları) rengi yeşile dönüştürülür; aksi halde siyah olur.

 **Rakam Kontrolü:** Girilen şifrede en az bir rakam bulunup bulunmadığı kontrol edilir. Eğer şifre bir rakam içeriyorsa, ilgili alanın rengi yeşile dönüştürülür; aksi halde siyah olur.

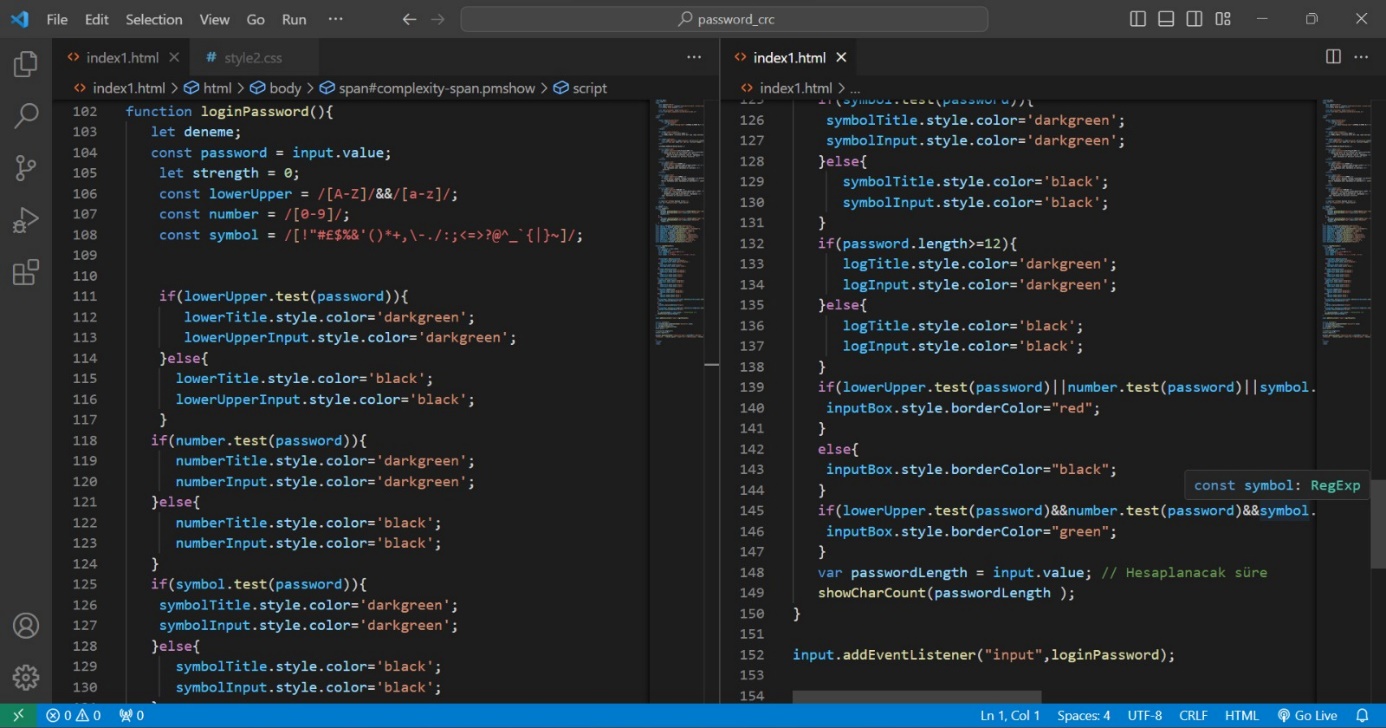
 **Sembol Kontrolü:** Girilen şifrede en az bir sembol bulunup bulunmadığı kontrol edilir. Eğer şifre bir sembol içeriyorsa, ilgili alanın rengi yeşile dönüştürülür; aksi halde siyah olur.

 **Uzunluk Kontrolü:** Girilen şifrenin uzunluğu 12 karakter veya daha fazlaysa, ilgili alanın rengi yeşile dönüştürülür; aksi halde siyah olur.

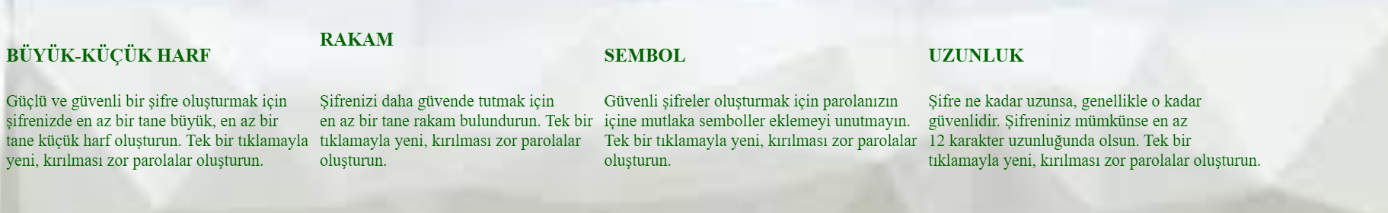
 **Büyük/Küçük Harf ve Rakam Zorunluluğu:** Şifrenin hem büyük/küçük harf, hem de rakam içermesi gerekiyorsa, girdi kutusunun kenar rengi kırmızıya dönüştürülür; aksi halde siyah olur.

 **Güçlü Şifre Kontrolü:** Şifrenin büyük/küçük harf, rakam, sembol içerip ve uzunluğu 12 karakter veya daha fazlaysa, girdi kutusunun kenar rengi yeşile dönüştürülür.

**Kod Kısmı:**



**Web Kısmı :**



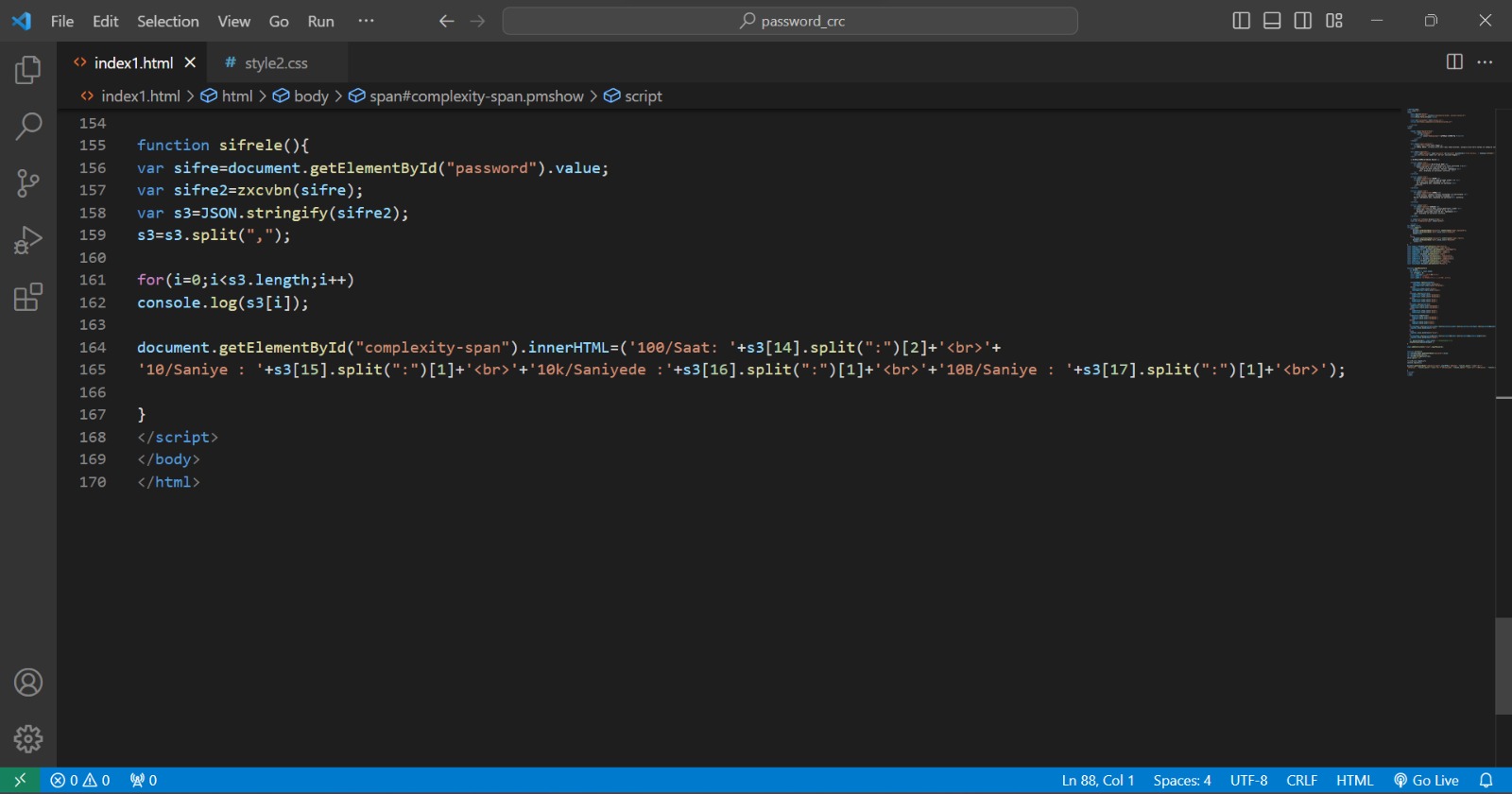
**3.Adım: Şifrenin Kırılma Süresi**

Şifrenin kırılma süresini gösteren bir alanın dinamik olarak güncellenmesi için JavaScript'te Zxcvbn kütüphanesini kullanılmıştır. Bu kütüphane, girilen şifrenin güvenlik düzeyini analiz eder ve şifrenin ne kadar sürede kırılabileceğine dair bir tahminde bulunur.

Örneğin, bir web sitesinde kullanıcı bir şifre oluştururken, Zxcvbn kütüphanesi kullanılarak şifrenin kırılma süresi dinamik olarak hesaplanabilir ve kullanıcıya gösterilebilir. Böylece kullanıcı, daha güçlü bir şifre oluşturmak için gerekli adımları atabilir.

JavaScript index kısmına eklenen Zxcvbn kütüphanesi, şifrenin kırılma süresini hesaplamak ve bu bilgiyi kullanıcıya sunmak için kullanılır. Bu sayede kullanıcılar, şifrelerinin güvenliğini daha iyi anlayabilir ve gerektiğinde daha güçlü şifreler oluşturabilirler.

**zxcvbn Fonksiyonu ile Bilgilerin Konsola Yazdırılma Kodu**



**Web Kısmı:**



**4.Adım: Rastgele Şifre Üretme**

Kullanıcılar istedikleri sayıda şifre oluşturabilmek için giriş alanına sahip olacaklar. “Oluştur” butonuna tıklandığında, JavaScript işlevi devreye girerek kullanıcının belirlediği sayıda rastgele şifre oluşturulması sağlanacak. Bu şifreler, belirli karakter kümesinden (rakamlar, harfler, semboller) rastgele seçilerek oluşturulup, oluşturulan şifreler, kullanıcıların görebileceği bir bölümde görüntülenerek, kullanıcılara alternatif bir şifre önerisinde bulunacak.

**Kod Kısmı:**



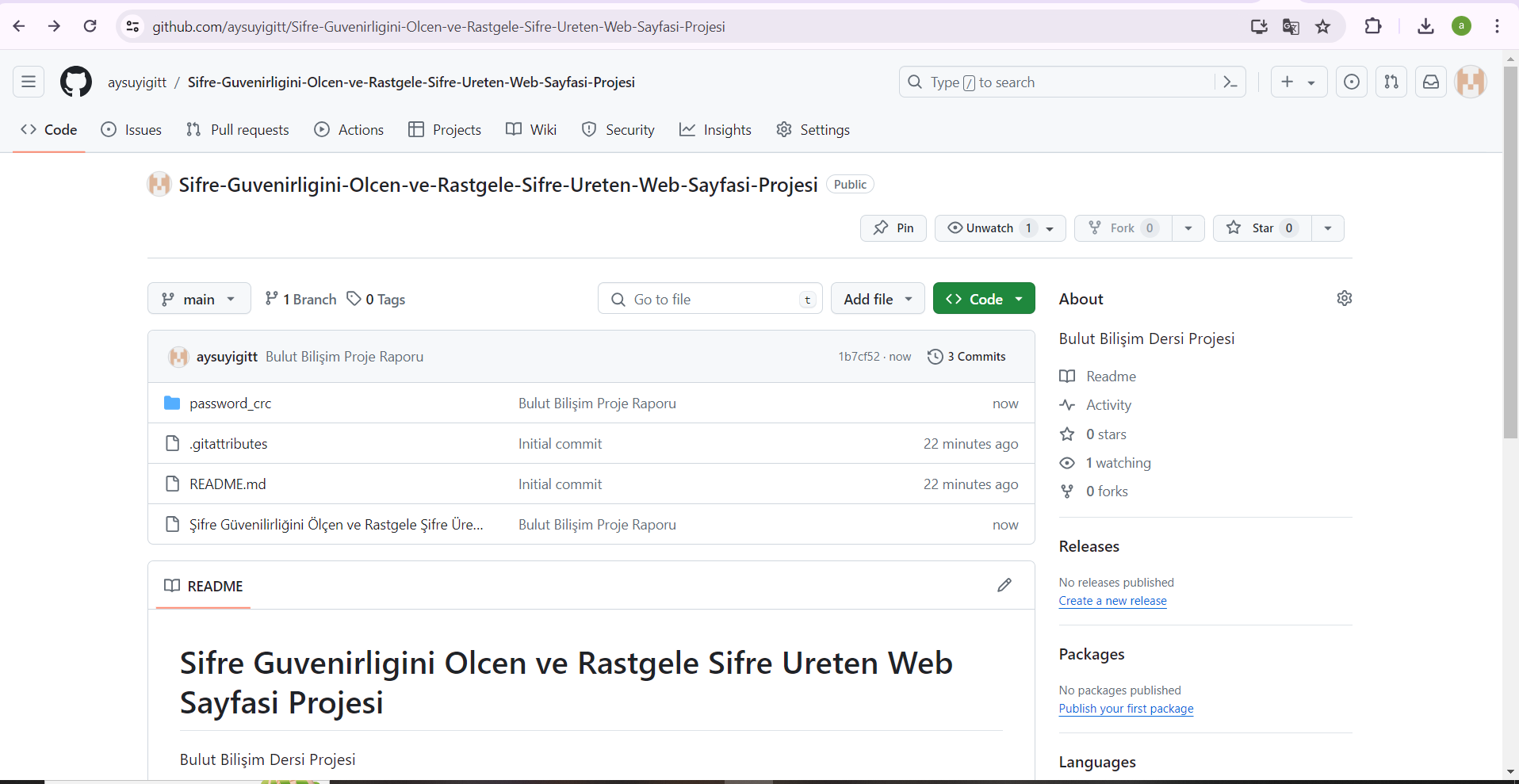
**Web Kısmı:**



**5.Adım: Projenin Bulut Ortamına Entegresi (Github)**

Proje, bulut tabanlı GitHub ortamında saklanarak depolanacak ve böylece kullanıcılara her yerden erişim, yedekleme, güvenlik, dağıtım kolaylığına imkan sağlanacaktır. Ayrıca Github’ın sunduğu araçlar sayesinde projemizin belgelerini ve açıklamalarını düzenlemek de daha kolay olur. Ayrıca Github’a yüklediğimiz web sayfası, farklı kişilerin daha kolay erişebilmesini sağlar.

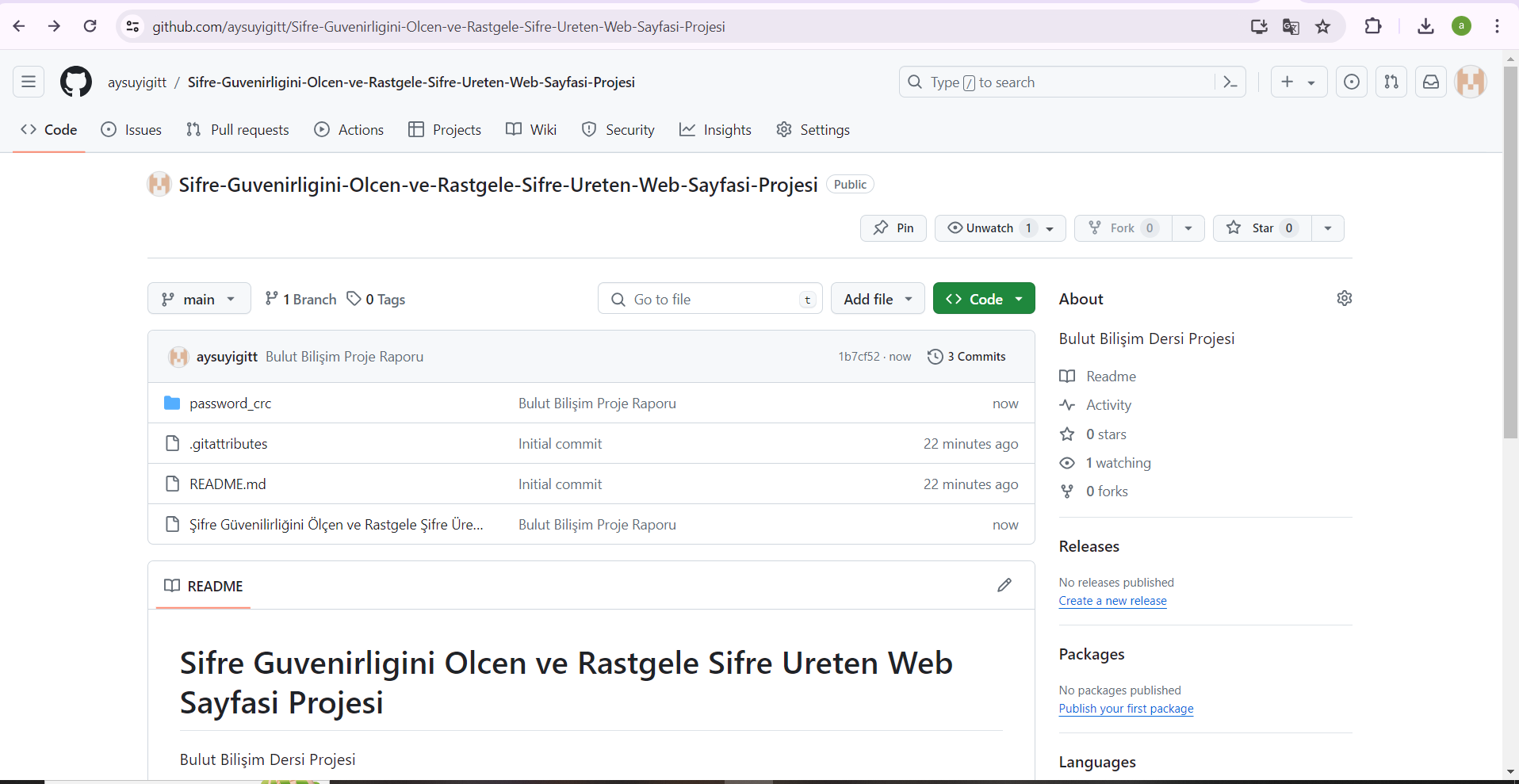
Github Adresi: <https://github.com/aysuyigitt?tab=repositories>

****

**Projenin Web Sayfası:**



**Projenin Github Sayfası:**

****

**SONUÇ**

Bu proje, Web sitesi kullanıcıları güçlü şifreler oluşturmaya teşvik etmek ve şifrelerinin güvenlik düzeyini değerlendirmelerine yardımcı olmak için çeşitli özellikler sunar.

Projenin merkezinde, kullanıcıların girdikleri şifreleri zxcvbn kütüphanesi aracılığıyla analiz etme yeteneği bulunmaktadır. Bu kütüphane, şifrelerin karmaşıklığını ve güvenlik seviyelerini değerlendirir. Kullanıcılar, girdikleri şifrelerin ne kadar güçlü olduğunu ve tahmini kırılma süresini görebilirler.

Kullanıcı dostu arayüz, şifre analizi sonuçlarını anlamayı kolaylaştırır. Analiz sonuçları, büyük harf, küçük harf, rakam, sembol kullanımı ve şifre uzunluğu gibi faktörleri içerir. Kullanıcılar, büyük harf, küçük harf, rakam veya sembol girdiklerinde ilgili alanın vurgulanmasıyla gerekli kriterlerin karşılandığını görsel olarak belirleyebilirler.

Proje ayrıca, kullanıcıların rastgele şifreler oluşturarak güvenlik seviyelerini hemen değerlendirebileceği bir özellik sunar. Bu araç, karmaşık ve tahmin edilmesi zor şifreler üretmeye yardımcı olur.

Kullanıcılara şifre güvenliği konusunda bilgilendirme yapılarak güçlü şifre alışkanlıkları kazanmaları sağlanır. Kullanıcılar, güvenli şifrelerin önemini ve nasıl oluşturulması gerektiğini öğrenerek dijital güvenliklerini artırabilirler.

Proje, GitHub üzerinde barındırılarak bulut ortamına entegre edilmiştir. Bu sayede proje her yerden erişilebilir hale gelmiş, kullanıcılar güncellemeleri kolayca takip edebilir olmuştur. GitHub, projelerin versiyon kontrolünü sağlayarak ekip içi iş birliğini kolaylaştırmakta ve projenin yedeklenmesini sağlamaktadır. Bu entegrasyon, projenin esnekliğini ve sürdürülebilirliğini artırmıştır.