Şiddete Karşı Farkındalık Platformu

Yazılım Gereksinimleri Belirtimi

01.14.2025

Mehmet Said HÜSEYİNOĞLU
Zehra Gökçe YAVUZ
Begüm AKSÜT
Murat Yusuf AKINAY

Revizyon Geçmişi

Tarih	Açıklama	Yazar	Yorumlar
01.14.25	Ver. 1	Mehmet Said Hüseyinoğlu	Proje Tamamlandı

İçindekiler Tablosu

1. **Giriş** 1.1 Amaç
   1.2 Kapsam
   1.3 Tanımlar ve Kısaltmalar
   1.4 Referanslar
   1.5 Genel Bakış
2. **Genel Açıklama** 2.1 Ürün Perspektifi
   2.2 Ürün İşlevleri
   2.3 Kullanıcı Özellikleri
   2.4 Genel Sınırlamalar
   2.5 Varsayımlar ve Bağımlılıkları
3. **Özel Gereksinimler** 3.1 Dış Arabirimi Gereksinimleri
   3.1.1 Kullanıcı Arayüzleri
   3.1.2 Donanım Arabirimleri
   3.1.3 Yazılım Arabirimleri
   3.1.4 İletişim Arabirimleri
   3.2 Fonksiyonel Gereksinimler
   3.3 Kullanım Durumları
   3.3.1 Kullanım Durumu #1: Şiddet Haritası Görüntüleme
   3.3.2 Kullanım Durumu #2: "Şiddete Uğruyor Musunuz?" Formu Doldurma
   3.4 Sınıflar / Nesneler
   3.5 İşlevsel Olmayan Gereksinimler
   3.5.1 Performans
   3.5.2 Güvenilirlik
   3.5.3 Kullanılabilirlik
   3.5.4 Güvenlik
   3.5.5 Sürdürülebilirlik
   3.5.6 Taşınabilirlik
   3.6 Ters Gereksinimler
   3.7 Tasarım Kısıtlamaları
   3.8 Mantıksal Veritabanı Gereksinimleri
   3.9 Diğer Gereksinimler
4. **Analiz Modelleri** 4.1 Aktivite Diyagramları
   4.2 Sequence Diyagramları
   4.3 Veri Akış Diyagramları
   4.4 Durum Geçişi Diyagramları
5. **Değişiklik Yönetimi Süreci** 5.1 Değişiklik Talepleri ve Gönderen Kişiler
   5.2 Değişikliklerin Değerlendirilmesi ve Kabul Edilmesi
   5.3 Değişikliklerin Uygulanması
   5.4 Değişikliklerin İzlenmesi ve Raporlanması
6. **Ekler** 6.1 Ek 1: Proje GitHub Bağlantısı
   6.2 Ek 2: Veritabanı Şema Tasarımı
   6.3 Ek 3: Kullanım Senaryosu Diyagramı
   6.4 Ek 4: Test Senaryoları ve Kabul Kriterleri
   6.5 Ek 5: Kullanıcı Hikayeleri
   6.6 Ek 6: Standartlar ve Referanslar
   6.7 Ek 7: Risk Yönetimi

---

1. Giriş

Bu Yazılım Gereksinimleri Belirtimi (SRS) dokümanı, "Şiddete Karşı Farkındalık Platformu" projesinin gereksinimlerini detaylı bir şekilde tanımlamaktadır. Bu belge, projenin teknik ekibi, paydaşları ve geliştiricileri için bir referans kaynağı olarak hazırlanmıştır.

Platform, toplumda artan şiddet olaylarına karşı farkındalık oluşturmak, şiddet mağdurlarına destek sağlamak ve önleyici tedbirlerin alınmasına katkıda bulunmak amacıyla geliştirilecek web tabanlı bir uygulamadır.

Bu belge:
- Sistemin temel işlevlerini
- Kullanıcı gereksinimlerini
- Sistem sınırlamalarını
- Arayüz gereksinimlerini
- Performans kriterlerini
- Güvenlik önlemlerini
- Veritabanı yapısını
- Sistem mimarisini

detaylı olarak açıklamaktadır.

1.1 Amaç

Bu Yazılım Gereksinimleri Belirtimi (SRS) dokümanının temel amacı, "Şiddete Karşı Farkındalık Platformu" projesinin detaylı teknik ve fonksiyonel gereksinimlerini tanımlamaktır. Bu belge aşağıdaki hedef kitleler için hazırlanmıştır:

Hedef Kitle:
- Yazılım Geliştiriciler: Sistemin nasıl geliştirileceğini ve uygulanacağını anlamaları için
- Proje Yöneticileri: Proje kapsamını, zaman planlamasını ve kaynak ihtiyaçlarını belirlemeleri için
- Test Mühendisleri: Test senaryolarını ve kabul kriterlerini oluşturmaları için
- Sistem Mimarları: Sistem tasarımını ve mimarisini planlamaları için
- Paydaşlar: Projenin teknik gereksinimlerini ve sınırlamalarını anlamaları için

Bu doküman:
1. Platformun temel işlevlerini ve özelliklerini tanımlar
2. Sistem gereksinimlerini açık ve net bir şekilde belirtir
3. Sistemin sınırlarını ve kısıtlamalarını ortaya koyar
4. Teknik ve fonksiyonel gereksinimleri detaylandırır
5. Kalite standartlarını ve beklentilerini belirler
6. Güvenlik ve performans kriterlerini tanımlar

Bu belge, projenin tüm aşamalarında referans olarak kullanılacak ve geliştirme sürecinin temel kılavuzu olacaktır. Belgedeki gereksinimler, projenin başarılı bir şekilde tamamlanması için gerekli tüm bilgileri içermektedir.

1.2 Kapsam

Bu bölüm, Şiddete Karşı Farkındalık Platformu'nun kapsamını, üretilecek yazılım bileşenlerini ve sistemin temel işlevlerini detaylandırmaktadır.

1. Üretilecek Yazılım Bileşenleri:

a) Web Tabanlı Kullanıcı Arayüzü
- Responsive tasarımlı frontend sistemi
- Kullanıcı kimlik doğrulama ve yetkilendirme modülü
- İnteraktif harita görüntüleme sistemi

b) Backend API Sistemi
- RESTful API servisleri
- Veri işleme ve analiz modülü
- Raporlama motoru

c) Veritabanı Yönetim Sistemi
- MongoDB tabanlı NoSQL veritabanı
- Veri yedekleme ve güvenlik sistemi
- Veri analiz araçları

2. Sistemin Yapacakları:

a) Şiddet Olayları Takibi
- Coğrafi konuma dayalı olay kaydı ve görüntüleme
- Olay türlerine göre filtreleme ve sınıflandırma
- İstatistiksel veri analizi ve görselleştirme

b) Kullanıcı Etkileşimi
- Anonim olay bildirimi
- Yardım talep formu oluşturma
- Destek merkezleri ile iletişim kurma

c) Veri Analizi ve Raporlama
- Bölgesel risk analizi raporları
- Dönemsel trend analizleri
- Özelleştirilebilir veri görselleştirme araçları

3. Sistemin Yapmayacakları:
- Kişisel sağlık verileri tutulmayacak
- Adli süreçlere müdahale edilmeyecek
- Kullanıcıların özel bilgileri paylaşılmayacak
- Doğrudan müdahale hizmeti sunulmayacak

4. Uygulama Hedefleri:

a) Teknik Hedefler:
- %99.9 sistem kullanılabilirliği
- 3 saniyeden az sayfa yüklenme süresi
- Eşzamanlı 10,000 kullanıcı desteği
- 256-bit SSL şifreleme ile güvenli veri iletimi

b) Fonksiyonel Hedefler:
- Gerçek zamanlı olay bildirimi ve takibi
- Kullanıcı dostu arayüz (maksimum 3 tıklama ile işlem tamamlama)
- Çoklu dil desteği (Türkçe, İngilizce)
- Otomatik veri yedekleme ve kurtarma

c) İş Hedefleri:
- Şiddet olaylarının %30 daha hızlı raporlanması
- Yardım kaynaklarına erişim süresinin %50 azaltılması
- Farkındalık seviyesinde %40 artış
- Kurumlar arası koordinasyonda %60 iyileştirme

5. Entegrasyon Kapsamı:
- Acil yardım hatları (112, 155, vb.)
- Sosyal hizmet kurumları
- Sivil toplum kuruluşları
- Sağlık kuruluşları
- Adli birimler

1.3 Tanımlar ve Kısaltmalar

Bu bölüm, dokümanda kullanılan teknik terimleri, kısaltmaları ve özel kavramları açıklamaktadır.

Kısaltmalar:
- API (Application Programming Interface): Uygulama Programlama Arayüzü
- SRS (Software Requirements Specification): Yazılım Gereksinimleri Belirtimi
- UI (User Interface): Kullanıcı Arayüzü
- DB (Database): Veritabanı
- REST (Representational State Transfer): Temsili Durum Transferi
- SSL (Secure Sockets Layer): Güvenli Soket Katmanı
- STK: Sivil Toplum Kuruluşu

Terimler:
- Frontend: Kullanıcıların etkileşimde bulunduğu arayüz katmanı
- Backend: Sunucu tarafında çalışan uygulama katmanı
- Responsive Tasarım: Farklı ekran boyutlarına uyum sağlayan tasarım
- Kullanıcı: Platformu kullanan herhangi bir birey veya kurum
- Mağdur: Şiddete maruz kalan kişi
- Olay Kaydı: Sisteme girilen şiddet vakası bildirimi
- Risk Analizi: Şiddet olaylarının bölgesel ve istatistiksel değerlendirmesi

Not: Bu liste, proje süresince gerektiğinde güncellenecek ve genişletilecektir.

1.4 Referanslar

Bu belge, aşağıdaki standartlar, yönetmelikler ve kaynak dokümanlar referans alınarak hazırlanmıştır:

1. Standartlar ve Yönetmelikler:
- IEEE 830-1998, "IEEE Recommended Practice for Software Requirements Specifications"
- ISO/IEC 25010:2011, "Systems and software Quality Requirements and Evaluation (SQuaRE)"
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)
- 5237 Sayılı Türk Ceza Kanunu'nun ilgili maddeleri
- 6284 Sayılı Ailenin Korunması ve Kadına Karşı Şiddetin Önlenmesine Dair Kanun

2. Teknik Dokümanlar:
- MongoDB Veritabanı Tasarım Rehberi v4.4
- Node.js Best Practices Guide 2024
- React.js Dokümantasyonu v18.0
- Google Maps API Dokümantasyonu v3.0
- Web Content Accessibility Guidelines (WCAG) 2.1

3. Kurumsal Kaynaklar:
- T.C. Aile ve Sosyal Hizmetler Bakanlığı İstatistikleri (2023)
- Türkiye İstatistik Kurumu (TÜİK) Şiddet Verileri
- Dünya Sağlık Örgütü (WHO) Şiddet Önleme Rehberi
- UNICEF Çocuk Koruma Politikaları

4. Proje Dokümanları:
- Proje Başlangıç Dokümanı (Project Charter), v1.0
- Sistem Tasarım Dokümanı, v1.0
- Veritabanı Şema Tasarımı, v1.0
- API Dokümantasyonu, v1.0

5. Akademik Kaynaklar:
- "Türkiye'de Şiddet Önleme Çalışmaları: Bir Değerlendirme", Sosyal Politika Çalışmaları Dergisi, 2023
- "Digital Platforms for Violence Prevention", International Journal of Software Engineering, 2023

Erişim Kaynakları:
- IEEE Standartları: https://standards.ieee.org/
- ISO Standartları: https://www.iso.org/
- KVKK: https://www.kvkk.gov.tr/
- T.C. Mevzuatı: https://www.mevzuat.gov.tr/

1.5 Genel Bakış

Bu belgenin geri kalan kısmı aşağıdaki şekilde düzenlenmiştir:

Bölüm 2 - Genel Açıklama:
- Şiddete Karşı Farkındalık Platformu'nun genel bir perspektifini sunar
- Platformun temel işlevlerini ve kullanıcı özelliklerini açıklar
- Sistemin genel sınırlamalarını ve bağımlılıklarını belirtir

Bölüm 3 - Özel Gereksinimler:
- Platformun arayüz gereksinimlerini detaylandırır
- Kullanıcı, donanım ve yazılım arayüzlerini tanımlar
- Sistemin fonksiyonel ve fonksiyonel olmayan gereksinimlerini listeler
- Güvenlik, performans ve kullanılabilirlik kriterlerini belirler
- Veritabanı yapısını ve gereksinimlerini açıklar

Bölüm 4 - Analiz Modelleri:
- Sistemin işleyişini gösteren diyagramları içerir
- Veri akışını ve sistem davranışlarını görselleştirir

Bölüm 5 - Değişiklik Yönetimi:
- Gereksinimlerdeki değişikliklerin nasıl yönetileceğini açıklar

Ekler:
- Destekleyici dokümanları ve ek bilgileri içerir

2. Genel Açıklama

Bu platform, şiddet olaylarının raporlanması, takibi ve önlenmesi için geliştirilecek web tabanlı bir sistemdir. Toplumsal bir sorun olan şiddetin önlenmesi ve farkındalığın artırılması amacıyla, kullanıcı dostu ve erişilebilir bir çözüm sunmayı hedeflemektedir.

2.1 Ürün Perspektifi

Şiddete Karşı Farkındalık Platformu, mevcut sistemlerden farklı olarak:

a) Bağımsız Sistem Özellikleri:
- Tamamen web tabanlı çalışma
- Mobil uyumlu tasarım
- Bağımsız veritabanı yönetimi

b) Diğer Sistemlerle Etkileşim:
- ALO 183 Sosyal Destek Hattı entegrasyonu
- Emniyet birimleri acil yardım hatları ile bağlantı
- Hastane acil servisleri ile koordinasyon
- Google Maps API entegrasyonu

c) Benzer Sistemlerden Farkları:
- Anonim raporlama özelliği
- Gerçek zamanlı veri analizi
- İnteraktif risk haritası
- Çok dilli destek

2.2 Ürün İşlevleri

Platform aşağıdaki temel işlevleri sağlayacaktır:

a) Olay Raporlama ve Takip:
- Şiddet olayı bildirimi
- Olay takip sistemi
- Durum güncelleme
- Coğrafi konumlandırma

b) Kullanıcı Yönetimi:
- Kayıt ve giriş sistemi
- Profil yönetimi
- Yetkilendirme seviyeleri
- Anonim kullanım seçeneği

c) Veri Analizi ve Raporlama:
- İstatistiksel analizler
- Risk haritası oluşturma
- Trend analizi
- Özelleştirilebilir raporlar.

2.3 Kullanıcı Özellikleri

Platform, farklı kullanıcı gruplarına hizmet verecektir:

1. Genel Kullanıcılar:
- Temel bilgisayar/mobil cihaz kullanım becerisi
- Her yaş ve eğitim seviyesinden kullanıcılar
- Türkçe veya İngilizce dil bilgisi
- Gizlilik ihtiyacı yüksek kullanıcılar

2. Kurum Temsilcileri:
- STK çalışanları
- Sağlık kurumu personeli
- Emniyet görevlileri
- Sosyal hizmet uzmanları

3. Sistem Yöneticileri:
- Teknik altyapı bilgisi
- Veri analizi yapabilme yetkinliği
- Sistem yönetimi deneyimi

2.4 Genel Sınırlamalar

1. Teknik Sınırlamalar:
- Yalnızca web tarayıcıları üzerinden erişim
- Minimum 2 Mbps internet bağlantısı gerekliliği
- SSL sertifikası zorunluluğu
- KVKK uyumlu veri saklama

2. Güvenlik Sınırlamaları:
- İki faktörlü kimlik doğrulama zorunluluğu
- Hassas verilerin şifrelenmiş saklanması
- IP bazlı erişim kısıtlamaları
- 30 dakika hareketsizlik sonrası oturum sonlandırma

3. Yasal Sınırlamalar:
- KVKK uyumluluk gereklilikleri
- Adli vaka bildirimleri için yasal prosedürler
- Veri saklama süre sınırlamaları
- Kullanıcı gizlilik politikaları

2.5 Varsayımlar ve Bağımlılıkları

1. Teknik Varsayımlar:
- Kullanıcıların modern web tarayıcıları kullanacağı
- Sunucu altyapısının 7/24 çalışır durumda olacağı
- Veritabanı yedekleme sistemlerinin düzenli çalışacağı
- API servislerinin sürekli erişilebilir olacağı

2. Operasyonel Bağımlılıklar:
- Google Maps API servislerinin kullanılabilirliği
- SMS/E-posta bildirim servislerinin çalışırlığı
- Acil yardım hatlarının erişilebilirliği
- Kurumsal entegrasyonların devamlılığı

3. Dış Faktör Bağımlılıkları:
- İnternet altyapısının sürekliliği
- Mobil cihaz uyumluluğu
- Yasal mevzuat değişiklikleri
- Kullanıcı gizlilik tercihleri

4. Kaynak Bağımlılıkları:
- Sunucu maliyetleri
- API kullanım limitleri
- Veritabanı depolama kapasitesi
- Teknik destek personeli

3. Özel Gereksinimler

Bu bölüm, Şiddete Karşı Farkındalık Platformu'nun detaylı gereksinimlerini içermektedir. Her gereksinim benzersiz bir ID ile numaralandırılmış ve öncelik seviyesi belirtilmiştir.

Öncelik Seviyeleri:
- KRİTİK (K): Sistemin çalışması için mutlaka gerekli
- YÜKSEK (Y): Önemli işlevsellik, eksikliği sistemi ciddi etkiler
- ORTA (O): Yararlı özellik, eksikliği tolere edilebilir
- DÜŞÜK (D): İsteğe bağlı özellik

Gereksinim Formatı:
[ID] [Öncelik] [Gereksinim Açıklaması] [Doğrulama Metodu]

Örnek Gereksinim:
REQ-001 [K] Sistem, kullanıcıların anonim olarak şiddet vakası bildirmesine izin vermelidir. [Test]

Doğrulama Metodları:
- Test (T): Yazılım testi ile doğrulanacak
- İnceleme (İ): Kod/tasarım incelemesi ile doğrulanacak
- Demo (D): Demonstrasyon ile doğrulanacak
- Analiz (A): Analiz/hesaplama ile doğrulanacak

İzlenebilirlik Matrisi:
Her gereksinim için:
- Kaynak: Hangi paydaş/doküman kaynaklı
- İlişki: Diğer gereksinimlerle bağlantıları
- Test: İlgili test senaryoları
- Risk: Olası riskler ve etki analizi

Bu bölüm aşağıdaki alt başlıklar altında organize edilmiştir:
3.1 Dış Arabirim Gereksinimleri
3.2 Fonksiyonel Gereksinimler
3.3 Kullanım Durumları
3.4 Sınıflar/Nesneler
3.5 İşlevsel Olmayan Gereksinimler
3.6 Ters Gereksinimler
3.7 Tasarım Kısıtlamaları
3.8 Mantıksal Veritabanı Gereksinimleri
3.9 Diğer Gereksinimler

3.1 Dış Arabirimi Gereksinimleri

3.1.1 Kullanıcı Arayüzleri

- **Açıklama**: Platformun kullanıcılar tarafından erişilen ve etkileşime girilen tüm görsel arayüzleri, kullanım kolaylığı, erişilebilirlik ve işlevsellik açısından belirli gereksinimleri karşılamalıdır. Kullanıcı arayüzleri, platformun tüm kullanıcı kitlesi (yetişkinler, kadınlar, acil yardım çalışanları, araştırmacılar vb.) için uygun olmalıdır.

- **Gereksinimler**:

  - Platform, **mobil cihazlar** (Android, iOS) ve **masaüstü bilgisayarlar** (Windows, macOS) için uyumlu olmalıdır.
  - Kullanıcı arayüzü, **basit ve kullanıcı dostu** olmalı, şiddet mağdurlarının kolayca kullanabilmesi için tasarlanmalıdır.
  - Arayüz, **yüksek erişilebilirlik** standartlarına uygun olmalı (örneğin, ekran okuyucularla uyumlu, renk körlüğü dostu).
  - Platformda, **görsel içerikler (video, grafikler)** ve **metinler** (formlar, açıklamalar) kullanıcıları bilgilendirecek şekilde düzenlenmelidir.

3.1.2 Donanım Arabirimleri

- **Açıklama**: Bu gereksinim, yazılımın dış donanım cihazlarıyla nasıl iletişim kurduğunu tanımlar. Bu donanımlar, platformun çalışması için gerekli olabilecek tüm cihazları içerebilir, örneğin, kamera, mikrofon, GPS modülü, sensörler ve diğer aygıtlar.

- **Gereksinimler**:

  - Platform, cihazın **kamerası** ve **mikrofonu** gibi özelliklerine erişebilmelidir. Özellikle video ve sesli şiddet bildirimlerinin gönderilmesi için bu tür arabirimlere ihtiyaç duyulabilir.
  - Mobil cihazlar üzerinden **konum verisi** (GPS) alınabilmeli ve şiddet olaylarının harita üzerinde konumları belirlenebilmelidir.
  - Platform, **dokunmatik ekran** arabirimiyle uyumlu olmalı, mobil cihazlarda parmakla yapılan etkileşimleri doğru şekilde algılayabilmelidir.

3.1.3 Yazılım Arabirimleri

- **Açıklama**: Platform, diğer yazılım sistemleri ve uygulamaları ile entegrasyon kurabilmelidir. Bu arabirimler, veri alışverişini sağlayacak ve platformun işlevlerini destekleyecek şekilde tasarlanmalıdır.

- **Gereksinimler**:

  - Platform, **veritabanı sistemleri** ile uyumlu olmalı ve **veri sorgulama** ve **güncelleme işlemleri** düzgün bir şekilde çalışmalıdır.
  - Platform, **REST API** veya **GraphQL API** gibi modern yazılım arabirimleri ile dış sistemlere veri gönderebilmeli ve dış verileri alabilmelidir.
  - Platform, **sosyal medya sistemleri** ile entegrasyon sağlamalıdır (örneğin, kullanıcıların anonim olarak şiddetle ilgili paylaşım yapabilmesi için sosyal medya hesaplarına bağlanabilmesi).
  - **E-posta sistemleri** ve **SMS hizmet sağlayıcıları** ile entegrasyon sağlanarak, şiddet mağdurlarına acil durum bildirimleri gönderilebilir.
  - Platform, şiddetle ilgili önemli verilerin **yerel ve ulusal veri tabanları** ile entegrasyonunu sağlamalı, bu sayede güncel ve doğru verilere erişim sağlanmalıdır.

3.1.4 İletişim Arabirimleri

- **Açıklama**: İletişim arabirimleri, platformun dış dünyaya, diğer sistemlere ve kullanıcılara nasıl veri ilettiği ve aldığı ile ilgili gereksinimleri tanımlar. İletişim ağları, platformun verilerinin güvenli bir şekilde iletilmesini ve kullanıcılara gerçek zamanlı geri bildirim verilmesini sağlar.

- **Gereksinimler**:

  - **İnternet bağlantısı** üzerinden **HTTP/HTTPS protokolleri** ile veri iletimi ve alımı yapılmalıdır.
  - Platform, **SSL/TLS şifrelemesi** ile kullanıcıların verilerini güvenli bir şekilde iletmelidir.
  - Platform, **gerçek zamanlı bildirim** sistemleri kullanarak, şiddet raporları ve kullanıcı uyarılarını hızlı bir şekilde kullanıcılara iletebilmelidir.
  - **Mobil ve web tabanlı push bildirimleri** ile acil durum bilgileri anında iletilmelidir.
  - Kullanıcıların, platform üzerinden **canlı destek hattı** ile iletişime geçebilmesi için uygun **chat bot** veya **mesajlaşma sistemi** entegrasyonu sağlanmalıdır.
  - **E-posta ve SMS entegrasyonu** ile kullanıcıların şiddet raporlarının durumu veya başvuruları hakkında bildirimler alabilmesi sağlanmalıdır.

3.2 Fonksiyonel Gereksinimleri

Bu bölüm, kadına yönelik şiddetle mücadele amacıyla geliştirilmiş olan Şiddet Karşı Farkındalık platformunun temel işlevselliklerini tanımlar. Platformun her bir özelliği, kullanıcı etkileşimini ve sistemin işleyişini belirleyen gereksinimlerle açıklanacaktır.

3.2.1 <Fonksiyonel Gereksinimi veya Özelliği #1>

3.2.1.1 Giriş
Platforma girişi sadece adminler yapabilir, kullanıcı adı ve şifre bilgilerini kullanarak sisteme erişim sağlar. Anıtsayaç, kadına yönelik şiddet nedeniyle hayatını kaybeden kadınları anmak amacıyla yıllık olarak güncellenen bir sayaçtır. Bu sayaç, toplumsal farkındalık yaratmak için önemlidir. Şiddet Haritası, Türkiye'deki kadına yönelik şiddet vakalarının coğrafi dağılımını görsel olarak gösterir. Kullanıcılar, harita üzerinde bu vakaları inceleyebilir. Bu form, kullanıcıların kendilerinin veya çevrelerinden birinin kadına yönelik şiddet mağduru olup olmadığını bildirmelerine olanak tanır. Kullanıcılar, şiddet mağdurlarına yönelik yardım kaynaklarıyla ilgili bilgilendirilecektir.

3.2.1.2 Girişleri
Kullanıcı adı ve şifre, giriş yapmak için gerekli olan bilgilerdir. Bu bilgilerin doğru bir şekilde girilmesi gerekir. Anıtsayaç, her yıl kaydedilen kadına yönelik şiddet ölümlerini veritabanından alır ve bu veriler ile güncellenir. Harita, şiddet vakalarına ait verileri alır. Kullanıcılar harita üzerinde belirli tarihler, bölgeler ve şiddet türlerine göre filtreleme yapabilir. Formda, kullanıcıdan kişisel bilgilerini (isim, yaş) ve şiddet türünü (fiziksel, psikolojik, ekonomik vb.) girmesi istenir.

3.2.1.3 İşleme
Sistem, kullanıcı adı ve şifreyi doğrular. Doğru bilgilerle giriş yapılması sağlanırken, hatalı bilgiler girildiğinde kullanıcıya hata mesajı gösterilir. Sayaç, kaydedilen veriler doğrultusunda her yıl öldürülen kadın sayısını sayar ve bu sayıyı platformda dinamik bir şekilde gösterir. Harita, filtrelere göre dinamik olarak güncellenir. Kullanıcı harita üzerinde tıkladığında, ilgili bölgedeki şiddet vakaları hakkında detaylı bilgiler görüntülenir. Form verileri analiz edilerek, kullanıcının şiddet mağduru olup olmadığı belirlenir. Kullanıcı, şiddetle ilgili yardım alabileceği telefon hatları veya destek kaynaklarıyla yönlendirilir.

3.2.1.4 Çıkışları
Sayaç, kullanıcıya yıllık ölü sayısını görsel ve sayısal olarak sunar. Sayaç verileri her yıl otomatik olarak güncellenir. Harita, kullanıcılara coğrafi bazda kadına yönelik şiddet vakalarıyla ilgili detaylı bilgi sunar. Kullanıcı, harita üzerindeki simgeler aracılığıyla detaylara ulaşabilir. Kullanıcı, formu doldurduktan sonra şiddetle ilgili yardım alabileceği yerel ve ulusal kaynaklar hakkında bilgilendirilir.

3.2.1.5 Hata işleme
Harita verisi güncellenemediğinde, kullanıcıya "Harita verisi mevcut değil, lütfen tekrar deneyin" mesajı gösterilir. Teknik bir hata oluştuğunda ise "Harita yüklenemedi, lütfen tekrar deneyin" mesajı verilir.

3.2.2 <Fonksiyonel Gereksinimi veya Özelliği #2>

Bu özellik, kullanıcıların kadına yönelik şiddet konusunda farkındalık yaratacak videolara bilgilendirme metinlerine erişebilmesini sağlar. Videolar, şiddet türleri, etkileri ve çözüm yolları hakkında bilgi sunar.

3.3 Kullanım Durumları

3.3.1 Kullanım Durumu #1 **Şiddet Haritası Görüntüleme**

- **Açıklama**: Kullanıcı, Türkiye genelindeki kadına yönelik şiddet vakalarının coğrafi dağılımını görmek için şiddet haritasını kullanır.
- **Aktör**: Kullanıcı
- **Önkoşul**: Kullanıcı platforma giriş yapmıştır.
- **Senaryo**:
    1. Kullanıcı, platformda "Şiddet Haritası" sekmesine tıklar.
    2. Sistem, harita üzerinde Türkiye'nin haritasını ve şiddet vakalarının bulunduğu noktaları gösterir.
    3. Kullanıcı, harita üzerinde belirli bir bölgeyi seçer veya filtreleme seçenekleriyle (yıl, şiddet türü vb.) verileri daraltır.
    4. Harita, kullanıcı tarafından seçilen parametrelere göre dinamik olarak güncellenir ve kullanıcı seçtiği bölgelerle ilgili detaylı bilgi alır.
- **Sonuç**: Kullanıcı, belirlediği kriterlere göre şiddet vakalarıyla ilgili bölgesel bilgilere ulaşır.
- **Alternatif Senaryo**:
    - Eğer harita verisi mevcut değilse, kullanıcıya "Veri alınamıyor, lütfen tekrar deneyin" mesajı gösterilir.

3.3.3 Kullanım Durumu #2: "Şiddete Uğruyor Musunuz?" Formu Doldurma

- **Açıklama**: Kullanıcı, kendisinin veya çevresindekilerin kadına yönelik şiddet mağduru olup olmadığını belirleyen formu doldurur.
- **Aktör**: Kullanıcı
- **Önkoşul**: Kullanıcı platforma giriş yapmıştır.
- **Senaryo**:
    1. Kullanıcı, platformda "Şiddete Uğruyor Musunuz?" sekmesine tıklar.
    2. Kullanıcı, formda kendisiyle ilgili kişisel bilgileri ve maruz kaldığı şiddet türünü (fiziksel, psikolojik, ekonomik vb.) doldurur.
    3. Kullanıcı formu göndermeye karar verir ve "Gönder" butonuna basar.
    4. Sistem, kullanıcının verdiği bilgilere göre ilgili destek kaynaklarını ve yardım hatlarını önerir.
    5. Kullanıcı, yardım kaynakları hakkında bilgilendirilir ve şiddetle mücadele için yönlendirilir.
- **Sonuç**: Kullanıcı, şiddet mağduru olup olmadığını belirler ve yardım alabileceği kaynaklar hakkında bilgilendirilir.

- **Alternatif Senaryo**:
    - Eğer formda eksik bilgi varsa, kullanıcıya "Lütfen tüm alanları doldurduğunuzdan emin olun" mesajı gösterilir.

"3.3 Kullanım Durumları" başlığı altında, kullanıcıların platformu nasıl kullanacaklarını ve platformun çeşitli işlevlerinin nasıl çalıştığını gösteren senaryolar yer alır. Kullanım durumu, belirli bir hedefe ulaşmak için bir kullanıcının gerçekleştireceği adımların bir özetidir. Bu başlık altında, platformunuzun her bir özelliği için kullanıcının platformla nasıl etkileşime girdiği ve sistemin bu etkileşimlere nasıl yanıt verdiği anlatılır.

Aşağıda, sizin şiddete karşı farkındalık platformunuz için bazı kullanım durumu örneklerini ve açıklamalarını bulabilirsiniz:

3.3 Kullanım Durumları

Bu bölümde, kullanıcıların platformda gerçekleştireceği temel işlemler ve bu işlemlerin adımları tanımlanacaktır.

3.3.1 Kullanım Durumu #1: Kullanıcı Girişi ve Kayıt

- **Açıklama**: Kullanıcı, sisteme giriş yapmak veya yeni bir hesap oluşturmak için platformu kullanır.
- **Aktör**: Kullanıcı
- **Önkoşul**: Kullanıcı platformu açmıştır.
- **Senaryo**:
    1. Kullanıcı platformun ana sayfasında "Giriş Yap" veya "Hesap Oluştur" seçeneğini tıklar.
    2. Eğer yeni kullanıcıysa, hesap oluşturma formu açılır ve kullanıcı adı, e-posta, şifre gibi bilgileri girer.
    3. Kullanıcı bilgilerini girdikten sonra "Kaydet" butonuna basar.
    4. Eğer kullanıcı mevcutsa, giriş ekranına yönlendirilir ve kullanıcı adı ile şifresini girerek sisteme giriş yapar.
    5. Kullanıcı başarılı bir şekilde giriş yaptıktan sonra, platformun ana fonksiyonlarına erişim sağlar.
- **Sonuç**: Kullanıcı platforma giriş yapar ve ana sayfaya yönlendirilir.
- **Alternatif Senaryo**:
    - Kullanıcı yanlış giriş yaparsa, hata mesajı gösterilir: "Yanlış kullanıcı adı veya şifre."

3.3.2 Kullanım Durumu #2: Şiddet Haritası Görüntüleme

- **Açıklama**: Kullanıcı, Türkiye genelindeki kadına yönelik şiddet vakalarının coğrafi dağılımını görmek için şiddet haritasını kullanır.
- **Aktör**: Kullanıcı
- **Önkoşul**: Kullanıcı platforma giriş yapmıştır.
- **Senaryo**:
    1. Kullanıcı, platformda "Şiddet Haritası" sekmesine tıklar.
    2. Sistem, harita üzerinde Türkiye'nin haritasını ve şiddet vakalarının bulunduğu noktaları gösterir.
    3. Kullanıcı, harita üzerinde belirli bir bölgeyi seçer veya filtreleme seçenekleriyle (yıl, şiddet türü vb.) verileri daraltır.
    4. Harita, kullanıcı tarafından seçilen parametrelere göre dinamik olarak güncellenir ve kullanıcı seçtiği bölgelerle ilgili detaylı bilgi alır.
- **Sonuç**: Kullanıcı, belirlediği kriterlere göre şiddet vakalarıyla ilgili bölgesel bilgilere ulaşır.
- **Alternatif Senaryo**:
    - Eğer harita verisi mevcut değilse, kullanıcıya "Veri alınamıyor, lütfen tekrar deneyin" mesajı gösterilir.

3.3.3 Kullanım Durumu #3: "Şiddete Uğruyor Musunuz?" Formu Doldurma

- **Açıklama**: Kullanıcı, kendisinin veya çevresindekilerin kadına yönelik şiddet mağduru olup olmadığını belirleyen formu doldurur.
- **Aktör**: Kullanıcı
- **Önkoşul**: Kullanıcı platforma giriş yapmıştır.
- **Senaryo**:
    1. Kullanıcı, platformda "Şiddete Uğruyor Musunuz?" sekmesine tıklar.
    2. Kullanıcı, formda kendisiyle ilgili kişisel bilgileri ve maruz kaldığı şiddet türünü (fiziksel, psikolojik, ekonomik vb.) doldurur.
    3. Kullanıcı formu göndermeye karar verir ve "Gönder" butonuna basar.
    4. Sistem, kullanıcının verdiği bilgilere göre ilgili destek kaynaklarını ve yardım hatlarını önerir.
    5. Kullanıcı, yardım kaynakları hakkında bilgilendirilir ve şiddetle mücadele için yönlendirilir.
- **Sonuç**: Kullanıcı, şiddet mağduru olup olmadığını belirler ve yardım alabileceği kaynaklar hakkında bilgilendirilir.
- **Alternatif Senaryo**:
    - Eğer formda eksik bilgi varsa, kullanıcıya "Lütfen tüm alanları doldurduğunuzdan emin olun" mesajı gösterilir.

3.3.4 Kullanım Durumu #4: Anıtsayaç Görüntüleme

- **Açıklama**: Kullanıcı, kadına yönelik şiddet nedeniyle hayatını kaybeden kadınları anmak amacıyla yıllık ölü sayısını gösteren anıtsayaç verilerini görüntüler.
- **Aktör**: Kullanıcı
- **Önkoşul**: Kullanıcı platforma giriş yapmıştır.
- **Senaryo**:
    1. Kullanıcı, platformda "Anıtsayaç" sekmesine tıklar.
    2. Sistem, kadına yönelik şiddet nedeniyle hayatını kaybeden kadınların sayısını yıl bazında görsel olarak gösterir.
    3. Kullanıcı, sayacın her yıl güncellenmesiyle kadına yönelik şiddetle ilgili farkındalık yaratır.
- **Sonuç**: Kullanıcı, her yıl için öldürülen kadın sayısını görsel olarak ve sayısal olarak görüntüler.
- **Alternatif Senaryo**:
    - Eğer sayaç verisi güncellenemezse, kullanıcıya "Veri alınamıyor, lütfen tekrar deneyin" mesajı gösterilir.

3.4 Sınıflar / Nesneler

Her sınıf, platformunuzun önemli bir bileşenini temsil edebilir. Aşağıda, "Kadına Şiddetle Mücadele" platformu için önerilen bazı sınıflar ve nesneler ile nasıl bir yapı kurulabileceğine dair örnekler bulabilirsiniz:

3.4.1 <Sınıf / Nesne #1>

3.4.1.1 Öznitelikler

- **Kullanıcı Adı**: Kullanıcının sisteme giriş yapabilmesi için kullandığı benzersiz isim.
- **Şifre**: Kullanıcının güvenliğini sağlayan gizli parola.
- **E-posta**: Kullanıcının platformla iletişime geçebileceği e-posta adresi.
- **Rol**: Kullanıcının platformdaki rolü (admin, normal kullanıcı, danışman vb.).
- **Profil Bilgileri**: Kullanıcıya ait kişisel bilgiler (ad, soyad, yaş vb.).
- **Konum Bilgileri**: Şiddet vakalarının harita üzerinde işaretlendiği coğrafi veriler (il, ilçe, koordinatlar).
- **Veri Kaynağı**: Şiddet verilerinin alındığı kaynak (yerel yönetimler, hükümet, STK'lar).
- **Tarih**: Harita üzerindeki verilerin hangi zaman dilimini kapsadığı.

3.4.1.2 İşlevleri

- **Giriş Yap()**: Kullanıcının sisteme giriş yapabilmesi için kullanıcı adı ve şifreyi doğrulayan işlev.
- **Kayıt Ol()**: Yeni bir kullanıcı hesabı oluşturulmasını sağlayan işlev.
- **Şifre Değiştir()**: Kullanıcının mevcut şifresini değiştirmesine imkan veren işlev

- **Bilgileri Güncelle()**: Kullanıcının profil bilgilerini güncellemesine imkan veren işlev.
- **Veri Al()**: Şiddetle ilgili verileri dış kaynaklardan alır ve haritada gösterir.
- **Filtrele()**: Kullanıcının harita üzerinde yıl, bölge, şiddet türü gibi kriterlere göre verileri filtrelemesine olanak sağlar.
- **Veri Topla()**: Kadına yönelik şiddet sonucu ölen kadınların sayısını toplar ve sisteme işler.
- **Sayaç Güncelle()**: Her yıl, yeni verilerle sayaç sayısını güncelle
- **Haritayı Güncelle()**: Yeni şiddet vakaları eklenince haritayı günceller.

3.4.2 <Sınıf / Nesne #2>

Bunlar dışında platformunuzda yer alabilecek diğer önemli sınıflar şunlar olabilir:

- **Eğitim Videoları**: Şiddetle ilgili bilgilendirme sınıfı.
- **Destek Kaynakları**: Şiddet mağdurları için yerel ve ulusal destek hatları, kriz merkezleri vb. bilgilerini içeren sınıf.

3.5 İşlevsel Olmayan Gereksinimler

İşlevsel olmayan gereksinimler aşağıdaki öznitelikler için var olabilir. Genellikle bu gereksinimler birim düzeyinde değilde, sistem düzeyinde sağlanmalıdır. Aşağıdaki bölümlerde gereksinimler ölçülebilir açısından ifade ediniz (örneğin, işlemlerin 95% en az 1 saniyenin altında işlenir, sistemin kapalı kalma süresini günde 1 dakika aşamaz, arızasız geçen ortalama sure (MTBF) > 30 gün olacak, vs.).

3.5.1 Performans

- **Açıklama**: Sistem, kullanıcıların taleplerini hızlı ve verimli bir şekilde yerine getirebilmelidir. Sistem üzerindeki yük arttıkça, performansın düşmemesi ve yanıt sürelerinin kabul edilebilir seviyede kalması gerekmektedir.
- **Örnek Gereksinimler**:

  - Kullanıcılar, sistemdeki her işlemde 2 saniye içerisinde yanıt almalıdır.
  - Kullanıcı sayısının artışıyla birlikte platformun yanıt süresi %10'dan fazla artmamalıdır.
  - Şiddet haritası verisi 1000'den fazla kayıt içerdiğinde, kullanıcı haritayı 5 saniye içinde yükleyebilmelidir.

3.5.2 Güvenilirlik

- **Açıklama**: Sistem, kesintisiz çalışmalı ve sürekli olarak güvenilir bir hizmet sunmalıdır. Kullanıcıların platforma güvenerek başvurdukları önemli bir uygulama olduğu için, hatasız bir deneyim sağlamak kritik önem taşır.
- **Örnek Gereksinimler**:

  - Platform, yılda en fazla 5 saat kesinti yaşamalıdır.
  - Sistemin ortalama arızasız çalışma süresi (MTBF - Mean Time Between Failures) en az 30 gün olmalıdır.
  - Platformun genel arıza oranı %99,9'un üzerinde olmalıdır.

3.5.3 Kullanılabilirlik

- **Açıklama**: Kullanıcıların platformu kolayca kullanabilmesi ve hedeflerine hızlıca ulaşabilmesi gerekir. Kullanıcı dostu bir tasarım, arayüzdeki öğelerin anlaşılır ve erişilebilir olması gerekmektedir.
- **Örnek Gereksinimler**:

  - Platformun kullanıcı arayüzü, 5 dakika içinde temel işlevlerin öğrenilebilmesini sağlayacak şekilde tasarlanmalıdır.
  - Platformda gerçekleştirilen işlemlerin %95'i, kullanıcılar tarafından herhangi bir eğitim veya teknik destek alınmadan tamamlanabilmelidir.
  - Kullanıcı arayüzü, erişilebilirlik standartlarına uygun olmalıdır (örneğin, WCAG 2.1).

3.5.4 Güvenlik

- **Açıklama**: Platformda yer alan tüm veriler güvenli bir şekilde saklanmalı ve kullanıcıların kişisel bilgileri korunmalıdır. Platformda yapılacak işlemlerin her biri, güvenlik tehditlerine karşı dayanıklı olmalıdır.
- **Örnek Gereksinimler**:

  - Kullanıcı bilgileri, 256-bit şifreleme algoritmaları kullanılarak saklanmalıdır.
  - Platformda tüm veri iletimi, SSL (Secure Socket Layer) şifreleme ile korunmalıdır.
  - Sistem, kullanıcı girişlerini 3 başarısız denemeden sonra geçici olarak kilitlemelidir.
  - Şiddetle ilgili veriler yalnızca yetkilendirilmiş kullanıcılar tarafından erişilebilir olmalıdır

3.5.5 Sürdürülebilirlik

- **Açıklama**: Sistem, uzun vadeli kullanım için sürdürülebilir olmalı ve her yıl güncellemeler, iyileştirmeler yapılabilmelidir. Ayrıca, yazılımın bakımı kolay olmalı ve sürdürülebilir teknoloji yığınları kullanılmalıdır.
- **Örnek Gereksinimler**:

  - Sistem, her yıl düzenli olarak güvenlik güncellemeleri ve bakım işlemleri almalıdır.
  - Kullanıcı geri bildirimlerine dayanarak, her yıl en az 2 ana sürüm güncellemesi yapılmalıdır.

- Sistem, açık kaynaklı kütüphaneler ve sürdürülebilir teknolojiler kullanılarak geliştirilecektir.
- Platformdaki kodun %80'i, sürdürülebilir yazılım geliştirme ilkelerine uygun olmalıdır.

3.5.6 Taşınabilirlik

- **Açıklama**: Sistem, farklı cihazlar ve platformlar üzerinde çalışabilmelidir. Bu, özellikle mobil cihazlar, tabletler ve masaüstü bilgisayarlar için geçerlidir. Kullanıcı deneyimi, her platformda benzer olmalıdır.
- **Örnek Gereksinimler**:

  - Sistem, Android ve iOS işletim sistemlerinde sorunsuz bir şekilde çalışmalıdır.
  - Platform, en az 3 farklı tarayıcıda (Chrome, Firefox, Safari vb.) sorunsuz çalışmalıdır.
  - Mobil uyumlu web tasarımı sağlanmalı, tüm cihazlarda kullanıcı dostu bir deneyim sunulmalıdır.
  - Sistem, farklı işletim sistemlerinde (Windows, macOS, Linux) minimum konfigürasyon gereksinimlerine sahip olmalıdır.

3.6 Ters Gereksinimleri

Ters gereksinimler, sistemin **uygulanabilir olmayan** veya **istenmeyen** özelliklerini tanımlar. Bu gereksinimler, yazılımın **hangi işlevleri yerine getirmemesi gerektiğini** veya **hangi davranışlardan kaçınılması gerektiğini** belirtir. Yani, sistemin **kısıtlamalar** ve **limitler** ile neler yapılmaması gerektiğine dair bir rehberdir. Ters gereksinimler, genellikle bir projenin **sınırlarını** belirler ve yazılımın yanlış kullanımları veya gereksiz karmaşıklıkları önlemeye yardımcı olur.

Örnek Ters Gereksinimler

Aşağıda, şiddetle mücadele platformunuz için örnek ters gereksinimler bulunmaktadır:

3.6.1 Kullanıcı Bilgilerinin Paylaşılmaması

- **Açıklama**: Kullanıcıların kişisel bilgileri, sistem tarafından yalnızca yetkili birimler ve kullanıcının kendisiyle paylaşılmalıdır. Platformda herhangi bir üçüncü taraf ile kullanıcı bilgileri paylaşılmamalıdır.
- **Ters Gereksinim**: Kullanıcı bilgileri **üçüncü taraflara** satılamaz, kiralanamaz ya da başka şekilde paylaşılamaz. Kullanıcılar, bilgilerini yalnızca kendi onayları ile sisteme girebilir.

3.6.2 Verilerin Silinmesi

- **Açıklama**: Platform, şiddet mağdurlarına yardım etmek amacıyla hassas veriler toplar. Bu verilerin güvenliği ve gizliliği son derece önemlidir. Ancak bazı durumlarda, kullanıcılar veri silme talep edebilirler.
- **Ters Gereksinim**: Sistemde, kullanıcıların **kişisel verilerinin kalıcı olarak silinmesi** işlemi yapılabilir, ancak veriler hiçbir şekilde **geri getirilemez**. Platform, kişisel bilgilerin silinmesi taleplerine tamamen uymalıdır.

3.6.3 Gereksiz Karmaşıklık

- **Açıklama**: Kullanıcı arayüzü mümkün olduğunca **basit ve sezgisel** olmalıdır. Şiddetle ilgili hassas bir konu olduğundan, kullanıcıların platformu kullanırken zorlanmamaları gerekir.
- **Ters Gereksinim**: Platform, **gereksiz karmaşık menüler, aşırı bilgili kullanıcı girişi veya kafa karıştırıcı arayüzler** içermemelidir. Karmaşık bir kullanıcı deneyimi veya gereksiz bilgi talepleri kullanıcıyı platformdan uzaklaştırabilir.

3.6.4 Platformun Sürekli Erişilebilirliği

- **Açıklama**: Platformun, şiddet mağdurları ve yardım arayanlar için her zaman erişilebilir olması gerekir. Ancak, bakım sırasında sistemin çevrimdışı olması gerekebilir.
- **Ters Gereksinim**: Platform **planlanmamış kesintiler** veya **uzun süreli erişim kayıpları** yaşatmamalıdır. Sistem bakımı dışındaki her türlü kesinti, platformun amacına ters düşer.

3.6.5 Yanıltıcı veya Eksik Bilgi Sağlanmaması

- **Açıklama**: Platform, kullanıcılarına doğru ve güvenilir bilgiler sağlamalıdır. Yanlış yönlendirmeler şiddet mağdurlarına zarar verebilir.
- **Ters Gereksinim**: Platform, **yanıltıcı**, **eksik** veya **şiddet mağdurlarını yanlış yönlendirecek** bilgiler sağlamamalıdır. Bu tür bilgilerin paylaşılması, platformun güvenilirliğini zedeler.

3.6.6 Yavaş Yükleme Süreleri

- **Açıklama**: Kullanıcıların platformda gezinirken hızlı bir deneyim yaşaması gerekir. Özellikle şiddetle ilgili acil yardım ve destek talepleri olduğunda, hızlı işlem süreleri kritik önem taşır.
- **Ters Gereksinim**: Platform, **uzun yükleme süreleri** veya **çok fazla gecikme** yaşatmamalıdır. Özellikle şiddetle ilgili acil bir durumu raporlayan kullanıcılar, işlemlerini hızla tamamlamak isteyeceklerdir.

3.7 Tasarım Kısıtlamaları

3.7.1 Yasal ve Düzenleyici Kısıtlamalar

- **Veri Gizliliği ve Koruma Yasaları**: Kullanıcıların kişisel verileri, **Kişisel Verilerin Korunması Kanunu (KVKK)** veya **Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR)** gibi yasal düzenlemelere uygun şekilde işlenmeli ve saklanmalıdır.
    - **Kısıtlama**: Platform, kullanıcı verilerinin toplanması, saklanması ve işlenmesi sırasında ilgili yasal düzenlemelere kesinlikle uymalıdır. Kullanıcıların izni alınmadan hiçbir kişisel veri toplanamaz veya üçüncü şahıslarla paylaşılamaz.
- **İçerik Denetimi ve Filtreleme**: Şiddetle mücadele platformunda kullanıcılar tarafından paylaşılan içerikler (yorumlar, video, fotoğraf vb.) doğru şekilde denetlenmeli ve zararlı, yanıltıcı veya şiddet içerikli veriler platformda yayımlanmamalıdır.
    - **Kısıtlama**: Yasal gerekliliklere uygun şekilde, kullanıcı tarafından yüklenen içerikler denetimden geçirilmeden yayımlanamaz. İçerik denetimi, yasa dışı ve zararlı içeriklerin engellenmesini sağlamalıdır.

3.7.2 Donanım Kısıtlamaları

- **Sunucu Altyapısı ve Veri Depolama**: Platformun barındırılacağı sunucuların özellikleri ve veri depolama kapasitesi belirli kısıtlamalar getirebilir. Ayrıca, kullanıcılara sunulacak hizmetlerin performansı donanım altyapısına bağlıdır.
    - **Kısıtlama**: Platform, mevcut sunucu kapasitesiyle uyumlu olmalı ve **yük dengeleme** (load balancing) ile performans sorunu yaşatmadan binlerce kullanıcıya hizmet verebilmelidir. Depolama kapasitesi, kullanıcı verilerinin güvenli ve verimli bir şekilde saklanmasını sağlamalıdır.
- **Mobil Cihaz ve Tarayıcı Desteği**: Kullanıcılar, platformu farklı cihazlar üzerinden erişebileceği için, mobil cihazlar ve masaüstü tarayıcılarla uyumluluk sağlanmalıdır. Ancak cihazların donanım özellikleri sınırlayıcı olabilir.
    - **Kısıtlama**: Platformun, özellikle düşük donanım özelliklerine sahip mobil cihazlarda da düzgün çalışması sağlanmalıdır. Hedeflenen cihazlar için minimum sistem gereksinimleri belirlenmelidir.

3.7.3 Performans Kısıtlamaları

- **Yüksek Trafik ve Ölçeklenebilirlik**: Şiddetle mücadele gibi toplumsal bir platformda, kullanıcı sayısının artması ve yoğun trafik durumları ortaya çıkabilir. Bu nedenle, platformun **yüksek trafik** altında dahi doğru şekilde çalışabilmesi için **ölçeklenebilirlik** sağlanmalıdır.
    - **Kısıtlama**: Yüksek kullanıcı trafiğinde, platformun performansı etkilenmeden sorunsuz çalışabilmelidir. Yazılım ve donanım altyapısı, sistemin trafik artışına göre genişletilebilecek şekilde tasarlanmalıdır.

3.7.4 Kullanıcı Deneyimi (UX) ve Arayüz Kısıtlamaları

- **Erişilebilirlik Standartları**: Platformun kullanıcı dostu ve erişilebilir olması için belirli erişilebilirlik standartlarına (örneğin WCAG 2.1) uygun olması gerekir. Şiddetle mücadele platformu, tüm kullanıcılar için erişilebilir olmalıdır, özellikle engelli bireyler için.
    - **Kısıtlama**: Arayüz tasarımı, **görme engelli** bireyler için ekran okuyucu uyumlu olmalı ve **fiziksel engeli olan kullanıcılar** için uygun navigasyon seçenekleri sunmalıdır. Yazılımda renk körlüğüne karşı duyarlı renkler ve kolay erişim araçları kullanılmalıdır.

3.7.5 Organizasyonel ve Şirket Politikaları

- **Veri Güvenliği Politikaları**: Şirketin iç politikaları gereği, sistemdeki verilerin güvenliği ve gizliliği sıkı bir şekilde korunmalıdır. İç politikalar, platformun güvenlik önlemlerinin belirli bir seviyeye ulaşmasını zorunlu kılabilir.
    - **Kısıtlama**: Veritabanı şifreleme, kullanıcı doğrulama süreçleri ve yetkilendirme sistemleri şirketin güvenlik politikalarına uygun şekilde tasarlanmalıdır. Herhangi bir güvenlik açığı, şirket politikalarına göre derhal düzeltilmelidir.
- **Destek ve Bakım Süreçleri**: Şirket içindeki bakım ve destek süreçleri, platformun sürekli erişilebilirliğini ve güvenliğini sağlamak için belirli gereklilikler sunabilir.
    - **Kısıtlama**: Platform, belirli aralıklarla yapılacak **bakım** ve **güncellemeler** sırasında **kesintiye uğramadan** kullanıcı hizmeti sunmaya devam etmelidir. Şirket içindeki bakım ekipleri, herhangi bir güvenlik açığı tespit ettiğinde hızlıca müdahale edebilmelidir.

3.8 Mantıksal Veritabanı Gereksinimleri

3.8.1 Veri Formatları ve Türleri

- **Açıklama**: Veritabanındaki veriler, belirli formatlarda ve türlerde saklanmalıdır. Bu, verilerin doğru şekilde işlenmesini ve kullanıcıların doğru bilgilere hızlı erişimini sağlamak için gereklidir.
- **Gereksinimler**:
    - Kullanıcı bilgileri (isim, e-posta, telefon numarası gibi) **metin** formatında saklanmalıdır.
    - Şiddetle ilgili veriler (ölen kadın sayısı, şiddet türü, raporlama tarihi vb.) **sayısal** ve **tarih** formatında tutulmalıdır.
    - Coğrafi veriler (yer, harita üzerinde koordinatlar) **coğrafi konum formatında** (örneğin, lat/lon) saklanmalıdır.
    - Veritabanı, dosya yüklemeleri için **BLOB (Binary Large Object)** formatını desteklemelidir (örneğin, video veya resim yüklemeleri).
    - Kullanıcı geri bildirimleri ve açıklamaları **metin** formatında saklanmalı, ancak metin boyutuna sınırlamalar getirilmelidir (örneğin, 5000 karakter ile sınırlı).

3.8.2 Depolama Yetenekleri

- **Açıklama**: Veritabanı, platformun işlevselliğine göre veri miktarını ve verilerin büyüklüğünü kaldıracak şekilde tasarlanmalıdır. Ayrıca, verilerin düzenli olarak depolanması ve gerektiğinde erişilmesi sağlanmalıdır.
- **Gereksinimler**:
    - Veritabanı, platformda kullanıcı sayısının artmasıyla birlikte büyüyebilecek kapasiteye sahip olmalıdır (yüzbinlerce kayıt).
    - Veritabanı, veri **yüksekliği** (high availability) ve **güncellemeleri** (real-time updates) desteklemeli, özellikle şiddetle ilgili acil verilerin hızla sisteme eklenebilmesi için optimize edilmelidir.
    - Veritabanı, **yedekleme** ve **felaket kurtarma** (disaster recovery) çözümleri ile desteklenmeli, veri kaybı durumunda hızlı bir şekilde geri yükleme yapılabilmelidir.
    - Veritabanı, tüm verilerin şifrelenmiş olarak saklanmasını desteklemeli (özellikle kişisel veriler ve şiddetle ilgili hassas bilgiler).

3.8.3 Veri Saklama Süreleri ve Arşivleme

- **Açıklama**: Veritabanında saklanan verilerin ne kadar süreyle tutulacağı ve eski verilerin nasıl arşivleneceği net bir şekilde tanımlanmalıdır. Kullanıcıların güvenliği ve gizliliği göz önünde bulundurularak verilerin saklanması gerekir.
- **Gereksinimler**:
    - Kullanıcı verileri, yasal gereklilikler doğrultusunda en az **5 yıl** saklanmalıdır. Ancak, kullanıcı talepleri doğrultusunda veriler bu süre zarfında silinebilir.
    - Şiddetle ilgili her türlü veri (şiddet mağdurlarının başvuruları, rapor edilen olaylar vb.) en az **10 yıl** boyunca saklanmalıdır, ancak daha uzun süreli saklama gereksinimleri olursa, kullanıcıların onayı ile saklama süresi uzatılabilir.
    - Eski veriler, veritabanında aktif olmayan ancak gerektiğinde geri alınabilir durumda **arşivlenmelidir**. Arşivleme işlemi, verilerin erişilebilirliğini etkilememelidir.

3.8.4 Veri Bütünlüğü

- **Açıklama**: Veritabanı, saklanan verilerin **bütünlüğünü** sağlamak için belirli kurallara, kısıtlamalara ve denetimlere sahip olmalıdır. Veri bütünlüğü, verilerin doğru, eksiksiz ve güvenli şekilde saklanmasını ve işlenmesini garanti eder.
- **Gereksinimler**:
    - **Referans bütünlüğü**: Veritabanındaki ilişkili veriler (örneğin, kullanıcı bilgileri ve başvurular) arasında doğru ilişkiler kurulmalı ve bu ilişkilerdeki hatalar engellenmelidir. Örneğin, bir kullanıcının başvuru kaydının silinmesi durumunda, başvuru kaydının da otomatik olarak silinmesi gerekir.
    - **Veri doğruluğu**: Platforma girilen verilerin doğruluğu ve tutarlılığı sağlanmalıdır. Örneğin, kullanıcı tarafından girilen tarihlerin doğru formatta ve mantıklı bir şekilde olması için doğrulama mekanizmaları kullanılmalıdır.
    - **Veri güncellemeleri**: Veritabanındaki verilerin doğru bir şekilde güncellenmesi sağlanmalıdır. Veri güncellemeleri sırasında **atomicity** sağlanmalı, yani işlem başarısız olduğunda tüm veritabanı değişiklikleri geri alınmalıdır.
    - **Veri tekrarı**: Aynı verinin (örneğin, aynı kullanıcı bilgisi) veritabanında tekrarı engellenmelidir. Aynı kullanıcının aynı başvuruya birden fazla kez başvurması engellenmelidir.

3.8.5 Erişim Kontrolü ve Güvenlik

- **Açıklama**: Veritabanı, sadece yetkilendirilmiş kullanıcıların erişebileceği şekilde yapılandırılmalıdır. Kullanıcıların kişisel verileri ve şiddetle ilgili hassas veriler yalnızca yetkili kişiler tarafından görülebilmelidir.
- **Gereksinimler**:
    - Veritabanı erişimi, kullanıcı türlerine göre yetkilendirilmiş olmalıdır. Örneğin, sistem yöneticisi, şiddetle mücadele uzmanı, araştırmacı ve genel kullanıcılar farklı seviyelerde erişime sahip olmalıdır.
    - **Veri şifreleme**: Veritabanındaki veriler, hem **veri transit (data in transit)** hem de **veri saklama (data at rest)** aşamalarında şifrelenmelidir. Bu, kişisel ve hassas verilerin güvenliğini sağlayacaktır.
    - **Veri erişim kayıtları**: Tüm veri erişim işlemleri (görüntüleme, güncelleme, silme vb.) kaydedilmelidir. Bu loglar, denetim ve güvenlik kontrolleri için kullanılabilir.

3.9 Diğer Gereksinimler

3.9.1 Ölçeklenebilirlik Gereksinimleri

- **Açıklama**: Şiddetle mücadele platformu, artan kullanıcı sayısı, veri miktarı veya işlem hacmi gibi değişen koşullara göre büyüyebilmelidir.
- **Gereksinimler**:
    - **Veritabanı ve sunucu altyapısı**, platformda kullanıcı sayısının arttığı durumlarda yüksek performans sağlamak için **dikey ve yatay ölçeklenebilir** olmalıdır.
    - Platformun, **yüksek trafik** dönemlerinde (örneğin, şiddetle ilgili önemli bir güncel olayın yaşandığı anlar) hizmet sunmaya devam edebilmesi için sistemin kapasitesi artırılabilmelidir.
    - **Yük dengeleme** ve **daha fazla sunucu ekleme** mekanizmaları ile platform, yoğun trafikte bile düzgün çalışabilir olmalıdır.

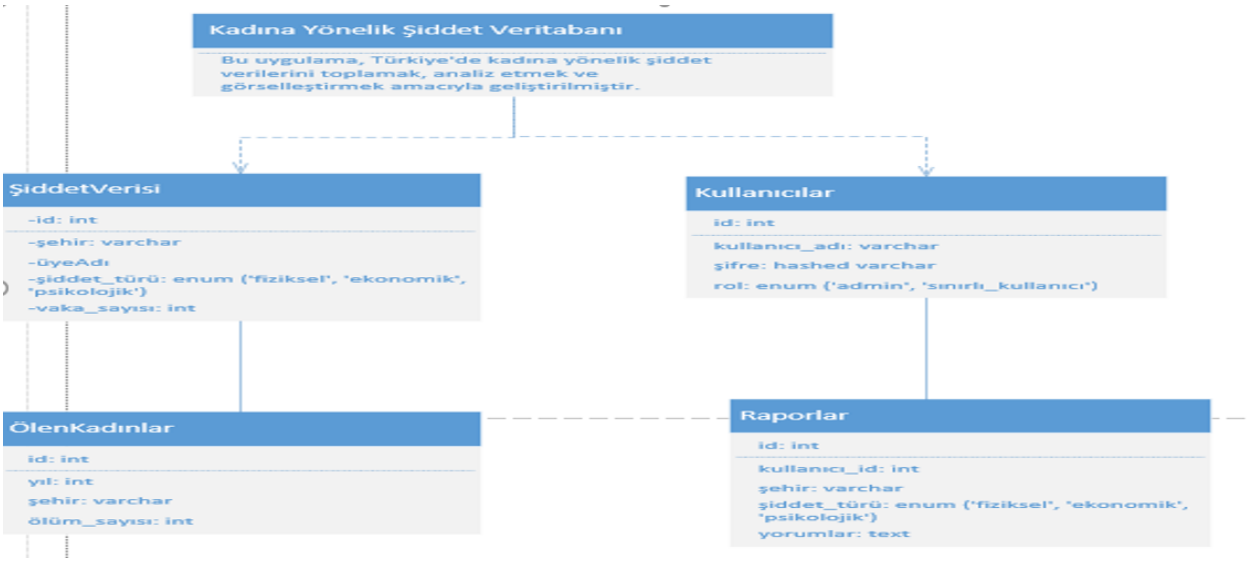
3.9.2 Performans ve Yanıt Süresi

- **Açıklama**: Platform, yüksek performans göstermeli ve kullanıcılara hızlı bir deneyim sunmalıdır. Kullanıcıların şiddetle ilgili raporları hızlıca bildirebilmesi çok önemlidir.
- **Gereksinimler**:
    - Platform, **herhangi bir kullanıcı etkileşimi** (veri giriş, form gönderme vb.) sonrasında yanıt süresinin 1 saniyeden fazla olmamalıdır.
    - **Sayfa yükleme süreleri** en fazla 3 saniye olmalıdır. Bu, platformun her tür cihazda hızlı yüklenmesini sağlamak için optimize edilmelidir.
    - Platform, **yüksek trafik** altında bile hizmet kalitesini kaybetmeden yanıt verebilmeli

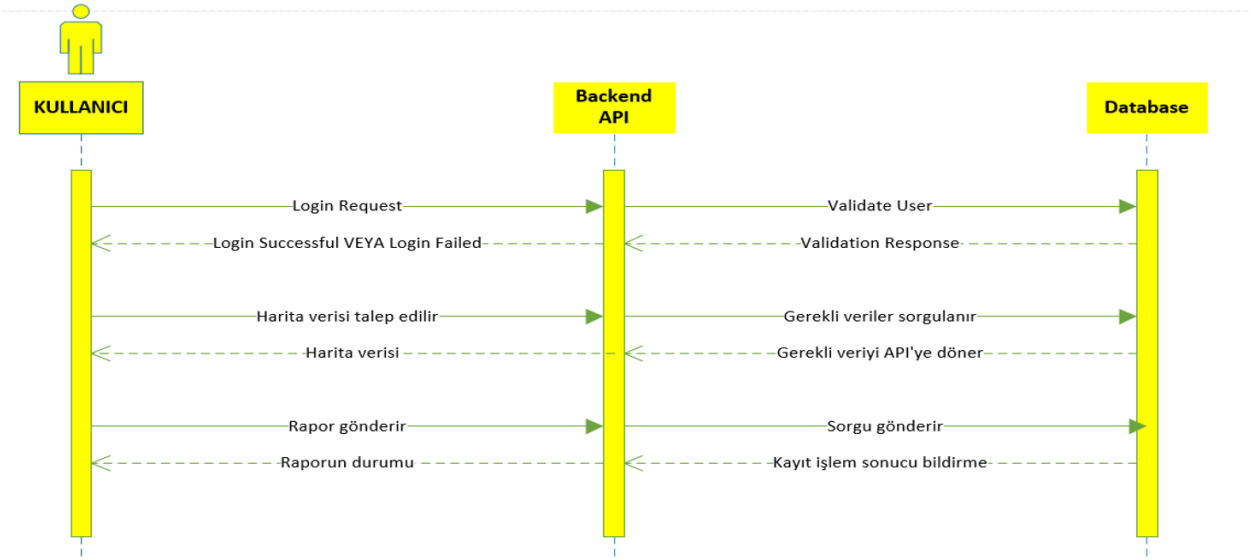
4. Analiz Modelleri

Bu belirtimde ifade edilen özel gereksinimlerin geliştirilmesinde kullanılan tüm analiz modellerini listeleyiniz. Her model bir giriş ve bir anlatı açıklama içermelidir. Ayrıca, her model belirtimdeki gereksinimlere izlenebilir olmalıdır.

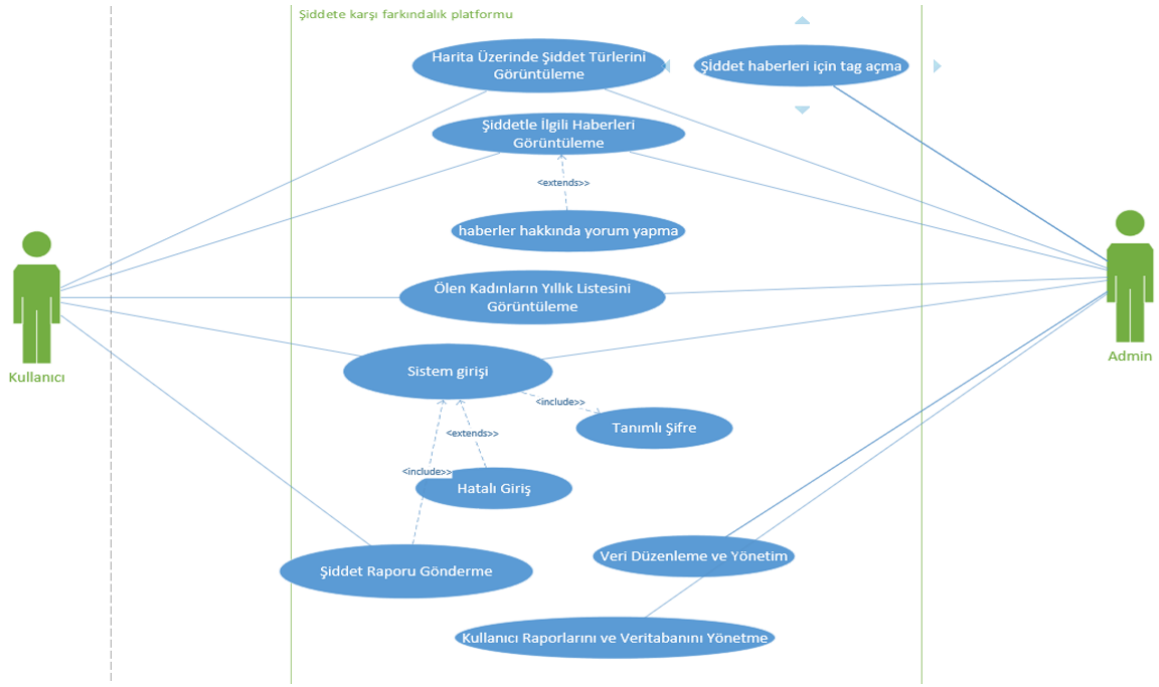
4.1 Class Diyagramları



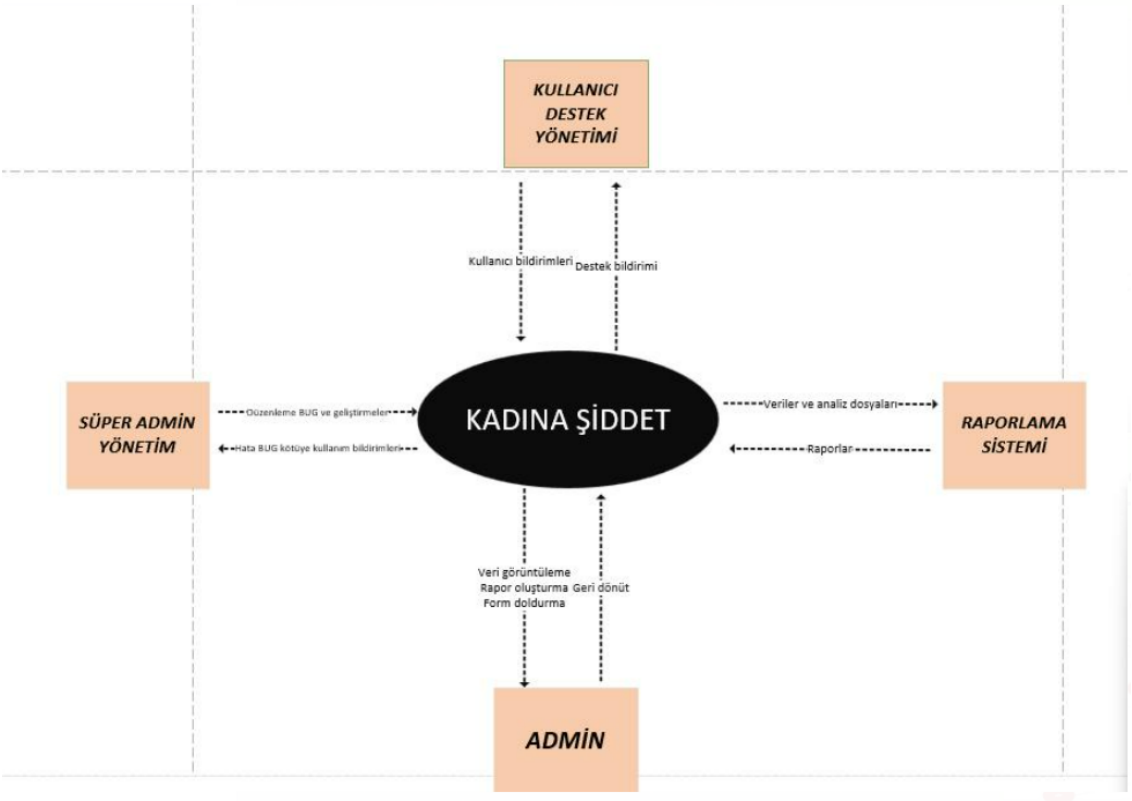
4.2 Sequence Diyagramları



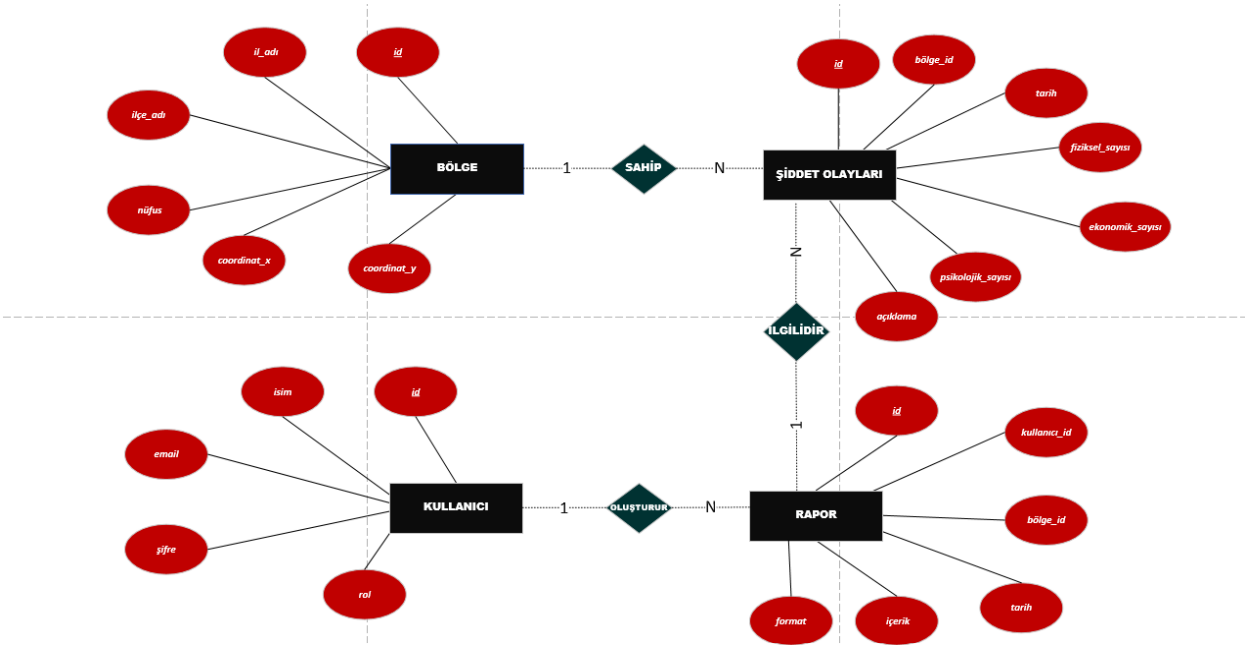
4.3 Use Case Diyagramları



4.4 Context Diyagramları



4.5 ER Diyagramları



5. Değişiklik Yönetimi Süreci

5.1 Değişiklik Talepleri ve Gönderen Kişiler

- **Kimler Değişiklik Gönderebilir?**
  - **Proje Yöneticisi**: Proje planına ve hedeflerine bağlı olarak gereksinimlerde veya şartlarda yapılacak değişiklikleri başlatabilir.
  - **Geliştirme Ekibi**: Yazılımın teknik gereksinimlerinde yapılması gereken değişiklikler, yazılımdaki hataların düzeltilmesi veya iyileştirmeler için değişiklik talepleri gönderebilir.
  - **İç Kullanıcılar**: İç kullanıcılar, platformu kullanan çalışanlar veya yöneticiler, yazılımda iyileştirmeler veya kullanım kolaylığı ile ilgili değişiklik talepleri gönderebilir.
  - **Dış Kullanıcılar / Müşteriler**: Şiddetle mücadele platformunu kullanan son kullanıcılar veya platformdan destek alanlar, yazılımın kullanımını etkileyen hataları veya ihtiyaçlarını belirterek değişiklik önerileri gönderebilir.
  - **Test Ekibi**: Test aşamasında tespit edilen hatalar veya eksiklikler için değişiklik talepleri iletebilir.

5.2 Değişikliklerin Değerlendirilmesi ve Kabul Edilmesi

- **Değişiklik Taleplerinin Değerlendirilmesi**:
  - **Proje Yöneticisi** ve **Geliştirme Ekibi**, her değişiklik talebini değerlendirir ve değişikliğin yazılımın genel yapısına ve mevcut planlara nasıl etki edeceğini inceler.
  - **Etkileri Analizi**: Değişiklik talebinin proje süresi, bütçesi ve işlevselliği üzerindeki olası etkileri değerlendirilir. Bu, **yeni zaman çizelgeleri**, **ekstra maliyetler** veya **ekstra kaynak gereksinimleri** gibi unsurları içerir.
  - **Risk Değerlendirmesi**: Değişikliklerin, platformun güvenliği, performansı ve kullanıcı deneyimi üzerindeki etkisi analiz edilir.
  - **Teknik Gereksinimler ve Gereksiz Değişikliklerin Filtrelenmesi**: Bazı talepler, teknik olarak geçerli olmayabilir veya önceden planlanmış bir yön ile çelişebilir, bu tür talepler reddedilebilir.
- **Değişikliklerin Kabul Edilmesi**:
  - **Onay Süreci**: Değişikliklerin kabul edilip edilmeyeceği, proje yöneticisi, gelişim ekibi ve gerektiğinde iş birimi temsilcilerinin oluşturduğu bir **değerlendirme komitesi** tarafından kararlaştırılır.
  - **Değişiklik Planı ve Takvim Belirleme**: Kabul edilen değişiklikler için net bir **değişiklik planı** ve **yeni zaman çizelgesi** belirlenir.
  - **Kaydedilen Değişiklikler**: Kabul edilen değişiklikler, proje gereksinimleri dokümanlarına, yazılım tasarımına ve mevcut kod tabanına uygun şekilde güncellenir.
  - **Paydaşlara Bildirim**: Değişiklikler onaylandıktan sonra, ilgili tüm paydaşlara (geliştiriciler, test uzmanları, kullanıcılar) bilgilendirme yapılır.

5.3 Değişikliklerin Uygulanması

- **Uygulama Süreci**:
  - Kabul edilen değişiklikler, yazılım geliştirme yaşam döngüsüne entegre edilir ve **geliştirme, test, dağıtım** süreçlerinden geçirilir.
  - Her değişiklik, sistemin bütünlüğünü koruyacak şekilde **modüler bir biçimde uygulanır**.
  - Uygulama sonrası, değişikliklerin etkileri **geri bildirim mekanizmaları** kullanılarak izlenir ve test edilir.

5.4 Değişikliklerin İzlenmesi ve Raporlanması

- **İzleme**:
  - Değişikliklerin uygulanmasının ardından, değişikliğin başarıyla gerçekleştirilip gerçekleştirilmediği takip edilir.
  - **Performans ve Kullanıcı Geri Bildirimleri**: Değişikliklerin, kullanıcılar ve sistem performansı üzerindeki etkisi sürekli olarak izlenir ve raporlanır.
- **Raporlama**:
  - **Değişiklik Kayıtları** düzenli olarak raporlanır ve paydaşlara sunulur. Değişikliklerin etkileri ve sonuçları, proje raporlarında belirtilir.
  - **Sonuçların Değerlendirilmesi**: Değişikliklerin, proje hedeflerine nasıl katkıda bulunduğu değerlendirilir.

A. Ekler

Ek 1: Proje GitHub Bağlantısı

Bu proje için oluşturulan GitHub deposuna aşağıdaki bağlantıdan ulaşabilirsiniz:

Şiddete Karşı Farkındalık Platformu - GitHub

Ek 2: Veritabanı Şema Tasarımı

Aşağıdaki ER (Entity-Relationship) diyagramı, platformun MongoDB tabanlı veritabanı yapısını göstermektedir. Diyagram, kullanıcı verileri, şiddet raporları ve coğrafi konum bilgileri arasındaki ilişkileri açıklamaktadır.

- **Kullanıcı Tablosu:** Kullanıcı bilgileri (ID, isim, e-posta, rol).
- **Rapor Tablosu:** Şiddet olaylarına ait bilgiler (ID, olay türü, tarih, coğrafi konum).
- **Destek Kaynakları Tablosu:** Kullanıcılara önerilen yardım kaynakları (ID, kurum adı, iletişim bilgisi).

Not: Bu şema detayları, ilgili API dokümantasyonuyla uyumludur.

Ek 3: Kullanım Senaryosu Diyagramı

Platformun temel işlevleri için hazırlanmış kullanım senaryoları diyagramları:

1. **Kullanıcı Girişi:** Kullanıcıların platforma giriş yapma ve şifre sıfırlama işlemleri.
2. **Şiddet Haritası Görüntüleme:** Türkiye genelindeki şiddet olaylarının harita üzerinde filtrelenmesi ve detayların incelenmesi.
3. **Anonim Raporlama:** Kullanıcıların kişisel bilgi girmeden şiddet olaylarını rapor edebileceği süreç.

Bu diyagramlar, kullanıcı akışını görselleştirmek için UML araçlarıyla hazırlanmıştır.

Ek 4: Test Senaryoları ve Kabul Kriterleri

Proje kapsamında gerçekleştirilen testler ve kabul kriterleri aşağıdaki gibidir:

- **Performans Testleri:**
    - Sayfa yükleme süresi: Maksimum 3 saniye.
    - Eş zamanlı kullanıcı desteği: 10,000 kullanıcı.
- **Fonksiyonel Testler:**
    - Şiddet raporlarının doğru şekilde kaydedilmesi ve görselleştirilmesi.
    - Kullanıcı oturum yönetimi ve yetkilendirme işlemleri.
- **Güvenlik Testleri:**
    - 256-bit SSL şifreleme doğrulaması.
    - 3 başarısız giriş denemesi sonrası hesap kilitlenmesi.

Not: Detaylı test sonuçları proje GitHub deposunda yer almaktadır.

Ek 5: Kullanıcı Hikayeleri

Farklı kullanıcı grupları için belirlenen kullanıcı hikayeleri:

1. **Genel Kullanıcı:**
    - Bir kullanıcı, çevresinde bir şiddet olayı gerçekleştiğinde anonim bir şekilde bu olayı rapor edebilir.
2. **STK Çalışanı:**
    - Bir STK çalışanı, platform üzerinden bölgesel şiddet istatistiklerini analiz ederek, risk bölgelerini belirleyebilir.
3. **Sistem Yöneticisi:**
    - Sistem yöneticisi, platforma eklenen raporları ve kullanıcı istatistiklerini analiz ederek veri bütünlüğünü sağlar.

Ek 6: Standartlar ve Referanslar

Bu proje aşağıdaki standartlara ve kaynaklara uygun olarak geliştirilmiştir:

1. **Standartlar:**
    - IEEE 830-1998: Yazılım Gereksinimleri Belirtimi için önerilen uygulamalar.
    - ISO/IEC 25010: Yazılım Kalite Gereksinimleri ve Değerlendirme (SQuaRE).
2. **Kaynaklar:**
    - T.C. Aile ve Sosyal Hizmetler Bakanlığı verileri.
    - Türkiye İstatistik Kurumu (TÜİK) şiddet verileri.
3. **Akademik Yayınlar:**
    - "Türkiye'de Şiddet Önleme Çalışmaları: Bir Değerlendirme" (2023).
    - "Digital Platforms for Violence Prevention" (2023).

Ek 7: Risk Yönetimi

Proje kapsamında tanımlanan temel riskler ve çözüm önerileri:

1. **Teknik Risk:** API hizmetlerinde kesinti yaşanması.
    - **Çözüm:** API erişimlerinde yedek sistemler ve zaman aşımı senaryoları uygulanması.
2. **Güvenlik Riskleri:** Kullanıcı verilerinin sızdırılması.
    - **Çözüm:** Verilerin şifrelenmesi ve iki faktörlü kimlik doğrulama uygulanması.
3. **Kullanıcı Etkileşim Sorunları:** Kullanıcıların platform arayüzünü karmaşık bulması.
    - **Çözüm:** Kullanıcı geri bildirimleri doğrultusunda UI/UX iyileştirmeleri yapılması.

Not: Yukarıdaki ekler proje dokümanını desteklemek amacıyla hazırlanmıştır ve detaylı bilgiler için GitHub reposu ziyaret edilmelidir.