Gereksinim Listesi (Requirement List)

-------------------------------------

- Kullanıcı doğrulama sistemi (giriş formu)

- Rol tabanlı erişim kontrolü (RBAC)

- Veritabanı işlemleri (ekleme, silme, güncelleme)

- Asenkron iletişim (AJAX) kullanımı

- Güvenlik zaafiyetlerini içeren uygulama (OWASP Top 10)

- Oturum yönetimi ve güvenlik

- Kaynak kodların sürüm kontrol sistemi (GitHub) ile yönetilmesi

- Kullanıcı doğrulama ve oturum yönetimi için PHP ve MySQL kullanımı

Kullanım Durum Diyagramı (Use Case Diagram)

-------------------------------------------

Use Case Diagram

+--------------------------+

| Kullanıcı |

+--------------------------+

/ | \

/ | \

Giriş Yap Veri Ekle Mesaj Gönder

Sıralama Diyagramı (Sequence Diagram)

-------------------------------------

Sequence Diagram

User Browser Web Server Database

| | | |

|--Login---->| | |

| |--Query---->| |

| | |--Result---->|

| |<--Response-| |

Sızma Testi Raporu (Penetration Testing Report)

-----------------------------------------------

1. SQL Injection:

- Test: admin' OR '1'='1

- Sonuç: Sisteme giriş başarılı

- Giderme: Parametrik sorgular kullanılarak giderildi

2. XSS:

- Test: <script>alert('XSS');</script>

- Sonuç: JavaScript kodu çalıştı

- Giderme: Kullanıcı girdilerini kaçırma (htmlspecialchars) kullanılarak giderildi

3. CSRF:

- Test: Harici form ile veri ekleme

- Sonuç: Veri ekleme başarılı

- Giderme: CSRF token kullanılarak giderildi

Tehdit Modeli (Threat Model)

----------------------------

1. Bileşenler:

- Kullanıcı Tarayıcısı

- Web Sunucusu

- Veritabanı Sunucusu

2. Harici Varlıklar:

- Kullanıcı

3. Giriş Noktaları:

- Giriş Formu

- Veri Ekleme Formu

- Mesaj Gönderme Formu

4. Güven Düzeyleri:

- Anonim Kullanıcı

- Yetkili Kullanıcı

5. Güven Sınırları:

- Kullanıcı Tarayıcısı ile Web Sunucusu Arası

- Web Sunucusu ile Veritabanı Sunucusu Arası

Güvenlik Zaafiyetlerinin Tanıtımı ve Nasıl Giderildiği

-----------------------------------------------------

1. SQL Injection:

- Tanım: SQL sorgularına eklenen kötü niyetli girdiler ile veritabanı sorgularının manipüle edilmesi.

- Giderme: Hazırlıklı ifadeler (prepared statements) ve parametrik sorgular kullanılarak giderildi.

2. XSS:

- Tanım: Kullanıcı girdilerinin uygun şekilde işlenmemesi sonucu kötü niyetli JavaScript kodlarının çalıştırılması.

- Giderme: Kullanıcı girdilerinin kaçırılması (htmlspecialchars) kullanılarak giderildi.

3. CSRF:

- Tanım: Kullanıcının izni olmadan, kullanıcı kimliğinde istekler gönderilmesi.

- Giderme: CSRF token kullanılarak giderildi.

Kaynak Kodların Yer Aldığı Deponun Bağlantı Adresi

-------------------------------------------------

GitHub: [https://github.com/kullaniciadi/projeadi](https://github.com/kullaniciadi/projeadi)

Videonuzun Adresi

-----------------

YouTube: [https://youtube.com/linktoyourvideo](https://youtube.com/linktoyourvideo)