

# Güvenlik ve Ödeme Sistemleri (Temel + Pratik)

Bu doküman, tek parça halinde takip edilebilecek şekilde hazırlanmış, uygulama odaklı bir eğitim paketidir. Bölümlerin sonunda kontrol listeleri, mini alıştırmalar ve örnek akışlar bulunur.

## İçindekiler

1. Temel güvenlik prensipleri
2. Şifreleme ve hash
3. OWASP Top 10 özeti
4. CSRF/XSS/SQLi önlemleri
5. Güvenli oturum yönetimi
6. Ödeme akışları tasarımı
7. PCI yaklaşımı (yüksek seviye)
8. Loglama ve izleme
9. Yedekleme
10. Olay müdahalesi

## Bölüm 1: Temel güvenlik prensipleri

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 2: Şifreleme ve hash

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/iş kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 3: OWASP Top 10 özeti

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınırlar durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 4: CSRF/XSS/SQLi önlemleri

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 5: Güvenli oturum yönetimi

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 6: Ödeme akışları tasarımı

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akışlar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akış uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/iş kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 7: PCI yaklaşım (yüksek seviye)

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?



## Bölüm 8: Loglama ve izleme

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 9: Yedekleme

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 10: Olay müdahalesi

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 11: Temel güvenlik prensipleri

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 12: Şifreleme ve hash

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 13: OWASP Top 10 özeti

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 14: CSRF/XSS/SQLi önlemleri

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve senar durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 15: Güvenli oturum yönetimi

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?



## Bölüm 16: Ödeme akışları tasarımı

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akışları çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akış uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/iş kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 17: PCI yaklařımı (yüksek seviye)

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 18: Loglama ve izleme

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 19: Yedekleme

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 20: Olay müdahalesi

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?

## Bölüm 21: Temel güvenlik prensipleri

Bu bölümde kavramlar, iyi uygulamalar ve tipik hatalar anlatılır. Ardından adım adım uygulama yönergeleri verilir. Her adım tamamlandıktan sonra kontrol listesi ile doğrulama yapılır.

### Uygulama Adımları

- Hedefi netleştirin ve kabul kriterini yazın.
- Gerekli veri/ekran/akıllar çıkarın.
- Önce en basit çalışan sürümü tamamlayın.
- Hata senaryolarını ve sınır durumlarını ekleyin.
- Test edin, gözden geçirin ve iyileştirin.

### Kontrol Listesi

- Akıllı uçtan uca çalışıyor mu?
- Doğrulama ve hata mesajları anlaşılır mı?
- Kayıtlar tutarlı mı (DB/i kuralı)?
- Performans darboğazı var mı?
- Güvenlik önlemleri yerinde mi?