

# CEN429 Güvenli Programlama

## Hafta-3

### Veri Güvenliği: Kullanımda, Aktarımda ve Depolamada

## İndir

- [PDF](#)
- [DOC](#)
- [SLIDE](#)
- [PPTX](#)



## Outline

- Veri Güvenliği: Kullanımda, Aktarımda ve Depolamada
- Yazılım Geliştirme Süreçleri
  - Kullanımda Veri Güvenliği
  - Aktarımda Veri Güvenliği
  - Depolamada Veri Güvenliği
- Dinamik ve Statik Varlıkların Korunması

## Hafta-3: Veri Güvenliği - Kullanımda, Aktarımda ve Depolama Halindeki Veri Güvenliği

## Teorik Konu Başlıkları ve Uygulamalar

Güvenli Programlama ve Veri Güvenliği

amaçlı yazılımlar tarafından ele geçirilmesini engellemek için kullanılır.

## Uygulamalar:

1. **Bellek Şifreleme:** Bellekteki hassas verilerin şifrlenmesi.
2. **Kötüye Kullanım Tespiti:** Bellekteki şüpheli hareketlerin izlenmesi ve müdahale edilmesi.
3. **Veri Manipülasyonu Testleri:** Çalışma zamanındaki verilerin yanlışlıkla veya kasıtlı olarak değiştirilip değiştirilmediğini test etme.
4. **Dinamik Bellek Yönetimi:** Bellek sızıntılarını engellemek ve veri sızıntılarını minimize etmek.
5. **Sürekli Kimlik Doğrulama:** Kullanıcıların oturumları süresince kimliklerinin tekrar tekrar doğrulanması.
6. **Veri Maskelenmesi:** Hassas verilerin yalnızca yetkili süreçler tarafından görülebilir olması.

## Uygulamalar:

1. **Oturum Anahtarı (Session Key):** İstemci ve sunucu arasında dinamik olarak oturum anahtarı oluşturma ve bu anahtar ile şifreleme yapma.
2. **Cihaz Bağlama (Device Binding):** Verilerin belirli bir cihaza bağlı olarak iletilmesini sağlayarak, verilerin farklı bir cihazda çözülmesini engelleme.
3. **Sürüm Bağlama (Version Binding):** Yalnızca belirli sürümlerin veri iletimine izin vererek, güvenlik açıkları barındıran eski sürümlerin veri almasını engelleme.
4. **Şifrelenmiş Yük (Confidential Payload):** Taşınan verinin şifrelenerek sadece yetkili taraflar tarafından okunabilir hale getirilmesi.
5. **Bütünlük Kontrolü (Integrity Control):** Veri aktarımı sırasında verilerin bozulmadan veya değiştirilmeden iletildiğini doğrulama.
6. **Kimlik Doğrulama (Authenticity Control):** Veri gönderenin ve alıcının kimliklerinin doğrulanması.



## Uygulamalar:

1. **Sunucu Kimlik Doğrulama Kodu (Server Authentication Code):** Sunucunun kimliğini doğrulayan özel bir kimlik doğrulama mekanizması geliştirme.
2. **Güvenli Sunucu İletişimi (Secure Server Communication):** Sunucu ve istemci arasında verilerin SSL/TLS ile şifrlenmesini sağlama.
3. **Oturum Anahtarı Şifreleme (Session Key Encryption):** Verilerin oturum anahtarları kullanılarak şifrlenmesini sağlama.
4. **Sunucu Üzerinde Veri İzleme (Data Monitoring):** Sunucuya gelen ve giden veri trafiğini izleyip anormallikleri tespit etme.
5. **Veri Bütünlüğü Doğrulama:** Verilerin sunucuya bozulmadan iletilildiğini doğrulayan bütünlük kontrol mekanizmalarını kullanma.
6. **Verilerin Şifrlenmesi (Data Encryption):** Verileri sunucuya göndermeden önce istemci tarafında şifreleme.
7. **Sunucu Yanıtlarını İmzalama (Response Signing):** Sunucudan gelen yanıtları dijital imza ile doğrulama.

verilerin izinsiz erişimlere ve saldırılara karşı korunmasını sağlar.

## Uygulamalar:

1. **Whitebox AES:** Depolama alanında AES algoritmasını whitebox yöntemiyle uygulayarak verilerin daha güvenli bir şekilde korunmasını sağlama.
2. **Whitebox DES:** Whitebox DES algoritmasıyla verilerin şifrlenmesi ve güvenlik testlerinin yapılması.
3. **Güvenlik Kabuk Matrisi (Security Shell Matrix):** Verilerin güvenli bir şekilde depolanmasını sağlamak için dosya sisteminde güvenlik kabuğu oluşturma.
4. **Anahtar Yönetimi:** Şifreleme anahtarlarının güvenli bir şekilde saklanması ve düzenli olarak değiştirilmesi.
5. **Şifreli Veritabanı:** Veritabanındaki hassas verilerin şifrlenmesi ve sadece yetkili kullanıcıların erişebilmesi.
6. **Depolanan Verilerin Şifrlenmesi:** Tüm verilerin şifreli bir formatta saklanması ve yetkisiz erişimlerin engellenmesi.

erişimleri engellemek için son derece önemlidir.

## Uygulamalar:

1. **Anahtarların Şifrelenmesi:** Statik anahtarların güvenli bir şekilde depolanması için şifreleme yöntemleri kullanma.
2. **Kaynak Kodları Koruma:** Kaynak kodlarının izinsiz kopyalanmasını ve değiştirilmesini engelleyen mekanizmalar geliştirme.
3. **Statik Dosyaların Bütünlük Kontrolü:** Sabit dosyaların bütünlüğünü sağlayarak izinsiz değişikliklerin önlenmesi.
4. **Veri İmzası:** Depolanan verilerin değiştirilemeyeceğini doğrulamak için dijital imza kullanma.
5. **Veritabanı Bütünlüğü:** Veritabanında bulunan kritik verilerin şifrelenmesi ve bütünlüğünün korunması.
6. **Dosya Erişim Kontrolü:** Statik dosyaların yetkisiz erişimlere karşı korunması için erişim kontrol mekanizmalarını devreye sokma.

## Uygulamalar:

1. **Dinamik Anahtarların Güvenliği:** Dinamik anahtarların yalnızca belirli oturumlar sırasında kullanılması ve güvenli bir şekilde değiştirilmesi.
2. **Oturum Bilgisi Şifreleme:** Kullanıcı oturumlarının gizliliğini sağlamak için oturum bilgilerini şifreleme.
3. **Cihaz Parmak İzlerinin Korunması:** Cihaz parmak izlerinin yalnızca yetkili taraflarca doğrulanmasını sağlama.
4. **Oturum Verisi Koruması:** Dinamik oturum verilerinin şifrelenerek güvence altına alınması.
5. **Dinamik Anahtar Yönetimi:** Oturum sırasında kullanılan dinamik anahtarların güvenli bir şekilde oluşturulması ve yönetilmesi.
6. **Oturum Zaman Aşımı:** Kullanıcı oturumları için otomatik zaman aşımı mekanizması uygulayarak güvenliği artırma.
7. **Verilerin Sürekli İzlenmesi:** Dinamik verilerin şifrelenerek izlenmesi ve güvenlik ihlallerinin anında tespit edilmesi.

## Uygulamalar:

1. **Varlık İsmi (Asset Name):** Varlığın adını belirleyerek bu varlığın ne olduğunu tanımlama.
2. **Tanım (Description):** Varlığın ne işlev gördüğünü ve hangi bilgileri içerdiğini açıklama.
3. **Konum (Location):** Varlığın bulunduğu veri tabanı, tablo veya kolon gibi fiziksel konumunu belirleme.
4. **Kaynak (Source):** Varlığın kaynağını belirleyerek hangi süreç veya veri kaynağından geldiğini tanımlama.
5. **Boyut (Size):** Varlığın boyutunu belirleyerek depolama ihtiyaçlarını optimize etme.
6. **Oluşturulma Zamanı (Creation Time):** Varlığın oluşturulduğu tarihi ve zamanı belirleyerek log kayıtlarını tutma.
7. **Silinme Zamanı (Destroy Time):** Varlığın ne zaman imha edileceğini ve bu sürecin nasıl yönetileceğini belirleme

## Haftanın Özeti ve Gelecek Hafta

### Bu Hafta:

- Kullanımda, Aktarımda ve Depolamada Veri Güvenliği
- Statik ve Dinamik Varlıkların Korunması

### Gelecek Hafta:

- Sertifikalar ve Şifreleme Yöntemleri
- Kimlik Doğrulama ve Veri Bütünlüğü

## *3.Hafta – Sonu*