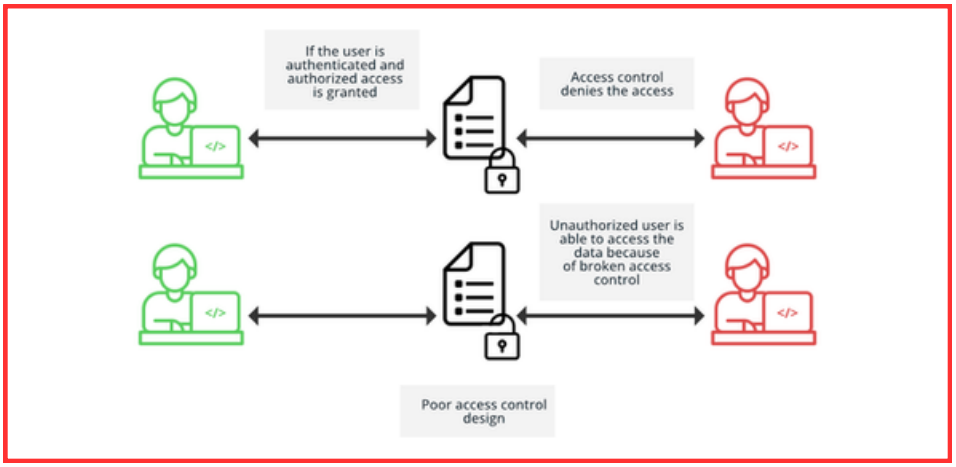
OWASP TOP 10

ZAFİYETLERİ

TARİH: 20.08.2024

A1 - BROKEN ACCESS CONTROL



Broken Access Control, OWASP Top Ten 2021 listesinde 1. sırada yer alan en kritik güvenlik zafiyetidir. Bu zafiyet, sistemdeki erişim kontrol mekanizmalarının yetersizliğinden kaynaklanır ve yetkisiz kişilerin hassas verilere erişmesine veya yasaklanmış işlemleri gerçekleştirmesine olanak tanır. Sistemler üzerinde ciddi güvenlik açıkları yaratan bu zafiyet, birçok güvenlik ihlalinin başlıca sebebidir.

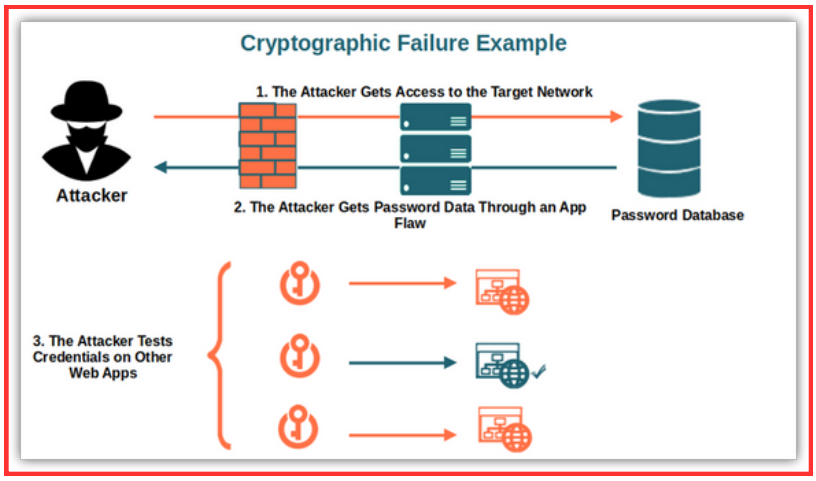
NEDEN KAYNAKLANIR?

- Yanlış Yapılandırılmış İzinler
- Eksik veya Yanlış Yetkilendirme
- Kimlik Doğrulama Kontrolü Eksikliği

NASIL ÖNLENİR?

- İzinleri ve Rollerini Doğru Tanımlama
- Sunucu Tarafında Erişim Kontrolleri Uygulama
- Kapsamlı Yetkilendirme Kontrolleri Ekleme
- Test ve Güvenlik İncelemeleri Yapma
- Kullanıcıların Yetkilerini İzleme ve Güncelleme

A2 - CRYPTOGRAPHIC FAILURES



Cryptographic Failures, verilerin güvenli bir şekilde şifrelenmemesi, anahtarların yanlış yönetilmesi veya zayıf şifreleme algoritmalarının kullanılması gibi durumları içerir. Bu tür zafiyetler, hassas bilgilerin yetkisiz kişiler tarafından erişilmesine, manipüle edilmesine veya çalınmasına yol açabilir.

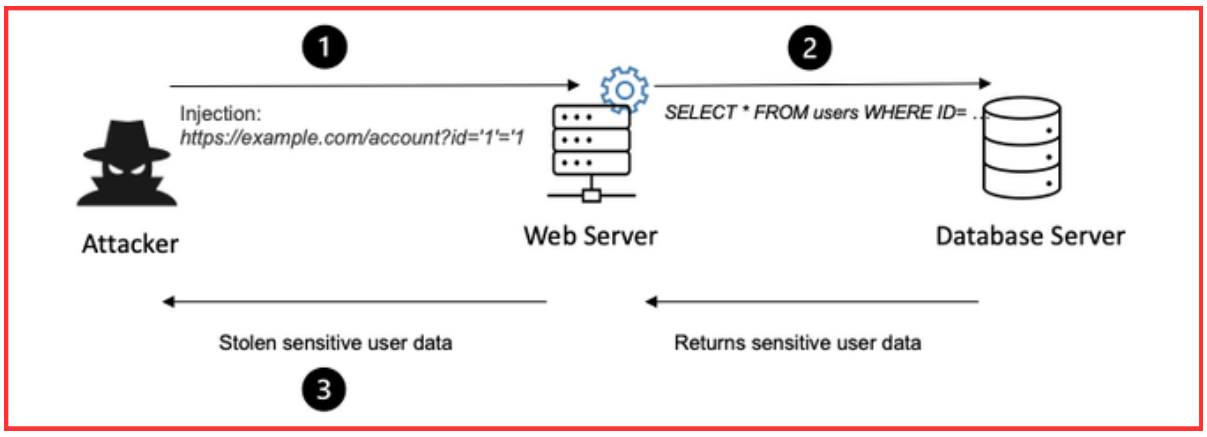
NEDEN KAYNAKLANIR?

- Zayıf veya Eskimiş Şifreleme Algoritmaları
- Yanlış Anahtar Yönetimi
- Yetersiz Şifreleme Parametreleri
- Şifrelenmiş Verinin Kötü Yönetimi

NASIL ÖNLENİR?

- Güçlü ve Güncel Şifreleme Algoritmaları Kullanma
- Anahtar Yönetimini Sağlamlaştırma
- Kriptografi Protokollerini Doğru Uygulama
- Yeterli Şifreleme Parametreleri Belirleme
- Şifrelenmiş Veriyi Güvenli Şekilde Saklama

A3 - INJECTION



Injection, saldırganların uygulamanın veritabanı veya diğer sistem bileşenleriyle etkileşiminde, zararlı veriler enjekte ederek kontrolü ele geçirmelerine veya verileri manipüle etmelerine olanak tanıyan bir güvenlik açığıdır. Enjeksiyon saldırıları, uygulama tarafından beklenmeyen veya kötü amaçlı veri girişi yaparak sistemin güvenliğini tehlikeye atar.

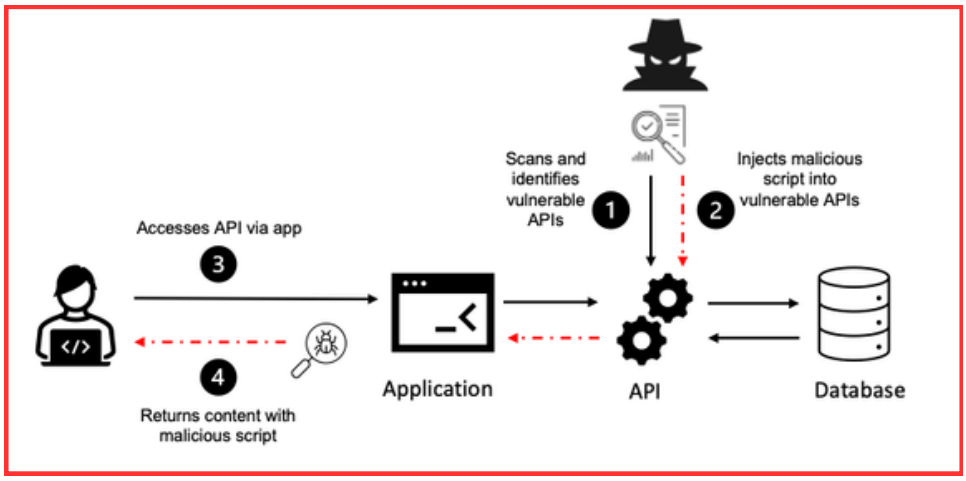
NEDEN KAYNAKLANIR?

- Eksik Girdi Doğrulama
- Hatalı Kullanıcı Girdi İşleme
- Güvenlik Açıkları İçeren Üçüncü Parti Kütüphaneler
- Yetersiz Kod Kontrolleri

NASIL ÖNLENİR?

- Girdi Doğrulama ve Temizlik
- Parametreli Sorgular ve Hazırlanmış İfadeler Kullanma
- Güncel Kütüphane ve Bileşenler Kullanma
- Güvenli Kodlamaya Uygun Geliştirme
- Güvenlik Testleri ve Penetrasyon Testleri

A4 - INSECURE DESIGN



Insecure Design, bir uygulamanın veya sistemin güvenlik risklerini dikkate almadan tasarlanmasıyla ortaya çıkan bir zafiyettir. Güvensiz tasarım, güvenlik açıklarının uygulamanın tasarım aşamasında yer alması ve bu nedenle uygulamanın kullanım süresi boyunca bu açıkların varlığını sürdürmesine neden olabilir. Bu tür zafiyetler, temel güvenlik gereksinimlerinin tasarım aşamasında göz ardı edilmesinden kaynaklanır.

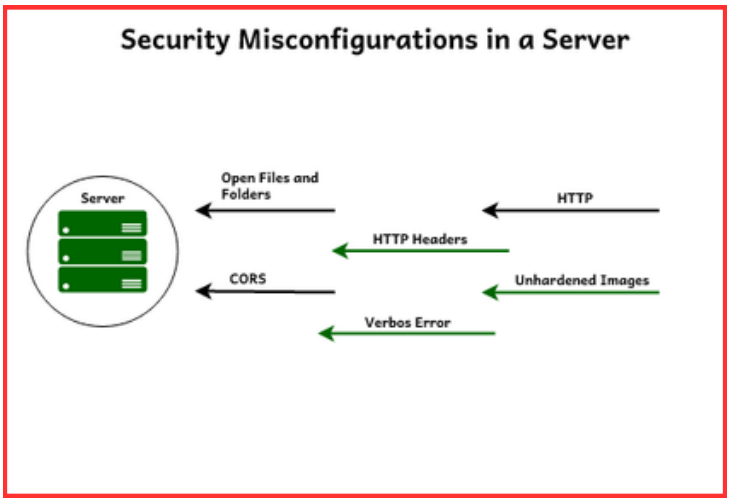
NEDEN KAYNAKLANIR?

- Güvenlik Gereksinimlerinin Eksik Tanımlanması
- Güvensiz Tasarım Prensiplerinin Kullanımı
- Yanlış veya Eksik Risk Değerlendirmesi
- Güvenlik Kültürünün Eksikliği

NASIL ÖNLENİR?

- Güvenlik Gereksinimlerini Erken Belirleme
- Güvenlik Tasarım Prensiplerini İzleme
- Güvenlik Testleri ve Risk Analizleri Yapma
- Güvenlik Bilincini Artırma ve Eğitim Sağlama
- Güvenlik İncelemeleri ve Denetimleri Yapma

A5 - SECURITY MISCONFIGURATION



Security Misconfiguration, bir uygulamanın, sunucunun veya sistem bileşeninin güvenlik ayarlarının yanlış yapılandırılmasından kaynaklanan bir güvenlik açığıdır. Yanlış yapılandırma, güvenlik duvarları, erişim izinleri, ağ ayarları, hizmetler veya yazılım bileşenleri gibi çeşitli alanlarda güvenlik açıklarına yol açabilir ve kötü amaçlı saldırganların sistemlere erişmesine veya verileri ele geçirmesine neden olabilir.

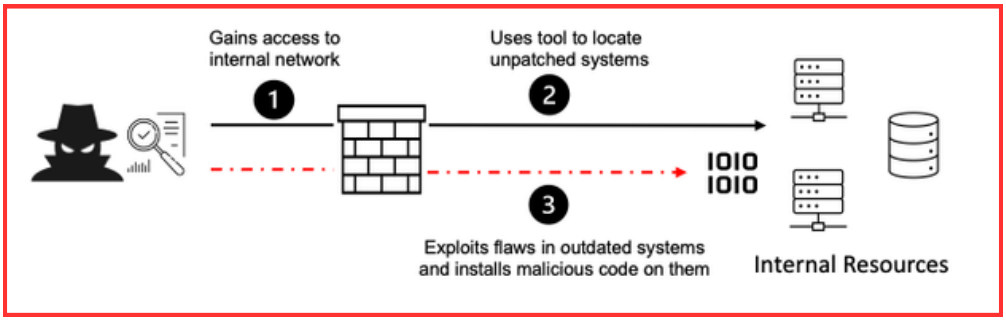
NEDEN KAYNAKLANIR?

- Varsayılan Ayarların Kullanımı
- Yetersiz Konfigürasyon Yönetimi
- Güvenlik Güncellemelerinin ve Yamalarının Uygulanmaması
- Yanlış veya Eksik Erişim Kontrolleri

NASIL ÖNLENİR?

- Güvenlik Ayarlarını Gözden Geçirme ve Yapılandırma
- Konfigürasyon Yönetimi ve Dokümantasyon
- Güvenlik Güncellemeleri ve Yamaları Uygulama
- Erişim Kontrollerini Doğru Yapılandırma
- Güvenlik Tarama ve Denetim Araçları Kullanma

A6 - VULNERABLE AND OUTDATED COMPONENTS



Vulnerable and Outdated Components, bir uygulamanın veya sistemin güvenlik açıklarına sahip eski veya güncel olmayan bileşenler kullanması sonucu ortaya çıkan bir güvenlik zafiyetidir. Bu bileşenler, kütüphaneler, çerçeveler, modüller veya diğer yazılım bileşenleri olabilir. Eski veya güvenlik açıkları içeren bileşenler, saldırganların bu açıklardan yararlanarak sisteme saldırmasına veya veri çalmasına neden olabilir.

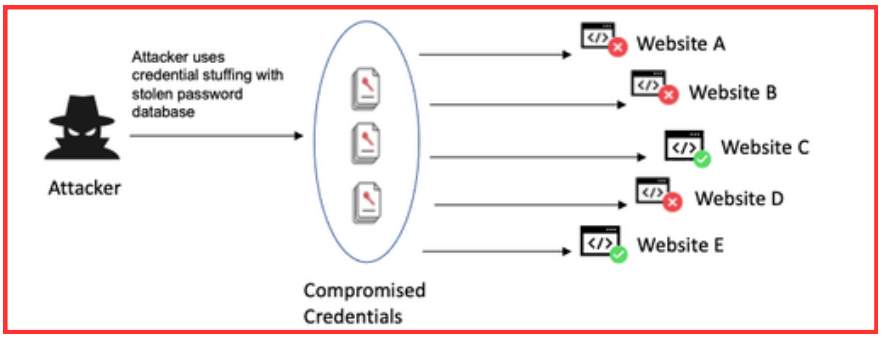
NEDEN KAYNAKLANIR?

- Güncellenmemiş Yazılım Bileşenleri
- Güvenlik Açığı İçeren Üçüncü Taraf Bileşenler
- Eksik Güvenlik Güncellemeleri
- Eski veya Desteklenmeyen Teknolojiler

NASIL ÖNLENİR?

- Bileşenleri Düzenli Olarak Güncelleme
- Güvenlik Açıkları İçin Tarama ve İzleme Yapma
- Desteklenen ve Güvenli Bileşenler Kullanma
- Bağımlılık Yönetimi Araçları Kullanma
- Güvenlik Politika ve Prosedürlerini Oluşturma

A7 - IDENTIFICATION AND AUTHENTICATION FAILURES



Identification and Authentication Failures, kullanıcıların kimlik doğrulama ve tanımlama süreçlerinde yaşanan hatalardan kaynaklanan güvenlik açıklarıdır. Bu tür hatalar, kötü niyetli kişilerin yetkisiz erişim elde etmesine, hesapların ele geçirilmesine veya kullanıcıların hassas bilgilere erişmesine neden olabilir. Bu zafiyetler, kimlik doğrulama ve tanımlama işlemlerinin zayıflığından kaynaklanır.

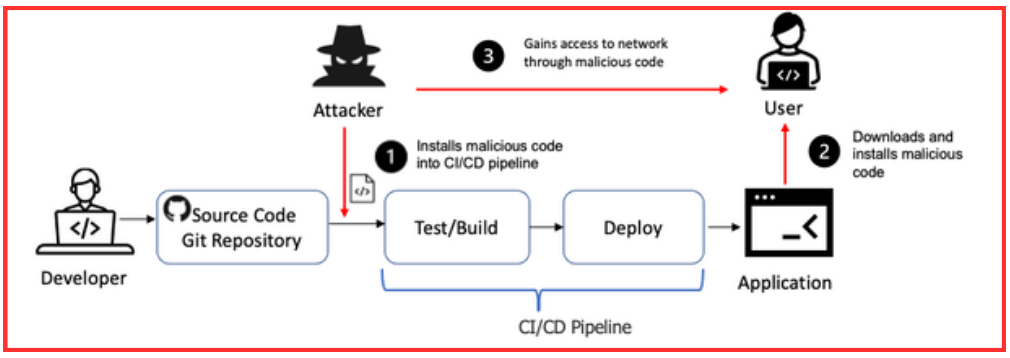
NEDEN KAYNAKLANIR?

- Zayıf Şifre Politikaları
- Kimlik Doğrulama Eksiklikleri
- Zayıf Çok Faktörlü Kimlik Doğrulama Uygulamaları
- Hatalı Yetkilendirme Kontrolleri

NASIL ÖNLENİR?

- Güçlü Şifre Politikaları Uygulama
- Kimlik Doğrulama Yöntemlerini Güçlendirme
- Etkin Çok Faktörlü Kimlik Doğrulama Kullanma
- Güvenli Oturum Yönetimi Sağlama
- Yetkilendirme Kontrollerini Doğru Yapılandırma

A8 - SOFTWARE AND DATA INTEGRITY FAILURES



Software and Data Integrity Failures, bir yazılımın veya verinin bütünlüğünün sağlanamaması sonucu oluşan güvenlik açıklarını ifade eder. Bu zafiyetler, yazılım güncellemeleri, veritabanları ve uygulama bileşenleri gibi bileşenlerin bütünlüğünün kontrol edilmemesi veya sağlanamaması durumunda ortaya çıkar. Saldırganlar, bu tür açıklardan yararlanarak zararlı kod ekleyebilir veya verileri değiştirebilir.

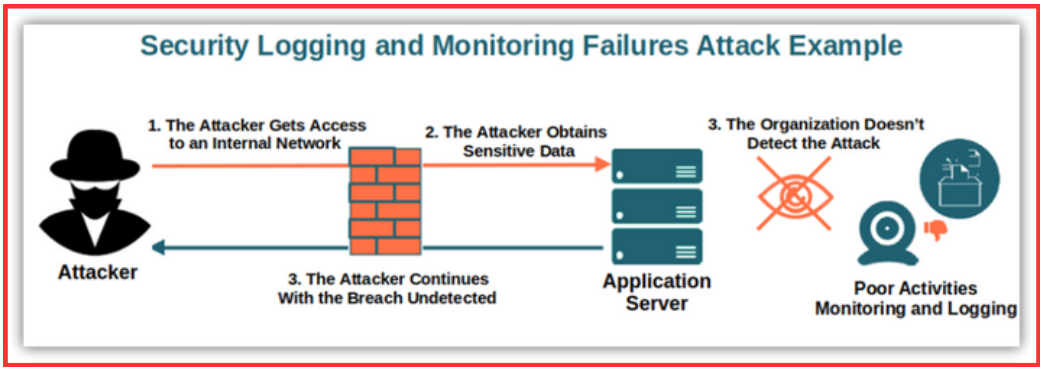
NEDEN KAYNAKLANIR?

- Yazılım Bütünlüğü Kontrollerinin Eksikliği
- Güvenli Olmayan Güncelleme ve Dağıtım Mekanizmaları
- Yetersiz Veri Doğrulama ve Temizlik
- Güvenlik Açıkları İçeren Üçüncü Taraf Bileşenler

NASIL ÖNLENİR?

- Yazılım Bütünlüğü Kontrolleri Sağlama
- Güvenli Güncelleme ve Dağıtım Prosedürleri Uygulama
- Veri Doğrulama ve Temizlik Prosedürleri Uygulama
- Güvenlik Açıkları İçeren Üçüncü Taraf Bileşenleri İzleme
- Erişim Kontrollerini Güçlendirme

A9 - SECURITY LOGGING AND MONITORING FAILURES



Security Logging and Monitoring Failures, bir sistemin güvenlik olaylarını yeterince detaylı ve etkili bir şekilde günlüğe kaydetmemesi ve izlememesi sonucu ortaya çıkan güvenlik açıklarını ifade eder. Bu zafiyet, sistemlerin güvenlik olaylarını, ihlalleri ve anormal davranışları yeterince izlemediği veya raporlamadığı durumlarda ortaya çıkar. Saldırıların tespit edilmesini, yanıt verilmesini ve analiz edilmesini zorlaştırır.

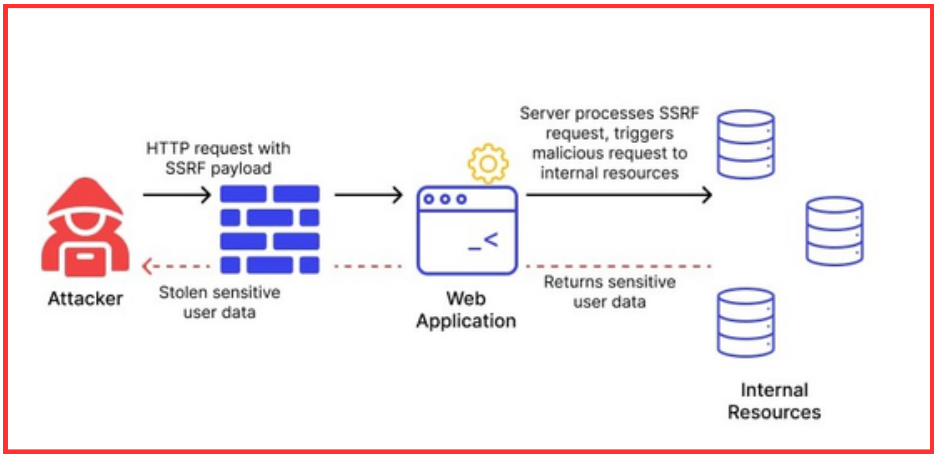
NEDEN KAYNAKLANIR?

- Yetersiz Günlük Kaydı ve İzleme
- Günlüklerin Güvenli Saklanmaması
- Günlük Yönetimi Prosedürlerinin Eksikliği
- Güvenlik Olaylarına Yetersiz Yanıt

NASIL ÖNLENİR?

- Detaylı Günlük Kaydı Yapma
- Günlükleri Güvenli Saklama
- Etkin İzleme Araçları Kullanma
- Olaylara Hızlı Yanıt Verme
- Günlük Yönetimi Prosedürleri Oluşturma

A10 - SERVER-SIDE REQUEST FORGERY



SSRF, bir saldırganın, uygulamanın sunucu tarafında istekler yapmasını sağladığı bir güvenlik açığıdır. Saldırgan, uygulama sunucusunun iç ağ kaynaklarına veya başka hedeflere istek göndermesini manipüle edebilir. Bu, iç sistemlere yetkisiz erişim sağlayabilir ve hassas bilgilerin sızmasına yol açabilir.

NEDEN KAYNAKLANIR?

- Dışarıdan Gelen İsteklerin İç Kaynaklara Yönlendirilmesi
- Yetersiz Girdi Doğrulama
- Hatalı Yetkilendirme ve İzinler
- Yanlış Yapılandırılmış URL İstemcileri

NASIL ÖNLENİR?

- Girdi Doğrulama ve Beyaz Liste Kullanımı
- İç Kaynaklara Erişimi Kısıtlama
- Yapılandırmaları Güvenli Hale Getirme
- Ağ İzolasyonu ve Güvenlik Duvarları
- Güvenlik Açıklarını İzleme ve Kapatma