Owasp top 10 ödevi

-Broken Access Control

Saldırganların uygulamalarda yapılan yanlış konfigürasyonlar sonucu istenmeyen bilgilere yetkiliymiş gibi denetimsiz erişim sağlamasıdır.

Nasıl önlenir?

-Halka açık veriler haricinde istekleri reddederek

-API isteklerine Rate Limiti ekleyerek

-Tokenler kullanılarak

-Cryptographic Failures

Şifrelenme kullanılarak korunan bilgilerin yanlış şifrelendiğinde yada şifrelenme sırasında hata olduğunda ortaya çıkan bir sorundur. Bir saldırgan eğer şifrelenmiş verileri ortaya çıkarsa yetkisiz erişimde bulunabilir yada istenmeyen verilerin yetkisiz erişimine sebep olabilir.

Nasıl Önlenir?

-Kullanımda olmayan tüm veriler şifrelenerek.

-Rastgele sayı üretimi doğru yapılarak.

-Güçlü şifre algoritmaları kullanılarak.

-Injection

Injection programa dahil olmaması gereken bir kod parçasını dahil ederek programın çalışmasını saldırganın isteğine göre değiştirebilme zaafiyetidir. Cookie'ler ve Database sızıntılarına sebep olabilirler.

Nasıl Önlenir?

-Sunucu tarafında kullanıcı girdisi filtrelenerek.

-WAF Kullanılarak.

-Insecure Design

Bir web sitenin güvensiz tasarımından kaynaklanır. Bu site içerisindeki verilerin ömrüyle kaynaklı olabilir. Kimlik doğrulama, Limitlenmiş verilerin değiştirilmesi ve veri gizliliği ihlaline sebep olabilir.

Nasıl Önlenir?

-Güvenli tasarım öğeleri

-Güvenlik açıklarının tespiti ve düzeltilmesi

-Security Misconfiguration

Bir sistem veya uygulama sırasında yapılan hatalar sonucu sistem içerisindeki bilgilerin hata vermesi veya hatalı çalışmasından kaynaklanır. Yanlış yapılandırma nedeniyle saldırgan aktörleri sisteme yetkisiz erişimde bulunabilir ve veri ihlaline sebep verebilirler.

Nasıl Önlenir?

-Sistem Güncellemeleri takip edilerek.

-Yazılım güvenlik düzeyini kontrole edilerek.

-Sistem hardening yapılarak.

-Vulnerable and Outdated Components

Bu zaafiyet İşletim sistemleri, Web/uygulama sunucuları, API'lar, Database sistemleri ve Plugin/Kütüphanelerden kaynaklanabilirler. Bilinen zaafiyetli uygulamaların kullanılması yada güncel olmayan uygulamaların kullanılması sonucu sistemde saldırganın kullanabileceği bir zaafiyet oluşur.

Nasıl Önlenir?

-Kullanılmayan eklentilerin kaldırılması.

-Doğru kaynaklardan eklenti alınması.

-Identification and Authentication Failures

Bir kullanıcının kimlik doğrulaması yada yetkilendirilme sırasında yaşanan hatalar sebebiyle oluşan zaafiyettir. Saldırgan başka biri gibi bilgilerine erişip sisteme yetkisiz erişimde bulunabilir. 2FA doğrulama, Şifreleme yöntemleri ile korunulabilir.

Nasıl önlenir?

-Sağlam şifreler kullanılarak

-Default şifrelerden kaçınılarak

-Hatalı girişlerin limitlendirilmesi yapılarak.

-Software and Data Integrity Failures

Bu Zaafiyet bütünlük ilkelerinin göz ardı edilmesiye oluşur. Örnek olarak bir wordpress sitesinin güvenilir bir kaynaktan olmayan plugin kullanması verilebilir. Böyle durumlarda güvenilir olmayan kaynaklar potansiyel bir saldırganın siteye erişim sağlamasına sebep olabilir.

Nasıl Önlenir?

-Güçlü erişim kontrolleri oluşturularak.

-Kullanılan kaynakların güvenilirliği araştırılarak.

-Veri yedekleri oluşturularak.

-Security Logging and Monitoring Failures

Bu zafiyet daha çok siteye yapılan saldırıların veya girişlerin yeterli denetimde bulunamaması sebebiyle kritik ihlallerin tespit edilememesi sonucu oluşur. Bunu önleyebilmek adına Günlük olarak log dosyalarının incelenmesi, Uyarı ve alarm sistemleri kullanılması (IDS, IPS) ve Güvenlik ihlallerini izleyebilmek adına uygun araçların kullanılması gerekir.

Nasıl önlenir?

-Bütün hareketlerin kaydedilmesi yapılarak.

-Uyarı ve alarm sistemleri kullanılması (IDS, IPS)

-Günlük olarak log dosyalarının incelenmesi

-Server-Side Request Forgery

Sunucu tarafına istek göndererek sunucunun özelliklerinden yararlanıp C.I.A. üçlemesini ihlal

edebilecek verilerin değiştirilebilmesine yada gizli kalması gereken verilere erişilebilmesine sebep olur.

Nasıl önlenir?

Ağ katmanından:

-Uzaktan kaynak erişimi limitlenerek.

-”deny by default” ayarı yapılarak.

Sunucu katmanından:

-Kullanıcı girdisi filtrelenerek.

-Raw cevap göndermeyerek.

-HTTP yönlendirmelerini engelleyerek.