ZAFİYET NEDİR?

Siber güvenlik zafiyeti elektronik bir sistemde tespit edilen arka kapılar, saldırılara açık olan zayıflıklar ve benzeri hatalar olarak tanımlanır. Siber saldırganlar bu zafiyetleri tespit ederek sistemlere saldırabilir, zarar verebilir, veyahut belirli işlemlerden sonra bu sistemleri ele geçirebilir. Hatalar, arka kapılar veyahut bunların benzerlerini siber güvenlik zafiyetleri olarak tanımlamaktayız.

ZAFİYET NEDEN KAYNAKLANIR?

Zafiyet oluşmasının birçok sebebi vardır. Büyük yazılımlarda hatalara daha sık rastlanır. Herkesçe bilinen yazılımların kullanılması, o koda aşinalığı arttırır. Dolayısıyla bir saldırgan, halihazırda bildiği bir kodda daha kolay bir şekilde zafiyet bulabilir. Bir yazılımın internete bağlığı artıkça da zafiyetlerin sayısı artar. Kullanıcı girdisinin kontrol edilmemesini de zafiyetlere sebep olabilir. Kısaca özetlemek gerekirse, kodlama ve kurulum -konfigürasyon- hataları zafiyetlerin temel sebepleridir.

OWASP TOP 10

1) BROKEN ACCESS CONTROLL

Uygulamalarda veya sistemlerdeki erişim kontrol mekanizmalarının yetersiz veya hatalı olması durumunu ifade eder. Bu tür bir zayıflık, yetkisiz kullanıcıların sistem kaynaklarına erişmesine veya hassas verilere ulaşmasına olanak tanıyabilir. Bu nedenle, güvenlik açısından bu tür hataların düzeltilmesi önemlidir.

Önlemler

-İyi bir yetkilendirme ve kimlik doğrulama sistemi kullanma

-İşlemlerin **logları** ***tutulmalı ki, kimin hangi kaynaklara eriştiği izlenebilir ve denetlenebilir olmalıdır.***

-İhtiyaçlar doğrultusunda erişim kontrolleri uygulama

2) CRYPTOGRAPHİC FAİLURES

Kriptografi kullanılarak korunan verilerin, yanlış bir şekilde şifrelendiği veya şifresinin çözüldüğü durumlardır. Kriptografik algoritmaların yanlış kullanımı, zayıf anahtar yönetimi, rastgele sayı üretimindeki eksiklikler veya protokollerin güvenli olmayan şekilde tasarlanması gibi nedenlerden kaynaklanabilir.

Önlemler

-Doğru şifreleme algoritmaları kullanılmalıdır.

-Rastgele sayı üretimi doğru kullanılmalıdır.

-Anahtar yönetimi hatalarından kaçınılmalıdır.

3) INJECTİON

Web uygulamalarında sıklıkla görülen bir güvenlik açığıdır. Enjeksiyon saldırıları, genellikle kullanıcı giriş alanlarına (örneğin web formları) girilen veriler aracılığıyla gerçekleştirilir. Kötü niyetli kullanıcılar, bu giriş alanlarına zararlı kodlar veya komutlar ekleyerek, uygulamaların beklenmeyen şekilde davranmasını sağlayabilirler. Bu tür saldırılar, veritabanı enjeksiyonu (SQL Injection), komut enjeksiyonu, XSS (Cross-Site Scripting) gibi çeşitli şekillerde gerçekleştirilebilir.

Önlemler

-Parametrelerin doğrulanması

-SQL parametrelestirme

-Kodlama standartları

-WAF Kullanımı

4) INSECURE DESİGN

Güvensiz tasarım, uygulamaların veya sistemlerin doğru güvenlik önlemleriyle tasarlanmaması sonucunda oluşabilir. Bu durum, kötü niyetli kişilerin sisteme sızmasını kolaylaştırabilir, hassas verilerin çalınmasına veya değiştirilmesine olanak tanıyabilir.

Önlemler

-Güvenlik ilkelerine uygun tasarım

-Güncel kalma

-Güvenlik açıkları düzeltilebilmelidir

5) SECURİTY MİSCONFİGURATİON

Bu terim, bilgisayar güvenliği alanında sıkça kullanılan bir terimdir ve genellikle sistemlerin veya uygulamaların güvenlik ayarlarının yanlış yapılandırılması durumudur.

Önlemler

-En iyi uygulamaları takip etmek

-Sistem yapılandırması güncellemek

-Varsayılan şifreleri değiştirmek

-Gereksiz hizmetleri kapatmak

6) VULNERABLE AND OUTDATED COMPONENTS

Bu ifade genellikle yazılım veya uygulamalardaki bileşenlerin güvenlik açıklarına sahip olması veya güncel olmayan sürümlerinin kullanılması durumunu belirtir. Bu

bileşenler genellikle web uygulama, veritabanı yönetim sistemleri, açık kaynak kütüphaneler gibi bileşenler olabilir

Önlemler

-Bileşenleri izlemek

-Güncelleme politikalarını oluşturmak

7) IDENTİFİCATİON AND AUTHENTİCATİON FAİLURES

Bu ifade genellikle kimlik doğrulama süreçlerinde veya mekanizmalarında yaşanan hataları ve zayıflıkları belirtir. Kimlik doğrulama, bir kullanıcının kimliğini belirlemek ve doğrulamak için kullanılan süreçtir. Kimlik doğrulama hataları, yanlış kimlik belirleme veya yanlış kimlik doğrulama gibi durumları içerebilir.

Önlemler

-Güçlü şifre politikaları uygulamak

-Kimlik bilgilerini şifrelemek

-Çok Faktörlü Kimlik Doğrulaması yapmak

8) SOFTWARE AND DATA INTEGRİTY FAİLURES

Yazılım ve veri bütünlüğü hataları, yazılımın veya verilerin beklenmedik şekilde değiştirilmesi, bozulması veya kaybolması durumlarını kapsar. Bu tür hatalar, yazılımın doğru şekilde çalışmasını engelleyebilir, veri kaybına veya güvenlik açıklarına yol açabilir.

Önlemler

-Veri yedekleme ve kurtarma stratejileri kullanmak

-Güvenlik yazılımları ve güncellemeler yapmak

-Güçlü erişim kontrolü uygulamak

9) SECURİTY LOGGİNG AND MONİTORİNG FAİLURES

Güvenlik kayıt tutma ve izleme hataları, sistemlerde veya ağlarda güvenlik olaylarının yeterince kaydedilmemesi, izlenmemesi veya yanlış yapılandırılması durumlarını ifade eder.

Önlemler

-Güvenlik olaylarının izlenmesi

-Güvenlik izleme araçları kullanmak

-Otomatik uyarılar ve bildirimler

10) SERVER-SİDE REQUEST FORGERY

Kötü niyetli bir saldırgan, sunucunun dışındaki kaynaklara doğrudan erişim sağlayarak sunucuda istekler yapmasını sağlayan bir saldırı türü. Saldırgan, sunucunun güvenlik önlemlerini aşar, sunucunun iç ağ yapısına veya dış kaynaklara erişebilir ve bu durum ciddi güvenlik riskleri oluşturur.

Önlemler

-Giriş doğrulaması

-Güvenlik duvarı kurulumu

-Güvenilir kaynak kontrolü

ZAFİYET İÇİN ÖRNEK RESİMLER