Owasp Top 10 Zafiyetler

1.Broken Authentication : Saldırganın sistemdeki kimlik doğrulama zayıflıklarından yararlanarak sisteme yetkisiz erişmesi ,elinde olan kullanıcı adı ve parola listesiyle herhangi bir kullanıcının hesabına erişim sağlamasıdır.

Neden kaynaklanır?

-Kullanıcıların zayıf ve tahmin edilebilir parola seçimi
-Base64 gibi zayıf şifreleme tekniklerinin kullanılması
-Session id lerinin zayıf olması
-Çok faktörlü kimlik doğrulamanın olmaması

Nasıl önlenir?

-En az iki farklı doğrulama yöntemi kullanılmalı.
-Başarısız oturum açma girişimlerini sıralamak ve her denemede giriş süresini uzatmak.
-Kullanıcı tokenlarının uzun süre aktif tutulmamasına özen gösterilmesi
-Oturum id değerlerinin url üzerinde bulunmaması.

2.Cryptographic Failures : Verilerin şifrelenip tutulması gerekirken düz metin halinde tutulması ya da verinin şifrelendiği halde zayıf algoritmalar kullanılmasından kaynaklı oluşan güvenlik açığıdır.

Neden Kaynaklanır ?

-Zayıf güvenlik algoritmalarının kullanılması
-Verilerin şifrelenmemiş olarak iletilmesi
-Zayıf algoritmaların rastgele değer üretememesi

Nasıl önlenir?

-Veriler sınıflandırılıp hassas olarak sınıflandırılmış gereksiz veriler saklanmamalı.
-Hassas verilerin saklanması gerekiyorsa şifrelenerek saklanmalı.
-Güçlü şifreleme algoritmaları kullanılmalı

3.Injection : Kullanıcıdan input alınan(arama kutuları, giriş formları veya yorum bölümleri gibi) kontrol edilmeyen ya da önlem alınmayan verilerin komut olarak çalıştırılmasıdır.

Neden kaynaklanır?

-Kullanıcı girdi doğrulamadaki eksiklikler
-Kullanıcıdan alınan verilerin filtrelenmemesi
-Uygulamanın parametrelendirilmiş sorgulardan yoksun olması

Türleri nelerdir?

-Sql injection: Saldırganın uygulama tarafından veri tabanına gönderdiği sql sorgularını manipüle edip çalıştırmasına olanak tanıyan bir güvenlik tehdidi türüdür.
-XSS: Saldırganın script kodları üzerinden web sayfasına saldırı yapmasıdır. Web tarayıcısı, zararlı kodu html kodunun bir parçası olarak çalıştırır.

-Command injection: Saldırganın, bir uygulamayı çalıştıran sunucuda işletim sistemi komutlarını yürütmesidir.

Nasıl önlenir?

-Client-side'da alınan input filtrelenmeli ve doğrulanmalı-> regex validation
-ORM kullanılmalı.
-Özel karakterler encode edilmeli.
-Inputlarda yer alanan sql komutları kabul edilmemeli.

4.Insecure Design : Web uygulamasının tasarımında yapılan hatalar veya eksiklikler nedeniyle ortaya çıkan bir güvenlik açığıdır.

Neden kaynaklanır?

-Kimlik doğrulama ,yetkilendirmede hata içermesi

-Veri gizliliği ve bütünlüğüne önem verilmemesi

Nasıl önlenir?

-Stride ,dread,pasta gibi tehdit modelleri kullanılabilir.

-AppSec profesyonelleriyle çalışılabilir.

5.Security Misconfiguration : Bir uygulamanın ya da sistemlerin yanlış yapılandırılması veya yapılandırılmamış olması sonucu oluşan bir güvenlik açığıdır.

Neden kaynaklanır?

-Güvenlik açıklarını gidermek için yayımlanan güncellemelerin takip edilip ,düzeltilmemesi

-Varsayılan hesapların parolalarının değiştirilmemesi.

Nasıl önlenir?

-Sistem yapılandırmasını güncellemek

-Güvenlik güncellemeleri takip etmek

---

6. Vulnerable and Outdated Components : Bir uygulamada kullanılan üçüncü taraf bileşenlerin güncellenmemesi veya bilinen güvenlik açıklarına sahip bileşenlerinin kullanılmasından dolayı oluşan bir güvenlik açığıdır.

Neden kaynaklanır?

-Artık desteklenmeyen, eski veya zafiyet barındırdığı bilinen bileşenlerin kullanılması

Nasıl önlenir?

-Kullanılan bileşenleri resmi kaynaklardan elde etmek
-CVE takip ederek buradaki açıkları barındıran bileşenlerden herhangi birinin sistemde mevcut olup olmadığını kontrol etmek
-Kullanılmayan tüm bileşenleri silmek

---

7. Identification and Authentication Failures :Kimlik doğrulama ve oturum yönetimindeki eksiklikler, yetkisiz

kullanıcıların sisteme erişimine yol açabilen güvenlik açığıdır.

Neden kaynaklanır?

-Zayıf parola politikaları

-Oturum yönetimi hataları

-Çok faktörlü kimlik doğrulama eksikliği

Nasıl önlenir?

-Otomatik kimlik bilgisi doldurma, kaba kuvvet ve çalınan kimlik bilgisi yeniden kullanma saldırılarını önlemek için çok faktörlü kimlik doğrulama uygulanabilir.

-Güçlü kimlik doğrulama yöntemleri kullanmak

-Kimlik bilgilerini şifrelemek

8.Software and Data Integrity Failures :Yazılım veya verinin yetkisiz veya beklenmedik şekilde değiştirilmesi durumunda ortaya çıkan güvenlik açığıdır.

Neden kaynaklanır?

- Bir yazılım güncellemesi sırasında, yazılımın kötü amaçlı bir saldırgan tarafından değiştirilmesi

-Saldırganın veri depolama ortamına kötü amaçlı yazılım yerleştirmesi

Nasıl önlenir?

-Yazılım veya verinin beklenen kaynaktan geldiğini ve değiştirilmediğini doğrulamak için dijital imzalar kullanılabilir.

-CI/CD süreçlerinin sadece yetkili kişiler tarafından erişilebilir olmasını sağlamak

-Web uygulamalarında JSON Web Tokens kullanırken, tokenların güvenli bir şekilde imzalandığından emin olmak.

9.Security Logging and Monitoring Failures :

Güvenlik olaylarının izlenmesi ve kaydedilmesi

işlevlerinin yetersizliği veya hatalı yapılandırılması sonucu ortaya çıkan bir güvenlik açığıdır.

Neden kaynaklanır?

-İzleme mekanizmalarının eksikliği

-Kayıtların yeterince detaylı olmaması

Nasıl önlenir?

-Giriş doğrulama hatalarının kaydedildiğinden emin olunmalı

-Adli analiz yapılabilmesi için yeterli süre saklanmalı

10.Server-Side Request Forgery (SSRF):

Saldırgan hedef sunucuya giden istekleri, zafiyetli web uygulamasındaki parametreleri değiştirip isteklerin varış noktalarını manipüle edebilir.Yani web uygulaması adına istek gönderebilir.

Neden kaynaklanır?

-URL validation olmaması

-Web sunucusunun uzak kaynakları çağırmasına izin verilen domainler ve protokoller denetlenmemesi

Nasıl önlenir?

-Kullanıcı girişlerinin doğrulanması

-Sadece izin verilen protokoller ve güvenli url'ler kabul edilmeli

-Uygulama, güvenilir hedeflerin white listini tutarak sadece bu hedeflere istek gönderilmesine izin vermeli

-file://, dict://, ftp:// gibi url şemaları kullanılmaması

-Http redirectionlarının kontrolünün yapılması

~Rukiye Esra Cizmeci