OWASP Top 10

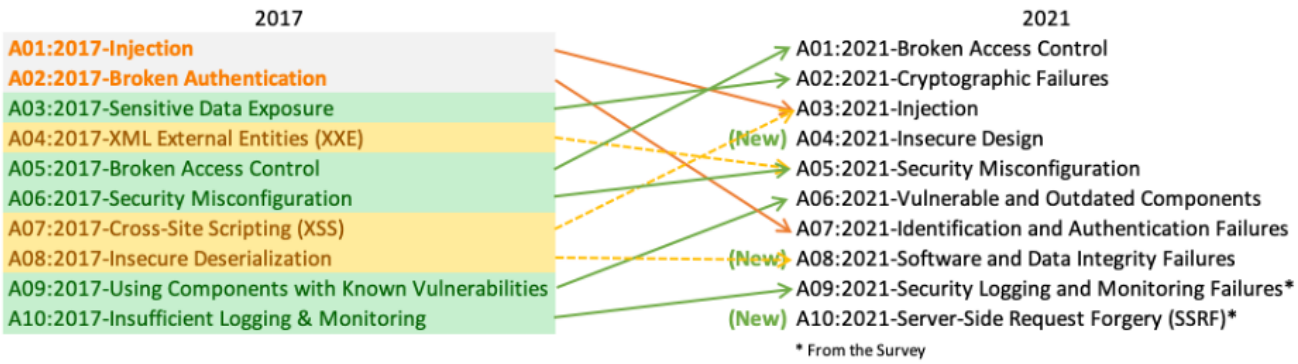
Öncelikle Siber güvenlikte zaafiyet elektronik bir sistem üzerinde yer alan donanım veya yazılımları, siber saldırılara açık hale getiren hatalar olarak tanımlayabiliriz

OWASP Top Ten, **Open Web Application Security Project (OWASP)**

OWASP Top Ten, **Open Web Application Security Project (OWASP)** tarafından hazırlanan ve web uygulamaları için en kritik güvenlik risklerini içeren bir listeyi ifade eder. Bu liste, geliştiriciler, güvenlik uzmanları ve organizasyonlar için bir rehber olarak kabul edilir ve web uygulamalarının güvenliğini sağlama konusunda en yaygın ve en tehlikeli güvenlik açıklarına odaklanır.

OWASP Top Ten listesi, belirli bir sabit periyotla yayınlanmaz, ancak genellikle yaklaşık **3 ila 4 yılda bir** güncellenir. Güncellemeler,yeni tehditlerin ortaya çıkmasıyla birlikte, en güncel ve yaygın güvenlik risklerini yansıtacak şekilde yapılır.

Güncel olarak OWASP Top Ten kategorileri şöyledir ;



- **A01:2021-Broken Access Control**
- **A02:2021-Cryptographic Failures**
- **A03:2021-Injection**
- **A04:2021-Insecure Design**
- **A05:2021-Security Misconfiguration**
- **A06:2021-Vulnerable and Outdated Components**
- **A07:2021-Identification and Authentication Failures**
- **A08:2021-Software and Data Integrity Failures**
- **A09:2021-Security Logging and Monitoring Failures**
- **A10:2021-Server-Side Request Forgery**

- ## A01:2021-Broken Access Control

Broken Access Control, uygulamalarda yapılan yanlış veya yetersiz erişim kontrolü ayarları sonucu, yetkisiz kullanıcıların uygulama içerisinde yer alan kaynaklara erişmesine olanak sağlayan bir güvenlik açığıdır. Bu açığın etkileri , yetkili olmayan bir kullanıcının sisteme veya uygulamaya erişim hakkı olmadan bu kaynaklara erişmesine veya bunları değiştirmesine olanak sağlayabilir.

Broken Access Control açığından korunmak için alınması gereken önlemler:

Erişim kontrolleri düzgün yapılandırılmalıdır

Token-based authentication kullanılmalıdır

İşlemlerin logları tutulmalı

- ## A02:2021-Cryptographic Failures

Cryptographic Failures, Burada odak noktası, genellikle hassas verilerin açığa çıkmasına veya sistemin tehlikeye atılmasına yol açan kriptografiyle ilgili hatalardır.

Cryptographic Failures açığından korunmak için alınması gereken önlemler:

Doğru şifreleme algoritmaları kullanılmalıdır

Anahtar yönetimi hatalarından kaçınılmalıdır

Rastgele sayı üretimi doğru yapılmalıdır

Kriptografik anahtarların düzenli olarak yenilenmesi gerekmektedir

- ## A03:2021-Injection

Injection,. Bu açık, uygulamalarda kullanılan veri girişleri yoluyla, kötü niyetli kullanıcıların uygulama tarafından yürütülen veritabanı sorgularına, komutlara veya diğer işlevlere veri girişlerinde yapılan hatalı denetlemeler veya filtrelemeler nedeniyle zararlı kod enjekte etmesini sağlar. Saldırganlar, bu açıktan yararlanarak, uygulamaların veritabanını veya sunucularını ele geçirerek, kullanıcı bilgilerine veya diğer hassas verilere erişim sağlayabilirler.

Injection açığından korunmak için alınması gereken önlemler:

· Parametrelerin Doğrulanması

· SQL Parametreleştirme

· Kodlama Standartları

· WAF Kullanımı

- ## A04:2021-Insecure Design

Insecure Design. Bir web uygulamasının tasarımında yapılan hatalar veya eksiklikler nedeniyle ortaya çıkan bir güvenlik açığıdır. Bu, uygulamanın tasarımında yapılan hataların, uygulamanın tüm yaşam döngüsü boyunca devam etmesine ve güvenliğini olumsuz etkilemesine neden olabilir. Güvensiz tasarım, uygulamanın özellikle kimlik doğrulama, yetkilendirme, veri gizliliği ve bütünlüğü gibi önemli güvenlik konularında hatalar içermesiyle ortaya çıkabilir.

Insecure Design açığından korunmak için alınması gereken önlemler:

· Güvenli tasarım ilkeleri uygulanmalıdır

· Uygulama geliştirme ekibi, güvenlik odaklı bir yaklaşım benimsemelidir

· Güvenlik açıkları düzeltilmelidir

· Uygulama güvenliği için en iyi uygulamalar kullanılmalıdır

- ## A05:2021-Security Misconfiguration

Security Misconfiguration, bu kategoride ise sitemin yanlış yapılandırılması veya yapılandırılmamış olması sonucu oluşan bir güvenlik açığıdır

Örnek olarak, bir web uygulaması sunucusunun yanlış yapılandırılması sonucu uygulamada zafiyet olabilir. Bu durumda, uygulama sunucusu için önerilen en iyi uygulamaların uygulanmamış olması nedeniyle, saldırganlar uygulama sunucusuna erişebilirler ve hassas verileri ele geçirebilirler.

Security Misconfiguration açığından korunmak için alınması gereken önlemler:

· En iyi uygulamaları takip etmek

· Yazılımın güvenlik düzeyini kontrol etmek

· Güvenlik yamalarını ve güncellemeleri takip etmek

· Sistem yapılandırmasını güncellemek

- ## A06:2021-Vulnerable and Outdated Components

Vulnerable and Outdated Components, Birçok modern uygulama, üçüncü taraf bileşenlerin kullanımını içerir(Bilgisayar programcılığında üçüncü parti bileşen, geliştirme platformunu sağlayan haricindeki şahıs ya da firma tarafından satılan veya dağıtılan, yeniden kullanılabilir bir yazılım bileşenidir.) Bu bileşenler, genellikle web uygulama çerçeveleri, veritabanı yönetim sistemleri, açık kaynak kütüphaneler, sunucu yazılımı ve diğer araçlar gibi yazılım bileşenleri olabilir. Bu bileşenlerde güvenlik açıkları keşfedilmesi halinde, uygulama da savunmasız hale gelebilir.

Vulnerable and Outdated Components açığından korunmak için alınması gereken önlemler:

· Bileşenleri izlemek

· Güncelleme politikaları oluşturmak

· Bileşenleri doğrulamak

- ## A07:2021-Identification and Authentication Failures

Identification and Authentication Failures, bir kullanıcının kimliğinin doğrulanması veya yetkilendirilmesi sırasında yaşanan sorunlar nedeniyle oluşan bir güvenlik açığıdır. Bu tür saldırların etkileri saldırganın kullanıcı kimliğini çalmasına veya sahte bir kimlik kullanarak uygulamaya erişim sağlamaya yol açabilir.

Örneğin, bir uygulama, kullanıcı adı ve parola kombinasyonu gibi temel kimlik doğrulama yöntemlerini kullanarak kimlik doğrulama yapabilir. Ancak, uygulama bu bilgileri doğru bir şekilde doğrulamazsa, saldırganların sahte kimlik bilgileri kullanarak sisteme giriş yapması mümkündür.

Identification and Authentication Failures açığından korunmak için alınması gereken önlemler:

· Güçlü kimlik doğrulama yöntemleri kullanmak

· Kimlik doğrulama işlemlerini izlemek

· Kimlik bilgilerini şifrelemek

· Düzenli olarak kimlik doğrulama politikalarını kontrol etmek

· Çok faktörlü kimlik doğrulama yöntemlerini kullanmak

- ## A08:2021-Software and Data Integrity Failures

Yazılım ve veri bütünlüğü hataları, bir yazılım veya veri sisteminin beklenmeyen şekilde değiştirilmesi bozulması sonucu meydana gelen bir güvenlik açığıdır. Bu zafiyet, bir saldırganın yazılım veya veri sistemini hedef alarak sistemi istismar etmesine veya manipüle etmesine izin verebilir.

Senaryo:

Saldırgan, e-ticaret platformunun API uç noktalarını tarar ve API uç noktalarının yazılım ve veri bütünlüğü doğrulama kontrollerinin eksik olduğunu fark eder.
Saldırgan, ödeme işlemi sırasında kullanılan bir API uç noktasına kötü niyetli bir veri paketi gönderir. Bu veri paketi, sahte bir ödeme tutarı içermektedir.
Saldırgan, platforma güncellemeler sağlayan bir bileşenin güncelleme paketini manipüle eder. Kötü niyetli kodlar içeren bu güncelleme paketi, yazılımın çalışmasını bozabilir veya arka planda gizli işlemler yapabilir.
Sipariş veritabanındaki veri bütünlüğü eksikliklerinden yararlanan saldırgan, kendi siparişlerini sistemde sahte ürünlerle değiştirebilir ve düşük fiyatlarla ödeme yapabilir. Bu, hem mali kayıplara hem de müşteri memnuniyetsizliğine yol açabilir.

· Yazılımın veya verilerin beklenen kaynaktan olduğunu ve değiştirilmediğini doğrulamak için dijital imzalar veya benzer mekanizmaların kullanımı

· Npm veya Maven gibi kitaplıkların ve bağımlılıkların güvenilir depoları kullandığından emin olmak

· Kod ve yapılandırma değişiklikleri için bir inceleme süreci oluşturmak

· Yazılım güncellemelerini düzenli olarak yükleme

· Güçlü erişim kontrolü uygulamak

· Güvenli yazılım geliştirme yöntemlerini kullanmak

· Yazılım ve veri yedeklemeleri oluşturmak

- ## A09:2021-Security Logging and Monitoring Failures

Security Logging and Monitoring Failures, güvenlik olaylarının izlenmesi ve kaydedilmesi işlevlerinin yetersizliği veya hatalı yapılandırılması sonucu ortaya çıkan bir güvenlik açığıdır

Security Logging and Monitoring Failures açığından korunmak için alınması gereken önlemler:

· Güvenlik olaylarının izlenmesi ve kaydedilmesi için uygun araçlar kullanmak

· Günlük kayıtlarının düzenli olarak incelenmesi

· Uyarı ve alarm sistemleri kullanmak

· Güvenlik politikalarının ve prosedürlerinin düzenli olarak gözden geçirilmesi

- ## A10:2021-Server-Side Request Forgery

Sunucu Taraflı İstek Sahtekarlığı (SSRF), bir saldırganın hedef sunucuda bir URL'ye istek gönderirken sahte bir kaynak IP adresi ve alan adı sağlayarak sunucunun kendi iç ağlarına veya diğer harici kaynaklara erişmesine izin veren bir web güvenliği açığıdır.

SSRF, hedef sunucu için ciddi bir güvenlik tehdidi oluşturur, çünkü saldırgan sunucuya istekler göndererek hassas verileri çalabilir, sunucunun kaynaklarını tüketebilir, sunucunun kontrolünü ele geçirebilir veya sunucunun çalışmasını bozabilir.

· Giriş doğrulaması

· Güvenlik duvarı kurulumu

· Güvenli URL işleme

· Sunucu ayarlarının kontrol edilmesi