OWASP Top 10 Zaafiyetleri ve Alınabilecek Önlemler

1-)Broken Access Control

Kırık Erişim Kontrolü, Web uygulamalarında kimlik doğrulama ve oturum yönetimine bağlıdır. Kimlik doğrulamanın amacı kullanıcıyı doğrulamaktır. Oturum yönetimi hangi HTTP isteklerinin aynı kullanıcı tarafından yapıldığını tanımlar Bozuk erişim kontrolü zafiyeti, bir kullanıcının görmemesi gereken hassas bilgilerin (örneğin kullanıcı adları, parolalar, kredi kartı numaraları, kişisel bilgiler vb.) verilerin çalınmasına, değiştirilmesine, yok edilmesine ve herhangi bir kullanıcının Bu tür bilgilerin açığa çıkması, kullanıcıların kimlik hırsızlığı, dolandırıcılık veya diğer kötü niyetli faaliyetler için hedef haline gelmelerine neden olabilir.

Bozuk erişim kontrolüne örnekler

Dikey yetki yükseltme, genellikle bir uygulamanın hassas işlevlerine yeterince güvenlik önlemi uygulamadığı durumlarda ortaya çıkar. Örneğin, bir yönetici paneline erişim sağlamak için sadece yönetici yetkilerine sahip kişilere özel bağlantılar verilmelidir. Ancak, eğer bu bağlantılar tüm kullanıcılar tarafından görülebilirse, bir kullanıcı doğrudan yöneticilere özel URL'lere erişim sağlayabilir.

Sonuç olarak, hassas işlevlerin güvenliği için yalnızca URL'leri gizlemek yeterli değildir; etkili bir erişim kontrolü uygulanması gerekmektedir.

Yatay yetki yükseltme, bir kullanıcının kendi verileri yerine başka bir kullanıcının verilerine erişim sağlaması durumunda ortaya çıkar. Örneğin, bir çalışanın yalnızca kendi işe alım ve bordro bilgilerine erişmesi gerekirken, diğer çalışanların bilgilerine de erişim sağlaması yatay yetki yükseltmedir.

Konum tabanlı erişim kontrolü, bazı web sitelerinde kullanıcının coğrafi konumuna göre belirli kaynaklara erişimi sınırlandırma yöntemidir. Bu tür kontroller, özellikle eyalet yasaları veya ticari kısıtlamalar gibi düzenlemelerin geçerli olduğu bankacılık ve medya hizmetleri gibi alanlarda uygulanır. Ancak, bu erişim denetimleri web proxy'leri, VPN'ler veya istemci tarafında kullanılan coğrafi konum belirleme yöntemlerinin manipülasyonu ile kolayca aşılabilir.

JSON Web Token veya Çerezlerin Manipülasyonu Kullanıcı tarafından düzenlenen JWT veya çerezler aracılığıyla yetki bilgilerini değiştirmek.

Broken Access Control'dan Korunma Yolları

Web uygulamalarını bozuk erişim kontrolü zafiyetlerinden korumak için şu önlemler alınmalıdır:

- Güçlü kimlik doğrulama ve oturum yönetimi uygulamak.
- En az ayrıcalık ilkesini benimsemek.
- Erişim kontrollerini düzenli testleri ve güncellemeleri gerçekleştirmek.
- Güvenli kodlama uygulamalarını kullanmek.
- Güvenlik güncellemelerini takip etmek ve yüklemek.

2-) **Injection**

Injection zafiyetleri, genellikle kullanıcıdan alınan ve yeterince kontrol edilmeyen veya güvenlik önlemi uygulanmayan verilerin doğrudan komutlara veya sorgulara dahil edilmesinden kaynaklanır. Bu tür zafiyetler, kötü niyetli verilerin sisteme zarar vermesine neden olabilir.

Injection açığından korunmak için alınması gereken önlemler:

Parametrelerin Doğrulanması

SQL Parametreleştirme

Kodlama Standartları

WAF Kullanımı

3-)SSRF

Sunucu Taraflı İstek Sahtekarlığı (SSRF), bir saldırganın hedef sunucuya sahte bir kaynak IP adresi veya alan adı vererek istek göndermesiyle oluşan bir güvenlik açığıdır. Bu tür bir saldırı, sunucunun kendi iç ağlarına veya dış kaynaklara erişimini tehlikeye atabilir. SSRF saldırıları, genellikle uygulamanın güvenlik doğrulama süreçlerini geçersiz kılmak veya güvenlik kontrolleri olmayan URL parametrelerini kullanmak suretiyle gerçekleştirilir.

SSRF, hedef sunucu için büyük bir güvenlik riski taşır. Saldırgan, sunucuya istekler göndererek hassas bilgileri çalabilir, sunucunun kaynaklarını tüketebilir, sunucunun kontrolünü ele geçirebilir veya sunucunun düzgün çalışmasını bozabilir.

Giriş doğrulaması

Güvenlik duvarı kurulumu

Sunucu ayarlarının kontrol edilmesi

4-)Cryptographic Failures

Kriptografik Hatalar, verilerin şifreleme veya şifre çözme işlemlerinde yanlışlıkla yapılan hatalardan kaynaklanır. Bu tür hatalar, kullanılan şifreleme yöntemlerinin hatalı seçilmesi ya da uygulanması, anahtar yönetimindeki eksiklikler veya rastgele sayı üretimindeki sorunlar yüzünden

ortaya çıkabilir. Kriptografik hatalar, uygulama güvenliği açısından büyük bir risk oluşturur çünkü kötü niyetli kişiler bu zayıflıklardan yararlanarak korunması gereken verilere erişebilir.

5-)Insecure Design

Güvensiz Tasarım, bir web uygulamasının tasarımında yapılan hatalar ya da eksikliklerden kaynaklanan güvenlik açıklarını ifade eder. Bu tür hatalar, uygulamanın tüm geliştirme süreci boyunca devam edebilir ve genel güvenliği zayıflatabilir. Özellikle kimlik doğrulama, yetkilendirme, veri gizliliği ve veri bütünlüğü gibi kritik alanlarda yapılan tasarım hataları, güvensiz tasarım sorunlarına yol açar.

6-)Vulnerable and Outdated Components

Güvenlik Açığına Sahip ve Güncellenmemiş Bileşenler, bir uygulamada kullanılan üçüncü taraf bileşenlerin eski olması veya bilinen güvenlik zafiyetlerine sahip bulunması durumunda ortaya çıkar. Modern uygulamalar genellikle çeşitli üçüncü taraf bileşenler içerir; bu bileşenler arasında web uygulama çerçeveleri, veritabanı yönetim sistemleri, açık kaynak kütüphaneler, sunucu yazılımları ve diğer yazılım araçları bulunabilir. Bu bileşenlerde güvenlik açıkları tespit edilirse, uygulama bu açıklar nedeniyle savunmasız hale gelebilir. Alınabilecek önlemler ise bileşenleri izlemek güncelleme politikaları oluşturmak bileşenleri doğrulamak

7. Identification and Authentication Failures

Kimlik Tanımlama ve Doğrulama Hataları, bir kullanıcının kimliğinin doğrulanması veya yetkilendirilmesi sürecindeki sorunlardan kaynaklanan güvenlik açıklarını ifade eder. Bu tür bir zafiyet, saldırganların kullanıcı kimliklerini çalmasına veya sahte kimliklerle uygulamaya giriş yapmasına yol açabilir.

Kimlik Tanımlama ve Doğrulama Hatalarından korunmak için uygulanması gereken önlemler şunlardır:

- Güçlü ve güvenilir kimlik doğrulama yöntemlerinin kullanılması
- Kimlik doğrulama süreçlerinin düzenli olarak izlenmesi
- Kimlik bilgileri üzerinde güçlü şifreleme tekniklerinin uygulanması

8.Software and Data Integrity Failures

Yazılım ve veri bütünlüğü problemleri, bir yazılım ya da veri sisteminin beklenmedik bir şekilde değiştirilmesi veya bozulması sonucu ortaya çıkan güvenlik açıklarını tanımlar. Bu tür

zayıflıklar, saldırganların yazılım veya veri sistemini hedef alarak bu sistemleri manipüle etmelerine veya kötüye kullanmalarına neden olabilir.

Bu tür hatalar, örneğin bir yazılım güncellemesi sırasında yazılımın kötü niyetli kişiler tarafından değiştirilmesi ya da veri depolama ortamına zararlı yazılım yerleştirilmesi gibi çeşitli yollarla meydana gelebilir. Sonuç olarak, saldırganlar verileri çalabilir, verilerin bütünlüğünü bozabilir veya sistemi kontrol altına alabilir.

9. Security Logging and Monitoring Failures

Güvenlik kayıtları ve izleme eksiklikleri, güvenlik olaylarının yeterince izlenmemesi veya yanlış yapılandırılması sonucu oluşan bir güvenlik açığıdır. Bu tür bir zafiyet, kötü niyetli faaliyetlerin belirlenememesi veya güvenlik olaylarına etkin bir şekilde müdahale edilememesi gibi sorunlara yol açabilir.

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

10. Security Misconfiguration

Güvenlik Yanlış Yapılandırması, bir uygulama veya sistemlerin hatalı veya eksik yapılandırılmasından kaynaklanan bir güvenlik açığıdır. Bu tür bir zafiyet, sistemlerin, uygulamaların veya sunucuların güvenliğini sağlamak için gerekli en iyi uygulamaların uygulanmaması veya eksik uygulanmasından meydana gelir.