YAVUZLAR WEB GÜVENLİĞİ & YAZILIM TAKIMI

OWASP Top 10 Genel Araştırma

Hazırlayan : Mustafa Batuhan ALUN

A01:2021-Broken Access Control:

Zafiyet nedir ?

Broken access control kullanıcıların yetkilendirmelerinin yanlış veya yetersiz olarak kontrol edilmesidir. Bunun sonucunda yetkisi olmayan kullanıcılar sistemde erişim izni olmadığı halde istediklerin kaynaklara istedikleri gibi erişmelerine olanak sağlar.

Neden kaynaklanır ?

1-**Yetersiz kimlik doğrulama**: Sistem kullanıcıların kimliklerini doğru bir şekilde kontrol edemediği takdir de yetkisiz kullanıcılar istenmeyen kaynaklara erişim sağlayabilir.

2-**Yanlış yapılandırılmış yetkilendirme:** Kullanıcılara veya rollere amaçlanandan daha fazla ayrıcalık verebilir.

3-**Güncel olmayan sistem kullanımı:** Varsayılan ayarlar, yama yapılmamış sistemler veya güncel olmayan uygulamalar, erişim kontrolünün bozulmasına yol açabilir.

4-**Direct Object Reference**: URL'ler aracılığıyla dosyalar, dizinler veya uygun bir şekilde kontrol etmeden çıkarırsa, kullanıcıların yetkisiz olarak kaynaklara erişebilir.

Nasıl Önlenir ?

1-**En Az Ayrıcalık İlkesi:** Kullanıcıların yalnızca işlevlerini gerçekleştirmek için gereken minimum erişime sahip olduğundan emin olun.

2-**Güvenli Kodlama Uygulamalarını Kullanın**: Kullanıcı girişini doğrulayın ve her erişim kontrolü kararının sunucu tarafında alındığından emin olun.

3-**Log Tutmak:** Logların düzenli olarak tutulmalı ve kontrol edilmelidir.

4-Token-Based Authentication kullanmalıdır.

A02:2021-Cryptographic Failures:

Zafiyet nedir ?

Cryptographic Failures, kriptografi kullanılarak saklanan verilerin yeterli güvenlik düzeyi sağlanmadığı için şifreleneme sağlanamadığı durumdur.

Neden kaynaklanır ?

1- **Yetersiz entropi:** Kriptografik işlemler için tahmin edilebilir entropi kaynaklarının kullanılması, bu da güvenlik açıklarına yol açabilir.

2-**Yetersiz şifreleme algoritmalarının kullanılması:** Artık kullanılmayan ya da kullanımı güvenli olmayan yetersiz şifreleme algoritmalarının kullanılması.

3-**Güvenli olmayan rastgele sayı üretimi:** Yeterli rastgeleliğin sağlanamaması durumunda ortaya çıkan tahmin edilebilir rastgele sayılar.

4-**Hard-Coded şifre kullanımı**: Varsayılan bir yönetim hesabı oluşturulur ve basit bir parola ürüne kazınır ve bu hesapla ilişkilendirilir. Bu kazınmış parola, ürünün her kurulumu için aynıdır ve genellikle sistem yöneticileri tarafından programı manuel olarak değiştirmeden veya ürüne başka bir şekilde yama uygulamadan değiştirilemez veya devre dışı bırakılamaz. Parola keşfedilirse veya yayınlanırsa, bu parolayı bilen herkes istediği gibi erişim sağlayabilir. (https://cwe.mitre.org/data/definitions/259.html)
5-**Anahtar kontrolünde eksiklik:** Sistemin anahtar kontrolünü sağlayamaması durumunda yetkisiz erişimin sağlanması.

Nasıl Önlenir ?

1-Parolaları, Argon2, scrypt, bcrypt veya PBKDF2 gibi bir çalışma faktörüne (delay factor) sahip güçlü uyarlanabilir ve ‘salted hashing’ fonksiyonlarını kullanarak saklayın.

2-Gerekli olamayan hiçbir veriyi sistemde tutmayın. İş biter bitmez silinmelidir. Saklanmayan bir veri de çalınamaz.

3-Hassas veriler içeren yanıtlar için önbelleğe(cache) almayı devre dışı bırakın.

4-Hassas verileri taşımak için FTP ve SMTP gibi eski protokolleri kullanmayın.

5-Yalnızca şifreleme yerine her zaman kimliği doğrulanmış şifrelemeyi kullanın.

A03:2021-Injection

Zafiyet nedir ?

Injection, kötü niyetli kullanıcıların veri girişi yoluyla uygulama tarafında yürütülen kısımlara istediği gibi müdahale etmesidir. 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 erişebilirler.

Neden kaynaklanır ?

1- **Kullanıcı girdileri düzgün şekilde temizlenmemesi:** Kullanıcılardan alınan hiçbir veriye güvenilmemelidir bu yüzden kullanıcılardan alınan her verinin güvenilirliği tasdik edilmeli gerektiğinde filtrelenmelidir.

2-**Kullanıcı girdisinin koda kazınması(hard-code):** Kullanıcı girişleri doğrudan SQL sorgularına, shell komutlarına veya diğer dinamik ifadelere gömülürse, bu durum enjeksiyon güvenlik açıklarına yol açabilir.

3-**Güvenli olmayan API'ler veya kütüphaneler:** Kullanıcı girdilerini otomatik olarak filtrelemeyen veya güvenli kodlama uygulamalarını desteklemeyen API'lerin, kitaplıkların veya çerçevelerin kullanılması da enjeksiyon güvenlik açıklarına yol açabilir.

4-**Hataların düzgünce ele alınmaması**: Uygulamalar hata mesajları yoluyla çok fazla bilgi ortaya çıkardığında, saldırganlar uygulamanın yapısına ilişkin öngörüler elde edebilir ve daha etkili enjeksiyon saldırıları gerçekleştirebilir.

Enjeksiyon Çeşitleri:

SQL:SQL enjeksiyonu, bir saldırganın bir sorguya kötü amaçlı SQL kodu eklemesi ve veritabanına yetkisiz erişime veya veritabanının değiştirilmesine olanak sağlamasıyla gerçekleşir.

NoSQL(Not-Only SQL): NoSQL enjeksiyonu, bir NoSQL sorgusuna kötü amaçlı kod enjekte ederek saldırganların veritabanını manipüle etmesine ve kimlik doğrulama veya yetkilendirme kontrollerini atlamasına olanak tanır.

OS Command:İşletim sistemi komut enjeksiyonu, bir saldırganın bir uygulama tarafından yürütülen bir sistem komutuna kötü amaçlı komutlar enjekte etmesi ve potansiyel olarak işletim sistemi üzerinde kontrol sahibi olması durumunda gerçekleşir.

Nasıl Önlenir ?

1-Kullanıcı girdileri her zaman kontrol edilir ve filtrelenir.

2-Parametre kullanarak sorgular direkt olarak kullanılmaz.

3-WAF kullanımı. Kötü niyetli kullanıcı girdilerini web uygulamasına ulaşmadan önce filtreleyip engelleyerek enjeksiyon saldırılarını önlemek için bir Web Uygulaması Güvenlik Duvarı (WAF) kullanmalıyız.

A04:2021-Insecure Design:

Zafiyet nedir ?

Insecure Design, güvenlik zafiyetlerinin tasarım aşamasında göz ardı edilmesi veya ihmal edilmesi durumudur. Bu, sistemin veya uygulamanın tasarımında güvenlik düşüncelerinin yeterince entegre edilmediği veya güvenlik gereksinimlerinin dikkate alınmadığı durumları ifade eder.

Neden kaynaklanır ?

1- **Yetersiz Güvenlik Gereksinimleri:** Güvenlik gereksinimlerinin tasarım aşamasında belirlenmemesi veya eksik belirlenmesi.

2-**Yetersiz güvenlik standartlarının kullanımı:** Tasarım sürecinde güvenlik standartlarının ve en iyi uygulamaların dikkate alınmaması.

3-**Yetersiz risk analizi:** Potansiyel tehditler ve riskler üzerinde yeterince detaylı analiz yapılmaması.

4-**Gelişmiş güvenlik önlemlerinin sağlanmaması:** Modern güvenlik önlemlerinin ve teknolojilerinin tasarımda kullanılmaması.

Nasıl Önlenir ?

1-**Modern güvenlik önlemleri kullanın:** Tasarımda modern güvenlik önlemlerini ve teknolojilerini kullanarak güvenlik açıklarını kapatın.

2-**Güvenlik gereksinimlerini belirleyin:** Tasarım aşamasında, güvenlik gereksinimlerini açıkça tanımlayın ve bu gereksinimlere uygun çözümler geliştirin.

3-**Risk analizi yapın:** Potansiyel tehditler ve riskler için kapsamlı bir risk analizi gerçekleştirin ve bu risklere yönelik önlemler geliştirin.

A05:2021-Security Misconfiguration:

Zafiyet nedir ?

Security Misconfiguration, sistemlerin, uygulamaların veya altyapıların yanlış veya yetersiz yapılandırılmasından kaynaklanan güvenlik zafiyetleridir. Bu tür zafiyetler, sistemlerin varsayılan ayarlarla, eksik yapılandırmalarla veya yanlış güvenlik ayarlarıyla çalışmasına neden olur.

Neden kaynaklanır ?

1- **Varsayılan ayarların kullanımı:** Varsayılan yapılandırma ayarlarının değiştirilmemesi ve sistemin bu varsayılan ayarlarla bırakılması.

2-**Eksik güvenlik yapılandırmaları:** Güvenlik ayarlarının veya kontrollerin eksik olması, örneğin, güvenlik duvarı kurallarının yetersiz olması.

3-**Güncelleme ve yamanın yapılmaması:** Güvenlik açıklarını giderecek güncellemelerin veya yamaların uygulanmaması.

4-**Güvenlik ayarlarının yetersiz denetimi:** Yapılandırma değişikliklerinin yeterince izlenmemesi ve denetlenmemesi.

Nasıl Önlenir ?

1-En iyi uygulamaları takip etmek

2-**Düzenli güncellemeler ve yamalar:** Sistemlerinizi ve yazılımlarınızı güncel tutun, güvenlik yamalarını düzenli olarak uygulayın.

3-**Güvenlik taramaları:** Yapılandırma hatalarını ve güvenlik açıklarını tespit etmek için güvenlik taramalarının yapılması.

A07:2021 – Identification and Authentication Failures

Zafiyet nedir ?

Identification and Authentication Failures, kimlik doğrulama ve yetkilendirme süreçlerinde meydana gelen zayıflıklardır. Bu tür zafiyetler, kötü niyetli kullanıcıların sistemlere yetkisiz erişim sağlamasına veya kullanıcıların kimliklerinin yanlış doğrulanmasına neden olabilir.

Neden kaynaklanır ?

1- **Eksik kimlik doğrulama:** Kullanıcı kimliklerinin yeterince doğrulanmaması veya oturum açma süreçlerinde eksiklikler.

2-**Hatalı yetkilendirme:** Yetkili kullanıcıların sistemde erişim yetkilerinin doğru bir şekilde kontrol edilmemesi ve sınırlamaların yetersiz olması.

3-**Oturum yönetimindeki açıklar:** Güvenli oturum yönetimi ve süre aşımının yetersiz olması, oturum ID'lerinin tahmin edilebilir veya çalınabilir olması.

4-**Zayıf şifre politikaları:** Güçlü ve karmaşık şifrelerin kullanılmaması, basit veya tahmin edilebilir şifrelerin tercih edilmesi.

Nasıl Önlenir ?

1-**Çok faktörlü kimlik doğrulama kullanın:** Ek güvenlik katmanları sağlayan çok faktörlü kimlik doğrulama (MFA) kullanarak yetkilendirme süreçlerini güçlendirin.

2-**Yetkilendirme kontrollerini uygulayın:** Kullanıcı erişim ve yetkilerini doğru bir şekilde kontrol edin. Kullanıcıların yalnızca yetkili oldukları kaynaklara erişebilmesini sağlayın.

3-**Güçlü şifre politikaları belirleyin:** Kullanıcıların güçlü, karmaşık ve tahmin edilmesi zor şifreler kullanmasını sağlayın.

A08:2021-Software and Data Integrity Failures

Zafiyet nedir ?

Software and Data Integrity Failures, yazılım ve veri bütünlüğü ile ilgili meydana gelen zayıflıklardır. Bu tür zafiyetler, verilerin veya yazılım bileşenlerinin yetkisiz değişikliklere, manipülasyonlara veya bozulmalara karşı korunamamasına neden olabilir.

Neden kaynaklanır ?

1- **Yetersiz veri doğrulama:** Verilerin kaydedilmeden önce yeterince doğrulanmaması, verilerin bozulması veya yanlışlıkla değiştirilmesine yol açabilir.

2-**Eksik imza doğrulama:** Yazılım bileşenlerinin veya güncellemelerin dijital imzalarının doğrulanmaması, zararlı yazılımların sisteme sızmasına neden olabilir.

3-**Güvenlik açıkları içeren bileşenler:** Yazılım bileşenlerinde bulunan güvenlik açıkları, yetkisiz değişikliklerin yapılmasına izin verebilir.

4-**Veri kaybı ve bozulma:** Verilerin düzenli olarak yedeklenmemesi veya veri bütünlüğü kontrollerinin eksik olması, veri kaybı ve bozulmasına neden olabilir.

Nasıl Önlenir ?

1-**Dijital imza kullanımı:** Yazılım bileşenleri ve güncellemeler için dijital imzalar kullanarak kaynakların bütünlüğünü doğrulayın. İmzalı bileşenlerin yalnızca güvenilir kaynaklardan geldiğinden emin olun.

2-**Yetkilendirme kontrollerini uygulayın:** Npm veya Maven gibi kütüphanelerin ve gereksinimlerin güvenilir depoları tükettiğinden emin olun. Daha yüksek bir risk profiliniz varsa, incelenmiş, iyi olduğu bilinen dahili bir veri havuzu barındırmayı düşünün.

A09:2021-Security Logging and Monitoring Failures

Zafiyet nedir ?

Security Logging and Monitoring Failures, güvenlik olaylarının yeterince kaydedilmemesi ve izlenmemesi durumunda ortaya çıkan güvenlik zafiyetleridir. Bu zafiyetler, güvenlik ihlallerinin veya anormal faaliyetlerin zamanında tespit edilmesini ve müdahale edilmesini zorlaştırabilir.

Neden kaynaklanır ?

1- **Eksik veya yanlış yapılandırılmış monitoring:** Güvenlik olaylarının izlenmesi için yeterli yapılandırmanın yapılmaması, potansiyel tehditlerin fark edilmesini engeller.

2-**Yanıt prosedürlerinin eksikliği:** Güvenlik olaylarına karşı nasıl yanıt verileceğini belirleyen prosedürlerin eksikliği veya var olan prosedürlerin yetersizliği.

3-**Log ve monitoring verilerinin yetersiz korunması:** Kaydedilen logların veya izleme verilerinin yetkisiz erişimlere karşı yeterince korunmaması.

Nasıl Önlenir ?

1-**Yanıt prosedürlerini belirleyin:** Güvenlik olaylarına karşı nasıl yanıt verileceğini belirleyen net prosedürler oluşturun ve bu prosedürlerin uygulanabilir olduğundan emin olun.

2-**Monitoring sistemlerini doğru yapılandırın:** Güvenlik olaylarını izlemek için yapılandırılmış izleme sistemleri kullanın ve izleme kurallarını sürekli olarak güncel tutun.

3-**Verilerin saklanması :** Tüm oturum açma, erişim kontrolü ve sunucu tarafı giriş doğrulama hatalarının, şüpheli veya kötü amaçlı hesapları tanımlamak için yeterli kullanıcı bağlamıyla loga kaydedilebildiğinden ve gecikmiş adli analize izin verecek kadar uzun süre tutulabildiğinden emin olun.

A10:2021 – Server-Side Request Forgery (SSRF)

Zafiyet nedir ?

Server-Side Request Forgery (SSRF), bir saldırganın, güvenliği ihlal edilmiş bir uygulamayı kullanarak sunucuya kötü niyetli istekler göndermesine olanak tanıyan bir güvenlik zafiyetidir. SSRF, genellikle sunucunun kendisi veya güvenlik duvarının arkasındaki diğer sistemler gibi, normalde erişilemeyen dahili kaynaklara erişim sağlamaya yöneliktir.

Neden kaynaklanır ?

1- **Kullanıcı girdilerinin yetersiz doğrulanması:** Kullanıcı tarafından sağlanan URL'lerin veya isteklerin yetersiz doğrulanması, kötü niyetli isteklerin sunucuya gönderilmesine olanak tanır.

2-**İç ağ kaynaklarının erişime açık olması:** Sunucunun dahili ağ kaynaklarına erişiminin olması ve bu kaynakların doğru bir şekilde sınırlandırılmaması.

3-**Yanlış yapılandırılmış güvenlik duvarları:** Güvenlik duvarlarının veya ağ ayarlarının yetersiz yapılandırılması, sunucunun dahili kaynaklara yetkisiz erişimi engelleme kapasitesini azaltır.

Nasıl Önlenir ?

1-**Kullanıcı girdilerini doğrulayın ve temizleyin:** Kullanıcı tarafından sağlanan URL'lerin ve diğer girdi verilerinin güvenliğini sağlamak için doğrulama ve temizleme işlemlerini uygulayın.

2-**Güvenlik duvarı ve ağ ayarlarını yapılandırın:** Sunucuya gelen dış istekleri sınırlandırmak ve yalnızca güvenli ve izin verilen kaynaklara erişim sağlamak için güvenlik duvarı ve ağ ayarlarını dikkatlice yapılandırın.

3-**Verilerin saklanması :** Tüm oturum açma, erişim kontrolü ve sunucu tarafı giriş doğrulama hatalarının, şüpheli veya kötü amaçlı hesapları tanımlamak için yeterli kullanıcı bağlamıyla loga kaydedilebildiğinden ve gecikmiş adli analize izin verecek kadar uzun süre tutulabildiğinden emin olun.

4-**Whitelist oluşturma:** İzin verilenler listesiyle URL şemasını, bağlantı noktasını ve hedefi zorunlu kılın.

5-HTTP yönlendirmelerini kapatın.