OWASP TOP 10

İçindekiler

OWASP TOP 10 3

Zafiyet Nedir? 3

OWASP TOP 10 - A01:2021 – Broken Access Control (Bozuk Erişim Kontrolü): 3

a. Zafiyet Nedir? 3

b. Neden Kaynaklanır? 3

c. Türleri: 3

d. Örnek: 4

e. Nasıl Önlenir? 4

OWASP TON 10 - A02:2021 – Cryptographic Failures (Kriptografik Hatalar): 4

a. Zafiyet Nedir? 4

b. Neden Kaynaklanır? 4

c. Örnek: 4

d. Nasıl Önlenir? 4

OWASP TON 10 - A03:2021 – Injection (Enjeksiyon): 4

a. Zafiyet Nedir? 4

b. Neden Kaynaklanır? 4

c. Türleri 4

d. Örnek: 5

e. Nasıl Önlenir? 5

OWASP TON 10 - A04:2021 – Insecure Design (Güvensiz Tasarım): 5

a. Zafiyet Nedir? 5

b. Neden Kaynaklanır? 5

c. Örnek: 5

d. Nasıl Önlenir? 5

OWASP TOP 10 - A05:2021 – Security Misconfiguration (Güvenlik Yanlış Yapılandırmaları) 5

a. Zafiyet Nedir? 5

b. Neden Kaynaklanır? 5

c. Örnek: 5

d. Nasıl Önlenir? 5

OWASP TOP 10 - A06:2021 – Vulnerable and Outdated Components (Zafiyetli ve Eski Bileşenler): . 6

a. Zafiyet Nedir? 6

b. Neden Kaynaklanır? 6

c. Örnek: 6

d. Nasıl Önlenir? 6

OWASP TOP 10 - A07:2021 – Identification and Authentication Failures (Kimlik Doğrulama ve Tanımlama Hataları) 6
a. Zafiyet Nedir? 6
b. Neden Kaynaklanır? 6
c. Örnek: 6
d. Nasıl Önlenir? 7
OWASP TOP 10 - A08:2021 – Software and Data Integrity Failures (Yazılım ve Veri Bütünlüğü Hataları): 7
a. Zafiyet Nedir? 7
b. Neden Kaynaklanır? 7
c. Örnek: 7
d. Nasıl Önlenir? 7
OWASP TOP 10 - A09:2021 – Security Logging and Monitoring Failures (Güvenlik Kayıtları ve İzleme Hataları): 7
a. Zafiyet Nedir? 7
b. Neden Kaynaklanır? 7
c. Nasıl Önlenir? 7
OWASP TOP 10 - A10:2021 – Server-Side Request Forgery (SSRF) (Sunucu Taraflı İstek Sahteciliği). 8
a. Zafiyet Nedir? 8
b. Neden Kaynaklanır? 8
c. Örnek: 8
d. Nasıl Önlenir? 8

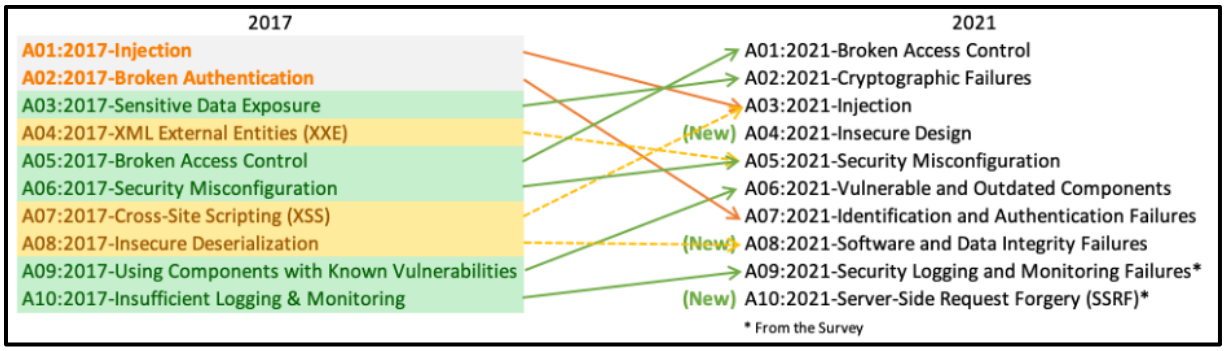
OWASP TOP 10

Zafiyet Nedir?

Zafiyet ya da güvenlik açığı, sistemin ya da uygulamanın kötü niyetli kişiler tarafından istismar edilebilecek zayıflık ya da eksiklik içermesidir.

Bunlar kategorilere ayrılmak istenirse yazılım, donanım, insan ve ağ zafiyetleri olarak kabaca sınıflandırılabilir.

Zafiyetler genellikle kodlama hataları, yetersiz güvenlik testleri güncellenmemiş yazılımlar, yanlış yapılandırmalar, insan hataları, istemci ya da sunucuların doğru yapılandırılamamasından açığa çıkar.



Şekil 1- OWASO TOP 10

OWASP TOP 10 - A01:2021 – Broken Access Control (Bozuk Erişim Kontrolü):

a. Zafiyet Nedir?

Broken Access Control, kullanıcının erişim yetkileri dışında kalan işlemlere ya da kaynaklara erişmesidir. Normalde o kullanıcının oraya erişmemesi gerekmemektedir fakat bu zafiyetin ortaya çıkması durumunda kullanıcı yetkisi dışında hareket eder.

b. Neden Kaynaklanır?

Erişim denetimlerinin yeterince iyi yapılmaması

Genel olarak yetkilendirmenin yetersiz, eksik ya da yanlış yapılandırılmasından kaynaklanır.

c. Türleri:

1. *Vertical privilege escalation(Dikey Ayrıcalık Yükseltme):*
   Dikey ayrıcalık yükseltme yetki farkının manipüle edilmesinden kaynaklanır. Örneğin normalde sadece admin herkese erişebilir ve kullanıcılar arasında düzenleme yapabilirken normal kullanıcının da admin gibi bir kullanıcıyı silebilmesidir.

2. *Horizontal privilege escalation(Yatay Ayrıcalık Yükseltme):*
   Yatay ayrıcalık yükseltme aynı yetkinin sadece aynı kişide olması değil de herkeste olmasından kaynaklanır. *B*ir kullanıcı kendi kaynakları yerine başka bir kullanıcıya ait kaynaklara erişebiliyorsa gerçekleşir. Örneğin, bir çalışan kendi kayıtlarının yanı sıra diğer çalışanların kayıtlarına da erişebiliyorsa, bu yatay ayrıcalık yükseltmesidir.

d. Örnek:

Admin yetkisi olmayan bir kullanıcının, URL manipülasyonu yaparak yönetim paneline erişmesi.

e. Nasıl Önlenir?

Yetki kontrollerinin hem yetki hem sunucu tarafında yapılması gerekir.

Erişilmemesi gereken “path”ler(yolllar) düzgün filtrelendirilmelidir.

Minimum yetki prensibi uygulanmalıdır.

İzinler ve yetkiler düzenli olarak kontrol edilmeli ve testler yapılmalıdır.

OWASP TON 10 - A02:2021 – Cryptographic Failures (Kriptografik Hatalar):

a. Zafiyet Nedir?

Veri şifreleme ve veri şifre çözme süreçlerinde meydana gelen eksiklik, zayıflıklardır.

b. Neden Kaynaklanır?

Zayıf veya eski şifreleme algoritmalarının kullanımı.

Yetersiz anahtar yönetimi.

Veri iletiminde şifreleme eksikliği

c. Örnek:

Kullanıcı şifrelerinin MD5 ile hashlenmesi ve güvenli bir şekilde saklanmaması.

d. Nasıl Önlenir?

Modern ve güçlü şifreleme algoritmaları (AES, SHA-256) kullanılmalıdır.

Güvenli iletim protokollerini kullanılmalıdır.

Şifreleme anahtarlarının yönetimi düzgün yapılandırılmalıdır.

OWASP TON 10 - A03:2021 – Injection (Enjeksiyon):

a. Zafiyet Nedir?

Kötü niyetli kullanıcıların uygulamanın çalıştırdığı komutlara, veritabanına ya da OS komutlarına kod enjekte etmesidir.

b. Neden Kaynaklanır?

Kullanıcı girdilerinin –inputların- yeterince iyi filtrelenmemesi

Kullanıcı girdilerinin minimum seviyeye indirilmemesi

Parametrelerin takibinin yeterince iyi yapılamaması ve yapılandırılma yanlışlığı, eksikliği

c. Türleri

1. *SQL Injection:* SQL komutlarının manipüle edilerek hassas erişim elde edilmesi
2. *Command Injection:* OS komutlarının manipüle edilerek hassas erişim elde edilmesi

d. Örnek:

Sql payload: SELECT * FROM users WHERE username = 'admin' -- ' AND password = 'password';

e. Nasıl Önlenir?

Kullanıcı girdilerini doğrulanmalı ve sanitize edilmelidir.

ORM (Object-Relational Mapping) araçlarını kullanılarak manuel sorgulardan kaçınılmalıdır.

OWASP TON 10 - A04:2021 – Insecure Design (Güvensiz Tasarım):

a. Zafiyet Nedir?

Yazılımın veya sistemin baştan itibaren güvenlik göz önünde bulundurulmadan tasarlanmasıdır. Burada temel güvenlik zafiyetleri sağlanmamıştır.

b. Neden Kaynaklanır?

Tehdit modellemesinin yapılmaması.

c. Örnek:

Kullanıcı şifrelerinin düz metin olarak saklanması.

d. Nasıl Önlenir?

Tehdit modellemesi yapılmalı potansiyel zafiyetleri belirlenmelidir.

Güvenlik odaklı tasarım ve geliştirme prensiplerini uygulanmalıdır.

OWASP TOP 10 - A05:2021 – Security Misconfiguration (Güvenlik Yanlış Yapılandırmaları)

a. Zafiyet Nedir?

Sistemlerin ya da uygulamaların yanlış yapılandırılmasıdır. Eksik ya da yanlış yapılandırılmadan ortaya çıkar.

b. Neden Kaynaklanır?

Varsayılan yapılandırmaların değiştirilmemesi.

Güvenlik yamalarının uygulanmaması.

Gereksiz özelliklerin veya servislerin aktif olması.

c. Örnek:

Web sunucusunun varsayılan yapılandırma ile yayınlanması, örneğin, Apache'nin varsayılan sayfasının açık olması.

d. Nasıl Önlenir?

Güvenlik yamalarını ve güncellemeleri düzenli olarak yapılmalı, kontrol edilmelidir.

Gereksiz servisler kapatılmalı ve yalnızca gerekli olanları etkinleştirilmelidir.

Varsayılan ayarlar gözden geçirilmelidir.

OWASP TOP 10 - A06:2021 – Vulnerable and Outdated Components (Zafiyetli ve Eski Bileşenler):

a. Zafiyet Nedir?

Zafiyetli ve Eski Bileşenler, kullanılan yazılım, kütüphane veya bileşenlerin güncel olmaması veya bilinen zafiyetlere sahip olması durumudur. Bir uygulamada kullanılan üçüncü taraf bileşenlerin güncellenmemesi veya bilinen güvenlik açıklarına sahip olması nedeniyle oluşan bir güvenlik açığıdır.

b. Neden Kaynaklanır?

Güncellemelerin veya yamaların zamanında uygulanmaması.

Eski veya desteği kesilmiş yazılım kullanımı.

c. Örnek:

Worpress'te açık çıkması ve yayınlanması bunun takip edilmemesinden ötürü eski bir sürümünün kullanılması ve buna bağlı olarak uzaktan kod çalıştırma zafiyetinin ortaya çıkması.

d. Nasıl Önlenir?

Bileşenlerin düzenli olarak güncellenmesi.

Üçüncü parti kütüphanelerin zafiyet taramalarının yapılması.

Gereksiz bileşenlerin kaldırılması.

OWASP TOP 10 - A07:2021 – Identification and Authentication Failures (Kimlik Doğrulama ve Tanımlama Hataları)

a. Zafiyet Nedir?

Kullanıcının kimliğini doğrulamada veya kullanıcıların yetkilendirilmesinde yapılan hatalardır. Bu, saldırganların yetkisiz olarak sisteme erişimine olanak tanır. Bu tür bir açık, bir saldırganın bir kullanıcının kimliğini çalmasına veya sahte bir kimlik kullanarak uygulamaya erişmesine izin verebilir.

b. Neden Kaynaklanır?

Zayıf parola yönetimi

2 faktörlü doğrulama eksikliği

Oturum yönetimi hataları

Parola şifreleme hataları veya eksiklikleri

Yetersiz parola yenileme, kurtarma ve sıfırlama süreçleri

c. Örnek:

"1234" gibi basit bir parolanın kabul edilmesi.

Kullanıcı oturum kimliğinin URL'de saklanması ve bir başkası tarafından kopyalanarak kullanılması.

d. Nasıl Önlenir?

Güçlü ve karmaşık parolalar zorunlu hale getirilmelidir.

Çok faktörlü kimlik doğrulama (MFA) uygulanmalıdır.

Oturum kimliklerini güvenli bir şekilde saklanmalı ve oturum süresi sınırlanmalıdır.

Düzenli olarak kimlik doğrulama politikalarını kontrol etmek.

OWASP TOP 10 - A08:2021 – Software and Data Integrity Failures (Yazılım ve Veri Bütünlüğü Hataları):

a. Zafiyet Nedir?

Yazılım ve veri bütünlüğü hataları, yazılım güncellemelerinin, kritik verilerin veya kodların yetkisiz kişiler tarafından değiştirilmesi veya manipüle edilmesi durumudur.

b. Neden Kaynaklanır?

Yetersiz dijital imzalama süreçleri, JWT expires in kısa tutulmalıdır.

Güvenilmeyen kaynaklardan güncellemelerin kabul edilmesi

Kod değişikliklerinin yeterince yapılandırılmaması

Veri değişikliklerinin üzerinde yeterli kontrol olmaması.

c. Örnek:

Sahte bir güncelleme ile zararlı yazılımın sisteme yüklenmesi.

d. Nasıl Önlenir?

Yazılım güncellemelerini yalnızca güvenilir kaynaklardan indirin.

OWASP TOP 10 - A09:2021 – Security Logging and Monitoring Failures (Güvenlik Kayıtları ve İzleme Hataları):

a. Zafiyet Nedir?

Güvenlik Kayıtları ve İzleme Hataları, sistemlerde gerçekleşen olayların, özellikle güvenlikle ilgili olayların yeterli ve doğru şekilde kaydedilmemesi, izlenmemesi veya analiz edilmemesi durumunda ortaya çıkan zafiyetlerdir.

b. Neden Kaynaklanır?

Eksik veya yanlış yapılandırma

Kapsamlı loglama eksikliği

Yetersiz izleme ve analiz

c. Nasıl Önlenir?

Günlük kayıtlarının düzenli olarak incelenmesi

Uyarı ve alarm sistemleri kullanmak

Logların Güvenli ve Uzun Süreli Saklanması:

OWASP TOP 10 - A10:2021 – Server-Side Request Forgery (SSRF) (Sunucu Taraflı İstek Sahteciliği)

a. Zafiyet Nedir?

SSRF'te arka tarafta kullanıcıdan gelen urllere isteklere sistem güvenir ve bu yüzden ortaya çıkar. uygulamanın farklı bir sunucuuya gitmesi osnucunda uzaktan erişim sağlamasıyla çıkar. Uygulamalar, bir URL veya diğer parametreleri kullanıcıdan alarak bu değerleri doğrudan kullanır ve bir istek yapar. Eğer bu girişler doğru şekilde doğrulanmazsa, saldırgan bu parametreleri manipüle ederek iç ağdaki sunuculara, hizmetlere veya dış kaynaklara yetkisiz erişim sağlayabilir. Uygulamanın, hangi kaynaklara erişim yapılabileceği konusunda kısıtlamaları doğru şekilde uygulamaması SSRF'ye yol açabilir.

b. Neden Kaynaklanır?

Sunucunun arka tarafa gelen istekleri yeterince doğru kontrol edememesinden kaynaklanır.

Kullanıcı girişinin yeterince doğrulanmaması.

Güvenlik duvarlarının ve ağ segmentlerinin yanlış yapılandırılması.

c. Örnek:

Saldırganın bir web uygulamasını kullanarak sunucu üzerinden dahili ağdaki diğer cihazlara istek göndermesi.

d. Nasıl Önlenir?

Network segmentation ve network isolotionu düzgün entegre edilmesi.

İsteklerin kapsamını kısıtlamak için izin verilen etki alanlarını veya IP adreslerini beyaz listeye eklenmesi.

Uygulamanızın harici kaynaklardan veri alması gerekiyorsa, belirli kaynaklara sınırlı ve kontrollü erişim sağlayan güvenli bir API kullanmak.