Geliştiriciler ve DevOps Profesyonelleri için Uygulama Güvenliği

Modül 1 Sözlüğü: Uygulama Geliştirme için Güvenliğe Giriş

Hoş geldiniz! Bu alfabetik sözlük, bu kursta yer alan birçok terimi içermektedir. Bu kapsamlı sözlük, kurs videolarında kullanılmayan ek endüstri tanınmış terimleri de içermektedir. Bu terimler, sektörde çalışırken, kullanıcı gruplarına katılırken ve diğer sertifika programlarına katılırken tanımanız için gereklidir.

Tahmini okuma süresi: 12 dakika

Terim	Tanım
Erişim kontrolü	Kullanıcılara, süreçlere veya bir sistem veya ağ içinde çalışan varlıklara sağlanan erişimi ve izinleri yönetmek ve kontrol etmek için kullanılan güvenlik önlemleri.
Uyarı	Metrik değerlerdeki değişikliklere dayalı olarak eylemler gerçekleştiren bir izleme sisteminin yanıt veren bileşeni.
Uygulama katmanı	Geliştiricilerin uygulama oluşturma ve dağıtma için kullandığı OSI modelinin yedinci ve en üst katmanı.
Uygulama Programlama Arayüzü (API)	Farklı yazılım uygulamalarının birbirleriyle iletişim kurmasını sağlayan kılavuzlar, protokoller ve araçlar topluluğu.
Asimetrik şifreleme	Farklı anahtarların şifreleme ve şifre çözme için kullanılması.
Kimlik doğrulama	Bir kullanıcının kimliğini doğrulama süreci.
Yetkilendirme	Bir kullanıcının erişim haklarını belirleme süreci.
Kontrol toplamları	Veri iletimi veya depolama sırasında meydana gelebilecek hataları tanımlamak için kullanılan verilerden türetilmiş değerler.
CI/CD	Sürekli entegrasyon (CI) ve sürekli teslimat (CD) anlamına gelen CI/CD, farklı kişilerin çalışmalarını bir bütün ürün haline getirmek için daha hızlı ve daha doğru bir yol oluşturur.
CI/CD boru hattı	Sürekli entegrasyon/sürekli teslimat (CI/CD) boru hattı, sık ve güvenilir bir yazılım teslimat sürecine odaklanan çevik bir DevOps iş akışıdır.
Kod tarayıcıları	Kütüphanelerinizdeki kodu taradıktan sonra güvenlik açıkları raporu ve içgörü sağlar.
CodeSonar	Kaynak ve ikili kodda hataları ve güvenlik açıklarını bulmak ve düzeltmek için GrammaTech tarafından kullanılan bir statik kod analiz aracıdır.
Konteyner tarama	Güvenlik açıkları ve tehditler içerebilecek konteynerlere dağıtılan kodu tarar.
Konteynerler	Uygulama kodunun, kütüphaneleri ve bağımlılıkları ile birlikte, kodu herhangi bir yerde çalıştırmak için ortak yollarla paketlendiği çalıştırılabilir yazılım birimleri.
Coverity	C, C++, Java ve Python gibi programlama dilleri için bir artımlı analiz tarayıcısı.
Kriptografik anahtarlar	Verileri siber saldırılardan korumak için iletim ve depolama sırasında kullanılan temel araçlar.
Kriptografik hizmet	Verileri gizli tutan bir gizlilik hizmetidir. Amacı, verilerin gerekli kimlik bilgileri olmadan güvenli olmayan bir ağdan geçerken bile başkalarından korunmasını sağlamaktır.
Veri bağlantı katmanı	OSI modelinin ikinci katmanı, iletilen ham verileri tespit edilemeyen hatalardan arındırılmış bir hataya dönüştürür.
DevSecOps	DevSecOps (güvenliğe vurgu yapan DevOps), yazılım geliştirme yaşam döngüsü (SDLC) boyunca güvenlik entegrasyonunu otomatikleştiren bir uygulama setidir; bu, tasarımın orijinalinden entegrasyona, test etmeye, dağıtıma ve yazılım teslimatına kadar uzanır.
Diyalog kontrolü	İki cihaz veya sistem arasındaki iletişim oturumlarının yönetimi ve koordinasyonunu ifade eder.
E-ticaret işlemleri	İnternet üzerinden mal ve hizmet alım satımını ifade eder.
Şifreleme	Bilgiyi kodlama süreci, böylece yalnızca yetkilendirilmiş erişime sahip kullanıcıların bunu çözebileceği şekilde.
Uç nokta güvenliği	Uygulama ve sistem anormalliklerini tespit eder ve sistemleri, sunucuları ve ağa bağlı çeşitli cihazları korur.
Kapsamlı belgeler	Erişilebilir, kesin, okunması ve takip edilmesi kolay güvenlik desen belgeleri. Yazılım geliştiricileri bu tür belgelere başvurmaya eğilimlidir.
Genişletilebilir Erişim Kontrolü İşaretleme Dili (XACML)	Erişim kontrolü politikalarını tanımlamak ve uygulamak için kullanılan bir standarttır. Farklı sistemler, uygulamalar ve hizmetler arasında erişim kontrolü kararlarını yönetmek ve uygulamak için kapsamlı bir çerçeve sunar. Bu, kuruluşların kaynak erişimini ve belirli eylemleri belirlenmiş politikalara göre düzenlemesini sağlar.
Genişletilebilir İşaretleme Dili (XML)	Verileri insan tarafından okunabilir ve platformdan bağımsız bir formatta düzenlemek, taşımak ve yapılandırmak için oluşturulmuş yaygın olarak kullanılan bir işaretleme dilidir.
Güvenlik duvarı	Güvenilir bir iç ağ ile internet gibi güvenilmeyen bir dış ağ arasında bir engel görevi gören bir ağ güvenlik cihazı veya yazılımıdır.
Fonksiyonel Doğrulama Testi (FVT)	Yazılımın işlevselliğini çözüm spesifikasyon belgesi, tasarım belgeleri ve kullanım durumu belgeleri kullanarak doğrular.
GitHub	Yazılım geliştirme projeleri için sürüm kontrolü sunan çevrimiçi bir platformdur; geliştiricilerin kod üzerinde işbirliği yapmalarını, değişiklikleri takip etmelerini ve kaynak kodu havuzlarını dağıtık bir şekilde yönetmelerini sağlar.
Hash algoritmaları	Hash algoritması, aynı zamanda hash fonksiyonu olarak da adlandırılan, herhangi bir boyutta girişi kabul eden ve sabit boyutta bir çıktı üreten matematiksel bir prosedürdür; bu çıktı hash değeri veya hash kodu olarak adlandırılır.
Hashicorp'un Vault	Kimlik tabanlı gizli ve şifreleme yönetim aracı olan açık kaynaklı bir araç.
Ele geçirme	İki tarafın doğrudan iletişim kurduğuna inandığı iletişimi kesen ve manipüle eden yetkisiz bir kişi veya varlığın neden olduğu bir siber saldırı türü.
Güvenli Hiper Metin Protokolü (HTTPS)	Bilgisayarlar arasında Güvenli iletişim için kullanılan bir protokoldür. Tarayıcı ile web sitesi arasındaki veri alışverişinin gizli kalmasını ve yetkisiz erişimden korunmasını sağlar.
Kimlik ve Erişim Yönetimi (IAM)	Bulut altyapılarındaki uygulamalara ve sistemlere izin vermek için önemli güvenlik mekanizmaları.
Bütünlük	Verilerin alım sırasında veya sonrasında değiştirilmediğini veya bozulmadığını garanti eden bir kriptografik hizmettir ve verilerin doğrulanması gereken kullanıcılar için veri bozulmasını önlemeye yardımcı olur.
Birbiriyle çalışabilir	Farklı sistemlerin, yazılımların veya bileşenlerin işbirliği yapabilme, uyumlu bir şekilde çalışabilme ve bilgiyi etkili ve kesintisiz bir şekilde değiştirebilme yeteneği.
Saldırı tespiti	Bir uygulama veya sistemi tehlikeye atabilecek herhangi bir siber saldırı, tehdit veya ihlalin sürekli tespiti.
Linux çekirdeği	Programların ve çeşitli hizmetlerin üzerinde çalışması için bir platform sağlayan bir işletim sisteminin temel bileşeni.
Ortada Adam saldırıları	Saldırganın gizlice iki taraf arasındaki iletişimi kesip potansiyel olarak değiştirdiği bir siber saldırı türüdür; bu iki taraf doğrudan iletişim kurduklarına inanmaktadır.
Mesaj özetleri	Veri bloklarının kontrol toplamlarını hesaplamak için kullanılan kriptografik hash fonksiyonlarıdır. Ayrıca imza imzalamak ve doğrulamak için de kullanılabilir.
Ağ güvenlik duvarı	Kurumsal bir ağ gibi iç bir ağ ile internet gibi dış bir ağ arasında koruyucu bir engel görevi gören bir güvenlik cihazı veya yazılımıdır. Rolü, gelen ve giden ağ trafiğini düzenlemek ve gözlemlemektir.
Ağ katmanı	OSI modelinin üçüncü katmanı, veri iletimi ve alt ağ kontrolü ile ilgilenir.
Ağ haritalayıcı (Nmap)	Bir bilgisayar ağındaki ana bilgisayarları ve hizmetleri keşfetmek için paketler gönderip yanıtları analiz eden bir araçtır.
Ağ güvenliği	Uygulama ve sistem anormalliklerini tespit eder ve Nmap veya Snort gibi bir ağ aracı kullanarak bir ağı izler.
Açık Sistemler Bağlantısı (OSI modeli)	Farklı iletişim sistemleri arasında standart protokoller kullanarak iletişimi sağlar.
Açık kaynak yazılım kütüphanesi (OpenSSL)	Güvenli Soket Katmanı (veya SSL) protokolünü uygulayan bir yazılım kütüphanesidir. Tüm iletişim türleri için kriptografi ile güvenli iletişim sağlamak için açık kaynaklı bir araçtır; kişisel, ticari ve e-ticaret işlemleri dahil.
Orkestrasyon	Bilgisayar sistemlerinin, uygulamalarının ve hizmetlerinin otomatik yapılandırması, yönetimi ve koordinasyonu.
OWASP	Açık Web Uygulama Güvenliği Projesi
PGP	Oldukça iyi gizlilik
Fiziksel katman	OSI modelinin en alt katmanı, ham bilgi bitlerini iletir.
Sunum katmanı	OSI modelinin altıncı katmanı, bir noktadan diğerine iletilen verilerin sözdizimi ve anlamsal yönlerine odaklanır.

Terim	Tanım
Özel anahtar	Dijital varlıkların mülkiyetini gösteren gizli bir bilgi parçası.
Saldırı Simülasyonu ve Tehdit Analizi Süreci (PASTA)	İş hedefleri ve teknik gereksinimlere bağlanan risk tabanlı bir modeldir.
Genel anahtar	Dijital imzaların şifrelenmesi ve doğrulanması için kullanılan bir kriptografik anahtardır.
Genel anahtar kriptografisi	Genel ve özel anahtarlar kullanan bir genel kriptografik algoritmadır. Rivest, Shamir ve Adleman (veya RSA), genel anahtar kriptografisinin en popüler uygulamasıdır. RSA, herkesin kullanması için gizlilik, kimlik doğrulama ve şifreleme sağlar. Ayrıca, gereken şifreleme seviyesine bağlı olarak farklı anahtar uzunlukları kullanarak özel anahtarlar oluşturmak için asal sayı üretimini uygulamak için de kullanılır.
Rol tabanlı erişim kontrolü (RBAC)	Önceden tanımlanmış rollere göre kaynak erişimini düzenleyen bir erişim kontrol çerçevesidir. RBAC sisteminde, kullanıcılara belirli roller atanır; her biri, o roldeki kullanıcıların erişebileceği eylemleri veya kaynakları belirleyen bir izin seti ile ilişkilidir.
Scrum çerçevesi	Bireylerin karmaşık uyum sağlama zorluklarını ele alırken yüksek değerli ürünler üretmelerini sağlayan bir çerçevedir.
Güvenli kabuk (SSH)	Fiziksel ve bulut sunucuları gibi uzak cihazlarla bağlantı kurmak için güvenli bağlantı koruması.
Güvenli Soket Katmanı (SSL)	İnternet üzerinden güvenli veri iletimi sağlayan şifreleme teknolojisine dayalı bir protokoldür. Bir web tarayıcısı ile bir web sunucusu arasında değiştirilen verilerin gizli kalmasını ve yetkisiz erişimden korunmasını sağlar.
Güvenlik İddası İşaretleme Dili (SAML)	Çeşitli varlıklar arasında kimlik doğrulama ve yetkilendirme verilerinin değişimini kolaylaştırır. Farklı alanlar arasında sorunsuz ve güvenli kimlik doğrulama sağlar; bu, kullanıcıların tek bir kimlik bilgisi seti kullanarak birden fazla uygulama ve hizmete erişimini sağlar.
Güvenlik deseni	Tekrar eden güvenlik tehditlerine veya sorunlarına yeniden kullanılabilir bir çözümü temsil eden ve tanımlayan bir dizi kuraldır. Güvenlik desenlerini takip ederek, kuruluşlar sistem verilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlarken sağlam güvenlik çerçeveleri oluştururlar.
Güvenlik deseni kataloğu	Yazılım geliştiricilerin uygulama kodları için gerekli ve ek güvenlik özelliklerini geliştirmek üzere güvenlik desenlerini gözden geçirmelerini ve seçmelerini sağlar. Dağıtım için geliştirme yaparken, iyi sınıflandırılmış bir güvenlik deseni kataloğu, geliştiricilerin birden fazla uygulama arasında güvenlik desenlerini yeniden kullanmalarını sağlar. Yazılım geliştiricileri, ilgili güvenlik mekanizmalarını daha iyi anlamak için güvenlik deseni kataloglarına da başvurur.
Sunucusuz bilişim	Geliştiricilerin sunucuları yönetmeden veya boşta kalan bulut altyapısı için ödeme yapmadan kod oluşturup çalıştırmalarına olanak tanıyan bir bulut uygulama geliştirme ve yürütme modelidir.
Oturum katmanı	OSI modelinin beşinci katmanı, farklı makinelerden birden fazla oturum kurarken bir çökme meydana gelirse tutarlı oturumlar kurar.
Snort	Ağ trafiğinin gerçek zamanlı analizini sağlayan bir ağ ihlal tespit ve önleme sistemidir.
Snyk Kod	Geliştirme aşamasında kodlama ve güvenlik hatalarını keşfetmek için anlamsal analiz gerçekleştiren entegre bir geliştirme aracıdır.
Yazılım Geliştirme Yaşam Döngüsü (SDLC)	Yazılım geliştirmede her aşamada yer alan adımları belirten bir çerçevedir. Bir programın geliştirilmesi, dağıtımı ve bakımı için stratejiyi detaylandırır.
Sahtecilik	Yetkisiz erişim elde etmek için ağ trafiğini veya verileri manipüle eden bir ağ saldırısı türüdür.
Statik İnceleyici	Bilinen güvenlik açıklarını ortadan kaldırır. Açık Web Uygulama Güvenliği Projesi (veya OWASP), Ortak Güvenlik Açıkları ve Maruziyetler (veya CVE'ler) ve Ulusal Standartlar ve Teknoloji Enstitüsü (veya NIST) gibi çerçevelerle uyumlu olan Güvenlik İnceleyici paketinin bir bileşenidir.
STRIDE	STRIDE, Kimlik sahteciliği, Veri ile oynama, Reddetme, Bilgi ifşası, Hizmet reddi ve Yetki yükseltilmesi anlamına gelir. Microsoft'tan gelen STRIDE, uygulamaları ve sistemleri tehditleri ve güvenlik açıklarını bulmak için değerlendirir.
Alt ağlar	Bir alt ağ (veya subnet), daha yüksek verimlilikle daha uygulanabilir ağ segmentleri oluşturmak için bölünmüş daha büyük bir ağın daha küçük bir bölümüdür.
Simetrik şifreler	Verilerin hem şifrelenmesi hem de şifre çözmesi için aynı anahtarı kullanan kriptografik algoritmalardır.
Simetrik şifreleme	Hem şifreleme hem de şifre çözme için aynı anahtarın kullanılması.
Sistem çağrı denetimi	Linux çekirdeği gibi bir çekirdekten sistem çağrı bilgilerini alma ve gözden geçirme.
Tehdit modelleme	Sürekli tehditleri analiz etmek ve yazılım kodlama zayıflıkları ve güvenlik açıkları potansiyelini ortadan kaldırmak için bir süreç sağlar.
Tehdit izleme	Güvenlik sorunlarını bulmak için kod havuzlarını ve konteynerleri tarama. Parola yanlış yönetimi, protokol güvensizlikleri ve yanlış izinler, tehdit izleme ile keşfedebileceğiniz sorunlara örneklerdir.
Token yönetimi	Farklı sistemler ve uygulamalarda kullanılan benzersiz veri parçaları veya dizeleri olan token'ları ele alma ve kontrol etme işlemleri ve protokollerini içerir.
Taşıma katmanı	OSI modelinin dördüncü katmanı, ağ katmanından iletim veya verileri kabul eder ve bunları daha küçük birimlere veya paketlere keserek geri ağ katmanına iletir.
Taşıma Katmanı Güvenliği (TLS)	Bilgisayar ağı üzerinden iletişimleri güvence altına almak için kullanılan şifreleme teknolojisine dayalı bir protokoldür. SSL'in halefidir ve gelişmiş bir şifreleme algoritması kullanılarak tasarlanmıştır.
İki faktörlü kimlik doğrulama	Kullanıcı hesaplarını ve dijital verileri korumak için kullanılan ek bir güvenlik önlemidir. Kullanıcıların bir sisteme, hizmete veya uygulamaya erişim elde etmeden önce iki farklı kimlik biçimi sunmalarını gerektirir.
Birleşik Modelleme Dili (UML)	Bir sistemin mimarisini ve tasarımını daha iyi anlamak için bir sistemi görsel olarak modelleyebilir ve temsil edebilir.
Görsel, Çevik ve Basit Tehdit (VAST)	Uygulama ve operasyonel tehdit modelleri ile çevik bir metodolojidir. VAST, mimari perspektifi temsil etmek için süreç akış diyagramları kullanır.
Güvenlik açığı yamanması	Güvenlik güncellemeleri veya yamalarının dağıtımı, bir BT sistemi veya hizmetindeki işlevselliği artırır veya güvenlik açıklarını ortadan kaldırır.
Güvenlik açığı tarayıcı	Bilgisayar sistemleri, ağlar, uygulamalar ve diğer dijital varlıklardaki güvenlik yetersizliklerini tespit etmek ve değerlendirmek için tasarlanmış özel bir yazılım aracıdır.
Güvenlik açığı taraması	Kodun içinden ve bir uygulamanın dışından güvenlik açıklarını arama.
Web hizmetleri güvenliği	İnternet üzerinden web hizmetleri ve müşterileri arasında değiştirilen verilerin gizliliğini, bütünlüğünü ve kimlik doğrulamasını sağlamak için uygulanan bir dizi önlem ve protokoldür.

Yazar(lar)

- Gagandeep Singh