EMA SECURITY

Kaynak Kod Analizi Hizmeti

AI-Powered Offensive Services

İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

Kaynak Kod Analizi Hizmeti

Hizmet Tanımı

Kaynak Kod Analizi Hizmeti (Source Code Analysis Service), yazılım geliştirme süreçlerinde güvenliği en üst seviyeye çıkarmak ve siber saldırılara karşı dayanıklı uygulamalar geliştirilmesini sağlamak amacıyla, kaynak kodun detaylı bir şekilde incelenmesini kapsayan bir güvenlik hizmetidir. Bu hizmet, yazılım geliştirme sürecinin erken aşamalarında veya üretim öncesi test süreçlerinde güvenlik açıklarını tespit ederek, potansiyel tehditlerin önüne geçilmesini amaçlar.

Kaynak kod analizi, statik analiz (SAST), dinamik analiz (DAST), interaktif uygulama güvenlik testi (IAST) ve yazılım bileşen analizi (SCA) gibi teknikler kullanılarak gerçekleştirilir. Bu analizler, kod içerisindeki güvenlik açıklarını, hatalı yapılandırmaları, kimlik doğrulama ve yetkilendirme eksikliklerini, güvenli olmayan veri işleme mekanizmalarını ve kötü amaçlı kod parçalarını tespit etmeye odaklanır. Aynı zamanda, kullanılan açık kaynak kütüphaneler ve üçüncü taraf bileşenler analiz edilerek, bağımlılıklardaki güvenlik riskleri belirlenir.

Bu hizmet, OWASP Top 10, SANS 25, MITRE CWE, NIST Secure Software Development Framework (SSDF), ISO/IEC 27034 ve PCI DSS, GDPR, KVKK gibi uluslararası güvenlik standartlarına ve uyumluluk gereksinimlerine uygun şekilde gerçekleştirilir. Yazılım tedarik zinciri güvenliği kapsamında, organizasyonların geliştirdiği veya kullandığı kodun bütünsel bir güvenlik değerlendirmesi yapılır.

Kaynak Kod Analizi Hizmeti, uygulama güvenliği ekipleri, DevSecOps süreçleri, güvenlik analistleri ve yazılım geliştiriciler için kritik bir güvenlik katmanı sunar. Özellikle finans, sağlık, kamu, telekomünikasyon, e-ticaret ve savunma sanayi gibi yüksek güvenlik hassasiyeti olan sektörlerde, uygulamaların güvenlik seviyesini artırarak saldırılara karşı daha dirençli hale gelmesini sağlar.

Siber tehditlerin sürekli geliştiği günümüzde, yazılım güvenliğinin en baştan itibaren sağlanması kritik bir gerekliliktir. Kaynak Kod Analizi Hizmeti, siber saldırılara karşı proaktif güvenlik önlemleri alınmasını sağlar, kod güvenliğini güçlendirir, güvenlik açıklarını azaltır ve organizasyonların güvenlik duruşunu iyileştirerek uyumluluk süreçlerine katkıda bulunur.

Hizmete Ait Bileşenler

Kod Güvenlik Açıklarının Tespiti

Kaynak kod analizi süreci, yazılımın güvenlik açıklarını belirlemek amacıyla detaylı bir tarama ile başlar. Statik (SAST), dinamik (DAST) ve interaktif analiz (IAST) teknikleri kullanılarak kod içerisinde bulunan kimlik doğrulama hataları, yetkilendirme eksiklikleri, veri sızıntıları, güvenli olmayan API çağrıları ve SQL enjeksiyonu gibi tehditler tespit edilir.

Bağımlılık ve Üçüncü Taraf Kütüphane Analizi

Yazılım içerisinde kullanılan açık kaynak kütüphaneler ve üçüncü taraf bileşenler, güvenlik ve uyumluluk açısından değerlendirilir. Yazılım Bileşen Analizi (SCA) ile, kütüphanelerdeki bilinen güvenlik açıkları (CVE) ve lisans uyumluluğu kontrol edilir.

Kod Kalitesi ve Güvenli Kod Geliştirme Pratikleri

Kod güvenliğinin sağlanmasının yanı sıra kod kalitesi, okunabilirlik, performans ve sürdürülebilirlik de analiz edilir. Güvensiz kod yazım teknikleri belirlenerek, geliştiricilere OWASP Secure Coding Practices, CERT Secure Coding Guidelines gibi en iyi uygulamalar doğrultusunda yönlendirmeler sunulur.

Yetkilendirme ve Kimlik Doğrulama Kontrolleri

Yazılımın kimlik doğrulama (authentication) ve yetkilendirme (authorization) mekanizmaları analiz edilerek, kullanıcı rollerinin yönetimi, parola politikaları ve erişim kontrol mekanizmaları incelenir. Yetkisiz erişim riskleri ve kimlik doğrulama bypass senaryoları değerlendirilerek güvenlik açıkları belirlenir.

Veri Güvenliği ve Şifreleme Analizi

Kod içerisindeki hassas veri işlemleri, şifreleme algoritmaları ve veri saklama yöntemleri analiz edilir. Zayıf şifreleme algoritmaları, hassas verilerin açık metin olarak saklanması, sertifikasız veri alışverişi (TLS eksiklikleri) gibi riskler tespit edilir ve güvenli veri yönetimi önerileri sunulur.

Güvenli API ve Web Servis Analizi

Kod içerisinde kullanılan REST, SOAP, GraphQL gibi API'ler detaylı bir şekilde incelenerek, API güvenliği açısından zafiyetler belirlenir. Yetkisiz erişim riskleri, eksik giriş doğrulama, güvenli olmayan veri alışverişi ve API anahtarı sızıntıları gibi potansiyel güvenlik açıkları analiz edilir.

Kod Enjeksiyon ve Güvenli Girdi Doğrulama

SQL, XSS, Command Injection, Deserialization saldırıları gibi kod enjeksiyon zafiyetleri, kodun güvenli giriş doğrulama mekanizmaları üzerinden incelenir. Girdi sanitizasyonu ve parametrik sorgular (prepared statements) kullanımı değerlendirilerek güvenlik açıkları belirlenir.

Otomatik ve Manuel Kod Analiz Teknikleri

Kod güvenlik açıklarının belirlenmesi için hem otomatik tarama araçları hem de manuel kod inceleme yöntemleri kullanılır. Otomatik araçlar geniş çaplı analiz sağlarken, manuel kod incelemesi ile gizli arka kapılar (backdoors), iş mantığı hataları ve güvenlik riskleri tespit edilir.

Uyumluluk ve Regülasyon Kontrolleri

Kod analiz süreci, organizasyonun uymakla yükümlü olduğu ISO 27034, PCI DSS, GDPR, KVKK, HIPAA, NIST Secure Software Development Framework (SSDF) gibi regülasyonlara göre değerlendirilir. Yazılımın ilgili standartlara uygunluğu denetlenerek, eksiklikler ve iyileştirme önerileri sunulur.

Kod Güvenliği Eğitimleri ve Danışmanlık

Kod analizi sonrası geliştirici ekipler için güvenli kod yazımı, en iyi güvenlik uygulamaları ve OWASP Top 10 eğitimleri sağlanır. Organizasyonların güvenlik farkındalığını artırmak ve gelecekte güvenli yazılım geliştirme süreçlerini benimsemelerini sağlamak amacıyla danışmanlık hizmeti sunulur.

Mevcut Durum Analizi

Kaynak Kod Analizi Hizmeti öncesinde, organizasyonun yazılım geliştirme süreçleri ve kod güvenliği uygulamaları değerlendirilir. SDLC, kullanılan programlama dilleri, versiyon kontrol sistemleri (Git, SVN) ve CI/CD süreçleri analiz edilerek mevcut güvenlik durumu belirlenir.

Statik (SAST), dinamik (DAST) ve interaktif (IAST) analiz araçları incelenerek güvenlik test kapasitesi ölçülür. Üçüncü taraf kütüphaneler ve açık kaynak bileşenleri, CVE, NVD ve GitHub Advisory Database gibi veri tabanları üzerinden taranarak zafiyetler belirlenir.

Kod inceleme süreçleri, erişim kontrolleri ve geliştirici ekiplerin güvenlik farkındalığı analiz edilir. ISO 27001, ISO 27034, NIST CSF, PCI DSS, GDPR ve KVKK uyumluluğu gözden geçirilerek eksiklikler tespit edilir. Sonuçlar doğrultusunda, güvenli kod geliştirme süreçlerini iyileştirmek için organizasyona özel bir yol haritası oluşturulur.

Strateji ve Yol Haritası Belirleme

Kaynak Kod Analizi Hizmeti kapsamında, organizasyonun yazılım güvenliği stratejisi belirlenir. Öncelikle, kod tabanında güvenlik riskleri, kullanılan programlama dilleri ve üçüncü taraf kütüphaneler analiz edilerek risk odaklı bir yaklaşım oluşturulur.

Statik (SAST), dinamik (DAST) ve kompozisyon (SCA) analiz araçları belirlenerek, otomatik ve manuel kod inceleme süreçleri tanımlanır. Kritik bileşenler ve potansiyel güvenlik açıkları önceliklendirilerek, güvenli kod geliştirme süreçleri iyileştirilir.

Son olarak, sürekli entegrasyon (CI/CD) güvenliği, güvenli kod yazımı eğitimleri ve güvenlik politikaları optimize edilerek organizasyona özel bir kaynak kod analizi yol haritası oluşturulur.

Kaynak Kod Analizi Hizmeti Aşamaları

Kaynak kod analizi süreci, öncelikle kod keşfi aşamasıyla başlar. Bu aşamada, kod tabanı, kullanılan diller, üçüncü taraf kütüphaneler ve bağımlılıklar analiz edilerek güvenlik riskleri belirlenir.

Ardından, statik kod analizi (SAST), dinamik analiz (DAST) ve yazılım bileşeni analizi (SCA) gibi teknikler kullanılarak güvenlik açıkları tespit edilir. Bulunan zafiyetler doğrulanarak, olası saldırı senaryoları ve risk seviyeleri değerlendirilir.

Gelişmiş manuel kod inceleme süreçleri ile kimlik doğrulama, erişim kontrolü, veri doğrulama ve şifreleme mekanizmaları detaylı olarak incelenir. Kod güvenliği için en iyi uygulamalar belirlenerek geliştiricilere yönelik düzeltme önerileri sunulur.

Son olarak, detaylı bir güvenlik raporu hazırlanarak tespit edilen açıklar, risk seviyeleri ve önerilen iyileştirme adımları paylaşılır. Süreç, CI/CD entegrasyonu ve düzenli kod taramalarıyla sürekli güvenlik iyileştirmeleri yapılarak sürdürülebilir hale getirilir.

Kaynak Kod Analizi Hizmeti Metodolojisi

Kaynak Kod Analizi Hizmeti, yazılım güvenliğini sağlamak, güvenlik açıklarını erken aşamada tespit etmek ve güvenli yazılım geliştirme süreçlerini teşvik etmek amacıyla OWASP Code Review Guide, NIST Secure Software Development Framework (SSDF), ISO/IEC 27034 ve CERT Secure Coding Standards gibi uluslararası güvenlik standartları temel alınarak yürütülür.

İlk olarak, organizasyonun yazılım geliştirme süreçleri ve kod tabanı detaylı şekilde analiz edilir. Kullanılan programlama dilleri, çerçeveler (frameworks), üçüncü taraf kütüphaneler, bağımlılıklar ve yazılımın mimari yapısı değerlendirilerek analiz kapsamı belirlenir. Bu süreçte, yazılım geliştirme yaşam döngüsü (SDLC) içindeki güvenlik açıklarını en aza indirmek amacıyla CI/CD süreçleri, kod gözden geçirme politikaları ve güvenlik kontrolleri gözden geçirilir.

Keşif sürecinde, statik kod analizi (SAST), dinamik analiz (DAST), yazılım bileşeni analizi (SCA) ve interaktif uygulama güvenlik testleri (IAST) gibi teknikler kullanılarak kod içindeki güvenlik açıkları tespit edilir. Kimlik doğrulama hataları, erişim kontrol zafiyetleri, veri doğrulama eksiklikleri, güvenli olmayan API kullanımları, bellek yönetimi açıkları ve kriptografik zayıflıklar gibi kritik güvenlik riskleri analiz edilir.

Ardından, manuel kod inceleme süreçleri ile iş mantığı açıkları, yetkilendirme problemleri, zararlı kod enjeksiyonları ve güvenlik yanlış yapılandırmaları değerlendirilir. Güvenlik açıkları tespit edildikten sonra, saldırı vektörleri belirlenerek istismar senaryoları oluşturulur ve risk seviyeleri belirlenir. Bu aşamada, güvenlik açıklarının istismar edilme ihtimali ve sistem üzerindeki potansiyel etkileri değerlendirilerek kapsamlı bir risk analizi gerçekleştirilir.

Toplanan bulgular ışığında, organizasyonun yazılım güvenliğini güçlendirmek için güvenli kod geliştirme en iyi uygulamaları, OWASP Secure Coding Practices, kod düzeltme önerileri ve güvenlik yamaları sunulur. CI/CD süreçlerine güvenlik entegrasyonu (DevSecOps), otomatik güvenlik testleri, kod gözden geçirme politikaları ve güvenli geliştirme eğitimleri ile yazılım güvenliği süreçlerinin sürdürülebilir hale getirilmesi sağlanır.

Raporlama ve İyileştirme

Kaynak Kod Analizi Hizmeti kapsamında, tespit edilen güvenlik açıkları ve kod zafiyetleri detaylı şekilde raporlanır. Bulgular; kimlik doğrulama hataları, SQL enjeksiyonu, XSS, güvenli olmayan API kullanımları ve bellek taşması gibi kritik güvenlik riskleri açısından değerlendirilir. Açıklar risk seviyelerine göre sınıflandırılarak düzeltici ve önleyici aksiyon planları sunulur.

Olay sonrası analizde, güvenli kod yazma standartları, CI/CD güvenliği, kod inceleme prosedürleri ve bağımlılık yönetimi gözden geçirilerek iyileştirme önerileri sunulur. Açıkların giderilmesi sonrası doğrulama testleri yapılır ve güvenlik taramaları düzenli olarak tekrarlanarak yazılım güvenliği sürdürülebilir hale getirilir.

Sıkça Sorulan Sorular (SSS)

Kaynak Kod Analizi Hizmeti neden önemlidir?

Kaynak kod analizi, yazılım geliştirme sürecinde güvenlik açıklarını erken aşamada tespit etmeye ve siber saldırılara karşı korunmaya yardımcı olur. Güvensiz kodların üretime alınmasını engelleyerek veri ihlalleri ve sistem açıklarını minimize eder.

Kaynak kod analizi manuel mi yoksa otomatik mi yapılır?

Kaynak kod analizi hem manuel incelemelerle hem de otomatik tarama araçları ile gerçekleştirilir. Manuel analiz, mantıksal hataları ve iş mantığı zafiyetlerini tespit etmek için kullanılırken, otomatik araçlar yaygın güvenlik açıklarını hızlı bir şekilde belirler.

Kaynak kod analizi hangi güvenlik standartlarına dayanır?

Bu hizmet, OWASP, SANS, NIST, CERT Secure Coding gibi uluslararası güvenlik çerçevelerine uygun olarak gerçekleştirilir.

Kaynak kod analizi hangi tür güvenlik açıklarını tespit eder?

SQL enjeksiyonu, XSS, kimlik doğrulama hataları, bellek taşması, API güvenlik açıkları ve güvenli olmayan bağımlılıklar gibi riskleri belirler.

Kaynak kod analizi hangi aşamada yapılmalıdır?

Analiz, yazılım geliştirme sürecinin (SDLC) erken aşamalarında yapılmalı ve düzenli olarak tekrarlanmalıdır. CI/CD süreçlerine entegre edilerek sürekli güvenlik sağlanabilir.

Kaynak kod analizi hangi programlama dillerini destekler?

Java, Python, C/C++, JavaScript, Go, PHP, .NET gibi yaygın diller analiz edilebilir.

Kaynak kod analizi ile güvenlik testleri arasındaki fark nedir?

Kaynak kod analizi, kod seviyesinde güvenlik açıklarını tespit ederken, sızma testleri (pentest) çalışan sistemler üzerindeki güvenlik açıklarını belirler.

Kaynak kod analizi bulut tabanlı yazılımlar için de uygulanabilir mi?

Evet, bulut tabanlı ve microservices mimarisiyle çalışan yazılımlar için de güvenlik analizi yapılabilir.

Kaynak kod analizi hizmeti ile yazılım geliştirme sürecine nasıl katkı sağlanır?

Geliştiricilerin güvenli kod yazımını öğrenmesini sağlar, yazılım güvenliğini artırır ve olası saldırıları minimize eder.