YÜKSEK GÜVENLİKLİ UYGULAMA GELİŞTİRME

Teknolojinin hızla gelişmesiyle birlikte yazılım güvenliği, her geçen gün daha kritik bir öneme sahip olmaktadır. Siber saldırıların artan sıklığı, güvenlik açıklarının hızla kötüye kullanılmasına yol açmakta ve hem bireyler hem de kurumlar için büyük riskler yaratmaktadır. Bu bağlamda, yazılım geliştiricilerinin güvenli yazılım geliştirme süreçleri hakkında derinlemesine bilgi sahibi olmaları hayati önem taşır.

YÜKSEK GÜVENLİKLİ UYGULAMA GELİŞTİRME

KURUMSAL ÖZEL EĞİTİM

Bu konuyu istediğiniz gibi özelleştirebilirsiniz. Kullandığınız teknolojiye özel uygulamalar ile anlatılmasını, projenize uygun içerik haline getirilmesini ...

Vebende
Bilişim, Eğitim ve Danışmanlık

YÜKSEK GÜVENLİKLİ UYGULAMA GELİŞTİRME EĞİTİMİ

- **Yazılım Güvenliği Temellerini Öğrenmek:** Güvenlik açıkları, tehditler ve güvenli yazılım geliştirme kavramlarını anlamak.
- **Yaygın Güvenlik Açıkları ve Çözümleri:** OWASP Top Ten gibi yaygın güvenlik açıklarını tespit etme ve bu açıkları nasıl önleyebileceğini öğrenmek.
- **Güvenli Kod Yazma Teknikleri:** Güvenli yazılım geliştirme metodolojilerini uygulayarak, güvenli kod yazma becerisi kazanmak.
- **Güvenlik Testlerini Uygulamak:** Penetrasyon testleri ve güvenlik taramaları gibi test yöntemlerini öğrenmek ve uygulamak.
- **Güvenli Yazılım Mimarisi ve Tasarımı:** Güvenli yazılım mimarisi ve tasarım prensiplerini anlamak ve bu bilgileri projelere entegre etmek.
- **Güncel Güvenlik Trendlerini Takip Etmek:** Bulut güvenliği, IoT güvenliği gibi güncel konularda bilgi sahibi olmak ve gelecekteki tehditlere karşı hazırlıklı olmak.
- **Proaktif Güvenlik Yönetimi:** Güvenlik politikaları oluşturmak, güvenlik bilincini artırmak ve yazılım geliştirme süreçlerinde güvenlik önlemleri almak.

EĞİTİMİN HEDEFİ

Bu eğitimin temel hedefi, katılımcılara yazılım güvenliği konusunda kapsamlı bir bilgi ve beceri kazandırmaktır. Katılımcılar, yazılım geliştirme süreçlerinde karşılaşılan güvenlik açıklarını tanıyıp etkili bir şekilde çözebilecek bilgiye sahip olacaklar. Eğitimin sonunda katılımcılar, güvenli kod yazma tekniklerini uygulayarak, yazılım projelerinde güvenlik önlemlerini entegre edebilecek, siber tehditlere karşı proaktif bir yaklaşım sergileyebilecektir.

EĞİTİM İÇERİĞİ

GİRİŞ VE TEMEL KAVRAMLAR

- Kod güvenliği ve güvenlik açıklarının tanımı
- Yazılım geliştirme sürecinde güvenliğin önemi
- Güvenlik kavramlarının yazılım yaşam döngüsü üzerindeki etkisi
- Farklı güvenlik türleri: fiziksel güvenlik, ağ güvenliği, uygulama güvenliği

YAYGIN GÜVENLİK AÇIKLARI

- **OWASP Top Ten:**
  - SQL Enjeksiyonu
  - Kimlik Doğrulama ve Oturum Yönetimindeki Hatalar
  - Hassas Verilerin Açığa Çıkması
  - XML Harici Entiteler (XXE)
  - Güvenlik Yapılandırma Hataları
  - Kötü Güvenlik Denetimleri
  - İstemci Tarafı Hataları
  - Güvenli İletişim Hataları
  - Yazılım ve Bağımlılık Yönetimi Hataları
  - Yetersiz Güvenlik İzleme ve Kaydetme
- **SQL Enjeksiyonu (SQL Injection):** Kullanıcı tarafından girilen verilerin doğrudan veritabanına sorgu olarak gönderilmesi, saldırganların kötü niyetli SQL kodları eklemesine olanak tanır. Bu, veritabanındaki hassas verilere erişim sağlayabilir.
- **XSS (Cross-Site Scripting):** Kullanıcı tarafından girilen verilerin doğrulanmadan veya filtre edilmeden web sayfalarına dahil edilmesi, kötü niyetli JavaScript kodlarının kullanıcıların tarayıcılarında çalışmasına neden olabilir. Bu, kullanıcıların çalınması, kimlik avı (phishing) ve oturum çalınması gibi saldırılara yol açabilir.
- **CSRF (Cross-Site Request Forgery):** Bir saldırganın, kullanıcıyı kandırarak, onun izni olmadan istemediği bir işlemi gerçekleştirmesini sağladığı bir saldırıdır. Kullanıcı, oturumu açıkken, zararlı bir bağlantıya tıklayarak, işlemi fark etmeden gerçekleştirebilir.
- **Yetersiz Girdi Doğrulaması ve Sanitizasyonu:** Kullanıcıdan gelen veri, uygulamanın beklediği formatta değilse veya doğrulama yapılmazsa, saldırganlar zararlı veri gönderebilir. Bu, örneğin, komut çalıştırma veya veritabanı sorgusu gibi işlemlere yol açabilir.
- **Yetkilendirme ve Kimlik Doğrulama Zayıflıkları:** Zayıf parola politikaları, kimlik doğrulama eksiklikleri veya yetki kontrolü hataları, kullanıcıların sisteme yetkisiz erişim sağlamasına neden olabilir. Ayrıca, oturum yönetimi hataları da önemli güvenlik açıklarıdır.
- **İnsecure Deserialization (Güvensiz Serileştirme):** Uygulama, dışarıdan gelen verileri deserialize (serileştirme) ederek okurken, saldırganlar zararlı veriler gönderebilir. Bu, kod enjeksiyonu, saldırıların sistemde çalışmasına yol açabilir.
- **Zayıf Şifreleme:** Verilerin yeterince güvenli bir şekilde şifrelenmemesi, şifreleme anahtarlarının kötü yönetilmesi veya şifreleme algoritmalarının zayıf olması, verilerin ele geçirilmesine neden olabilir. Özellikle hassas veriler (şifreler, kredi kartı numaraları) şifrelenmeden saklanması ciddi bir güvenlik açığı oluşturur.
- **İzin Kontrolü ve Erişim Hataları:** Yetersiz erişim kontrolü, kullanıcıların sadece yetkili oldukları verilere erişmesini engellemez. Bu, özellikle gizli verilere veya yönetici seviyesinde kaynaklara izinsiz erişim sağlanmasına yol açabilir.
- **Gizli Anahtarlar ve Şifreler Kodu İçinde Saklanması:** Yazılımda gizli anahtarlar veya şifreler düz metin olarak saklanması veya kaynak kodunda yer alması, siber saldırganlar için kolayca erişilebilen bir hedef haline gelir. Bu tür bilgiler güvenli bir şekilde saklanmalı ve yönetilmelidir.
- **İnsecure Direct Object References (IDOR):** Bir kullanıcı, URL veya API üzerinden sistemdeki bir kaynağa (dosya, veri tabanı kaydı, vb.) izinsiz erişim sağlayabilir. Bu, genellikle URL parametreleri üzerinden gerçekleşen bir güvenlik açığıdır.
- **Bileşenlerin Güncel Olmaması (Outdated Components):** Kullanılan yazılım bileşenlerinin, kütüphanelerin ve framework'lerin eski versiyonları, bilinen güvenlik açıklarına sahip olabilir. Güncel olmayan yazılım bileşenleri, güvenlik açıklarını artırır.
- **Hatalı veya Eksik Hata Yönetimi:** Hataların, kullanıcıya veya saldırganlara anlamlı bilgi sağlamadan düzgün bir şekilde işlenmemesi, uygulamanın güvenlik açıklarının keşfedilmesine yol açabilir. Bu, saldırganlara sistemin zayıf noktalarını gösterebilir.
- **Server-Side Request Forgery (SSRF):** SSRF saldırılarında, saldırgan sunucuya dış bir kaynağa (yerel ağlar veya harici hizmetler gibi) istekte bulunması için yönlendirme yapar. Bu, veritabanlarına veya yerel ağlara erişimi sağlayabilir.
- **Denial of Service (DoS) ve Distributed Denial of Service (DDoS):** Sistemleri aşırı yükleyerek veya kötüye kullanarak, hizmetin çökmesine veya performansın ciddi şekilde düşmesine neden olabilir. Bu tür saldırılar, yazılımın ölçeklenebilirliğini ve dayanıklılığını test eder.

EĞİTİM İÇERİĞİ

GÜVENLİ KOD YAZMA PRENSİPLERİ

- Kod güvenliği için en iyi uygulamalar
- Girdi doğrulama ve sanitizasyon
- Çıktı kodlaması ve güvenli veri işleme
- Doğru kimlik doğrulama ve yetkilendirme yöntemleri
- Güvenli oturum yönetimi
- Şifreleme yöntemleri ve veri koruma
- Hata yönetimi ve güvenlik bildirimleri

GÜVENLİK ARAÇLARI VE TEKNOLOJİLERİ

- Statik ve dinamik analiz araçları
- Güvenlik tarayıcıları ve güncel güvenlik açıkları veritabanları
- Güvenli yazılım geliştirme yaşam döngüsü (SDLC) araçları
- Kaynak kodu güvenlik analizi araçları: SonarQube, Veracode, Checkmarx
- Otomatik test ve sürekli entegrasyon araçları (CI/CD)

GÜVENLİ UYGULAMA GELİŞTİRME SÜRECİ

- Güvenli uygulama geliştirme yaşam döngüsü (SDL)
- Proje planlama aşamasında güvenlik gereksinimlerinin belirlenmesi
- Tasarım aşamasında güvenlik mimarisi
- Geliştirme sürecinde güvenlik uygulamaları
- Test aşamasında güvenlik testleri ve değerlendirmeleri

Dağıtım ve bakım aşamalarında güvenliğin sürdürülmesi

GÜVENLİK TESTLERİ VE DEĞERLENDİRMELERİ

- Penetrasyon testleri (Pentest) ve güvenlik değerlendirmeleri
- Manuel güvenlik testleri ve otomatik testlerin rolü
- Güvenlik açığı tarama yöntemleri
- Kırılganlık değerlendirme süreçleri
- Test sonuçlarının raporlanması ve iyileştirme önerileri

GÜVENLİ UYGULAMA MİMARİSİ VE TASARIMI

- Güvenli yazılım mimarisi kavramları
- Servis odaklı mimari (SOA) ve mikro hizmet mimarisi güvenlik uygulamaları
- Güvenlik tasarım kalıpları (security design patterns)
- API güvenliği ve güvenli iletişim protokolleri

GÜVENLİK YÖNETİMİ VE POLİTİKA GELİŞTİRME

- Yazılım güvenliği politikalarının oluşturulması
- Güvenlik standartları ve düzenlemeleri (OWASP, ISO 27001, GDPR)
- Ekip içinde güvenlik bilincinin artırılması
- İlgili paydaşlarla güvenlik iletişimi ve işbirliği

GÜNCEL GÜVENLİK EĞİLİMLERİ VE GELECEKTEKİ TEHDİTLER

- Bulut güvenliği ve uygulama güvenliği
- IoT güvenliği ve mobil uygulama güvenliği
- Yapay zeka ve makine öğrenimi ile güvenlik
- Gelecekteki güvenlik tehditleri ve savunma stratejileri

PRATİK UYGULAMALAR VE VAKA ÇALIŞMALARI

- Gerçek dünya örnekleri ve vaka çalışmaları
- Güvenlik açıklarının nasıl tespit edileceği ve düzeltileceği üzerine simülasyonlar
- Güvenli yazılım geliştirme projelerinde karşılaşılan zorluklar ve çözümleri
- Grup çalışmaları ve uygulamalı projelerle güvenlik becerilerinin pekiştirilmesi

EĞİTİM SÜRESİ

- 10 Gün
- Ders Süresi: 50 dakika
- Eğitim Saati: 10:00 - 17:00

Eğitim formatında eğitimler 50 dakika + 10 dakika moladır. 12:00-13:00 saatleri arasında 1 saat yemek arasındaki verilir. Günde toplam 6 saat eğitim verilir. 10 günlük formatta 60 saat eğitim verilmektedir.

Eğitimler uzaktan eğitim formatında tasarlanmıştır. Her eğitim için teams linkleri gönderilir. Katılımcılar bu linklere girerek eğitimlere katılırlar. Ayrıca farklı remote çalışma araçları da eğitmen tarafından tüm katılımlara sunulur. Katılımcılar bu araçları kullanarak eğitimlere katılırlar.

Eğitim içeriğinde github ve codespace kullanılır. Katılımcılar bu platformlar üzerinden örnek projeler oluşturur ve eğitmenle birlikte eğitimlerde sorulan sorulara ve taleplere uygun iceriğe cevap verir. Katılımcılar bu araçlarla eğitimlerde sorulan sorulara ve taleplere uygun iceriğe cevap verir. Eğitim yapay zeka destekli kendi kendine öğrenme formasyonu ile tasarlanmıştır. Katılımcılar eğitim boyunca kendi kendine öğrenme formasyonu ile eğitimlere katılırlar. Bu eğitim formatı sayesinde tüm katılımcılar gelecek tüm yaşamlarında kendilerini güncellemeye devam edebilecekler ve her türlü sorunun karşısında çözüm bulabilecekleri yeteneklere sahip olacaklardır.

KOD KALİTE VE ÖLÇÜMLEME

Günümüzde siber tehditler hızla artarken, güvenli yazılım geliştirme her zamankinden daha önemli hale gelmiştir. Bu eğitim, yazılım geliştiricilere güvenlik açıklarını tespit etme, güvenli kod yazma ve proaktif güvenlik önlemleri alma konusunda kapsamlı bilgi ve beceriler kazandırmayı amaçlamaktadır. OWASP Top Ten, güvenli yazılım mimarisi, penetrasyon testleri ve güncel güvenlik trendleri gibi konuların ele alınacağı bu eğitimle, katılımcılar yazılım projelerine güvenliği en baştan entegre ederek siber tehditlere karşı güçlü bir savunma oluşturabilecekler

KATILIMCILARDAN BEKLENTİLERİMİZ

- **Aktif Katılım:** Katılımcıların eğitim boyunca aktif bir şekilde derse katılmaları ve sorular sormaları beklenmektedir. Eğitim içeriği interaktif olduğundan, katılımcıların tartışmalara katılması, grup çalışmaları ve örnek vakalar üzerinden görüş paylaşmaları önemli olacaktır.
- **Temel Yazılım Bilgisi:** Eğitim, yazılım geliştirme ve güvenlik konularında temel bilgiye sahip katılımcılara yönelik tasarlanmıştır. Katılımcıların yazılım geliştirme süreçleri hakkında temel bilgilere sahip olmaları ve temel programlama bilgisine sahip olmaları beklenmektedir.
- **Pratik Uygulamalara Katılım:** Eğitimde verilen teorik bilgilerin pekiştirilmesi amacıyla pratik uygulamalar yapılacaktır. Katılımcıların uygulamalı bölümlere aktif katılım göstermeleri ve öğrendikleri bilgileri gerçek dünya senaryolarına uygulamaları beklenmektedir.

EĞİTİM YÖNTEMİ

- **Teorik Bilgi:** Güncel bilgiler ve konseptlerin anlatımı.
- **Uygulamalı Örnekler:** Gerçek senaryolarla pratik uygulamalar.
- **Etkileşimli Tartışmalar:** Katılımcıların aktif katılım sağlayacağı, soru-cevap şeklinde tartışmalar yapılacak oturumlar.
- **Proje Tabanlı Öğrenme:** Eğitimin son günü, katılımcıların öğrendiklerini pratikte uygulayacakları kapsamlı bir proje çalışması yapılacak.

HEDEF KİTLE

- **Yazılım Geliştiriciler ve Programcılar:** Yazılım geliştiren ve güvenli yazılım uygulamaları oluşturmak isteyen yazılımcılar, yazılım güvenliği konularında bilgi ve becerilerini artırmak amacıyla bu eğitime katılabilir.
- **DevOps ve Sistem Yöneticileri:** Yazılım geliştirme ve dağıtım süreçlerinde güvenliği sağlamakla sorumlu olan DevOps mühendisleri ve sistem yöneticileri, altyapı ve uygulama güvenliğini güçlendirecek yeni teknikler öğrenebilir.
- **Yazılım Mimarı ve Tasarımcılar:** Yazılımın güvenliğini tasarlama ve güvenli yazılım mimarileri oluşturma konusunda bilgi sahibi olmak isteyen yazılım mimarları ve tasarımcıları, güvenlikli yazılım geliştirme ilkelerini öğrenmek için bu eğitimi alabilirler.
- **Kalite Güvence (QA) ve Test Uzmanları:** Yazılım ürünlerinin güvenlik testlerini gerçekleştiren ve güvenlik açıklarını tespit etmek için testler yapan QA uzmanları ve test mühendisleri, güvenlik testleri konusunda daha derinlemesine bilgi edinmek isteyebilir.

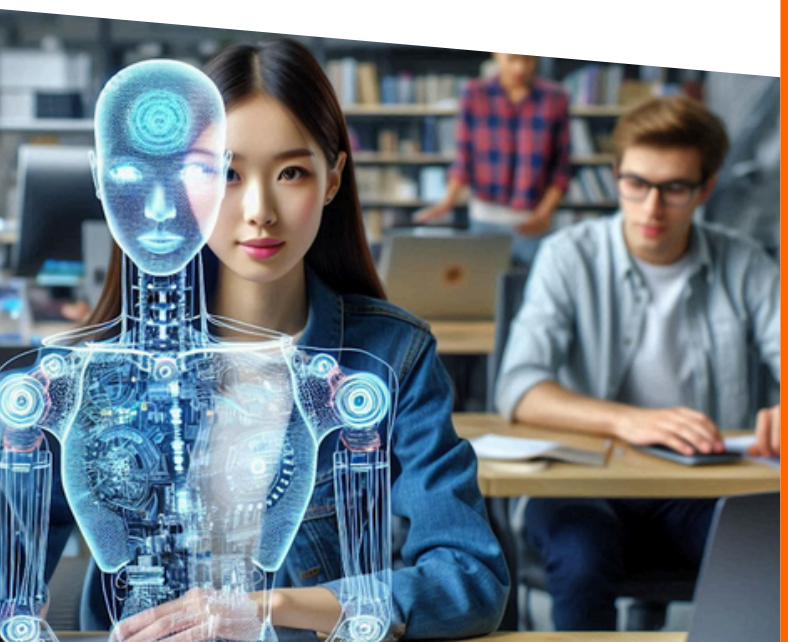
"

Kurumsal size özel eğitimler hazırlıyoruz. Her eğitim yeni bir heyecan.

Vebende A.Ş.

Kurumsal Terzi Usulü Butik Eğitimler.

Size özel hazırlanan seminer, danışmanlık, eğitim ve hizmetlerimizle yüksek verim elde edin. Paranızı boşa harcamayın. Zaman çok değerli.



Her Eğitim Yeni Bir Heyecan

2000 yılından günümüze devam eden eğitim heyecanı. Uluslararası tecrübe, proje geliştirme deneyimleri, danışmanlıklar ve arge mühendislik deneyimlerimizi ülkemize sunmak için yeni bir konsept tasarladık.
Sizi dinliyor, takımınıza uygun özel içerikler ile hazırlanmış eğitimler hazırlıyoruz. Her eğitim özel bir çalışma, içerik üretimi, uygulama örnekleri hazırlıkları, sunumlar hazırlamayı gerektiriyor. Aynı eğitimi yönetim kadrosuna farklı, teknik ve mimar ekiplerinize farklı içerikler ile hazırlıyoruz. Her eğitim yeni bir macera ve heyecan.

Bizimle İletişime Geçin

iletisim@vebende.com

www.vebende.com.tr

İzmir - Türkiye

Kurumsal
Eğitimler

www.vebende.com.tr

İletişime Geçin

Whatsapp 0542 5505704

iletisim@vebende.com

www.vebende.com.tr

Adalet Mah. Manas Bulvarı
No:39 İç Kapı N0: 3107 Bayraklı
İZMİR






Sürekli Güncellenen Eğitimlerimizi Sitemizden Takip Edin.

"

Kurumsal terzi usulu size özel eğitimler ve uluslararası deneyime sahip eğitmenler ile çalışmanın keyfi

"

Size Neler Sunuyoruz?

- Kitaptan okunan eğitimler sunmuyoruz. Sizin için özel hazırlanan içerikler ve uygulamalı eğitimler hazırlıyoruz.
- Her eğitim için sunumlar, materyaller, örnek senaryolar size özel hazırlıyoruz.
- Her eğitim için katılımcılara özel github repoları hazırlanıyor. Eğitimden sonra da katılımcılar hayat boyu kaynaklara ulaşmaya devam edebilsinler diye, **"katılımcılar ve eğitmenle birlikte yapılan tüm çalışmaları"** github repolarında saklıyoruz.

Misyonumuz

1. Ülkemizde dünyanın en güncel teknolojilerini kazandırmak. En güncel teknolojilerine hakim takımlarına katkı sağlamak.
2. Alışılmışın dışında en güncel teknolojileri deneyimli eğitmenler ve uygulamalar ile sunmak.
3. Siber güvenlik konusunda hassas çalışmalar sunarak, çağımızın büyük kabusu siber tehditler konusunda deneyimli bilgili takımların oluşmasına katkı sağlamak.