Güvenli Yazılım Geliştirme Eğitimi

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Süre: **3 Gün**

Günümüz bilgi güvenliği ortamında en önemli risk alanlarından biri, güvenlik gereksinimleri yeterince dikkate alınmadan geliştirilen yazılımlardır. Uygulama güvenliği sağlanmadan kurumsal bilgi güvenliğinin tam anlamıyla oluşturulması mümkün değildir.

Yazılım geliştirme ekipleri çoğu zaman teslimat hızı, yeni özellikler ve işlevsellik üzerine yoğunlaşırken güvenlik kontrolleri ikinci planda kalabilir. Bu durum; kimlik doğrulama hataları, zayıf session yönetimi, injection açıkları, XSS, yetkilendirme problemleri ve güvensiz veri işleme gibi ciddi uygulama güvenliği risklerinin ortaya çıkmasına neden olabilir.

Güvenli Yazılım Geliştirme Eğitimi, geliştiricilere ve yazılım güvenliği denetimi gerçekleştiren profesyonellere daha güvenli, kontrol edilebilir ve sürdürülebilir uygulamalar geliştirmek için gerekli yaklaşımı kazandırmak amacıyla hazırlanmıştır.

Program boyunca güvenlik yalnızca teorik bir konu olarak ele alınmaz. Java ve .NET platformlarına yönelik kod örnekleri kullanılarak yaygın yazılım güvenliği açıkları, bu açıkların nedenleri ve güvenli kodlama teknikleri uygulamalı olarak incelenir.

Katılımcılar, yazılım geliştirme yaşam döngüsü boyunca güvenliğin nasıl ele alınabileceğini, kullanıcı girdilerinin nasıl kontrol edilmesi gerektiğini, authentication ve session mekanizmalarının nasıl korunacağını ve kodun güvenlik açısından nasıl analiz edilebileceğini öğrenir.

Önkoşullar

Bu eğitime katılmak için temel programlama bilgisine sahip olmak yeterlidir.

Katılımcıların aşağıdaki konulara aşinalığı faydalıdır:

- Temel programlama kavramları
- Web uygulamalarının çalışma prensipleri
- HTTP request/response yapısı
- Java veya .NET ile temel geliştirme bilgisi

Güvenli Yazılım Geliştirme Eğitimi

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Süre: **3 Gün**

Kimler Katılmalı

Bu eğitim özellikle:

- Kurumsal ortamlarda çalışan yazılım geliştiriciler
- Java geliştiricileri
- .NET geliştiricileri
- Application Security uzmanları
- Software Security profesyonelleri
- Kod güvenliği denetimi gerçekleştiren uzmanlar
- Güvenli yazılım geliştirme süreçlerinden sorumlu ekip liderleri
- QA ve test ekipleri
- DevSecOps süreçlerinde çalışan profesyoneller

için uygundur.

Neler Öğreneceksiniz

Eğitimin sonunda katılımcılar:

- Secure coding yaklaşımının temel prensiplerini açıklayabilir
- Yaygın uygulama güvenliği açıklarını tanımlayabilir
- Kullanıcı girdilerini daha güvenli şekilde doğrulayabilir
- Injection saldırılarını ve önleme yöntemlerini anlayabilir
- XSS açıklarını tespit edip azaltabilir
- Dosya upload süreçlerini daha güvenli tasarlayabilir
- Authentication mekanizmalarını daha güvenli yapılandırabilir
- Multi-Factor Authentication yaklaşımlarını değerlendirebilir
- Brute-force saldırılarına karşı koruma mekanizmaları geliştirebilir
- Session hijacking ve CSRF gibi session tabanlı saldırıları açıklayabilir
- Secure session management tekniklerini uygulayabilir
- Hassas parametrelerin korunması için uygun yöntemleri değerlendirebilir
- Static ve Dynamic Code Analysis yöntemlerini açıklayabilir
- Kod analiz araçlarının kullanım alanlarını değerlendirebilir
- Java ve .NET uygulamalarında güvenlik kontrollerini geliştirme sürecine dahil edebilir

Eğitim İçeriği

Güvenli Kodlamanın Temelleri

Bu bölüm güvenli yazılım geliştirme yaklaşımının temel prensiplerini ele alır.

Konular:

- Yazılım güvenliğinin temelleri
- Güvenli yazılım geliştirme yaklaşımı
- Temel güvenlik kavramları
- Confidentiality, Integrity ve Availability

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

- Threat, vulnerability ve risk kavramları
- Application attack surface
- Defense in Depth
- Least Privilege
- Secure Defaults
- Güvenlik kontrollerinin yazılım geliştirme sürecine dahil edilmesi
- Java SE Security temel kavramları

Katılımcılar, güvenliğin yalnızca test aşamasında ele alınacak bir konu olmadığını, tasarımdan geliştirmeye kadar tüm lifecycle boyunca düşünülmesi gerektiğini öğrenir.

Güvenli Girdi Yönetimi

Kullanıcı veya harici sistemlerden alınan verilerin kontrol edilmemesi uygulama güvenliğinin en önemli risk kaynaklarından biridir.

Bu bölümde:

- Input validation
- Buffer Overflow
- Cross Site Scripting (XSS)
- XSS attack patterns
- XSS prevention techniques
- SQL Injection
- XML Injection
- LDAP Injection
- Injection prevention
- Arbitrary File Uploads
- Güvenli file upload
- Image dosyalarının güvenli yüklenmesi
- File type validation
- Canonicalization
- Normalization
- Regular Expressions
- Allowlist / Whitelist yaklaşımı
- Blocklist / Blacklist yaklaşımı

ele alınır.

Katılımcılar, girdilerin kaynağına güvenmemek ve validation işlemlerini server-side gerçekleştirmek gibi temel secure coding prensiplerini uygular.

Cross Site Scripting ve XSS Önleme

Bu bölüm XSS açıklarının oluşma nedenlerine ve savunma yöntemlerine daha detaylı odaklanır.

Konular:

- XSS nedir?
- Reflected XSS
- Stored XSS
- Kullanıcı girdilerinin browser'a güvenli aktarılması
- Input validation

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Output encoding
- Context-aware encoding
- XSS prevention techniques

Injection Saldırıları

Bu bölüm uygulamaların backend sistemlerine gönderdiği kullanıcı kontrollü verilerden kaynaklanan injection risklerini inceler.

Konular:

- SQL Injection
- XML Injection
- LDAP Injection
- Injection attack logic
- Parameterized queries
- Safe API usage
- Input validation
- Injection prevention techniques

Güvenli Dosya Yükleme

Dosya yükleme özellikleri uygulamalar için önemli saldırı yüzeyleri oluşturabilir.

Konular:

- Arbitrary File Upload
- File extension validation
- MIME type kontrolü
- Dosya içeriğinin doğrulanması
- Image upload güvenliği
- Upload location güvenliği
- Dosya adı kontrolü
- Canonicalization riskleri
- Zararlı dosya yüklemelerini önleme

Güvenli Çıktı Yönetimi

Bu bölüm uygulamadan kullanıcıya gönderilen verilerin güvenli biçimde encode edilmesini ele alır.

Konular:

- Output encoding
- Anti-XSS output encoding
- HTML context encoding
- Attribute context
- JavaScript context
- URL context
- Kullanıcı kontrollü verinin güvenli şekilde render edilmesi

Amaç, verinin kullanıldığı context'e uygun encoding uygulanarak özellikle XSS risklerinin azaltılmasıdır.

Hassas Parametrelerin Güvenliği

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Bu bölüm uygulama içerisinde kullanılan hassas bilgilerin korunmasına odaklanır.

Konular:

- Sensitive parameters
- Passwords
- Tokens
- API keys
- Session identifiers
- Query string içerisinde hassas veri kullanımı
- Log kayıtlarında hassas veri
- Secure storage
- Secrets management
- Hassas bilgilerin gereksiz şekilde istemciye gönderilmemesi

Güvenli Kimlik Doğrulama

Bu bölüm authentication mekanizmalarının güvenli tasarımını inceler.

Konular:

- Authentication kavramı
- Authentication çeşitleri
- Basic Authentication
- Digest Authentication
- Windows Authentication
- Forms Authentication
- Secure authentication approaches
- Credential protection
- Password security
- Multi-Factor Authentication
- Brute-force attacks
- Account lockout
- Rate limiting
- Brute-force prevention algorithms

Katılımcılar kimlik doğrulama sistemlerinde yaygın görülen güvenlik problemlerini ve bunları azaltabilecek kontrolleri değerlendirir.

Güvenli Session Yönetimi

Bu bölüm kullanıcı session'larının oluşturulması, korunması ve sonlandırılmasına odaklanır.

Konular:

- Session management
- Session attacks
- Session fixation
- Session hijacking
- Secure session identifiers
- Session timeout
- Logout işlemleri
- Cookie security

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

- HttpOnly
- Secure flag
- Java Servlet Filters
- Session invalidation

Cross Site Request Forgery

Konular:

- CSRF nedir?
- CSRF attack flow
- State-changing requests
- Anti-CSRF tokens
- SameSite cookie yaklaşımı
- CSRF Prevention Cheat Sheet yaklaşımı
- Request validation
- Session ile CSRF arasındaki ilişki

Güvenli Yetkilendirme

Program kapsamında authentication sonrası kullanıcıların hangi kaynaklara erişebileceğinin güvenli şekilde kontrol edilmesi de ele alınır.

Konular:

- Authentication vs. Authorization
- Access control
- Role-Based Access Control
- Privilege validation
- Server-side authorization
- Least Privilege
- Broken access control riskleri
- Function-level access control
- Object-level authorization

Güvenli Tasarım

Katılımcılar güvenlik problemlerinin yalnızca kodlama hatalarından değil, tasarım kararlarından da kaynaklanabileceğini inceler.

Konular:

- Secure by Design
- Threat modelling yaklaşımı
- Attack surface reduction
- Trust boundaries
- Defense in Depth
- Fail Secure
- Least Privilege
- Secure architecture decisions
- Güvenlik gereksinimlerinin tasarıma dahil edilmesi

Güvenli Kod Analizi

Güvenli Yazılım Geliştirme Eğitimi

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Süre: **3 Gün**

Bu bölüm uygulama kodundaki güvenlik problemlerinin geliştirme ve test süreçlerinde nasıl tespit edilebileceğine odaklanır.

Konular:

- Secure code review
- Static Application Security Testing
- Dynamic Application Security Testing
- Static code analysis
- Dynamic analysis
- False positive / false negative kavramları
- Code analysis tools
- Security findings değerlendirmesi
- Güvenlik açıklarının önceliklendirilmesi
- Düzeltmelerin doğrulanması

Güvenli Web Servisleri ve AJAX

Modern web uygulamalarında API ve asynchronous communication yapılarının güvenliği ele alınır.

Konular:

- Web service security
- API authentication
- API authorization
- Input validation
- JSON/XML security
- AJAX security
- Sensitive data exposure
- Cross-origin riskleri
- Secure error handling
- Web service üzerinde session ve token güvenliği