Application Security in the Cloud Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Bulut teknolojilerine geçiş, kurumlar ve bireyler için maliyet, ölçeklenebilirlik ve operasyonel verimlilik açısından önemli avantajlar sağlar. Ancak güvenlik söz konusu olduğunda tablo daha karmaşıktır. Bulut hizmetlerinin güvenliği olumlu yönde etkilediği düşünülse de, bulut kaynaklarının korunmasından kimin sorumlu olduğu ve güvenlik sorumluluklarının nasıl paylaşılması gerektiği konusunda farklı yaklaşımlar bulunabilir.

Bu eğitim; **IaaS, PaaS ve SaaS** modellerini kapsayarak bulut ortamlarında güvenliğin hem altyapı hem de uygulama katmanında nasıl ele alınması gerektiğini inceler. İlk aşamada altyapı güvenliği, hardening, güvenli yapılandırma, authentication, authorization ve identity management konuları ele alınır. Kimlik ve erişim yönetiminin, güvenli bir bulut mimarisinin merkezinde nasıl konumlandırılması gerektiği açıklanır.

Program ayrıca bulut hizmetlerinde güvenin nasıl oluşturulduğunu ve yönetildiğini anlamak amacıyla temel hukuki ve sözleşmesel konulara da değinir.

Eğitim ilerledikçe katılımcılar buluta özgü tehditleri, saldırganların motivasyonlarını ve bulut sistemlerine yönelik tipik saldırı adımlarını inceler. Bulut ortamlarının güvenlik açısından denetlenmesi, değerlendirilmesi, vulnerability analysis ve penetration testing gibi konulara özel önem verilir.

Eğitimin temel odağı uygulama güvenliğidir. Hem verilerin güvenliğinin hem de uygulamaların kendisinin korunması ele alınır. Bulut ortamındaki uygulama güvenliği, geleneksel yazılım güvenliğinden tamamen farklı değildir; bu nedenle OWASP tarafından tanımlanan birçok yaygın güvenlik açığı bulut tabanlı sistemler için de geçerlidir. Asıl fark, bulut ortamlarının getirdiği yeni tehdit modelleri, riskler ve saldırı vektörlerinde ortaya çıkar.

Prerequisites

Katılımcıların aşağıdaki konularda temel bilgi sahibi olmaları önerilir:

- Cloud computing kavramları
- Yazılım geliştirme prensipleri

Application Security in the Cloud Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Eğitimin sonunda katılımcılar:

- Bilgi güvenliği, IT security ve secure coding temel kavramlarını anlayabilecek,
- Bulut ortamındaki başlıca tehdit ve riskleri değerlendirebilecek,
- Temel cloud security çözümlerini tanıyabilecek,
- Web service güvenlik prensiplerini anlayabilecek,
- XML security konusunda temel ve uygulamalı bilgi kazanabilecek,
- Kriptografinin uygulamalı kullanımını anlayabilecek,
- OWASP Top Ten ötesindeki web güvenlik açıklarını tanıyabilecek ve bunlardan kaçınma yöntemlerini öğrenebilecek,
- Denial-of-Service saldırılarını ve savunma yaklaşımlarını açıklayabilecek,
- Yaygın input validation hatalarını tanıyabilecek,
- Bulut ortamında veri güvenliğinin temel problemlerini değerlendirebilecek,
- NoSQL güvenliği hakkında bilgi sahibi olabilecek,
- MongoDB güvenlik yapılarını ve yaygın zafiyetlerini anlayabilecek,
- Bulut sistemlerinin denetlenmesi ve güvenlik açısından değerlendirilmesindeki zorlukları analiz edebilecek,
- Bulut altyapısını ve çalışma ortamını daha güvenli hale getirebilecek,
- Deployment ortamlarını güvenli şekilde yapılandırabilecek,
- Secure coding konusunda ileri çalışma için güvenilir kaynaklara erişebilecektir.

Outline

1. Gün

IT Security ve Secure Coding

Bu bölümde bilgi güvenliğinin temel yapısı ve güvenli yazılım geliştirme yaklaşımı incelenir.

- Güvenliğin doğası
- Risk kavramı
- IT security ile secure coding arasındaki fark
- Güvenlik açıklarından botnet ve siber suça uzanan süreç
- Güvenlik kusurlarının temel özellikleri
- Enfekte sistemlerden hedefli saldırılara geçiş
- Seven Pernicious Kingdoms
- OWASP Top Ten 2017

Cloud Security Temelleri

Bulut ortamlarını geleneksel sistemlerden ayıran güvenlik özellikleri ele alınır.

- Cloud security'ye giriş
- Cloud uygulamalarını farklı kılan unsurlar
- Cloud delivery modelleri ve güvenlik
- Public cloud ve private cloud
- Bulut ortamındaki temel güvenlik problemleri

Application Security in the Cloud Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Bulutta Tehditler ve Riskler

Bulut sistemlerine yönelik risklerin sistematik biçimde nasıl değerlendirilebileceği incelenir.

Cloud Computing Gereksinimleri ve Tehditleri

- Jericho Cloud Cube modeli
- Jericho Cloud Cube üzerinden gereksinim belirleme
- Cloud deployment modelleri ile risk ilişkisi

Threat Modeling

- Saldırgan profilleri
- Bulut ortamındaki temel attacker profilleri
- Threat modeling yaklaşımı
- Attack tree tabanlı threat modeling
- Misuse/abuse case tabanlı modelleme
- Basit misuse/abuse case örnekleri
- SDL threat modeling
- STRIDE tehdit kategorileri
- Data Flow Diagram (DFD) bileşenleri
- Örnek veri akış diyagramı
- STRIDE ile DFD öğelerinin eşleştirilmesi
- Risk analizi ve tehdit sınıflandırması
- Microsoft SDL mitigation teknikleri

Buluta Özgü Tehditler

- Bulut hizmetlerinin saldırganlar tarafından kötüye kullanılması
- Insider threats ve kötü niyetli tenant'lar
- Virtualization kaynaklı problemler
- Privilege escalation
- Hassas bilgi sızıntıları
- Hard-coded secrets
- **Egzersiz:** Hard-coded password
- Intellectual property exposure
- Insecure delegation

Cloud Security Çözümleri

Container Security

- Sanallaştırma teknikleri
- Container ve virtual machine karşılaştırması
- Process isolation yaklaşımının gelişimi
- POSIX capabilities
- Linux Containers (LXC)
- Docker
- Docker container'larının birbirine bağlanması
- Docker ve POSIX capabilities
- Docker API
- Container tabanlı tehditler

- Docker için güvenlik best practice'leri

XML Security

- XML security'ye giriş
- XML parsing
- XML injection
- CDATA alanlarının XSS payload saklamak için kötüye kullanılması
- **Egzersiz:** XML injection
- Sanitization ve XML validation ile koruma
- XML bomb
- **Egzersiz:** XML bomb

2. Gün

Uygulamalı Kriptografi

Kriptografiye Giriş

- Kriptografi uygulamalarındaki temel kural
- Cryptosystem kavramı
- Bir cryptosystem'in temel bileşenleri

Symmetric-Key Cryptography

- Simetrik kriptografi ile gizlilik sağlama
- Symmetric encryption algoritmaları
- Modes of operation

Diğer Kriptografik Algoritmalar

- Hash ve message digest
- Hash algoritmaları
- SHAttered örneği
- Message Authentication Code (MAC)
- Simetrik anahtarla integrity ve authenticity
- Random number generation
- Kriptografide rastgele sayıların önemi
- Cryptographically secure PRNG'ler
- Hardware tabanlı TRNG'ler
- Random number generator testleri

Asymmetric Cryptography

- Public-key encryption ile gizlilik
- Private key sahipliği prensibi
- Simetrik ve asimetrik algoritmaların birlikte kullanılması

Public Key Infrastructure (PKI)

- Man-in-the-Middle saldırısı
- MitM saldırılarına karşı digital certificate kullanımı
- Certificate Authority kavramı
- X.509 digital certificate

Web Application Security

Injection

- Injection prensipleri
- SQL injection
- **Egzersiz:** SQL injection
- Yaygın SQL injection saldırı teknikleri
- Blind ve time-based SQL injection
- SQL injection'dan korunma yöntemleri
- SQL injection tespiti
- Tipik detection testleri
- Savunma mekanizmalarını bypass etme teknikleri
- Diğer injection açıkları
- Command injection
- Command injection tespiti
- **Case Study:** ImageMagick

Broken Authentication

- Session handling tehditleri
- Session handling best practice'leri
- Cookie attribute yapılandırma önerileri

XML External Entity (XXE)

- XML Entity kavramına giriş
- XXE ile resource inclusion
- XXE ile URL invocation
- Parameter entity saldırıları
- **Egzersiz:** XXE attack
- **Case Study:** Google Toolbar'da XXE

Cross-Site Scripting (XSS)

- Persistent XSS
- Reflected XSS
- DOM-based XSS
- **Egzersiz:** Cross-Site Scripting
- XSS önleme teknikleri
- XSS açığı tespiti
- XSS filtrelerinin aşılması

Denial of Service

- DoS saldırılarına giriş
- Economic Denial of Sustainability (EDoS)
- Asymmetric DoS

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Regular Expression DoS (ReDoS)

- ReDoS prensipleri
- **Egzersiz:** ReDoS
- ReDoS azaltma yöntemleri
- **Case Study:** Stack Exchange ReDoS problemi

Hashtable Collision Attacks

- Hashtable ile veri saklama
- Hashtable collision
- Java'da hashtable collision

3. Gün

Input Validation

Input validation hatalarının uygulama güvenliğine etkileri incelenir.

Integer Problems

- Negatif integer gösterimi
- Integer overflow
- **Egzersiz:** IntOverflow
- `Math.abs(Integer.MIN_VALUE)` davranışı
- Integer işlemlerinde best practice'ler
- Addition overflow önleme
- Multiplication overflow önleme
- Java 8 ile arithmetic overflow tespiti
- **Egzersiz:**`addExact()` kullanımı
- Integer problem testleri

Path Traversal

- Path traversal açığı
- Zayıf koruma yöntemleri
- Path traversal best practice'leri

Diğer Input Validation Problemleri

- Unvalidated redirects and forwards
- Log forging
- Log dosyalarıyla ilgili diğer yaygın problemler

Bulutta Veri Güvenliği

Data at Rest ve Data in Motion

- Buluttaki veri güvenliği yaşam döngüsü
- Data at rest için güvenlik kontrolleri

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Data in motion için güvenlik kontrolleri

NoSQL Security

- NoSQL'e giriş
- NoSQL attack vector'leri
- NoSQL authentication problemleri

MongoDB Security

- MongoDB'ye giriş
- MongoDB security architecture
- Authentication ve access control
- Document validation
- TLS ile MongoDB communication güvenliği
- Secure configuration ve hardening
- Yaygın MongoDB güvenlik problemleri
- MongoDB NoSQL injection
- **Egzersiz:** MongoDB NoSQL injection
- Mongoose ile NoSQL injection önleme
- Geçmiş MongoDB güvenlik açıklarından case study'ler

Bulutta Security Audit

- Functional testing ve security testing karşılaştırması
- Security vulnerabilities
- Risk bazlı prioritization
- Security testing teknikleri ve araçları
- Genel test yaklaşımları

Dynamic Security Testing

- Manual ve automated security testing karşılaştırması
- Web vulnerability scanner'lar
- **Egzersiz:** Vulnerability scanner kullanımı
- SQL injection araçları
- **Egzersiz:** SQL injection testing tools

Bulut Ortamını Güvenli Hale Getirme

Environment Assessment

- Ortam güvenliğinin değerlendirilmesi

Patch ve Vulnerability Management

- Patch management
- Buluttaki insecure API'ler
- Vulnerability repository'leri
- Vulnerability attribute'ları
- Common Vulnerability Scoring System (CVSS)
- Vulnerability management yazılımları
- **Egzersiz:** Vulnerable package kontrolü

Application Security in the Cloud Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Shellshock Case Study

- Shellshock'a giriş
- Bash fonksiyonlarının temel kullanımı
- Bash Shellshock açığı
- **Egzersiz:** Shellshock
- Shellshock fix yöntemleri ve counterattack yaklaşımları
- **Egzersiz:** Environment variable ile command override