Application Security in the Cloud Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Moving applications and services to the cloud can deliver substantial advantages in cost efficiency, scalability and operational flexibility. From a security perspective, however, the impact is more complex. Cloud services are often seen as improving overall security, yet organisations still face important questions around responsibility, ownership and the protection of cloud resources.

This course examines cloud security across **IaaS, PaaS and SaaS** environments, with a particular focus on application security. It begins with the security of the underlying infrastructure, including hardening, configuration, authentication, authorisation and identity management. Identity and access management are presented as central elements of a secure cloud architecture.

The programme also introduces the legal and contractual considerations that influence how trust is established and governed in cloud environments.

As the course progresses, participants examine cloud-specific threats, attacker motivations and the common stages involved in attacks against cloud solutions. Special attention is given to cloud auditing, security evaluation, vulnerability analysis and penetration testing.

The core focus of the programme is application security. Both data protection and the security of the applications themselves are addressed. From an application security perspective, cloud computing is not fundamentally different from general software security, which means many vulnerabilities listed by OWASP remain highly relevant. The major differences arise from the threat models, risk profiles and attack vectors that are specific to cloud environments.

Prerequisites

Participants should have a basic understanding of:

- Cloud computing concepts
- Software development principles

Application Security in the Cloud Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of the course, participants will be able to:

- Understand fundamental concepts of information security, IT security and secure coding
- Recognise major threats and risks in cloud environments
- Understand essential cloud security solutions
- Explain key security concepts associated with web services
- Understand the fundamentals of XML security
- Apply practical cryptography concepts
- Recognise web vulnerabilities beyond the OWASP Top Ten and understand how to mitigate them
- Explain common denial-of-service attacks and relevant defensive approaches
- Identify typical input validation errors
- Understand key data security challenges in cloud environments
- Explain NoSQL security concepts
- Understand MongoDB security controls and common weaknesses
- Assess the challenges involved in auditing and evaluating cloud systems for security
- Apply techniques for securing cloud environments and infrastructure
- Set up and operate deployment environments more securely
- Identify useful resources for further study in secure coding

Outline

Day 1

IT Security and Secure Coding

This section introduces the foundations of information security and secure software development.

- Nature of security
- Understanding risk
- IT security versus secure coding
- From vulnerabilities to botnets and cybercrime
- Nature of security flaws
- From infected systems to targeted attacks
- The Seven Pernicious Kingdoms
- OWASP Top Ten 2017

Cloud Security Basics

Explore the security characteristics that distinguish cloud environments from traditional systems.

- Introduction to cloud security
- What makes cloud applications different
- Cloud delivery models and security
- Public and private clouds
- Security challenges in cloud environments

Threats and Risks in the Cloud

Application Security in the Cloud Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Examine how risks and threats can be modelled and assessed systematically.

Cloud Computing Requirements and Threats

- The Jericho Cloud Cube model
- Using the Jericho Cloud Cube for requirements specification
- Cloud deployment models versus risk

Threat Modeling

- Attacker profiles
- Main attacker profiles in cloud environments
- Threat modeling principles
- Attack tree-based threat modeling
- Misuse and abuse case-based modeling
- Simple misuse and abuse case examples
- SDL threat modeling
- STRIDE threat categories
- Data Flow Diagram elements
- Example data flow diagrams
- Mapping STRIDE to DFD elements
- Risk analysis and threat classification
- Standard Microsoft SDL mitigation techniques

Cloud-Specific Threats

- Abuse of cloud services by attackers
- Insider threats and malicious tenants
- Risks created by virtualisation
- Elevation of privilege
- Leakage of sensitive information
- Hard-coded secrets
- **Exercise:** Hard-coded passwords
- Intellectual property exposure
- Insecure delegation

Cloud Security Solutions

Container Security

- Virtualisation techniques
- Containers versus virtual machines
- Evolution of process isolation
- POSIX capabilities
- Linux Containers (LXC)
- Docker
- Linking Docker containers
- Docker and POSIX capabilities
- Docker API
- Container-related threats
- Docker security best practices

XML Security

- Introduction to XML security
- XML parsing
- XML injection
- Abusing CDATA to store XSS payloads
- **Exercise:** XML injection
- Protection through sanitisation and XML validation
- XML bomb attacks
- **Exercise:** XML bomb

Day 2

Practical Cryptography

Introduction to Cryptography

- The fundamental rule of cryptographic implementation
- Cryptosystems
- Core elements of a cryptosystem

Symmetric-Key Cryptography

- Providing confidentiality with symmetric cryptography
- Symmetric encryption algorithms
- Modes of operation

Other Cryptographic Algorithms

- Hashes and message digests
- Hash algorithms
- SHAttered
- Message Authentication Code (MAC)
- Using symmetric keys for integrity and authenticity
- Random number generation
- Random numbers in cryptography
- Cryptographically strong PRNGs
- Hardware-based TRNGs
- Testing random number generators

Asymmetric Cryptography

- Public-key encryption for confidentiality
- The importance of private key ownership
- Combining symmetric and asymmetric algorithms

Public Key Infrastructure

- Man-in-the-Middle attacks
- Digital certificates as protection against MitM attacks

- Certificate Authorities
- X.509 digital certificates

Web Application Security

Injection

- Injection principles
- SQL injection
- **Exercise:** SQL injection
- Common SQL injection techniques
- Blind and time-based SQL injection
- SQL injection prevention methods
- Detecting SQL injection
- Typical detection tests
- Bypassing defensive controls
- Other injection flaws
- Command injection
- Detecting command injection
- **Case Study:** ImageMagick

Broken Authentication

- Session handling threats
- Session handling best practices
- Best practices for cookie attributes

XML External Entity

- Introduction to XML entities
- XXE resource inclusion
- XXE URL invocation
- Parameter entity attacks
- **Exercise:** XXE attack
- **Case Study:** XXE in Google Toolbar

Cross-Site Scripting

- Persistent XSS
- Reflected XSS
- DOM-based XSS
- **Exercise:** Cross-Site Scripting
- XSS prevention
- Detecting XSS vulnerabilities
- Bypassing XSS filters

Denial of Service

- Introduction to DoS
- Economic Denial of Sustainability (EDoS)
- Asymmetric DoS

Regular Expression DoS

- ReDoS concepts
- **Exercise:** ReDoS
- ReDoS mitigation
- **Case Study:** ReDoS in Stack Exchange

Hashtable Collision Attacks

- Using hashtables to store data
- Hashtable collision
- Hashtable collision in Java

Day 3

Input Validation

Explore common input validation problems and their impact on application security.

Integer Problems

- Representation of negative integers
- Integer overflow
- **Exercise:** IntOverflow
- Behaviour of `Math.abs(Integer.MIN_VALUE)`
- Integer handling best practices
- Preventing arithmetic overflow in addition
- Preventing arithmetic overflow in multiplication
- Detecting arithmetic overflow in Java 8
- **Exercise:** Using `addExact()` in Java
- Testing for integer problems

Path Traversal

- Path traversal vulnerabilities
- Weak path traversal protections
- Path traversal best practices

Other Validation Issues

- Unvalidated redirects and forwards
- Log forging
- Other common problems involving log files

Data Security in the Cloud

Data at Rest and Data in Motion

- Cloud data security lifecycle
- Controls for data at rest

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Controls for data in motion

NoSQL Security

- Introduction to NoSQL
- NoSQL attack vectors
- NoSQL authentication issues

MongoDB Security

- Introduction to MongoDB
- MongoDB security architecture and features
- Authentication and access control
- Document validation
- Securing MongoDB communications with TLS
- Secure configuration and hardening
- Common MongoDB security issues
- NoSQL injection in MongoDB
- **Exercise:** MongoDB NoSQL injection
- Preventing NoSQL injection with Mongoose
- Case studies covering past MongoDB weaknesses and vulnerabilities

Security Auditing in the Cloud

- Functional testing versus security testing
- Security vulnerabilities
- Risk-based prioritisation
- Security testing techniques and tools
- General testing approaches

Dynamic Security Testing

- Manual versus automated security testing
- Web vulnerability scanners
- **Exercise:** Using a vulnerability scanner
- SQL injection tools
- **Exercise:** Using SQL injection tools

Securing the Cloud Environment

Environment Assessment

- Assessing the security of the environment

Patch and Vulnerability Management

- Patch management
- Insecure APIs in cloud environments
- Vulnerability repositories
- Vulnerability attributes
- Common Vulnerability Scoring System (CVSS)
- Vulnerability management software
- **Exercise:** Checking for vulnerable packages

Application Security in the Cloud Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Shellshock Case Study

- Introduction to Shellshock
- Basics of using functions in Bash
- The Shellshock vulnerability in Bash
- **Exercise:** Shellshock
- Shellshock remediation and countermeasures
- **Exercise:** Command override through environment variables