DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

Cloud Application Security in C# for Azure (CASEC-CAZ)

ID CY-CASEC-CAZ **Price** US$ 3,750 **Duration** 5 days

Course Overview

Your cloud application written in C# works as intended, so you are done, right? But did you consider feeding in incorrect values? 16Gbs of data? A null? An apostrophe? Negative numbers, or specifically -1 or -231? Because that's what the bad guys will do – and the list is far from complete.

The cloud has become a critical aspect of online services. No matter which model you're using (SaaS, PaaS, IaaS), part of your service is now operated by someone else. This may look like a net positive, but it also greatly expands the attack surface and brings in several new risks that may not be obvious. Have you configured all security settings correctly? Are you prepared for supply chain attacks? How can you protect the confidentiality of user data in the cloud? And most importantly: can the bad guys use your exposure to their advantage?

Handling security needs a healthy level of paranoia, and this is what this course provides: a strong emotional engagement by lots of hands-on labs and stories from real life, all to substantially improve code hygiene. Mistakes, consequences, and best practices are our blood, sweat and tears.

The curriculum goes through the common Web application security issues following the OWASP Top Ten but goes far beyond it both in coverage and the details.

All this is put in the context of C#, and extended by core programming issues, discussing security pitfalls of the C# language and the Azure cloud platform.

So that you are prepared for the forces of the dark side.

So that nothing unexpected happens.

Nothing.

Who should attend

C# developers working on Web applications and Azure

Prerequisites

General C# and Web development

Course Objectives

- Getting familiar with essential cyber security concepts
- Understand cloud security specialties
- Understanding Web application security issues
- Detailed analysis of the OWASP Top Ten

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

elements
- Putting Web application security in the context of C#
- Going beyond the low hanging fruits
- Managing vulnerabilities in third party components
- Learn to deal with cloud infrastructure security
- Identify vulnerabilities and their consequences
- Learn the security best practices in C#
- Input validation approaches and principles
- Understanding how cryptography can support application security
- Learning how to use cryptographic APIs correctly in C#
-

Course Content

- Cyber security basics
- The OWASP Top Ten
- Cloud infrastructure security
- API security
- JSON security
- XML security
- Denial of service
- Cryptography for developers
- Wrap up

Detailed Course Outline

DAY 1

Cyber security basics

- What is security?
- Threat and risk
- Cyber security threat types
- Consequences of insecure software
    - Constraints and the market
    - The dark side
- Cloud security basics
    - Cloud infrastructure basics
    - Cloud architectures and security
    - The Cloud Cube Model
    - Attack surface in the cloud
- Cloud data security
    - Data confidentiality and integrity in the cloud
    - Data privacy in the cloud
    - Compliance considerations
- Cloud deployment security
    - Hardening cloud deployments
    - Security of jump boxes
    - Serverless computing and security
- Cloud security standards and best practices
    - SOC compliance
    - CSA controls
    - Other standards

The OWASP Top Ten

- OWASP Top 10 – 2017
- A1 - Injection
    - Injection principles
    - Injection attacks
    - SQL injection
        - SQL injection basics
        - Lab – SQL injection
        - Attack techniques
        - Content-based blind SQL injection
        - Time-based blind SQL injection
    - NoSQL injection
        - NoSQL injection specialties
        - NoSQL injection in MongoDB
        - NoSQL injection in CosmosDB
    - SQL injection best practices
        - Input validation
        - Parameterized queries
        - Lab – Using prepared statements
        - Additional considerations
        - Case study – Hacking Fortnite accounts
        - SQL injection protection and

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

ORM
- Parameter manipulation
  - CRLF injection
    - Log forging
    - Log forging – best practices
    - HTTP response splitting
    - Header checking in ASP.NET
  - HTTP parameter manipulation
    - HTTP parameter pollution
    - Variable shadowing
    - Value shadowing
- Code injection
  - OS command injection
    - Lab – Command injection
    - OS command injection best practices
    - Avoiding command injection with the right APIs
    - Lab – Command injection best practices
    - Case study – Command injection via ping
- Script injection
- Dangerous file inclusion

DAY 2

The OWASP Top Ten

- A2 - Broken Authentication
  - Authentication
    - Authentication basics
    - Multi-factor authentication
    - Multi-factor authentication best practices
    - Authentication weaknesses - spoofing
    - Spoofing on the Web
    - Case study – PayPal 2FA bypass
    - User interface best practices
- Single sign-on (SSO)
  - Single sign-on concept
  - OAuth2
    - OAuth2 basics
    - OAuth2 in practice
    - Best practices
    - Configuration best practices
    - Case study – Stealing SSO tokens from Epic Games accounts
  - SAML
    - SAML basics
    - SAML profiles
    - SAML security
- Password management
  - Inbound password management
    - Storing account passwords
    - Password in transit
    - Lab – Is just hashing passwords enough?
    - Dictionary attacks and brute forcing
    - Salting
    - Adaptive hash functions for password storage
    - Lab – Using adaptive hash functions in C#
    - Password policy
    - NIST authenticator requirements for memorized secrets
    - Password hardening
    - Using passphrases
    - Password change
    - Password recovery issues
    - Password recovery best practices
    - Lab – Password reset weakness
    - Case study – The Ashley

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

Madison data breach
        - The dictionary attack
        - The ultimate crack
        - Exploitation and the lessons learned
        - Password database migration
        - (Mis)handling null passwords
    - Outbound password management
        - Hard coded passwords
        - Best practices
        - Lab – Hardcoded password
        - Protecting sensitive information in memory
        - Challenges in protecting memory
        - Storing sensitive data in memory
        - Lab – Using secret-handling classes in C#
- Session management
    - Session management essentials
    - Why do we protect session IDs – Session hijacking
    - Session fixation
    - Session invalidation
    - Session ID best practices
    - Cross-site Request Forgery (CSRF)
        - Lab – Cross-site Request Forgery
        - CSRF best practices
        - CSRF defense in depth
        - Lab – CSRF protection with tokens
    - Cookie security
        - Cookie security best practices
        - Cookie attributes
- A3 - Sensitive Data Exposure
    - Information exposure
    - Exposure through extracted data and aggregation
    - Case study – Strava data exposure
    - System information leakage
        - Leaking system information
    - Information exposure best practices
- A4 - XML External Entities (XXE)
    - DTD and the entities
    - Entity expansion
    - External Entity Attack (XXE)
        - File inclusion with external entities
        - Server-Side Request Forgery with external entities
        - Lab – External entity attack
        - Case study – XXE vulnerability in SAP Store
        - Preventing XXE
        - Lab – Prohibiting DTD

DAY 3

The OWASP Top Ten

- A5 - Broken Access Control
    - Access control basics
    - Failure to restrict URL access
    - Confused deputy
        - Insecure direct object reference (IDOR)
        - Lab – Insecure Direct Object Reference
        - Case study – Authorization bypass on Facebook
        - Authorization bypass through user-controlled keys
        - Lab – Horizontal authorization
    - File upload
        - Unrestricted file upload
        - Good practices
        - Lab – Unrestricted file upload
- A7 - Cross-site Scripting (XSS)
    - Cross-site scripting basics
    - Cross-site scripting types
        - Persistent cross-site scripting
        - Reflected cross-site scripting
        - Client-side (DOM-based) cross-site scripting
        - Lab – Stored XSS
        - Lab – Reflected XSS

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

        - Case study – XSS in Fortnite accounts
    - XSS protection best practices
        - Protection principles - escaping
        - XSS protection APIs
        - Request validation in ASP.NET
        - Further XSS protection techniques
        - Lab – XSS fix / stored
        - Lab – XSS fix / reflected
        - Additional protection layers
        - Client-side protection principles
- A8 - Insecure Deserialization
    - Serialization and deserialization challenges
    - Integrity – deserializing untrusted streams
    - Integrity – deserialization best practices
    - Property Oriented Programming (POP)
        - Creating payload
        - Summary – POP best practices
        - Lab – Creating a POP payload
        - Lab – Using the POP payload
- A9 - Using Components with Known Vulnerabilities
    - Using vulnerable components
    - Assessing the environment
    - Hardening
    - Untrusted functionality import
    - Importing JavaScript
    - Lab – Importing JavaScript
    - Case study – The British Airways data breach
    - Vulnerability management
        - Patch management
        - Vulnerability management
        - Bug bounty programs
        - Vulnerability databases
        - Vulnerability rating – CVSS
        - Lab – Finding vulnerabilities in third-party components
        - DevOps, the build process and CI / CD
        - Dependency checking in C#
        - Lab – Detecting vulnerable components
- A10 - Insufficient Logging & Monitoring
    - Logging and monitoring principles
    - Insufficient logging
    - Case study – Plaintext passwords at Facebook
    - Logging best practices
    - Monitoring best practices

Web application security beyond the Top Ten

- Client-side security
- Same Origin Policy
- Tabnabbing
- Lab – Reverse tabnabbing
- Frame sandboxing
    - Cross-Frame Scripting (XFS) attack
    - Lab - Clickjacking
    - Clickjacking beyond hijacking a click
    - Clickjacking protection best practices
    - Lab – Using CSP to prevent clickjacking

DAY 4

Cloud infrastructure security

- Container security
    - Container security concerns
    - Containerization, virtualization, and security
    - Attack surface of container technologies
    - Container security tools
    - Docker security
        - Docker and security
        - Docker security features
        - Common Docker security mistakes

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

        - Docker security best practices
        - Hardening Docker
        - Lab – Static analysis of Docker image
    - Kubernetes security
        - The Kubernetes architecture and security
        - Common Kubernetes security mistakes
        - Securing Kubernetes hosts
        - Best practices for Kubernetes access control
        - Building secure Kubernetes images
        - Secure deployment of Kubernetes containers
        - Protecting Kubernetes deployments at runtime
        - Lab – Scanning a Kubernetes image for vulnerabilities
- Azure security
    - Security considerations for Azure
        - Azure and security
        - Azure security features
        - The Azure shared responsibility model
        - Azure cloud compliance
        - Azure hardening
        - Security tools for Azure
    - Identity and access management (IAM)
        - Identity and access management in Azure
        - Azure Active Directory
        - Multi-factor authentication with Azure
        - Azure RBAC
        - Azure Active Directory Federation Services
        - Azure Shared Access Signatures (SAS)
    - Data security
        - Data security in Azure
        - Storing cryptographic keys in Azure
        - Protecting data in transit
        - Protecting data at rest
    - Detection and monitoring
        - Utilizing Azure monitoring for security
        - The Azure Application Gateway WAF
        - The Azure Security Center

API security

- Input validation
    - Input validation principles
    - Blacklists and whitelists
    - Data validation techniques
    - Lab – Input validation
    - What to validate – the attack surface
    - Where to validate – defense in depth
    - When to validate – validation vs transformations
    - Output sanitization
    - Encoding challenges
    - Unicode challenges
    - Lab – Encoding challenges
    - Validation with regex
- Integer handling problems
    - Representing signed numbers
    - Integer visualization
    - Integer overflow
    - Lab – Integer overflow
    - Signed / unsigned confusion
    - Case study – The Stockholm Stock Exchange
    - Lab – Signed / unsigned confusion
    - Integer truncation
    - Best practices
        - Upcasting
        - Precondition testing
        - Postcondition testing
        - Using big integer libraries
        - Integer handling in C#
        - Lab – Checked arithmetics

JSON security

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

- JSON validation
- JSON injection
- Dangers of JSONP
- JSON/JavaScript hijacking
- Best practices
- Case study – ReactJS vulnerability in HackerOne

DAY 5

API security

- Input validation
  - Files and streams
    - Path traversal
    - Lab – Path traversal
    - Path traversal-related examples
    - Additional challenges in Windows
    - Virtual resources
    - Path traversal best practices
    - Lab – Path canonicalization
  - Unsafe reflection
    - Reflection without validation
    - Lab – Unsafe reflection

XML security

- XML validation
- XML injection
  - XPath injection
  - Blind XPath injection

Denial of service

- Denial of Service
- Flooding
- Resource exhaustion
- Sustained client engagement
- Denial of service problems in C#
- Infinite loop
- Economic Denial of Sustainability (EDoS)
- Algorithm complexity issues
  - Regular expression denial of service (ReDoS)
    - Lab – ReDoS in C#
    - Dealing with ReDoS
    - Hash table collision
      - How do hash tables work?
      - Hash collision in case of hash tables

Cryptography for developers

- Cryptography basics
- Crypto APIs in C#
- Elementary algorithms
  - Hashing
    - Hashing basics
    - Hashing in C#
    - Lab – Hashing in C#
- Confidentiality protection
  - Symmetric encryption
    - Block ciphers
    - Modes of operation
    - Modes of operation and IV – best practices
    - Symmetric encryption in C#
    - Symmetric encryption in C# with streams
    - ProtectedData and ProtectedMemory
    - Lab – Symmetric encryption in in C#
  - Asymmetric encryption
  - Combining symmetric and asymmetric algorithms
- Integrity protection
  - Message Authentication Code (MAC)
    - Calculating HMAC in C#
    - Lab – Calculating MAC in C#
  - Digital signature
    - Lab – Digital signature with ECDSA in C#
- Public Key Infrastructure (PKI)
  - Some further key management challenges
  - Certificates

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

        - Certificate management – best practices
- Transport security
    - Transport security weaknesses
    - The TLS protocol
        - TLS basics
        - TLS features (changes in v1.3)
        - The handshake in a nutshell (v1.3)
        - TLS best practices
        - TLS authentication best practices
        - HTTP Strict Transport Security (HSTS)
        - Lab – Setting HSTS in C#

Wrap up

- Secure coding principles
    - Principles of robust programming by Matt Bishop
    - Secure design principles of Saltzer and Schröder
- And now what?
    - Software security sources and further reading
    - .NET and C# resources

Fast Lane
Consulting & Education Services, Inc.
5565 Centerview Drive, Suite 310, Raleigh, NC 27606
Tel: (919) 674-3100 | Toll Free: (855) 778-7246
Info.US@FastLane.Net