Application & Cloud Security

Investment Studies Center (ISC) @ Union of Investment Companies, is delighted to invite you to a training program on **Application & Cloud Security** and to through it exploring essential strategies for safeguarding digital assets in today's dynamic online environment, according to the following details:	يسر مركز دراسات الاستثمار لدى اتحاد شركات الاستثمار الإعلان عن تنظيم برنامج تدريبي حول **أمن التطبيقات وسحابة التخزين** والذي من خلاله سنستكشف الاستراتيجيات الأساسية لحماية الأصول الرقمية في بيئة الإنترنت الديناميكية اليوم، وذلك وفقاً للتفاصيل التالية:

Training Program:	Application & Cloud Security	**البرنامج التدريبي:**
Instructor:	Ala'a Hijazi	**المحاضر:**
Dates:	(Sunday - Tuesday) 02nd - 04th June 2024	**التاريخ:**
Timing:	09:00AM – 03:00PM	**الوقت:**
Language:	English	**لغة البرنامج:**
Venue:	In Person at UIC Premises	**المكان:**
Course Details, Registration & Fees in link below		**تفاصيل البرنامج، التسجيل والرسوم في الرابط أدناه**
http://unioninvest.org/upcomingevents.aspx Registration is open according to availability		
Discounted Fees for UIC Members	KWD 250	**الرسوم بعد الخصم لأعضاء الاتحاد**
Non-Members	KWD 295	**غير أعضاء الاتحاد**

Application & Cloud Security

Introduction:

Welcome to our comprehensive training program, Application & Cloud Security. In this dynamic training, participants will delve into advanced strategies and practical methodologies to fortify applications and cloud infrastructure against cyber threats. Gain invaluable insights and hands-on experience to navigate the complexities of modern cybersecurity challenges and safeguard your organization's digital assets effectively. Join us on this transformative journey toward enhanced security and resilience in the digital realm.

Outline:

Day 1

Module 1: Application Concepts

a. Introduction to Applications
b. Web Application Architecture
c. Web Services
d. Vulnerability Stack

Module 2: Web Application Threats

a. OWASP TOP 10 Application Security Risks
b. A01 – Broken Access Control
c. A02 – Cryptographic Failures
d. A03 – Injection Flaws
e. SQL Injection Attacks
f. Command Injection Attacks and Examples
g. File Injection Attacks
h. LDAP Injection Attacks
i. Cross Site Scripting (XSS)
j. A04 – Insecure Design
k. A05 – Security Misconfiguration
l. XML External Entity (XXE)

m. A06 – Vulnerable and Outdated Components
n. A07 – Identification and Authentication Failures/Broken Authentication
o. A08 - Software and Data Integrity Failures
p. Insecure Deserialization
q. A09 – Security Logging and Monitoring Failures
r. A10- Server-Side Request Forgery (SSRF)
s. Directory Traversal
t. CSRF Attacks
u. Other Attacks

Day 2

Module 3: Application Hacking Methodology

a. Footprinting
b. Analyzing
c. Bypass Client-Side Controls
d. Authentication Mechanism
e. Authorization Schemes
f. Access Controls
g. Session Management
h. Injection/Input Validation
i. Logic Flaws

Module 4: Web API, Web Shells

a. What is Web API
b. Web Services API
c. Webhooks
d. OWASP Top 10 API Security Risks
e. API Vulnerabilities
f. REST API vulnerability Scanning
g. Web Shells
h. Web Shells Tools
i. How to Prevent the Installation of a Web Shell
j. API Security Risks and Solutions
k. Best Practices for API Security

Day 3

Module 5: Application Security

a. Web Application Security Testing/Fuzzing
b. Source Code Review
c. How to defend against injection attacks
d. Web Application Attack Counter measures
e. How to defend against web application attacks
f. Web Application Security Tools
g. Web Application Firewalls

Module 6: Cloud Security

a. Cloud Computing Concepts
b. Container Technology
c. Serverless Computing
d. Cloud Computing Threats
e. Cloud Hacking
f. Cloud Security

Objectives:

- Understand the fundamental principles of application and cloud security.
- Identify common security vulnerabilities and threats in applications and cloud environments.
- Learn best practices for securing applications and data in cloud platforms.
- Foster a culture of security awareness and proactive risk management within the organization.

Target Audience:

1- IT professionals responsible for managing applications and cloud infrastructure.
2- System administrators and network engineers involved in cloud deployments.
3- Software developers and DevOps engineers responsible for building and deploying applications in cloud environments.
4- Information security professionals seeking to enhance their expertise in application and cloud security.
5- Compliance officers and risk managers concerned with regulatory requirements and cybersecurity best practices.

Expert's Profile: Ala'a Hijazi

As an experienced Cyber Security Engineer, my background reflects a successful tenure in the information technology and services sector. Proficient in Python, reverse engineering and information security, I hold a Master's degree in Cybersecurity from Saint Joseph University of Beirut, attesting to my strong academic foundation.

In addition to my technical proficiency, I play a pivotal role in advancing the field by offering comprehensive cybersecurity training. Specializing in areas such as reverse engineering, ethical hacking, and forensics, I contribute my expertise to empower others in navigating the complexities of the cybersecurity landscape. Functioning as a senior consultant, I provide strategic guidance, leveraging my extensive knowledge to enhance cybersecurity strategies.

Moreover, I am actively engaged in furthering my understanding of the field by pursuing a Ph.D. in Security AI. This ongoing commitment underscores my dedication to staying at the forefront of cybersecurity knowledge and contributing to its evolution.