BLENDED DELIVERY - ON-DEMAND & LIVE INSTRUCTOR LED ONLINE

SYLLABUS

SMART CONTRACT SECURITY COURSE

Duration: 20 Hours

Delivery: Online On-Demand

Instructor(s): Howard Poston

Office Hours: 10:00 AM to 6:00 PM Eastern Standard Time

Email: support@on360.io

Prerequisites: None

Continuing Education Units: TBD

Microcredential Exam: Smart Contract Security Microcredential
Certification Body: Blockchain Certification Association (BCA)

Course Overview:
The Smart Contract Security Course provides an in-depth introduction to smart contract security. Course attendees will start with an introduction to smart contracts, explore four different classes of smart contract vulnerabilities, and discuss best practices for securing smart contracts.

Course Composition:

Online On-Demand:	Smart Contract Security	Modules 1 - 6
LIVE Instrucotr Led Online	Blockchain Security Workshop	
LIVE Instrucotr Led Online	Ask Me Anything - Weekly Session	

Learning Objectives:

- Understand the challenges of smart contract security
- Explore common smart contract vulnerabilities via sample code and case studies
- Identify best practices for mitigating common smart contract errors
- Discuss best practices for smart contract security
- Identify key components of a smart contract security audit

Demonstration of Learning Outcomes:
After the Smart Contract Security Course, students understand common smart contract vulnerabilities and how to identify and correct them.

Evaluation:
Evaluation is based on participation and a final exam.
Weighted:

50% participation
50% on the final grade

80% overall grade is required to receive a Certificate of Completion.

Grading Policy:
Pass or Fail. No Credit (NC).

Attendance Requirements:
Students are expected to complete all online self-paced modules and assessments. Certificate of Completion will not be issued until all online modules are complete, including the final exam.

Student conduct and etiquette:
Students will be expected to be courteous in their conduct and communications to the instructor and classmates at all times, whether such conduct or communication is in person, by telephone, or electronic communications.

Behavior that persistently or grossly interferes with the instructor or other student activities is considered disruptive behavior and may be subject to disciplinary action. Such behavior inhibits other students' ability to learn, and an instructor's ability to teach. The instructor may require a student responsible for disruptive behavior to leave the learning environment pending discussion and resolution of the problem and may report a disruptive student to the Student Affairs Office.

Note: Disruptions or any other distraction in the learning environment may result in a failing grade.

Course Evaluations
Course evaluations and program surveys are important components of the educational process. Students are encouraged to complete the student course evaluation form issued after the course. The review is anonymous.

Computer/Information Literacy Expectations for Students enrolled in this class.
Students in this class are expected to:

1. Use a word processing program for writing assignments (e.g., Microsoft Word)
2. Be able to access assigned websites through the internet.
3. Have access to PC or mobile device for participation in course content

Course Module Overview:

SMART CONTRACT SECURITY COURSE – 6 MODULES

Module 1: Introduction to Smart Contract Security
Introduction to Smart Contracts
Smart Contract Security and Vulnerabilities

Module 2: General Programming Vulnerabilities
What Are General Programming Vulnerabilities?
Arithmetic Vulnerabilities
External Library Functions
Right-to-Left Control Characters

Module 3: Blockchain-Specific Vulnerabilities
What are Blockchain-Specific Vulnerabilities?
Access Control
Denial of Service
Frontrunning
Rollback Attacks
Timestamp Dependence
Weak Randomness

Module 4: Ethereum-Specific Vulnerabilities
Introduction to Common Ethereum Mistakes
Denial of Service: Block Gas Limits
Denial of Service: Unexpected Revert
Forced Send of Ether
Reentrancy
Short Addresses
Unchecked Return Values
Unsafe External Calls

Module 5: Decentralized Finance (DeFi) Vulnerabilities
Introduction to DeFi Vulnerabilities
Access Control
Control and Governance Issues
Frontend Vulnerabilities
Price Manipulation

Module 6: Smart Contract Security Best Practices
Secure Smart Contract Development
Secure Smart Contract Auditing