QUARTERLY RELEASE UPDATE
April 2023

SECURITY INNOVATION

NEW Courses

available April 25, 2023

To meet the demand for feature-rich solutions, tech stacks constantly evolve. To reduce the risk increased complexity brings, teams need to collectively get smarter, from coding to configuration.

CMD+CTRL offers the industry's largest security library for those who build, operate, and defend software. Our micro-learning approach makes it a cinch to build target skills.

DES 219
Securing Google's Firebase Platform
60 minutes

Learn how to leverage Firebase security rules, security concepts, and setup to define what data your users can access.

DES 261
Securing Serverless Environments
20 minutes

Learn how to protect a serverless architecture from common threats using best practices.

DES 262
Securing Enterprise Low-Code Application Platforms
20 minutes

Learn how to identify and mitigate the security risks associated with Low-Code Application Platforms (LCAP).

NEW Skill Labs

available April 25, 2023

LAB 211
Defending Java Applications Against Credentials in Code Medium
10 minutes

Demonstrate ability to fix code in a Java application that contains unprotected credentials such as a password or cryptographic key.

LAB 212
Defending Python Applications Against Credentials in Code Medium
10 minutes

Demonstrate ability to fix code in a Python application that contains unprotected credentials such as a password or cryptographic key.

LAB 213
Defending Node.js Applications Against Credentials in Code Medium
10 minutes

Demonstrate ability to fix code in a Node.js application that contains unprotected credentials such as a password or cryptographic key.

LAB 214
Defending C# Applications Against Credentials in Code Medium
10 minutes

Demonstrate ability to fix code in a C# application that contains unprotected credentials such as a password or cryptographic key.

LAB 215
Defending Java Applications Against Business Logic Error for Input Validation
10 minutes

Fix business logic errors in an application written in Java that may leave your application vulnerable to manipulation by attackers.

LAB 216
Defending Python Applications Against Business Logic Error for Input Validation
10 minutes

Fix business logic errors in an application written in Python that may leave your application vulnerable to manipulation by attackers.

LAB 217
Defending Node.js Applications Against Business Logic Error for Input Validation
10 minutes

Fix business logic errors in an application written in Node.js that may leave your application vulnerable to manipulation by attackers.

LAB 218
Defending C# Applications Against Business Logic Error for Input Validation
10 minutes

Fix business logic errors in an application written in C# that may leave your application vulnerable to manipulation by attackers.

LAB 224
Defending Java Applications Against Forceful Browsing
10 minutes

Fix an application written using Java that does not adequately enforce appropriate authorization on all restricted URLs, scripts, or files.

LAB 225
Defending Python Applications Against Forceful Browsing
10 minutes

Fix an application written using Python that does not adequately enforce appropriate authorization on all restricted URLs, scripts, or files.

LAB 226
Defending Node.js Applications Against Forceful Browsing
10 minutes

Fix an application written using Node.js that does not adequately enforce appropriate authorization on all restricted URLs, scripts, or files.

LAB 227
Defending C# Applications Against Forceful Browsing
10 minutes

Fix an application written using C# that does not adequately enforce appropriate authorization on all restricted URLs, scripts, or files.

LAB 310
ATT&CK: File and Directory Discovery Permissions Modification
12 minutes

Understand how attackers may modify file or directory permissions/attributes to access protected files.

LAB 311
ATT&CK: File and Directory Discovery
12 minutes

Understand how attackers enumerate files and directories or search for certain information within a file system.

NEW Learn Labs

available April 25, 2023

LAB 133
Identifying Exposure of Sensitive Information Through Environmental Variables
5 minutes

Display understanding of how an existing Improper Restriction of XXE References vulnerability in a cloud-native marketing automation SaaS suite can be discovered and exploited.

LAB 134
Identifying Plaintext Storage of a Password
5 minutes

Demonstrate understanding of how an existing security misconfiguration in a cloud-native marketing automation SaaS suite can be discovered and exploited.

LAB 135
Identifying URL Redirection to Untrusted Site
5 minutes

Fix code in an application written in Node.js that allows attackers to exploit the application to send HTTP requests to arbitrary URLs.

LAB 136
Identifying Improper Neutralization of Script in Attributes in a Web Page
5 minutes

Fix C# code that allows attackers to exploit the application to send HTTP requests to arbitrary URLs.

UPDATED Courses

available April 25, 2023

AWA 101
Fundamentals of Application Security
20 minutes

Learn the fundamentals and primary drivers of application security.

AWA 102
Secure Software Concepts
20 minutes

Learn secure software concepts for web applications and secure development best practices.

COD 246
PCI DSS Requirement 3: Protecting Stored Cardholder Data
20 minutes

Ensure compliance with latest version of PCI DSS 4.0 Requirement 3 for protecting stored cardholder data.

COD 247
PCI DSS Requirement 4: Encrypting Transmission of Cardholder Data
15 minutes

Ensure compliance with latest version of PCI DSS 4.0 Requirement 4 for encrypting transmission of cardholder data.

COD 248
PCI DSS Requirement 6: Develop & Maintain Secure Systems and Software
15 minutes

Ensure compliance with latest version of PCI DSS 4.0 Requirement 6 for Developing and Maintaining Secure Systems and Software.

COD 249
PCI DSS Requirement 11: Regularly Test Security Systems and Processes
15 minutes

Ensure compliance with latest version of PCI DSS 4.0 Requirement 11 for regularly testing security systems and processes.

Get in **Touch**

187 Ballardvale Rd. Suite A195, Wilmington, MA 01887
887-839-7598 X1 www.securityinnovation.com