LinkedIn Learning

Spring: Spring Security

Course completed by BJ Dela Cruz, CISSP/CCSP/CSSLP/CCSK
Feb 09, 2024 at 04:12AM UTC • 1 hour 31 minutes

Top skills covered

Spring Security | Spring Framework

Head of Content Strategy, Learning

COURSE COMPLETION

Certificate ID: 6527478421de16e215bea434a6aad12bc7b73a393f29bbf158c2aae6d2fa83c4

LinkedIn Learning

Ethical Hacking: Vulnerability Analysis

Course completed by BJ Dela Cruz, CISSP/CCSP/CSSLP/CCSK
Feb 11, 2024 at 10:03PM UTC • 1 hour 26 minutes

Top skills covered

Ethical Hacking

Head of Content Strategy, Learning

COURSE COMPLETION

Certificate ID: 459bb73d905f77c981f0179d8df35991f1978ab30b93f1193386705139ca85bf

LinkedIn Learning

Threat Modeling: Information Disclosure in Depth

Course completed by BJ Dela Cruz, CISSP/CCSP/CSSLP/CCSK
Feb 23, 2024 at 02:28PM UTC • 29 minutes

Top skills covered

Threat Modeling

Head of Content Strategy, Learning

COURSE COMPLETION

Certificate ID: a6504760060c732911be361a2923d3941e76f3e33098e54c611b0895934e990c

LinkedIn Learning

The Cybersecurity Threat Landscape

Course completed by BJ Dela Cruz, CISSP/CCSP/CSSLP/CCSK

Feb 27, 2024 at 01:11AM UTC • 59 minutes

Top skills covered

Cybersecurity | Threat & Vulnerability Management

Head of Content Strategy, Learning

Certificate ID: eef220e8059eb3842dfb45847bf50ca4191e5a0be81e5497688ea93bbaa8d0e2

Spring: Spring Security

Developers sometimes struggle to see their apps as attackers do. They don't automatically recognize the vulnerabilities. That is where frameworks like Spring Security come in. Spring Security offers built-in authentication and authorization features for securing your apps and services, and easy ways to extend the framework to maximize its value. Join security architect Frank Moley, as he shows how to secure your Java projects with Spring Security, LDAP, Active Directory, and WebFlux. Along the way, learn how to use Spring Security to set up your own OAuth 2.0 servers to secure your apps and network services.

Ethical Hacking: Vulnerability Analysis

To assess—and ultimately, decrease—an organization's risk, IT security professionals must first evaluate and reduce existing vulnerabilities. If you're working to strengthen network security at your organization, it's essential to have a solid grasp of the processes, methodologies, and tools needed to assess vulnerabilities. In this course, security expert Lisa Bock takes a deep dive into the topic of vulnerability scanning, covering what you need to know to find and address weaknesses that attackers might exploit. Lisa goes over the basics of managing organizational risk, discusses vulnerability analysis methodologies, and shows how to work with vulnerability assessment tools, including Nikto and OpenVAS. Plus, she shares tools and strategies for defending the LAN. Lisa also includes challenge chapters to test your knowledge of each section, along with solutions videos for each challenge.

Learning objectives

- Common causes of vulnerabilities
- Identifying and assessing vulnerabilities
- The Common Vulnerability Scoring System (CVSS)
- Outsourcing vulnerability analysis
- Leveraging Nikto and other vulnerability assessment tools
- Securing mobile devices
- Defending the LAN

Threat Modeling: Information Disclosure in Depth

STRIDE is a popular threat modeling framework that helps security pros and software developers think strategically about risk. This course addresses the I in STRIDE, which

stands for information disclosure. You can learn how to preserve the confidentiality of the data, secrets, and other information you store, and the policies you need to put into place to share that information safely. Topics include classic models such as data at rest and data in motion as well as information disclosure in processes and information disclosure in certain technologies such as cloud, Internet of Things and mobile, and AI and machine learning. Expert Adam Shostack also reviews the side effects of computation, the physical effects of CPUs, and the defenses you can put into place at your organization to manage metadata, secrets, and other sensitive information.

Learning objectives

- Authorized access
- Metadata in motion
- Intentional disclosure
- Side effects of disclosure
- Disclosure in the cloud
- Cryptography and other defenses

The Cybersecurity Threat Landscape

As tech systems continue to grow in complexity, cybersecurity threats are becoming increasingly more effective and damaging. News headlines regularly announce enormous data breaches and sophisticated hacks. How are these attackers getting in, and what actions can you take to protect against them? In this course, Marc Menninger describes some of the most common cybersecurity threats, including phishing and ransomware, deepfakes, unmanaged Internet of Things (IoT) devices, business email compromise, and more. He then teaches the best countermeasures for reducing or eliminating the impact of these threats.