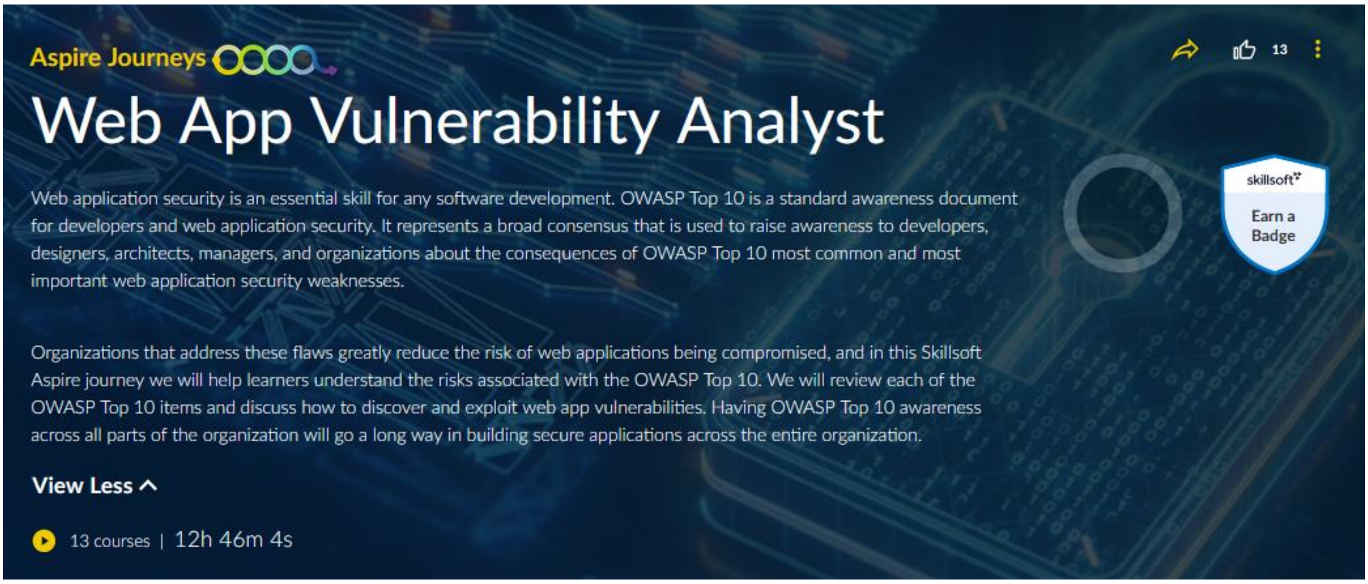
Web App Vulnerability Analyst

SKILLSOFT ASPIRE JOURNEY

skillsoft percipio™

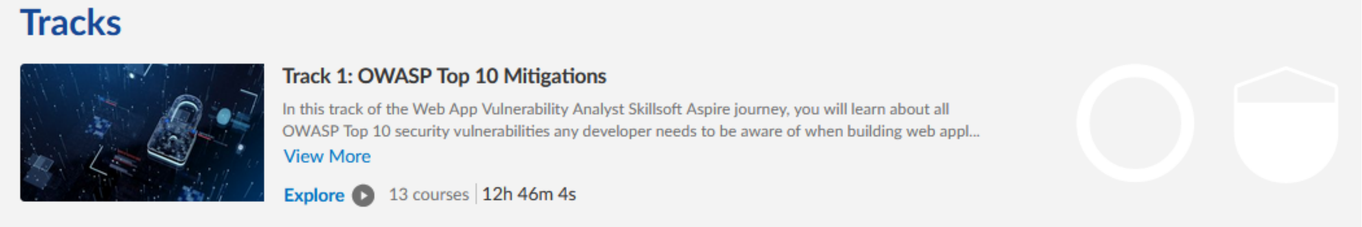


Web App Vulnerability Analyst

Web application security is an essential skill for any software development. OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus that is used to raise awareness to developers, designers, architects, managers, and organizations about the consequences of OWASP Top 10 most common and most important web application security weaknesses.

Organizations that address these flaws greatly reduce the risk of web applications being compromised, and in this Skillsoft Aspire journey we will help learners understand the risks associated with the OWASP Top 10. We will review each of the OWASP Top 10 items and discuss how to discover and exploit web app vulnerabilities. Having OWASP Top 10 awareness across all parts of the organization will go a long way in building secure applications across the entire organization.

13 courses | 12h 46m 4s



Tracks

Track 1: OWASP Top 10 Mitigations

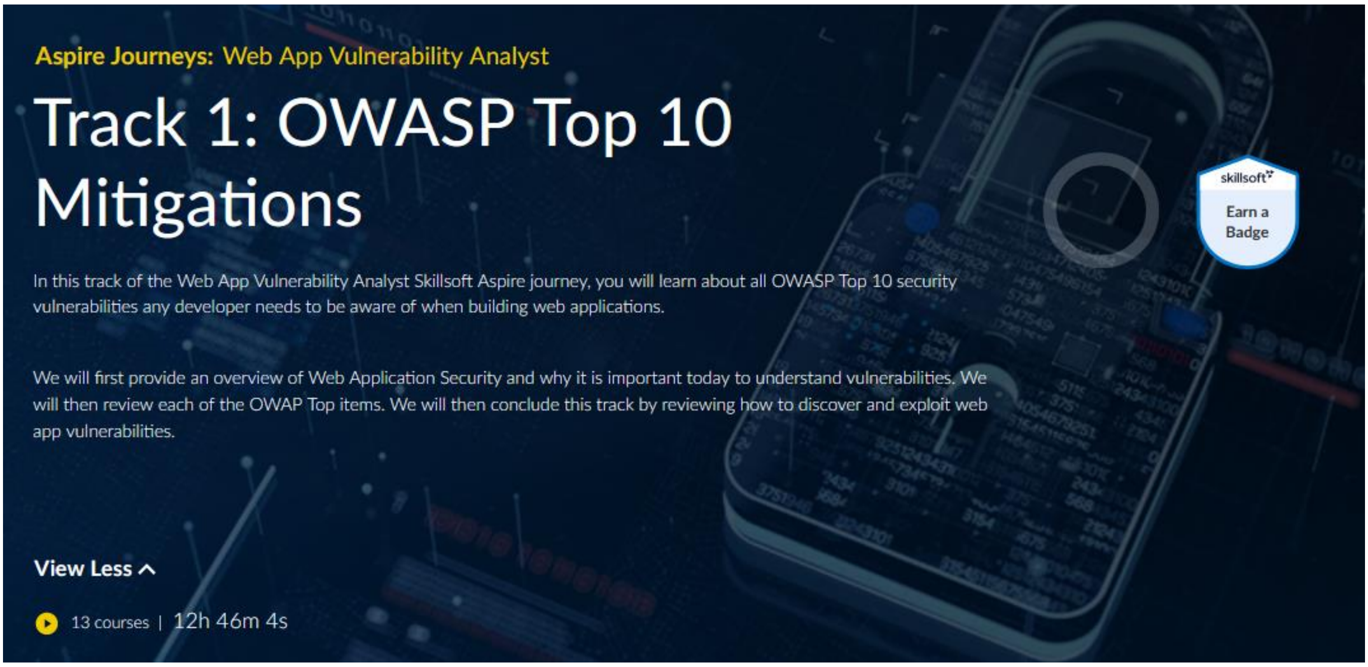
In this track of the Web App Vulnerability Analyst Skillsoft Aspire journey, you will learn about all OWASP Top 10 security vulnerabilities any developer needs to be aware of when building web appl...

13 courses | 12h 46m 4s

PREREQUISITES

In order to fully profit from the potential of this Aspire Journey we recommend the following prerequisite skills:

- Familiar with web application development
- Familiar with security tools



Aspire Journeys: Web App Vulnerability Analyst

Track 1: OWASP Top 10 Mitigations

In this track of the Web App Vulnerability Analyst Skillsoft Aspire journey, you will learn about all OWASP Top 10 security vulnerabilities any developer needs to be aware of when building web applications.

We will first provide an overview of Web Application Security and why it is important today to understand vulnerabilities. We will then review each of the OWAP Top items. We will then conclude this track by reviewing how to discover and exploit web app vulnerabilities.

View Less ^

13 courses | 12h 46m 4s

OWASP Top 10: Web Application Security

Objectives

- identify components related to developing and running a web application
- recognize how to securely write code
- describe the purpose of the Open Web Application Security Project (OWASP)
- recognize the relevance of web application security testing
- list the benefits of using a secure API when writing web app code
- differentiate between static and dynamic software testing
- download and run the Metasploitable intentionally vulnerable web app VM
- plan for various types of security testing
- identify active network hosts and services using Nmap
- identify host vulnerabilities using OpenVAS
- compare past network scans with current scans to identify changes
- describe how a web application firewall differs from other types of firewalls
- deploy a web application firewall solution in the Microsoft Azure cloud

OWASP Top 10: A1 - Injection

Objectives

- recognize types of injection attacks
- test a web app for injection vulnerabilities using the OWASP Zed Attack Proxy (ZAP) tool
- use freely available tools to run a SQL injection attack against a web application
- use freely available tools to run a command injection attack against a web application
- mitigate injection attacks using techniques such as fuzzing and input validation and sanitization

OWASP Top 10: A2 - Broken Authentication

Objectives

- differentiate between authentication and authorization
- recognize how weak authentication configurations can lead to system compromise
- hash user credentials
- encrypt user credentials
- use Wireshark to view plain text credential transmissions
- harden user authentication settings using Microsoft Group Policy
- use the Hydra tool to crack web form user passwords
- use Burp Suite to crack web form user password
- crack RDP passwords using Hydra
- use John the Ripper to crack Linux passwords
- use the Social Engineering Toolkit (SET) to steal user credentials
- enable multi-factor authentication for a Microsoft Azure cloud user account
- configure a conditional access policy in Microsoft Azure
- recognize how to mitigate broken authentication attacks

OWASP Top 10: A3 - Sensitive Data Exposure

Objectives

- list methods by which malicious actors can gain access to sensitive data
- describe what Personally Identifiable Information (PII) is and how it relates to data classification and security
- list common data privacy standards
- use Microsoft File Server Resource Manager (FSRM) in Windows to discover and classify files
- discover and classify sensitive data using Amazon Macie
- enable Data Loss Prevention (DLP) using Azure Information Protection (AIP)
- hash files using Windows commands
- hash files using Linux commands
- encrypt files in Windows using Encrypting File System (EFS)
- encrypt files in Windows using BitLocker
- describe the PKI hierarchy
- configure HTTPS for a web application
- enable IPsec to protect LAN traffic
- encrypt cloud storage
- identify methods by which sensitive data exposure attacks can be mitigated

OWASP Top 10: A4 - XML External Entities

Objectives

- identify how Extensible Markup Language (XML) is used to describe data
- list various ways that XML attacks can be executed
- scan a web application for XML vulnerabilities
- execute an XML external entity attack
- describe how to mitigate XXE attacks

OWASP Top 10: A5 - Broken Access Control

Objectives

- differentiate between mandatory, discretionary, role-based, and attribute-based access control
- identify how broken access control attacks occur
- identify how HTTP requests and responses interact with web applications
- manage Windows file system permissions
- manage Linux file system permissions
- configure attribute-based file system permissions in Windows
- configure permissions for Microsoft Azure managed identities
- digitally sign a Microsoft PowerShell script
- recognize the role of identity and resource providers in a federated identity environment
- navigate through web server subdirectories through a web application
- capture user keystrokes using a hardware keylogger
- apply security controls to mitigate broken access control attacks

OWASP Top 10: A6 - Security Misconfiguration

Objectives

- provide examples of security misconfigurations
- describe how application containers work
- manage Docker containers on a Linux computer
- deploy a cloud-based container registry
- deploy a cloud-based container
- apply security settings to users and computers using Microsoft Group Policy
- assign Azure policies to check Azure resources for security compliance
- install and configure Windows Server Update Services (WSUS)
- describe how security misconfigurations can be mitigated

OWASP Top 10: A7 - Cross-site Scripting

Objectives

- describe how Java and JavaScript are used in web applications
- recognize how Cross-site Scripting (XSS) attacks occur
- run a XSS attack through web page forms
- run a XSS attack to hijack a client web browser
- deploy security controls to mitigate XSS attacks

OWASP Top 10: A8 - Insecure Deserialization

Objectives

- describe how the concept of objects, methods, and properties applies to scripting and software development
- identify how deserialization attacks occur
- recognize how to deploy security controls to mitigate deserialization attacks

OWASP Top 10: A9 - Using Components with Known Vulnerabilities

Objectives

- recognize the importance of logging at all levels, including application logging
- differentiate between SIEM and SOAR monitoring and incident response solutions
- configure syslog-ng in Linux to forward log entries to a central logging host
- monitor web app performance metrics in the cloud
- describe how intrusion detection and prevention can be deployed and used
- install the Snort IDS
- configure and test Snort IDS rules
- use an online service to analyze a Wireshark packet capture
- deploy security controls to correct monitoring deficiencies

OWASP Top 10: A10 - Insufficient Logging & Monitoring

Objectives

- recognize the importance of logging at all levels, including application logging
- differentiate between SIEM and SOAR monitoring and incident response solutions
- configure syslog-ng in Linux to forward log entries to a central logging host
- monitor web app performance metrics in the cloud
- describe how intrusion detection and prevention can be deployed and used
- install the Snort IDS
- configure and test Snort IDS rules
- use an online service to analyze a Wireshark packet capture
- deploy security controls to correct monitoring deficiencies

OWASP Top 10: Discovering & Exploiting Web App Vulnerabilities

Objectives

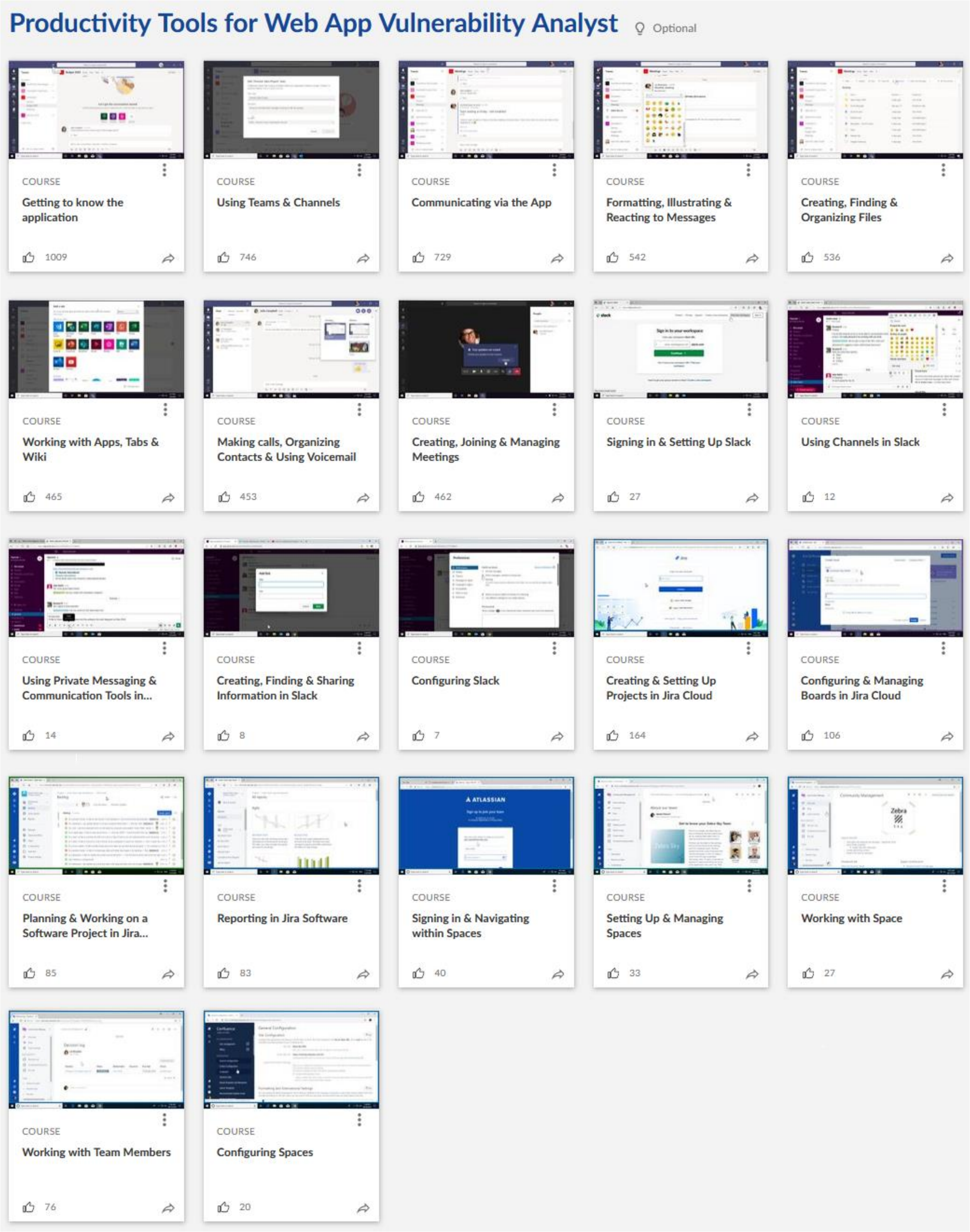
- download and enable the free Metasploitable virtual machine for testing web application vulnerabilities
- discover network hosts running a web application
- download, install, and use the free OWASP ZAP tool to identify web application vulnerabilities
- execute a denial of service (DoS) attack against a web application
- execute a cross-site scripting (XSS) attack against a vulnerable web application
- execute a cross-site request forgery (CSRF) attack against a vulnerable web application
- execute a SQL injection attack against a vulnerable web application
- execute a file inclusion attack against a vulnerable web application
- capture user keystrokes using a hardware keylogger
- capture cleartext HTTP credentials using Wireshark
- assemble fake TCP/IP packets using hping3
- deploy a web app in the Microsoft Azure cloud

Final Exam: OWASP Top 10 Mitigations

Objectives

- apply security controls to mitigate broken access control attacks
- apply security settings to users and computers using Microsoft Group Policy
- browse vulnerable devices on the Shodan.io website
- configure and test Snort IDS rules
- configure syslog-ng in Linux to forward log entries to a central logging host
- crack RDP passwords using Hydra
- deploy a web application firewall solution in the Microsoft Azure cloud
- deploy security controls to correct monitoring deficiencies
- deploy security controls to mitigate XSS attacks
- describe how application containers work
- describe how a web application firewall differs from other types of firewalls
- describe how intrusion detection and prevention can be deployed and used
- describe how Java and JavaScript are used in web applications
- describe how security misconfigurations can be mitigated
- describe how the concept of objects, methods, and properties applies to scripting and software development
- describe how to mitigate XXE attacks
- describe the PKI hierarchy
- describe the purpose of the Open Web Application Security Project (OWASP)
- describe what Personally Identifiable Information (PII) is and how it relates to data classification and security

- differentiate between authentication and authorization
- differentiate between mandatory, discretionary, role-based, and attribute-based access control
- differentiate between SIEM and SOAR monitoring and incident response solutions
- differentiate between static and dynamic software testing
- digitally sign a Microsoft PowerShell script
- enable IPsec to protect LAN traffic
- encrypt user credentials
- harden user authentication settings using Microsoft Group Policy
- hash files using Linux commands
- hash files using Windows commands
- hash user credentials
- identify active network hosts and services using nmap
- identify components related to developing and running a web application
- identify how broken access control attacks occur
- identify how Extensible Markup Language (XML) is used to describe data
- identify how HTTP requests and responses interact with web applications
- identify methods by which sensitive data exposure attacks can be mitigated
- install and configure Windows Server Update Services (WSUS)
- install the Snort IDS
- list common data privacy standards
- list methods by which malicious actors can gain access to sensitive data
- list various ways that XML attacks can be executed
- manage Docker containers on a Linux computer
- manage Linux file system permissions
- manage Windows file system permissions
- mitigate injection attacks using techniques such as fuzzing and input validation, and sanitization
- navigate through web server subdirectories through a web application
- plan for various types of security testing
- provide examples of security misconfigurations
- recall methods by which sensitive data exposure attacks can be mitigated
- recognize how Cross-site Scripting (XSS) attacks occur
- recognize how security must be integrated into all aspects of Continuous Integration and Continuous Delivery (CI/CD)
- recognize how to deploy security controls to mitigate deserialization attacks
- recognize how to mitigate broken authentication attacks
- recognize how to securely write code
- recognize how weak authentication configurations can lead to system compromise
- recognize types of injection attacks
- search vulnerable devices on the Shodan.io website
- use freely available tools to run a SQL injection attack against a web application
- use the Hydra tool to crack web form user passwords
- use Wireshark to view plain text credential transmissions



Productivity Tools for Web App Vulnerability Analyst

Optional

COURSE
Getting to know the application
1009

COURSE
Using Teams & Channels
746

COURSE
Communicating via the App
729

COURSE
Formatting, Illustrating & Reacting to Messages
542

COURSE
Creating, Finding & Organizing Files
536

COURSE
Working with Apps, Tabs & Wiki
465

COURSE
Making calls, Organizing Contacts & Using Voicemail
453

COURSE
Creating, Joining & Managing Meetings
462

COURSE
Signing in & Setting Up Slack
27

COURSE
Using Channels in Slack
12

COURSE
Using Private Messaging & Communication Tools in...
14

COURSE
Creating, Finding & Sharing Information in Slack
8

COURSE
Configuring Slack
7

COURSE
Creating & Setting Up Projects in Jira Cloud
164

COURSE
Configuring & Managing Boards in Jira Cloud
106

COURSE
Planning & Working on a Software Project in Jira...
85

COURSE
Reporting in Jira Software
83

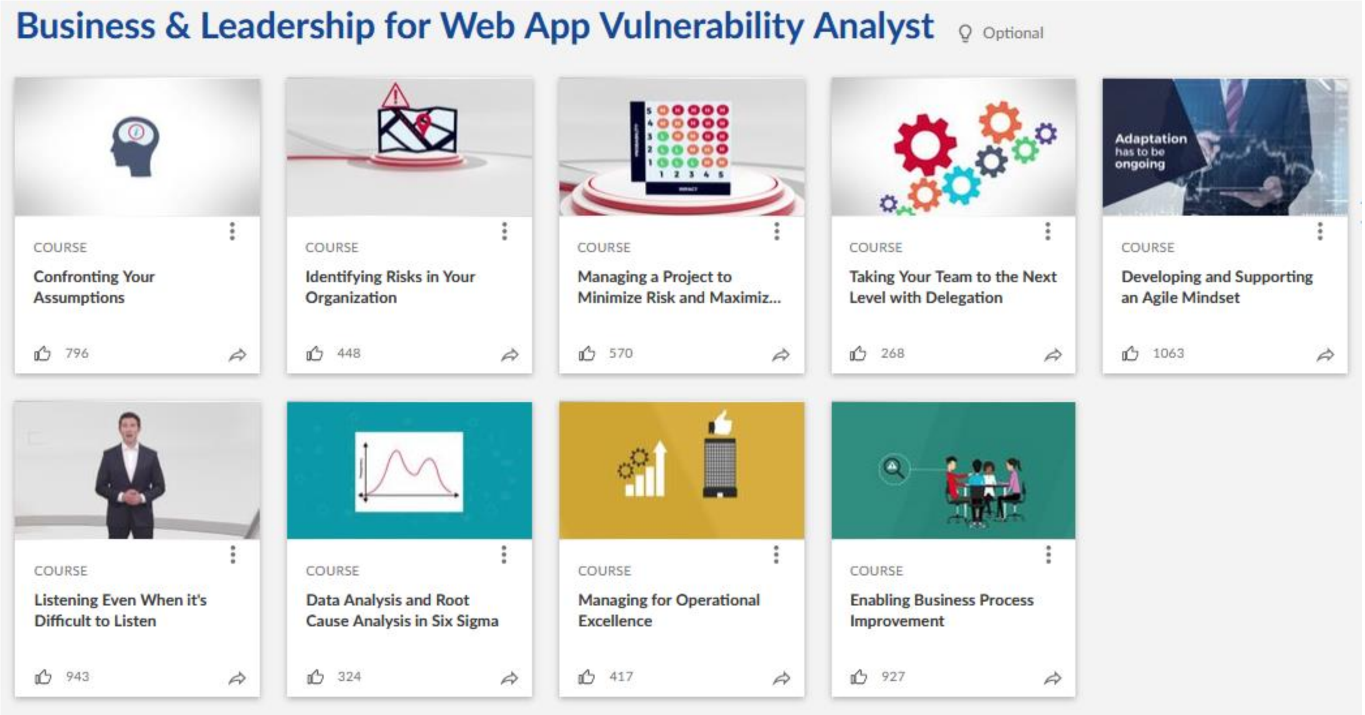
COURSE
Signing in & Navigating within Spaces
40

COURSE
Setting Up & Managing Spaces
33

COURSE
Working with Space
27

COURSE
Working with Team Members
76

COURSE
Configuring Spaces
20



Business & Leadership for Web App Vulnerability Analyst Optional

COURSE
Confronting Your Assumptions
796

COURSE
Identifying Risks in Your Organization
448

COURSE
Managing a Project to Minimize Risk and Maximiz...
570

COURSE
Taking Your Team to the Next Level with Delegation
268

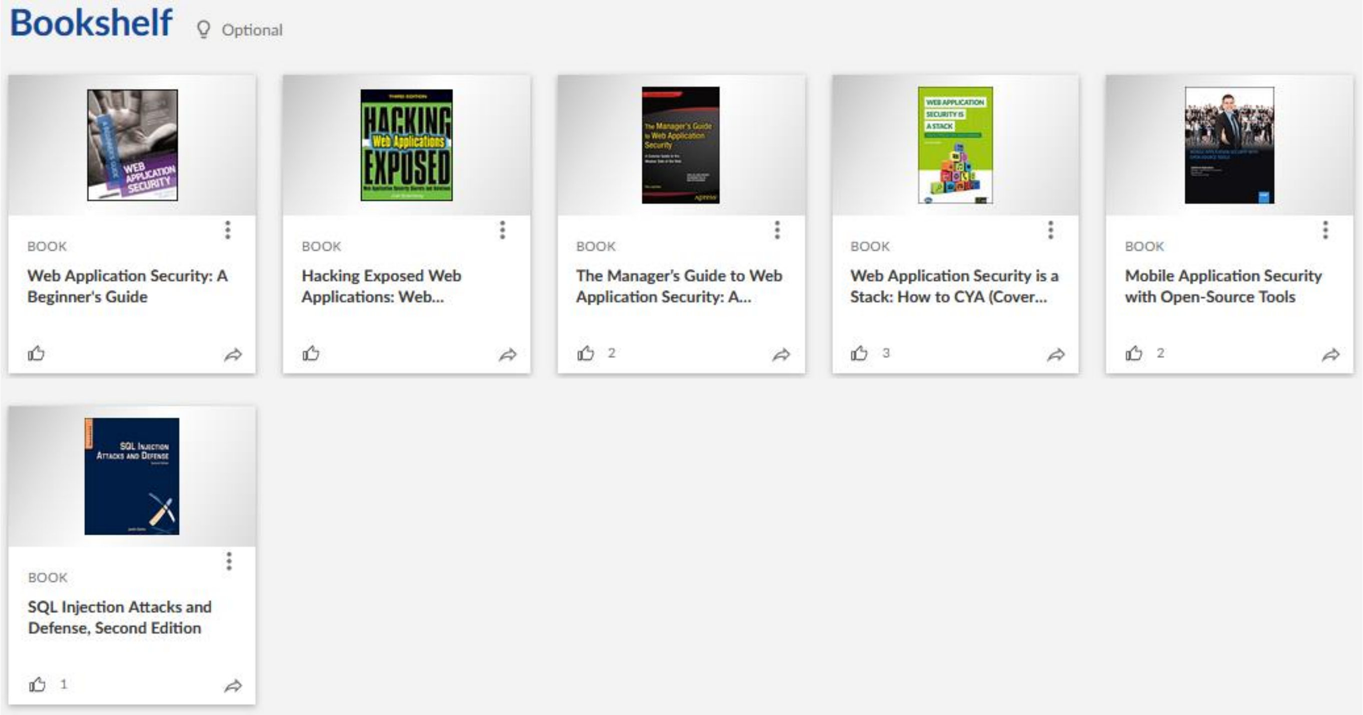
COURSE
Developing and Supporting an Agile Mindset
1063

COURSE
Listening Even When it's Difficult to Listen
943

COURSE
Data Analysis and Root Cause Analysis in Six Sigma
324

COURSE
Managing for Operational Excellence
417

COURSE
Enabling Business Process Improvement
927



Bookshelf Optional

BOOK
Web Application Security: A Beginner's Guide

BOOK
Hacking Exposed Web Applications: Web...

BOOK
The Manager's Guide to Web Application Security: A...
2

BOOK
Web Application Security is a Stack: How to CYA (Cover...
3

BOOK
Mobile Application Security with Open-Source Tools
2

BOOK
SQL Injection Attacks and Defense, Second Edition
1

FOLLOW US ON:

www.skilltech.pl

email: biuro@skilltech.pl

tel. +48 22 44 88 827

SkillTech
Technology hired for excellence