GH-500: GitHub Advanced Security

IMPORTANT: This course is designed to be delivered in one full day. The activities are approximately 60% instructional led and 40% student interactive exercises and/or instructor demos.

Learning objectives

After completing this course, students will be able to:

- Define GitHub Advanced Security (GHAS): Understand the importance of integral features such as Secret scanning, Code scanning, and Dependabot.
- Utilize GHAS: Learn how to maximize security impact using GHAS features.
- Understand GHAS in the Security Ecosystem: Recognize GHAS's role and its integration into the security workflow.
- Configure Dependabot: Learn to enable and configure Dependabot alerts and security updates.
- Implement Secret Scanning: Understand how to enable and use secret scanning to prevent secret leaks.
- Configure Code Scanning: Learn to implement and configure code scanning using CodeQL and other tools

Audience profile

Audience profile for this course is the following:

- A security professional or developer responsible for implementing and managing security measures within their organization.
- Possesses a foundational understanding of GitHub and its basic functionalities but are looking to deepen their knowledge of advanced security features.
- Desire to learn how to effectively use GitHub Advanced Security (GHAS) to enhance the security of their codebase and development workflow.

Audience prerequisites

The audience for this 1-day course consists of security professionals and developers who are responsible for implementing and managing GitHub security measures within their organizations.

NOTE: The exercise activities in this 1-day class are Advanced and require and intermediate knowledge of Git and GitHub functions and features.

Candidates should have the following:

- Experience in using and administering GitHub repositories.

- Experience of working with Microsoft Azure services.
- Technical skills in code scanning, dependency management, and secret scanning, and are familiar with tools like CodeQL and Dependabot.

Student training content

The student training content for this course is in Microsoft Learn and the exercises (hands-on or demonstrations) are included within the Learn modules.

Learning Path: GitHub Advanced Security Part 1 of 2

Module 1: Introduction to GitHub Advanced Security

- Introduction
- Define GHAS and the importance of its integral features
- How to utilize GHAS to get the most impact
- Understand GHAS and its role in the security ecosystem
- Knowledge check
- Summary

Module 2: Configure Dependabot security updates on your GitHub repo

- Introduction
- Manage your dependencies on GitHub
- Dependabot alerts
- Dependabot security updates
- Manage Dependabot notifications and reports
- Dependency review
- Exercise - Configure Dependabot security updates
- Knowledge check
- Summary

Module 3: Configure and use secret scanning in your GitHub repository

- Introduction
- What is secret scanning?
- Configure secret scanning
- Use secret scanning
- Exercise - Introduction to secret scanning
- Knowledge check
- Summary

Module 4: Configure code scanning on GitHub

- Introduction
- What is code scanning?
- Enable code scanning with third party tools
- Configure code scanning
- Exercise - Configure code scanning
- Knowledge check
- Summary

Learning Path: GitHub Advanced Security Part 2 of 2

Module 5: Identify security vulnerabilities in your codebase by using CodeQL

- Introduction
- Prepare a database for CodeQL
- Run CodeQL in a database
- Understand CodeQL results
- Troubleshoot CodeQL results
- Knowledge check
- Summary

Module 6: Code scanning with GitHub CodeQL

- Introduction
- What is CodeQL?
- How does CodeQL analyze code?
- What is QL?
- Code scanning and CodeQL
- Customize your code scanning workflow with CodeQL - Part 1
- Exercise - Reference a CodeQL query
- Customize your code scanning workflow with CodeQL - Part 2
- Use the CodeQL CLI
- Customize languages and builds for code scanning
- Exercise - Configure a CodeQL language matrix
- Knowledge check
- Summary

Module 7: GitHub administration for GitHub Advanced Security

- Introduction
- What is GitHub Advanced Security?
- Enable GitHub Advanced Security
- Manage access to GitHub Advanced Security
- Manage the GitHub Advanced Security features and alerts

- Knowledge check
- Summary

Module 8: Manage sensitive data and security policies within GitHub

- Introduction
- Setting security policies
- Create and manage repository rulesets
- Reporting and logging
- Exercise - Removing a commit from the git history
- Knowledge check
- Summary

Exercises and Demos (6 exercises, 2.5 hours)

Exercises are to be used as hands-on activities for individual students which are led by the instructor, or demonstrations led by the instructor. The decision to lead hands-on activities or perform demonstrations is the instructor's responsibility.

Module 2: Configure Dependabot security updates on your GitHub repo

- Exercise - Configure Dependabot security updates

Module 3: Configure and use secret scanning in your GitHub repository

- Exercise - Intro to secret scanning exercise

Module 4: Configure code scanning on GitHub

- Exercise - Configure code scanning exercise

Module 6: Code scanning with GitHub CodeQL

- Exercise - Reference a CodeQL query
- Exercise - Configure a CodeQL language matrix

Module 8: Manage sensitive data and security policies within GitHub

- Exercise - Removing a commit from git history