Cybersecurity for Developers

INSTRUCTOR-LED | 30 HOURS | ONSITE OR REMOTE

OVERVIEW

It's estimated that as many as 80% of all web applications feature a significant security flaw, ranging from exposing sensitive data to broken authentication and session management. In this training, developers learn how to add security features to their web applications in order to shrink the attack surface.

DELIVERY OPTIONS

- Ten 3-hour sessions over 1 week or multiple weeks

OUTCOMES

- **Level 1 Development Skills:** Add input validation to an application.
- **Level 2 Development Skills:** Implement authentication and authorization features in an application. Add features that defend against CSRF and XSS attacks.

IDEAL FOR

- Web developers who want to learn how to make their applications more secure.

AGENDA

3 hrs

Intro to Cybersecurity for Web Applications

Learn key cybersecurity topics and terms, compare front-end and back-end security responsibilities, and vet 3rd-party libraries, frameworks, and applications for their security.

9 hrs

Front-End Security

Examine the many different ways an application's front-end can be attacked (including CSRF, XSS, and clickjacking) and how front-end apps can be hardened against such attacks.

12 hrs

Back-End Security

Add protections against common back-end vulnerabilities (e.g. SQL injection attacks), and add other features like data encryption and role-based authorization to further strengthen the system.

6 hrs

Final Project

Take a provided application and add security features.

