OWASP

In this lesson, we'll learn about the Open Web Application Security Project.

We'll cover the following

- The Open Web Application Security Project

The Open Web Application Security Project

Truth to be told, I would strongly recommend you visit the OWASP website and find out what they have to say:

- OWASP Cheat Sheet Series (https://cheatsheetseries.owasp.org): a collection of brief practical information. You can find articles about how to harden Docker containers or in what form passwords be should stored. It is a technical and comprehensive list of guides that inspired the practical approach used in this chapter of this course.
- OWASP Developer Guide (https://github.com/OWASP/DevGuide): a guide on how to build secure applications. It is slowly being rewritten (the original version was published in 2005) but most of the content is still very useful.
- OWASP Testing Guide (https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents): on how to test for security holes.

These are three very informative guides that should help you infuse resistance against attacks across your architecture; I'd strongly suggest going through them at some point in time. The Cheat Sheet Series, in particular, is extremely recommended.

We'll conclude this chapter with the next lesson.