# Chapter 37. Part III Summary

Today's web applications include numerous complexities ranging from third-party dependencies to intricate caching and distribution architectures. Each of these layers adds attack surface area, making exploitation easier than ever, and reinforcing the need for wise mitigations at every step.

If you read this book from start to finish, you should now have a good understanding of how modern hackers attack web applications. You should understand that defensive solutions against these hackers must be comprehensive, meticulous, and regularly revised and updated.

Fortunately, some of the burden of this task can be reduced with the smart architectures we discussed in Part III, such as Zero Trust Architecture, framework-level mitigations, automated vulnerability discovery, and threat modeling. By understanding how to mitigate the most common and effective forms of web application vulnerability—and being capable of implementing security workflows and processes that minimize manual repeated security efforts—you can provide great positive impacts to any web application's security posture.

The specific mitigations discussed in Part III may change over time as hackers choose different methods of attack and browsers and tooling get better at implementing out-of-the box mitigations. The design philosophies, methods of analysis, and architectural patterns, however, should benefit you throughout your entire career.