Part III. Defense

This is the final part of *Web Application Security*. Building on Parts I and II, we will deeply analyze what goes into building a modern, full stack web application. At each point in our analysis, we will consider significant security risks and concerns. Following our concerns, we will evaluate alternative implementations as well as mitigations that alleviate security risk.

Throughout this process, you will learn about techniques that you can integrate into your software development life cycle to reduce the vulnerabilities in your production code. These techniques range from secure-by-default application architecture, to avoidance of insecure anti-patterns, all the way to proper security-oriented code-review technique and countermeasures for specific types of exploits.

By the end of Part III, you will have a strong foundation in web application reconnaissance, offensive pen-testing techniques, and secure software development. At that point, I encourage you to reread points of interest in the first two parts (but with added context) or go on to apply your new skills in the real world.

Let's move on and begin learning about software security and the skills required to build hacker-resistant web applications.