Part I. Recon

Instead of a technical overview, which you can find in several places throughout *Web Application Security*, I start this part of the book with a philosophical overview.

To exploit web applications efficiently, a wide array of skills is required. On the one hand, a hacker needs knowledge of network protocols, software development techniques, and common vulnerabilities found in various types of applications. But on the other hand, the hacker also needs to understand the application they are targeting. The more intimate this knowledge is, the better and more applicable it will be.

The hacker should understand the purpose of the application from a functional perspective. Who are its users? How does the application generate revenue? For what purpose do users select the application over competitors? Who are the competitors? What functionality is found in the application?

Without deep understanding of the target application from a nontechnical perspective, it is actually difficult to determine what data and functionality matter. For example, a web application used for car sales may consider the storage of objects representing cars for sale (price, inventory, etc.) to be mission-critical data. But a hobby website where car enthusiasts can post and share modifications done to their own cars may consider the user accounts more valuable than the inventory listed on a user's profile.

The same can be said when talking about functionality rather than just data. Many web applications generate revenue in a number of ways rather than just relying on one income stream.

A media-sharing platform may offer a monthly subscription, serve ads, and offer paid downloads. Which one of these is most valuable to the company? How does the usage of these monetization functions differ from a usability perspective? How many users contribute revenue to each stream?

Ultimately, web application reconnaissance is about collecting data and building a model that combines a web application's technical and functional details in a way that allows you to fully understand the purpose and usage of a web application. Without one or the other, a hacker cannot properly target their attacks. Thus, philosophically speaking, web application reconnaissance is about generating a deeper understanding of a target web application. And in this philosophical model, information is key—regardless of whether it is technical in nature or not.

Because this is a technical book, most of our focus will be on finding and analyzing components of web applications from a technical perspective. However, we will also discuss the importance of functional analysis as well as a few information organization techniques. Beyond this, I implore you to perform your own nontechnical research when a recon opportunity presents itself in the future.