Chapter 8. Part I Summary

By now you should have a solid, fundamental understanding of the purpose of web application recon, and a few techniques from which to bootstrap your recon toolkit. Recon techniques are constantly evolving, and it can be difficult to accurately determine which techniques outshine others. Because of this, you should always be on the lookout for new and interesting recon techniques—especially those that can be performed rapidly and automated to eliminate valuable time otherwise spent on repeated manual effort.

From time to time, your old techniques might become stale, and you might have to develop newer techniques to replace them. An example of this would be improving security in web server packages over time, which now go to great lengths to prevent any state from being leaked that would give away the web server software and version number.

The basic skills in your recon toolkit will probably never go away entirely, but you may find that new technologies emerge. You will want to develop methods of mapping the new technologies in addition to understanding current era and legacy technology.

In Part I, I stressed the importance of writing down and organizing your recon findings. But I would also suggest writing down and recording your recon techniques. Eventually your recon toolkit will expand to cover many unique technologies, frameworks, versions, and methodologies.

Recording and organizing your recon techniques in an effective manner will make it easier to turn them into automation in the future, or to distribute and teach them to others if you find yourself in a mentorship position. Too often, powerful recon techniques are held as institutional knowledge. If you develop effective new recon techniques, do consider

sharing them with the greater security community. The techniques you discover not only will help penetration testers, but may also lead to advances in application security.

Ultimately, the way you choose to accumulate, record, and distribute these techniques is up to you. I hope the foundations laid out in this book become a cornerstone in your recon toolkit and serve you well throughout your future ventures in the world of application security.