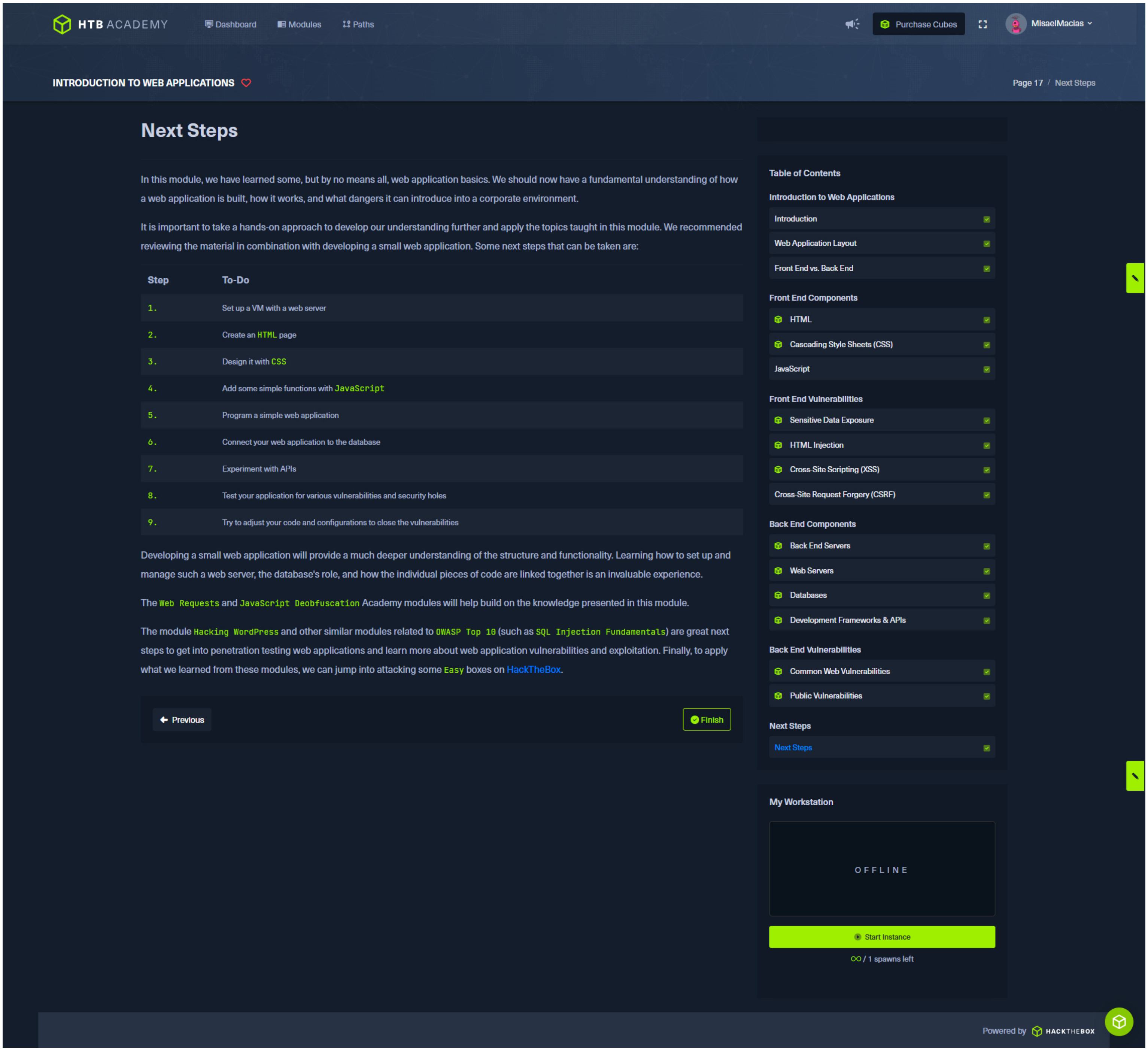

INTRODUCTION TO WEB APPLICATIONS

Next Steps

In this module, we have learned some, but by no means all, web application basics. We should now have a fundamental understanding of how a web application is built, how it works, and what dangers it can introduce into a corporate environment.

It is important to take a hands-on approach to develop our understanding further and apply the topics taught in this module. We recommended reviewing the material in combination with developing a small web application. Some next steps that can be taken are:

Step	To-Do
`1.`	Set up a VM with a web server
`2.`	Create an `HTML` page
`3.`	Design it with `CSS`
`4.`	Add some simple functions with `JavaScript`
`5.`	Program a simple web application
`6.`	Connect your web application to the database
`7.`	Experiment with APIs
`8.`	Test your application for various vulnerabilities and security holes
`9.`	Try to adjust your code and configurations to close the vulnerabilities

Developing a small web application will provide a much deeper understanding of the structure and functionality. Learning how to set up and manage such a web server, the database's role, and how the individual pieces of code are linked together is an invaluable experience.

The `Web Requests` and `JavaScript Deobfuscation` Academy modules will help build on the knowledge presented in this module.

The module `Hacking WordPress` and other similar modules related to `OWASP Top 10` (such as `SQL Injection Fundamentals`) are great next steps to get into penetration testing web applications and learn more about web application vulnerabilities and exploitation. Finally, to apply what we learned from these modules, we can jump into attacking some `Easy` boxes on HackTheBox.

Table of Contents

My Workstation