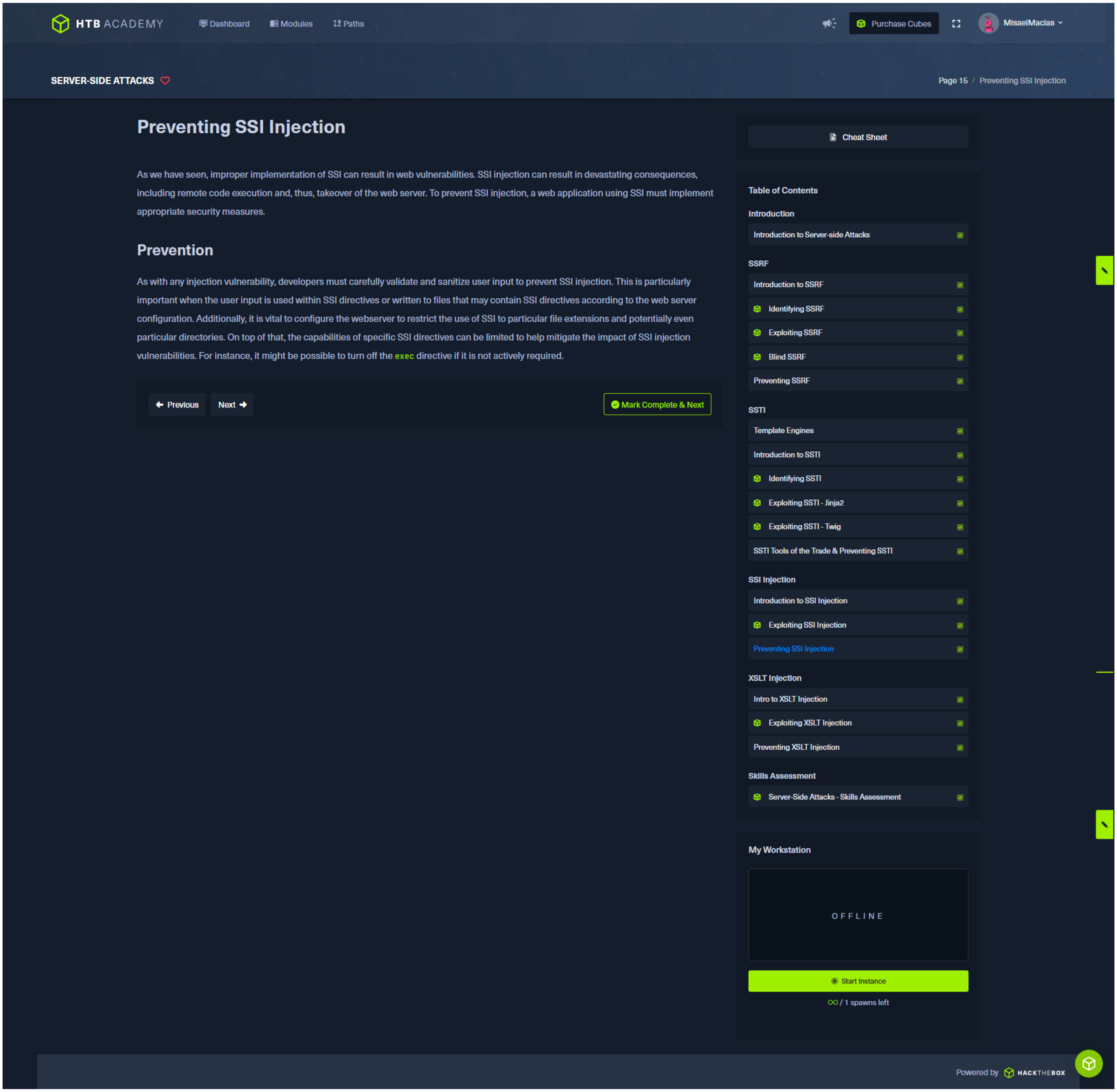

Preventing SSI Injection

As we have seen, improper implementation of SSI can result in web vulnerabilities. SSI injection can result in devastating consequences, including remote code execution and, thus, takeover of the web server. To prevent SSI injection, a web application using SSI must implement appropriate security measures.

Prevention

As with any injection vulnerability, developers must carefully validate and sanitize user input to prevent SSI injection. This is particularly important when the user input is used within SSI directives or written to files that may contain SSI directives according to the web server configuration. Additionally, it is vital to configure the webserver to restrict the use of SSI to particular file extensions and potentially even particular directories. On top of that, the capabilities of specific SSI directives can be limited to help mitigate the impact of SSI injection vulnerabilities. For instance, it might be possible to turn off the `exec` directive if it is not actively required.

Table of Contents

Introduction

SSRF

SSTI

SSI Injection

XSLT Injection

Skills Assessment

My Workstation