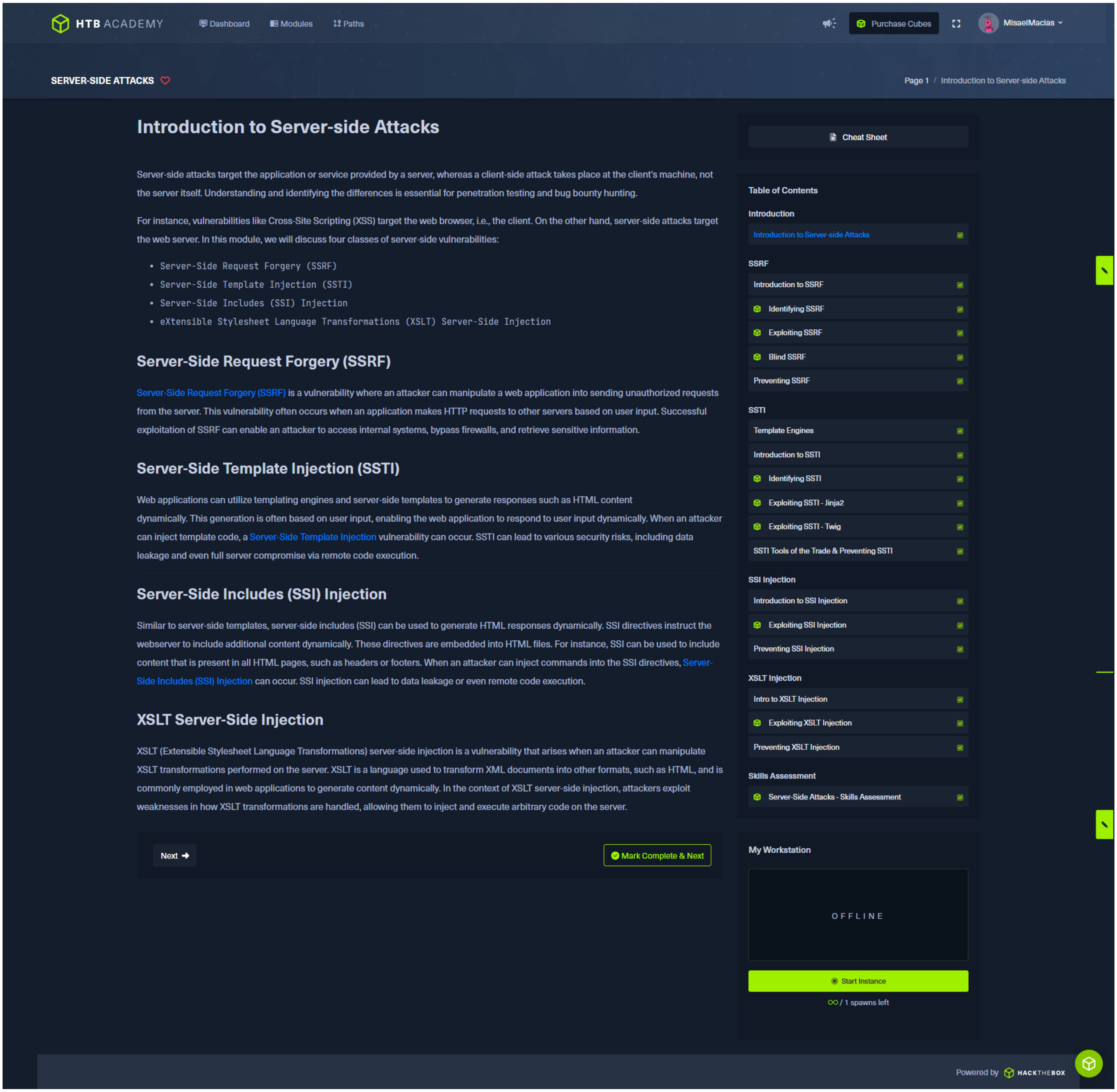

Introduction to Server-side Attacks

Server-side attacks target the application or service provided by a server, whereas a client-side attack takes place at the client's machine, not the server itself. Understanding and identifying the differences is essential for penetration testing and bug bounty hunting.

For instance, vulnerabilities like Cross-Site Scripting (XSS) target the web browser, i.e., the client. On the other hand, server-side attacks target the web server. In this module, we will discuss four classes of server-side vulnerabilities:

- `Server-Side Request Forgery (SSRF)`
- `Server-Side Template Injection (SSTI)`
- `Server-Side Includes (SSI) Injection`
- `eXtensible Stylesheet Language Transformations (XSLT) Server-Side Injection`

Server-Side Request Forgery (SSRF)

Server-Side Request Forgery (SSRF) is a vulnerability where an attacker can manipulate a web application into sending unauthorized requests from the server. This vulnerability often occurs when an application makes HTTP requests to other servers based on user input. Successful exploitation of SSRF can enable an attacker to access internal systems, bypass firewalls, and retrieve sensitive information.

Server-Side Template Injection (SSTI)

Web applications can utilize templating engines and server-side templates to generate responses such as HTML content dynamically. This generation is often based on user input, enabling the web application to respond to user input dynamically. When an attacker can inject template code, a Server-Side Template Injection vulnerability can occur. SSTI can lead to various security risks, including data leakage and even full server compromise via remote code execution.

Server-Side Includes (SSI) Injection

Similar to server-side templates, server-side includes (SSI) can be used to generate HTML responses dynamically. SSI directives instruct the webserver to include additional content dynamically. These directives are embedded into HTML files. For instance, SSI can be used to include content that is present in all HTML pages, such as headers or footers. When an attacker can inject commands into the SSI directives, Server-Side Includes (SSI) Injection can occur. SSI injection can lead to data leakage or even remote code execution.

XSLT Server-Side Injection

XSLT (Extensible Stylesheet Language Transformations) server-side injection is a vulnerability that arises when an attacker can manipulate XSLT transformations performed on the server. XSLT is a language used to transform XML documents into other formats, such as HTML, and is commonly employed in web applications to generate content dynamically. In the context of XSLT server-side injection, attackers exploit weaknesses in how XSLT transformations are handled, allowing them to inject and execute arbitrary code on the server.

Table of Contents

Introduction

SSRF

SSTI

SSI Injection

XSLT Injection

Skills Assessment

My Workstation

OFFLINE