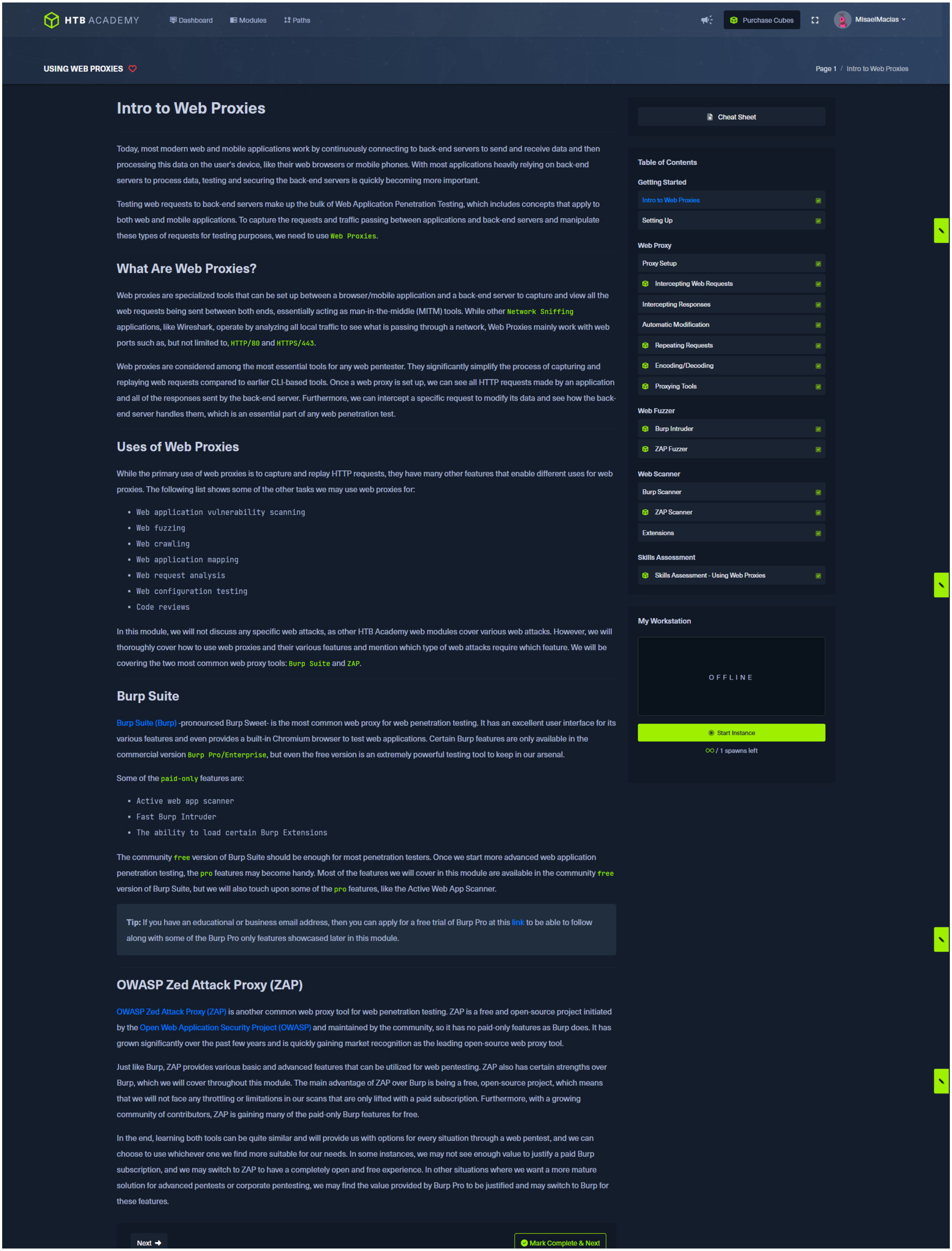

Intro to Web Proxies

Today, most modern web and mobile applications work by continuously connecting to back-end servers to send and receive data and then processing this data on the user's device, like their web browsers or mobile phones. With most applications heavily relying on back-end servers to process data, testing and securing the back-end servers is quickly becoming more important.

Testing web requests to back-end servers make up the bulk of Web Application Penetration Testing, which includes concepts that apply to both web and mobile applications. To capture the requests and traffic passing between applications and back-end servers and manipulate these types of requests for testing purposes, we need to use `Web Proxies`.

What Are Web Proxies?

Web proxies are specialized tools that can be set up between a browser/mobile application and a back-end server to capture and view all the web requests being sent between both ends, essentially acting as man-in-the-middle (MITM) tools. While other `Network Sniffing` applications, like Wireshark, operate by analyzing all local traffic to see what is passing through a network, Web Proxies mainly work with web ports such as, but not limited to, `HTTP/80` and `HTTPS/443`.

Web proxies are considered among the most essential tools for any web pentester. They significantly simplify the process of capturing and replaying web requests compared to earlier CLI-based tools. Once a web proxy is set up, we can see all HTTP requests made by an application and all of the responses sent by the back-end server. Furthermore, we can intercept a specific request to modify its data and see how the back-end server handles them, which is an essential part of any web penetration test.

Uses of Web Proxies

While the primary use of web proxies is to capture and replay HTTP requests, they have many other features that enable different uses for web proxies. The following list shows some of the other tasks we may use web proxies for:

- `Web application vulnerability scanning`
- `Web fuzzing`
- `Web crawling`
- `Web application mapping`
- `Web request analysis`
- `Web configuration testing`
- `Code reviews`

In this module, we will not discuss any specific web attacks, as other HTB Academy web modules cover various web attacks. However, we will thoroughly cover how to use web proxies and their various features and mention which type of web attacks require which feature. We will be covering the two most common web proxy tools: `Burp Suite` and `ZAP`.

Burp Suite

Burp Suite (Burp) -pronounced Burp Sweet- is the most common web proxy for web penetration testing. It has an excellent user interface for its various features and even provides a built-in Chromium browser to test web applications. Certain Burp features are only available in the commercial version `Burp Pro/Enterprise`, but even the free version is an extremely powerful testing tool to keep in our arsenal.

Some of the `paid-only` features are:

- `Active web app scanner`
- `Fast Burp Intruder`
- `The ability to load certain Burp Extensions`

The community `free` version of Burp Suite should be enough for most penetration testers. Once we start more advanced web application penetration testing, the `pro` features may become handy. Most of the features we will cover in this module are available in the community `free` version of Burp Suite, but we will also touch upon some of the `pro` features, like the Active Web App Scanner.

> **Tip:** If you have an educational or business email address, then you can apply for a free trial of Burp Pro at this link to be able to follow along with some of the Burp Pro only features showcased later in this module.

OWASP Zed Attack Proxy (ZAP)

OWASP Zed Attack Proxy (ZAP) is another common web proxy tool for web penetration testing. ZAP is a free and open-source project initiated by the Open Web Application Security Project (OWASP) and maintained by the community, so it has no paid-only features as Burp does. It has grown significantly over the past few years and is quickly gaining market recognition as the leading open-source web proxy tool.

Just like Burp, ZAP provides various basic and advanced features that can be utilized for web pentesting. ZAP also has certain strengths over Burp, which we will cover throughout this module. The main advantage of ZAP over Burp is being a free, open-source project, which means that we will not face any throttling or limitations in our scans that are only lifted with a paid subscription. Furthermore, with a growing community of contributors, ZAP is gaining many of the paid-only Burp features for free.

In the end, learning both tools can be quite similar and will provide us with options for every situation through a web pentest, and we can choose to use whichever one we find more suitable for our needs. In some instances, we may not see enough value to justify a paid Burp subscription, and we may switch to ZAP to have a completely open and free experience. In other situations where we want a more mature solution for advanced pentests or corporate pentesting, we may find the value provided by Burp Pro to be justified and may switch to Burp for these features.

Next ➜   Mark Complete & Next

Cheat Sheet

Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Powered by HACKTHEBOX