cs-sa07-24019
John_Mbithi_Mutave

Attacking Web Applications with Ffuf

Introduction

There are many tools and methods to utilize for directory and parameter fuzzing/brute-forcing. In this module, we will mainly focus on the ffuf tool for web fuzzing, as it is one of the most common and reliable tools available for this purpose.

Tools such as ffuf provide us with a handy automated way to fuzz the web application's individual components or a web page. This means, for example, that we use a list that is used to send requests to the web server. If the page with the name from our list exists on the web server, and we get a response code 200, then we know that this page exists on the web server, and we can look at it manually.

Basic Fuzzing

In this section, we covered the basics of using ffuf for directory and file fuzzing. We explored how to identify common directories and files within a web application by using wordlists and automated scripts. This foundational knowledge is crucial for uncovering hidden paths and resources that might otherwise go unnoticed.

Domain Fuzzing

This part of the module focused on identifying hidden virtual hosts (vhosts) on a target server. By fuzzing subdomains and virtual hosts, we can discover additional entry points and services running on the same server, potentially leading to more vulnerabilities.

Parameter Fuzzing

Parameter fuzzing is a technique used to identify vulnerabilities within web applications by testing various input parameters. This section covered how to use ffuf to fuzz for PHP parameters and parameter values, helping us uncover potential security flaws like SQL injection, XSS, and other input-based attacks.

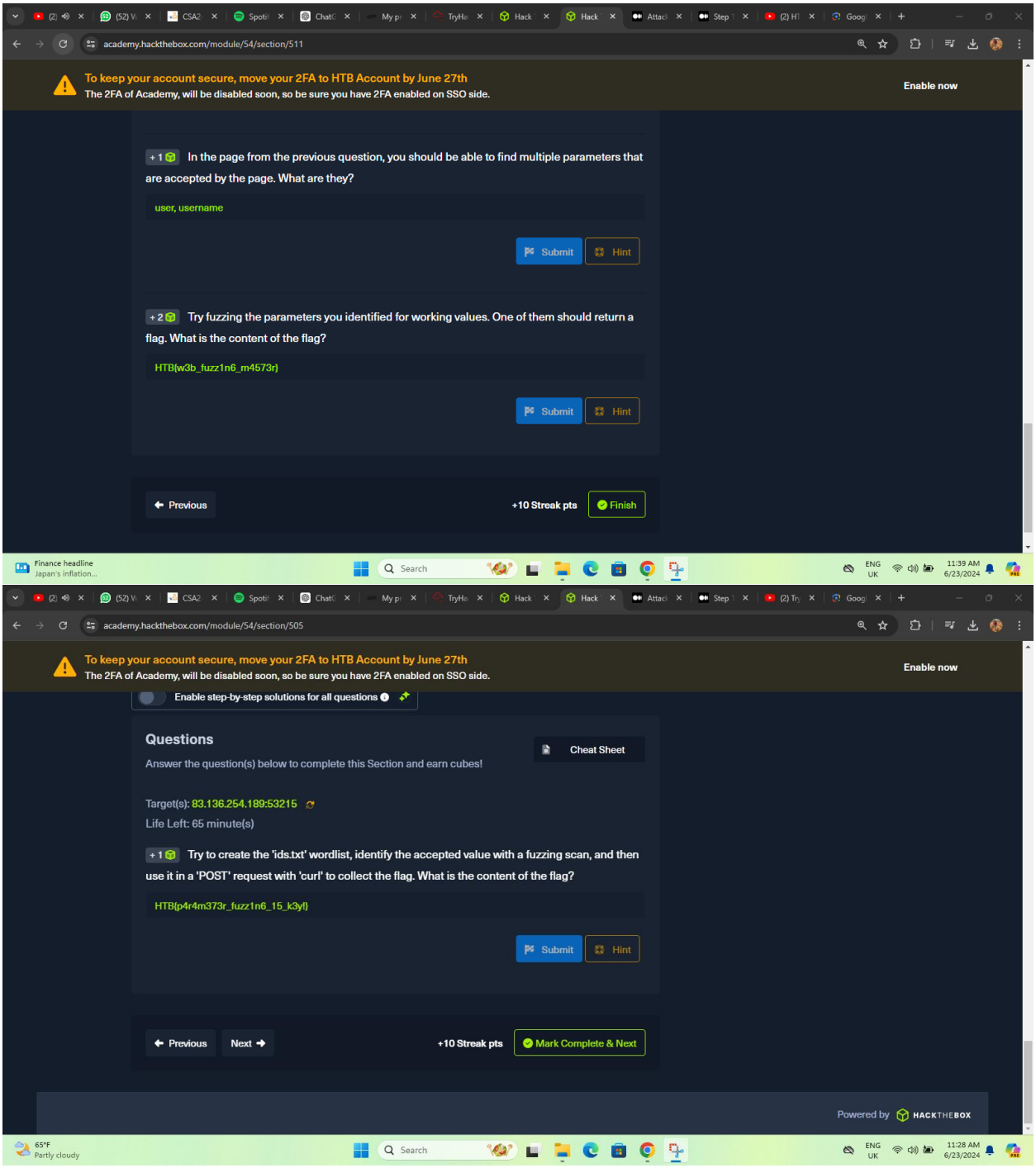
Skills Assessment

The skills assessment section provided practical exercises to test our understanding and application of the techniques learned throughout the module. These assessments reinforced our knowledge and ensured we were capable of effectively using ffuf for web application fuzzing.

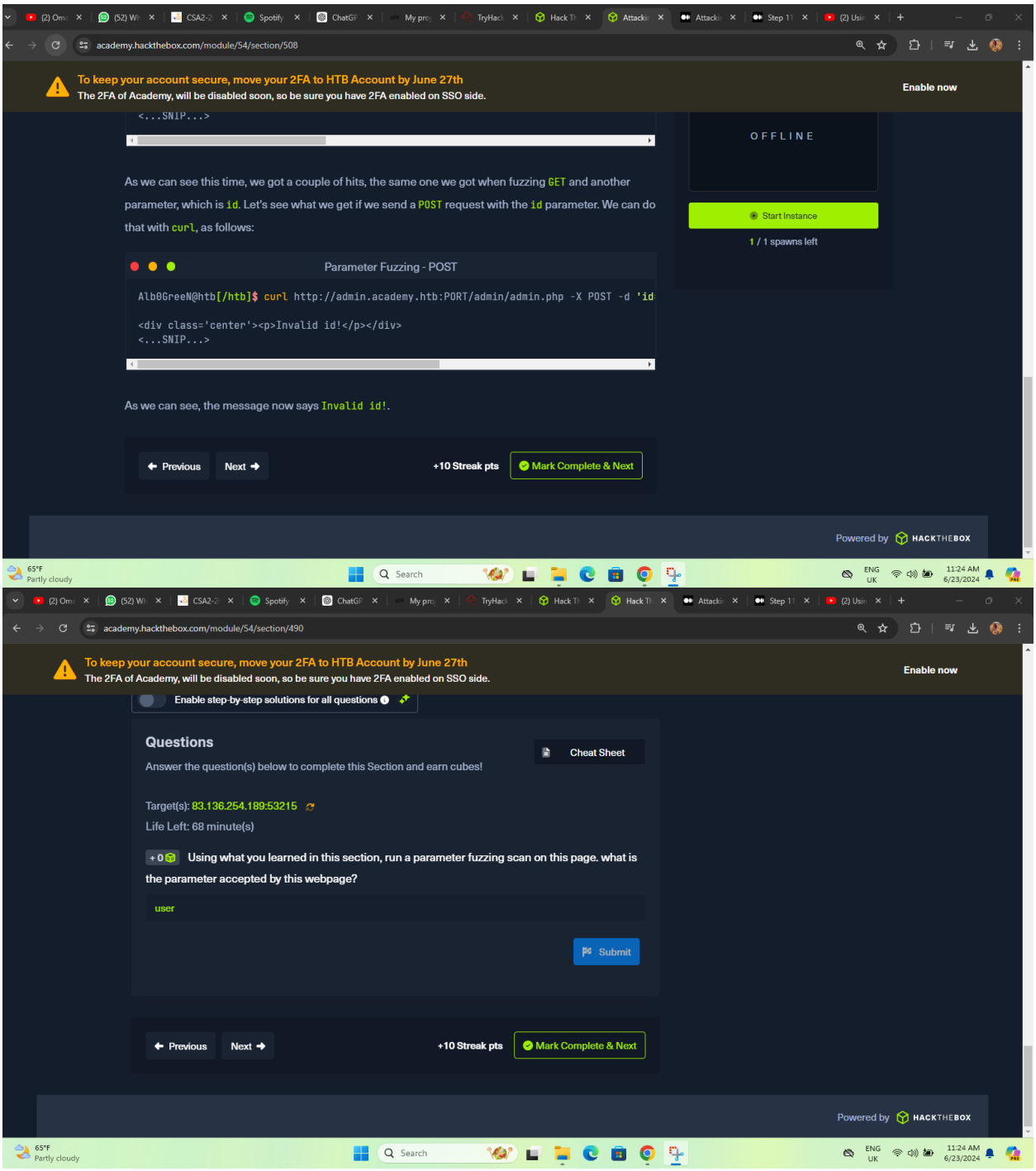
My Workstation

Throughout the module, we utilized a dedicated workstation setup specifically for security testing. This setup included all necessary tools and environments required to perform comprehensive fuzzing and vulnerability assessments using ffuf.

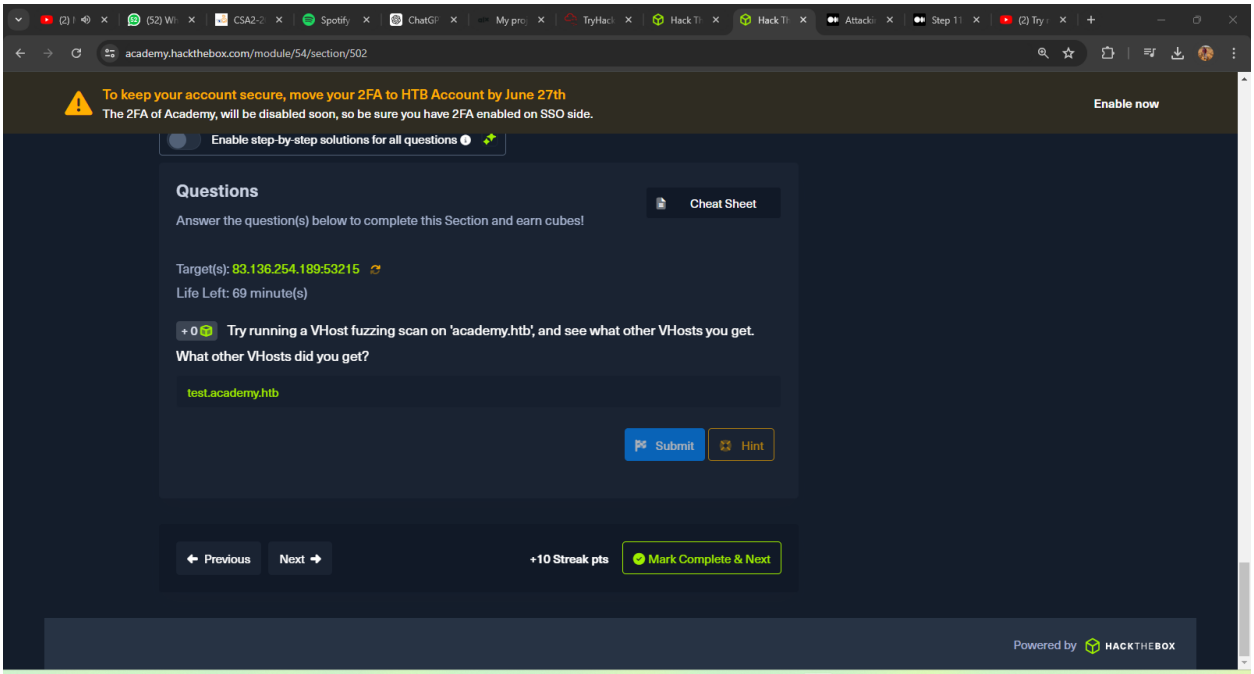
cs-sa07-24019
John_Mbithi_Mutave

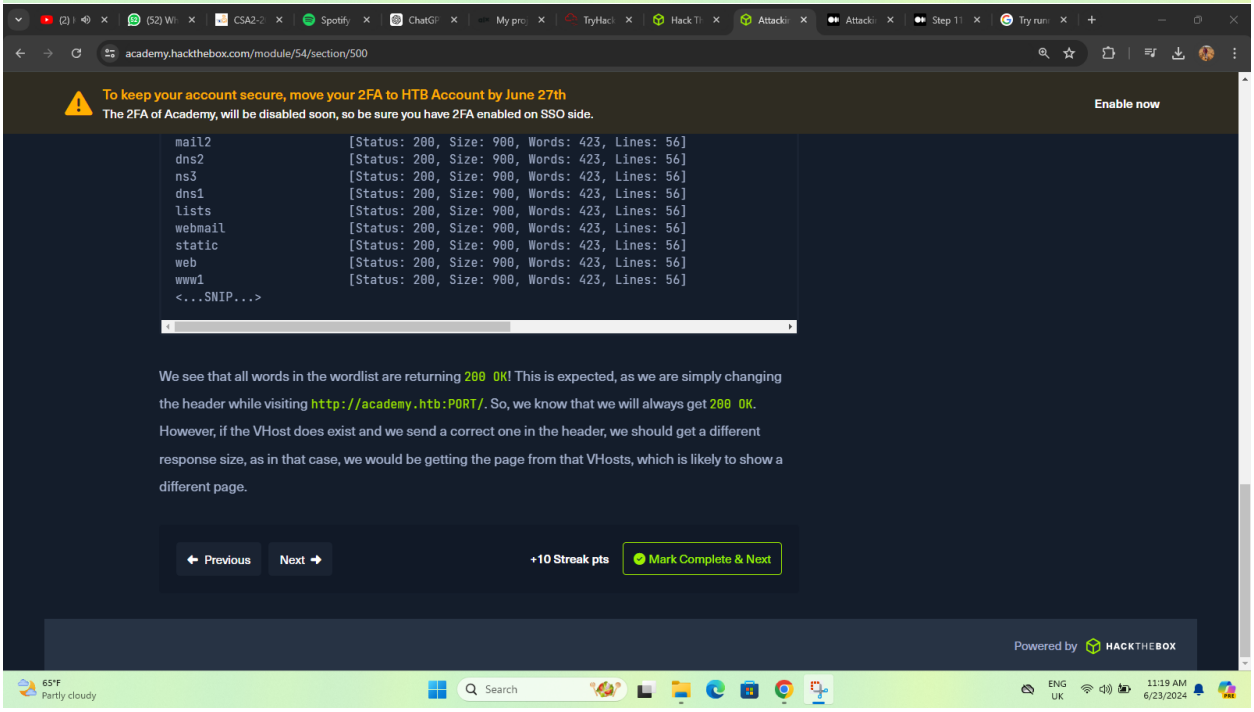


cs-sa07-24019
John_Mbithi_Mutave

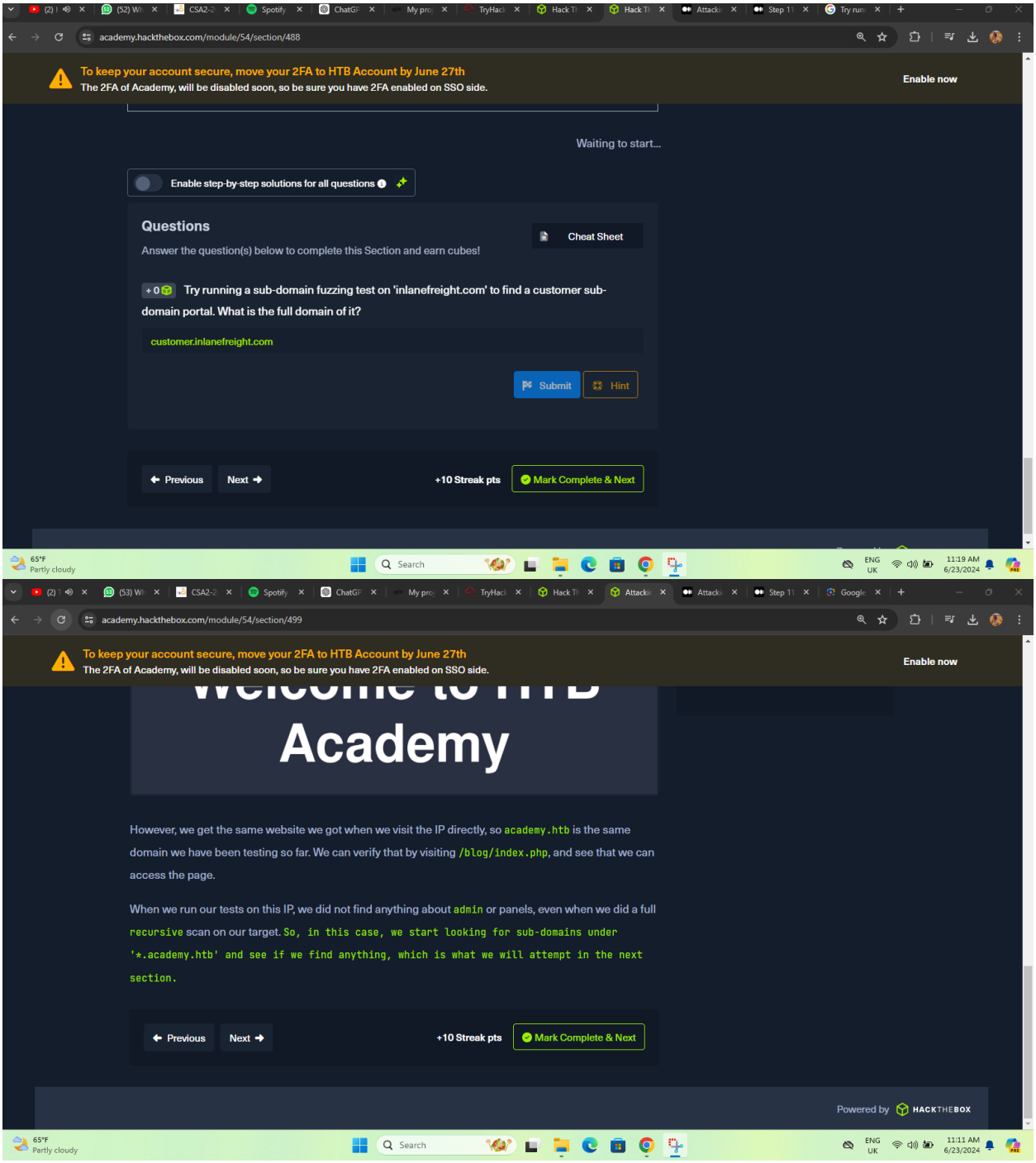


cs-sa07-24019
John_Mbithi_Mutave

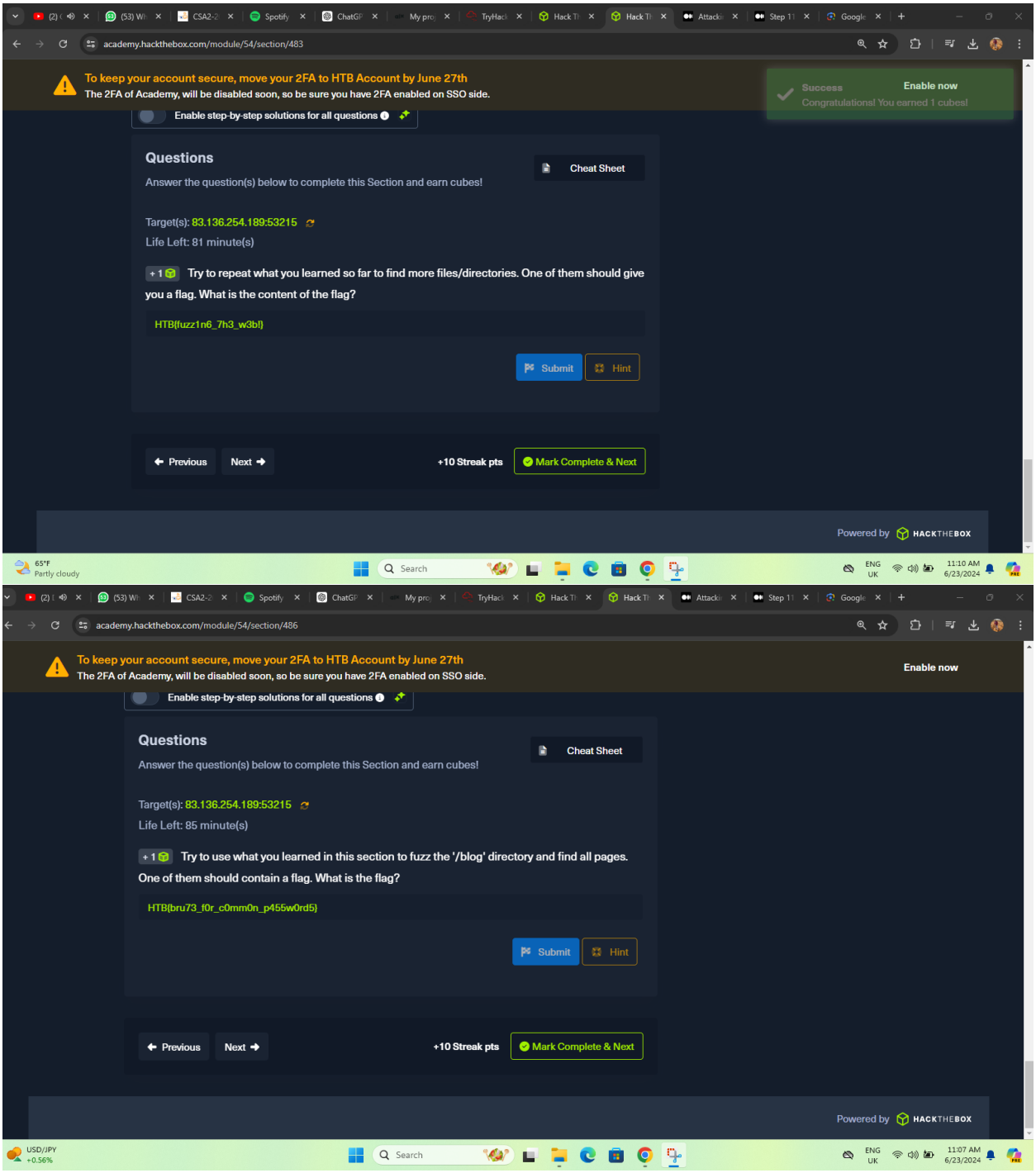




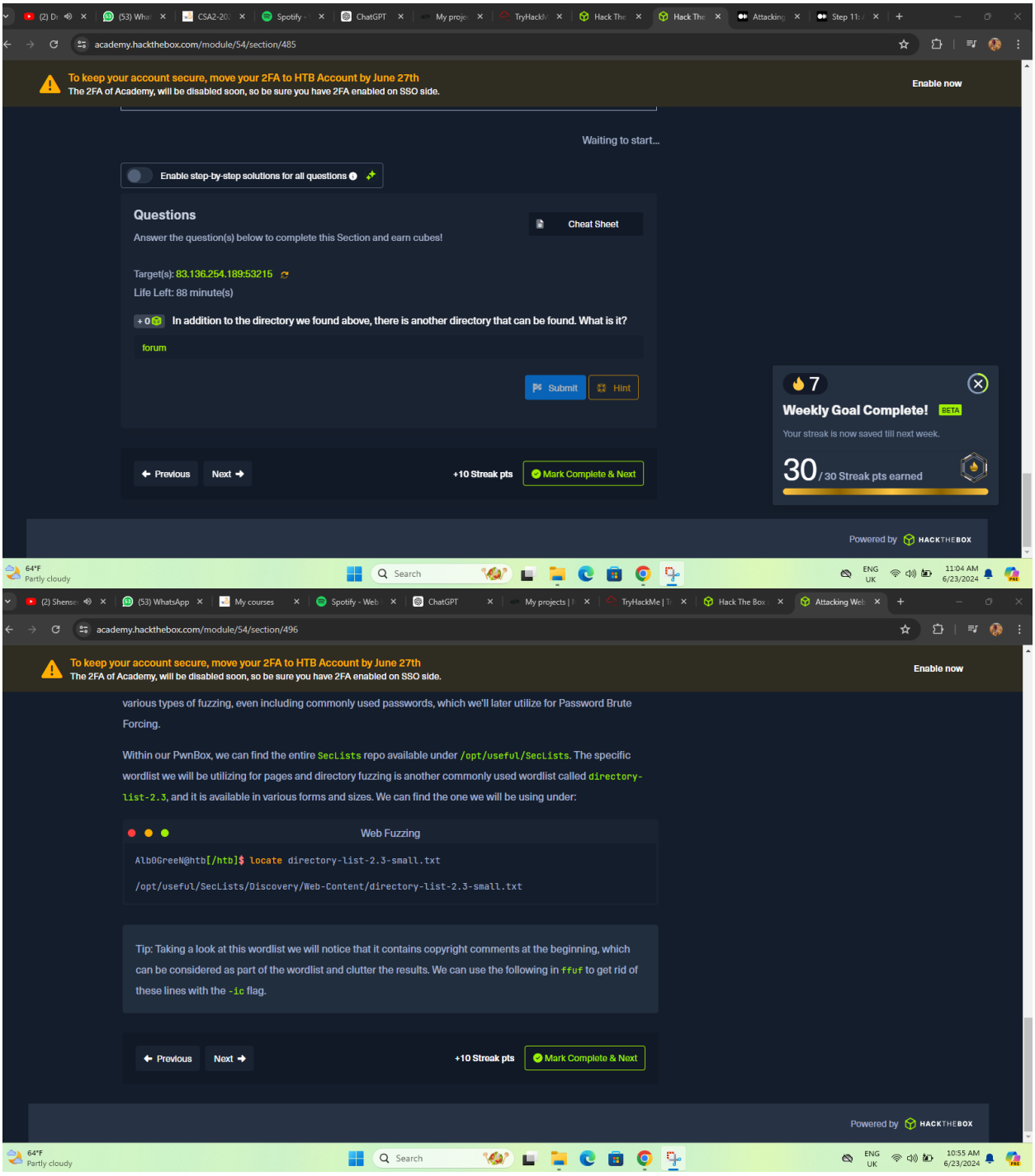
cs-sa07-24019
John_Mbithi_Mutave



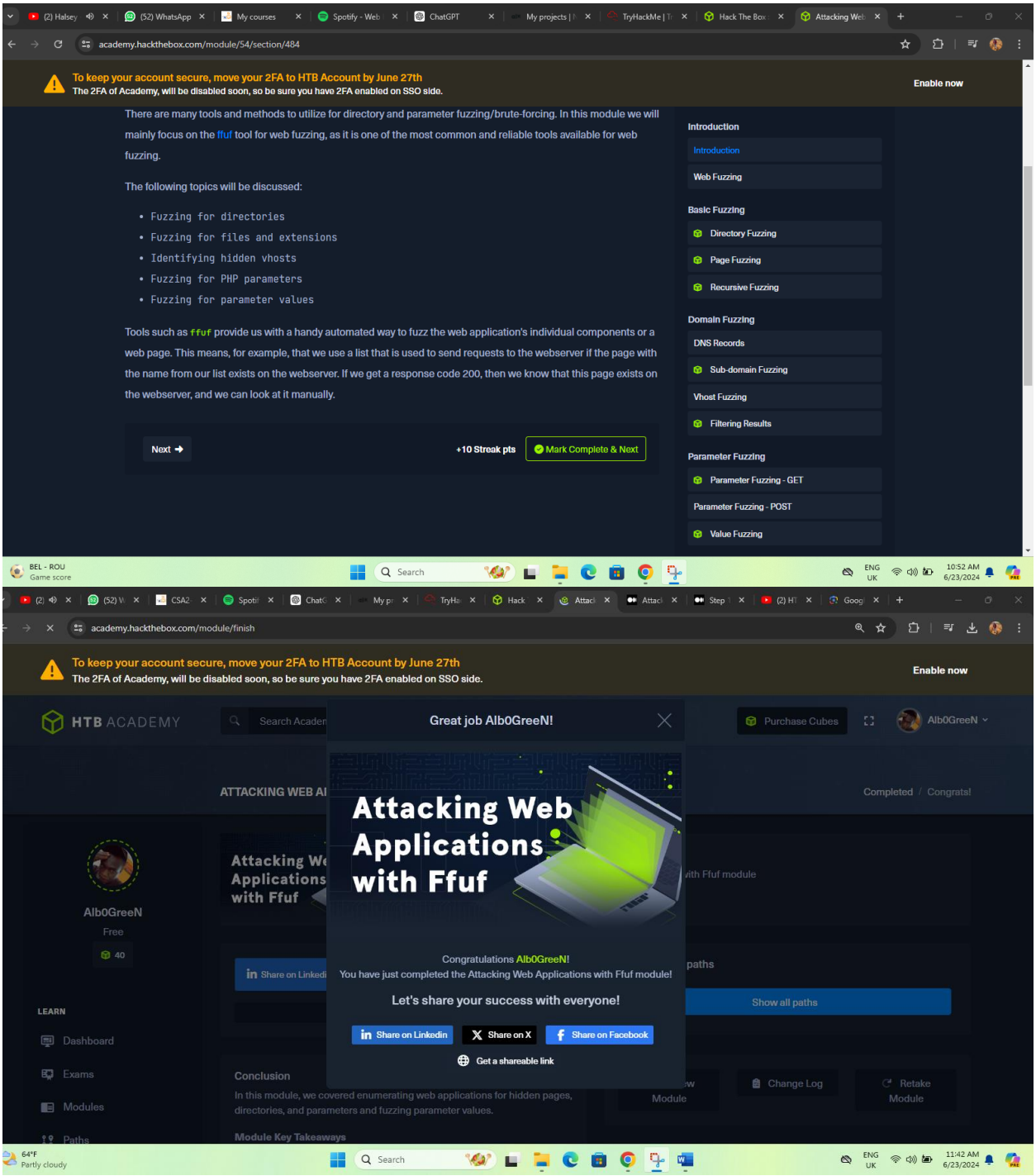
cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019
John_Mbithi_Mutave



Shareable links - https://academy.hackthebox.com/achievement/1296187/54

Conclusion

Completing the Attacking Web Applications with Ffuf module on Hack The Box has been an enlightening experience. The hands-on approach and in-depth coverage of fuzzing techniques have significantly enhanced my skills in web application security testing. Armed with the knowledge and tools from this module, I am now better equipped to identify and exploit vulnerabilities in web applications, making the internet a safer place.