cs-sa07-24019
John_Mbithi_Mutave

OWASP Top 10 - 2021

Introduction

The OWASP Top 10 - 2021 course on TryHackMe provided an in-depth learning experience on the ten most critical web security risks identified by the Open Web Application Security Project (OWASP). This training involved both theoretical learning and practical exercises to exploit and mitigate these vulnerabilities. The completion of this course enhances our ability to identify, understand, and protect against common web application security threats.

Introduction to the OWASP Top 10 - 2021 vulnerabilities and their significance in web security.

Accessing Machines

Instructions on how to set up and access the virtual machines required for the practical exercises.

Broken Access Control

Task: Learn about broken access control, where users can act outside of their intended permissions.

Challenge: Practical exploitation of Insecure Direct Object References (IDOR).

Cryptographic Failures

Task: Understand issues related to cryptography, such as weak encryption and improper key management.

Supporting Material 1 & 2: Supplementary content to reinforce understanding.

Challenge: Exploit cryptographic weaknesses in a given scenario.

Injection

Task: Explore various types of injection attacks, such as SQL, NoSQL, and command injection.

Command Injection: Specific focus on exploiting command injection vulnerabilities.

Insecure Design

Task: Learn about the importance of secure design principles and the risks associated with poor design.

Security Misconfiguration

Task: Identify and exploit security misconfigurations, which are often due to incomplete or improper configurations.

Vulnerable and Outdated Components

Task: Recognize the dangers of using components with known vulnerabilities.

Exploit: Practical exploitation of a system using outdated components.

Lab: Hands-on lab to reinforce learning.

Identification and Authentication Failures

Task: Understand the importance of robust authentication mechanisms to prevent unauthorized access.

Practical Exercise: Implement and test secure authentication practices.

Software and Data Integrity Failures

Task: Focus on ensuring the integrity of software and data.

Software Integrity Failures: Specific examples of software integrity issues.

Data Integrity Failures: Practical scenarios highlighting data integrity vulnerabilities.

Security Logging and Monitoring Failures

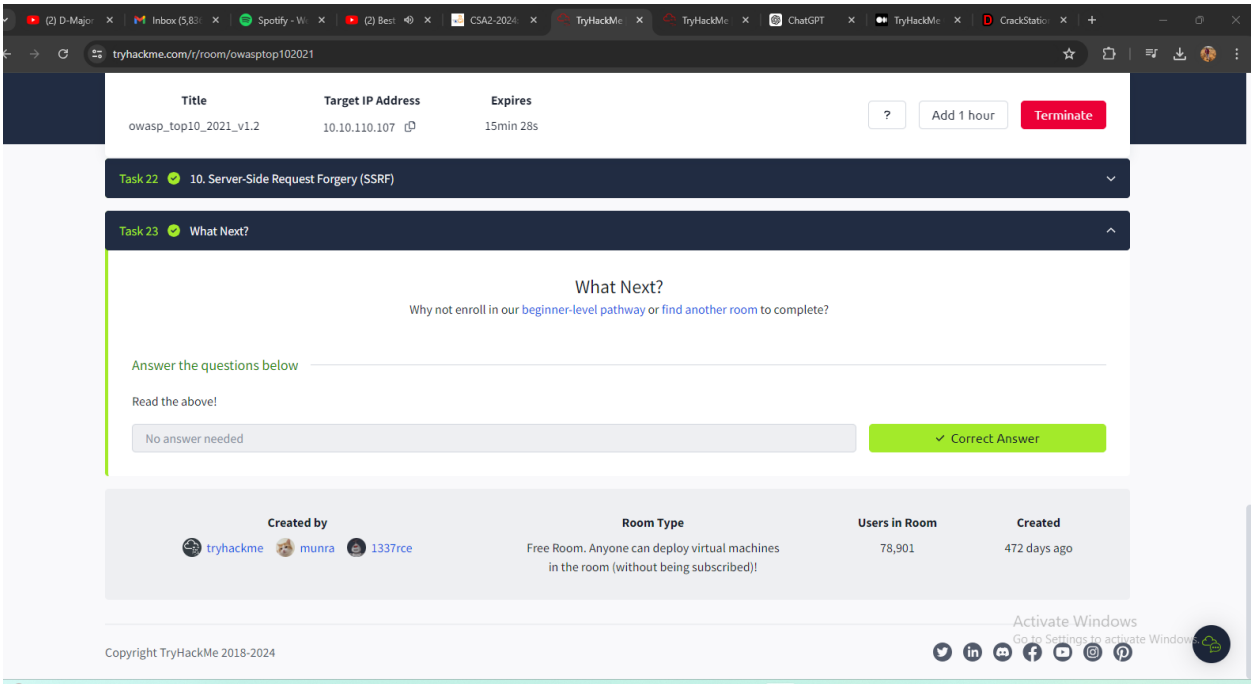
Task: Learn the significance of effective logging and monitoring in detecting and responding to security incidents.

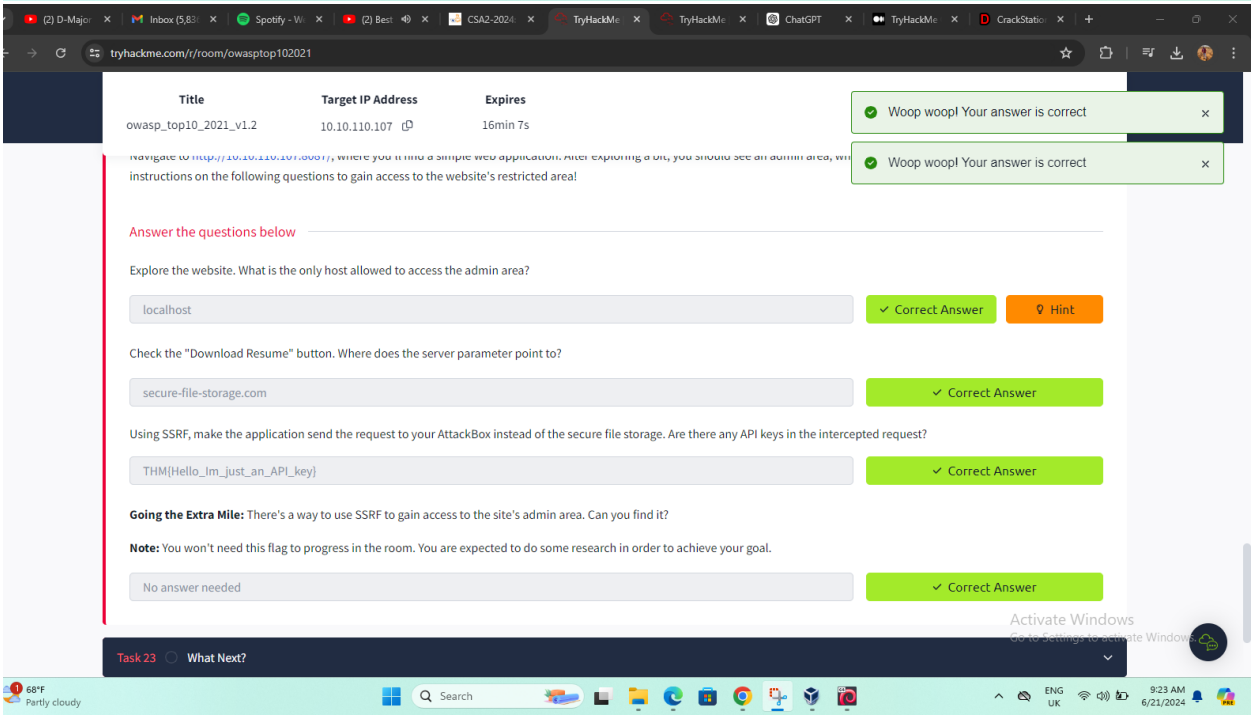
Server-Side Request Forgery (SSRF)

Task: Explore SSRF vulnerabilities, where an attacker can make requests to unintended destinations on behalf of the server.

cs-sa07-24019

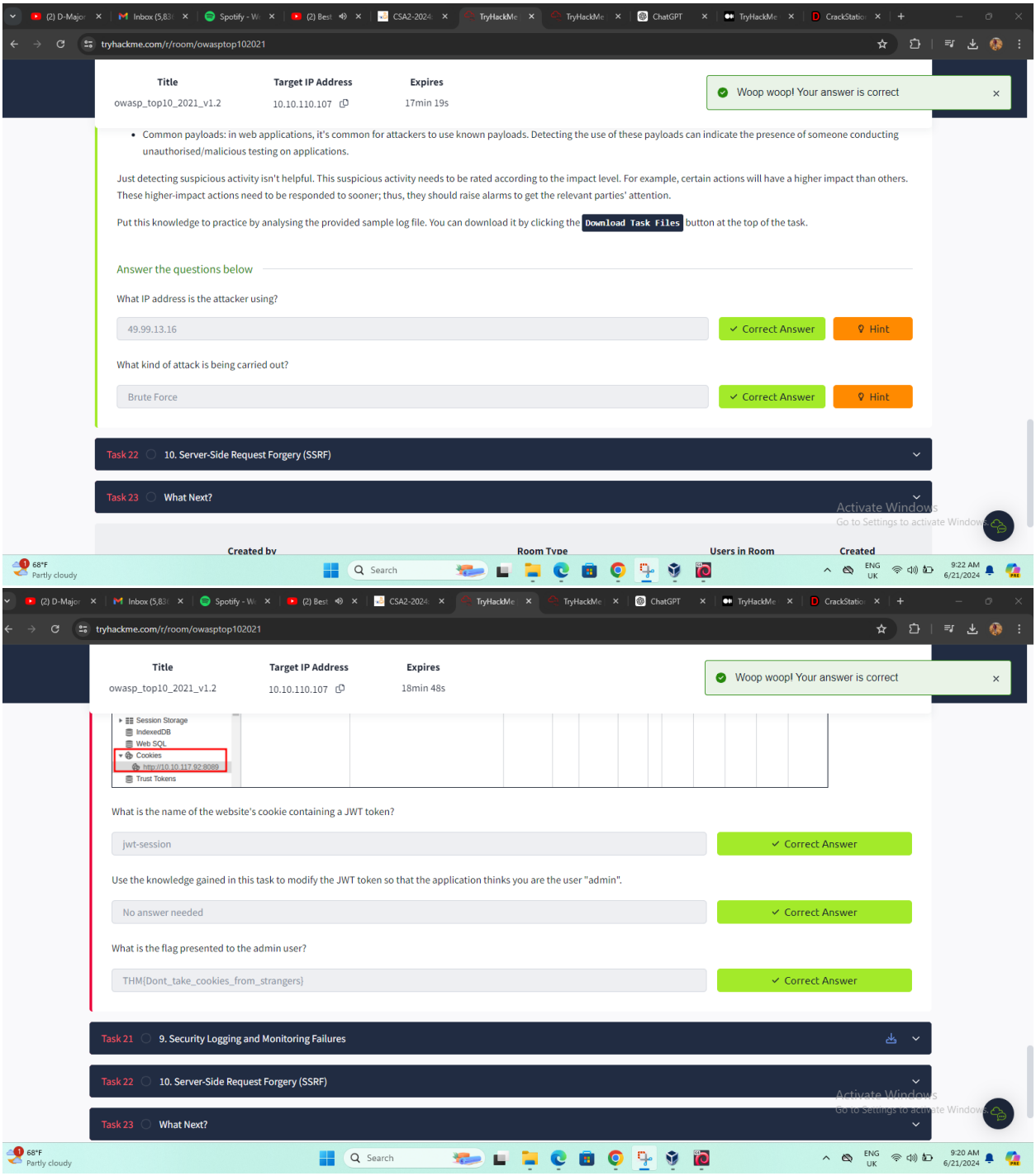
John_Mbithi_Mutave





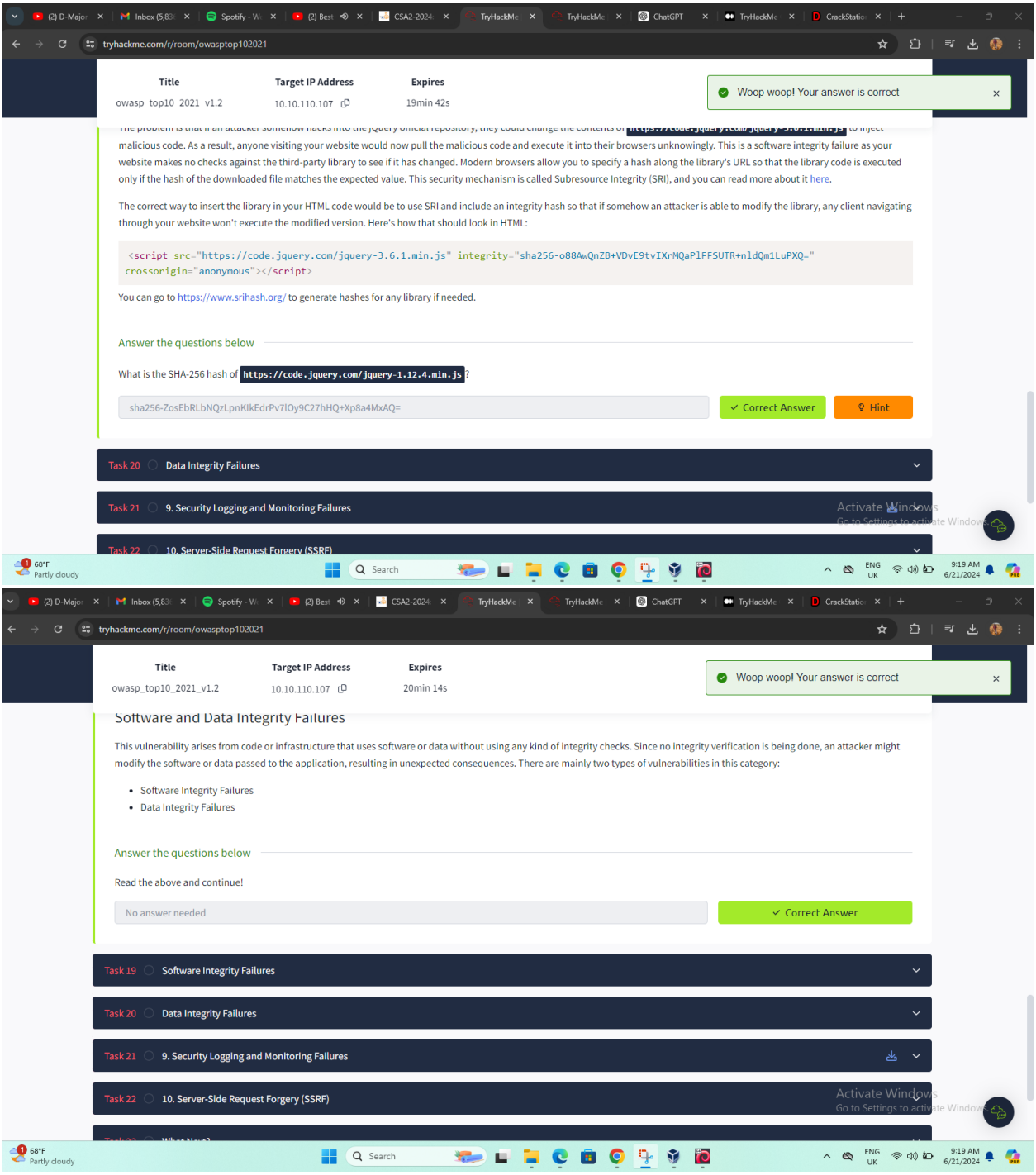
cs-sa07-24019

John_Mbithi_Mutave



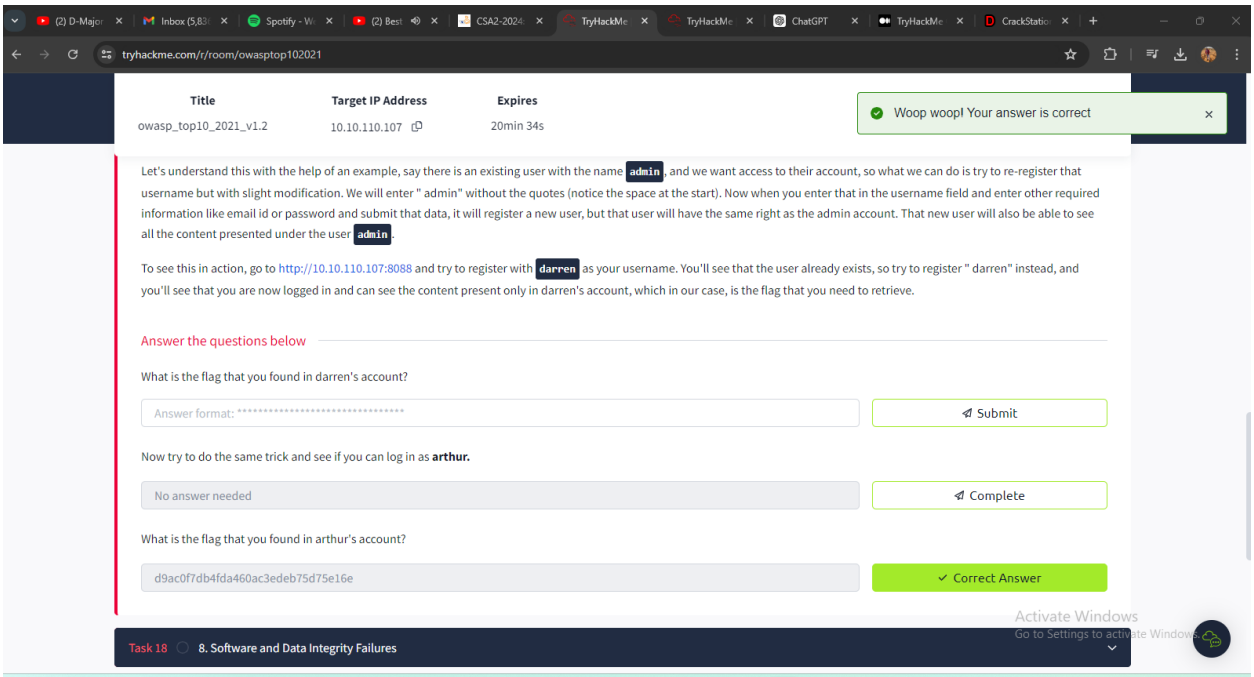
cs-sa07-24019

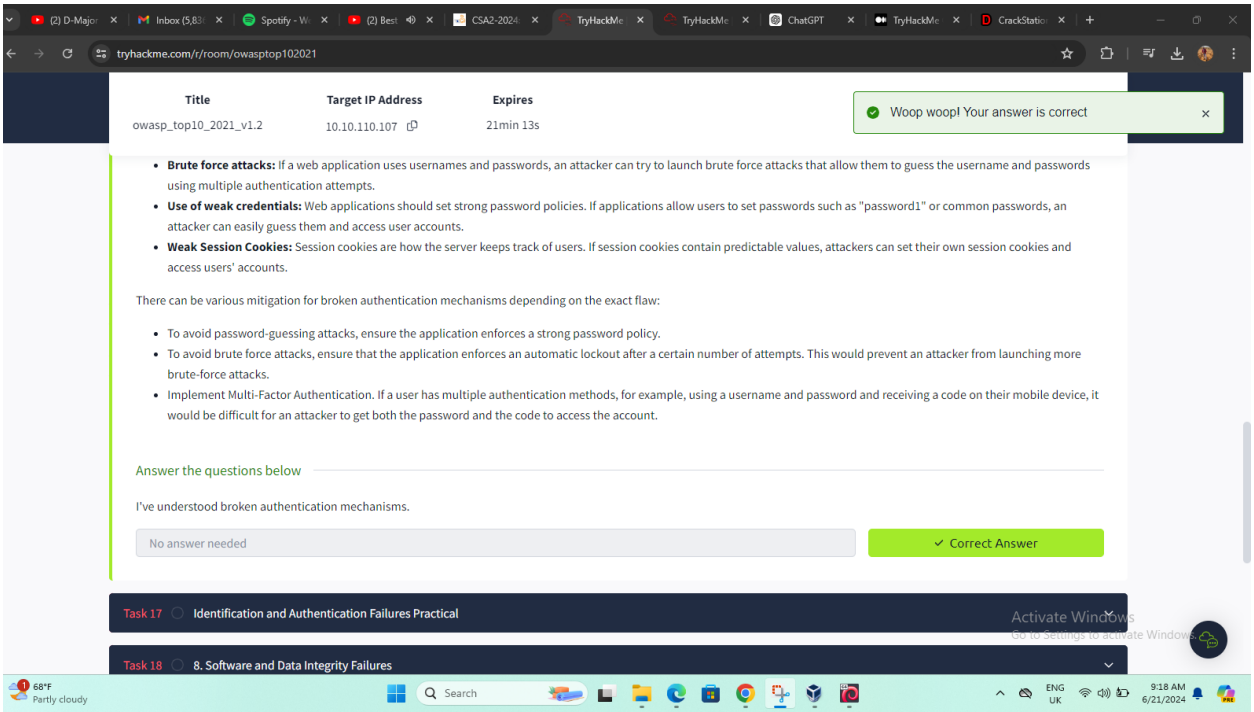
John_Mbithi_Mutave



cs-sa07-24019

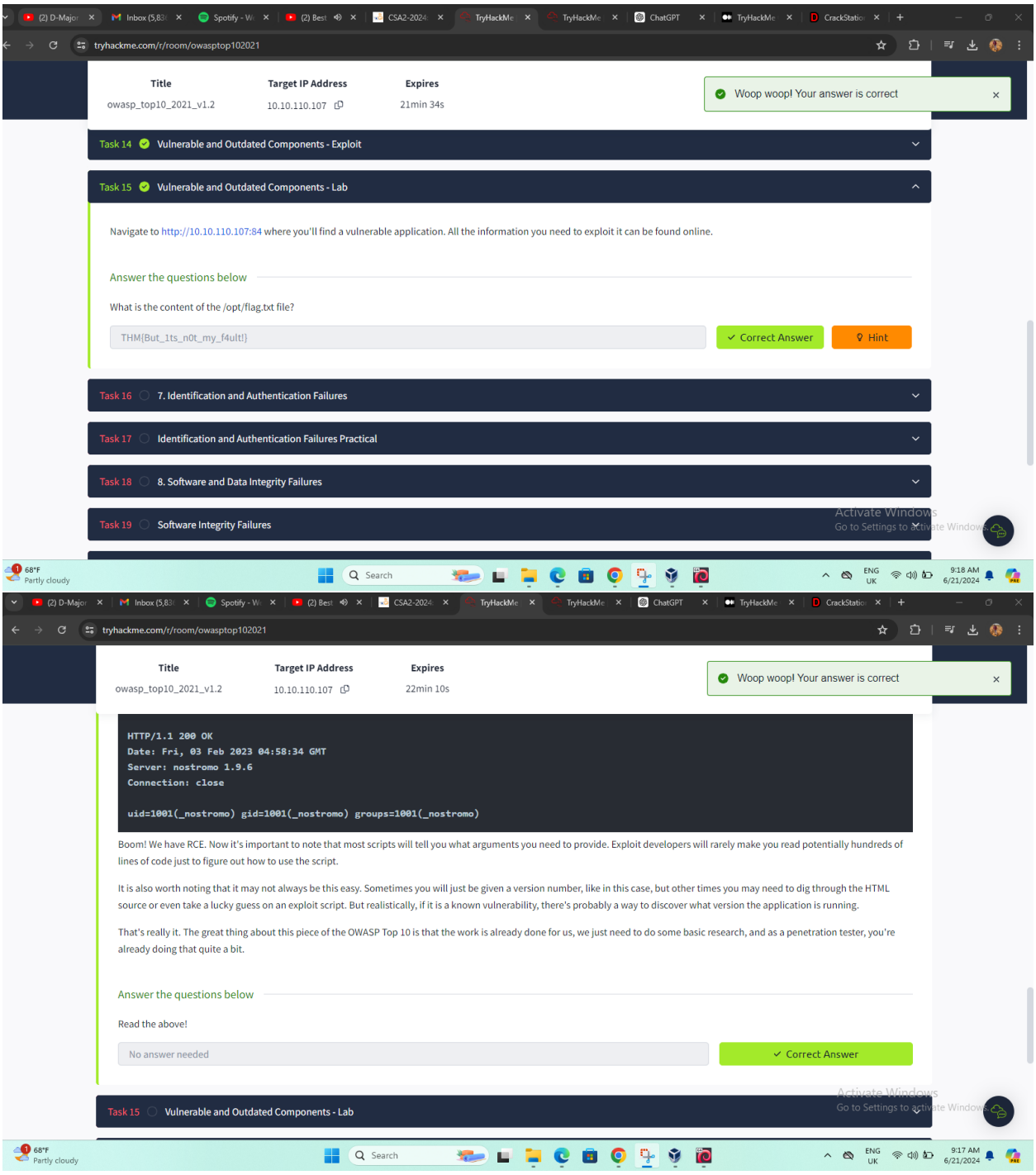
John_Mbithi_Mutave





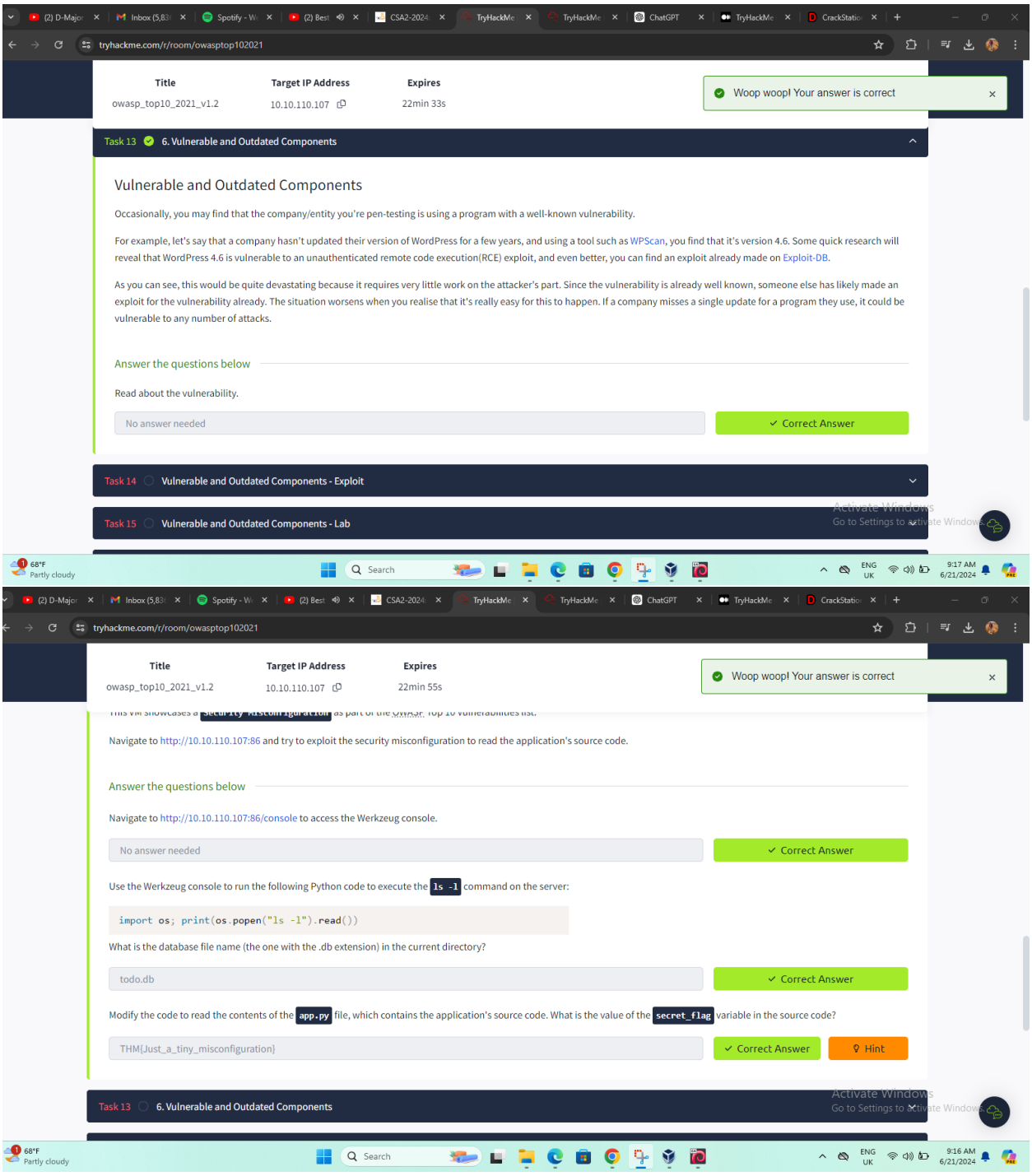
cs-sa07-24019

John_Mbithi_Mutave



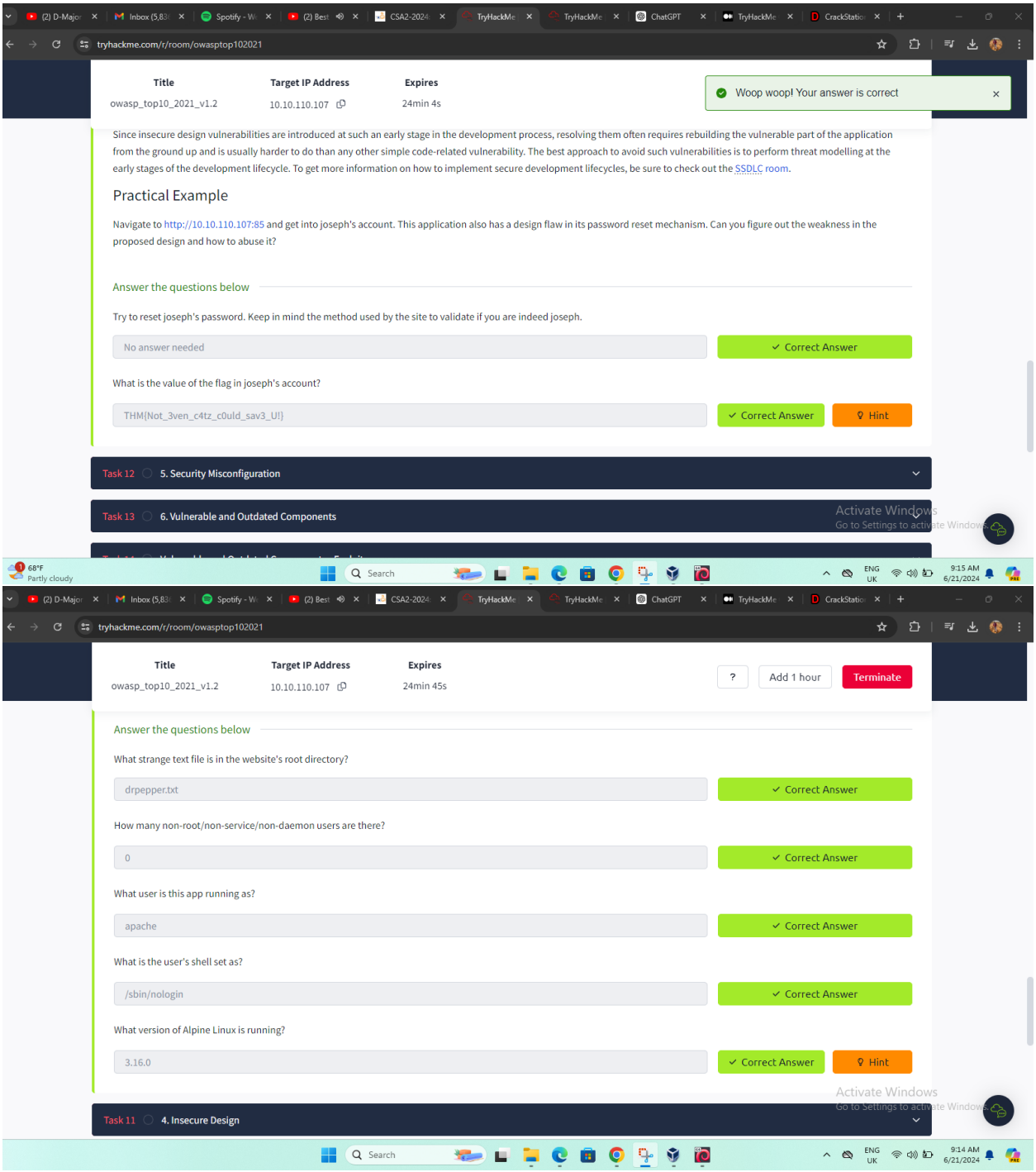
cs-sa07-24019

John_Mbithi_Mutave



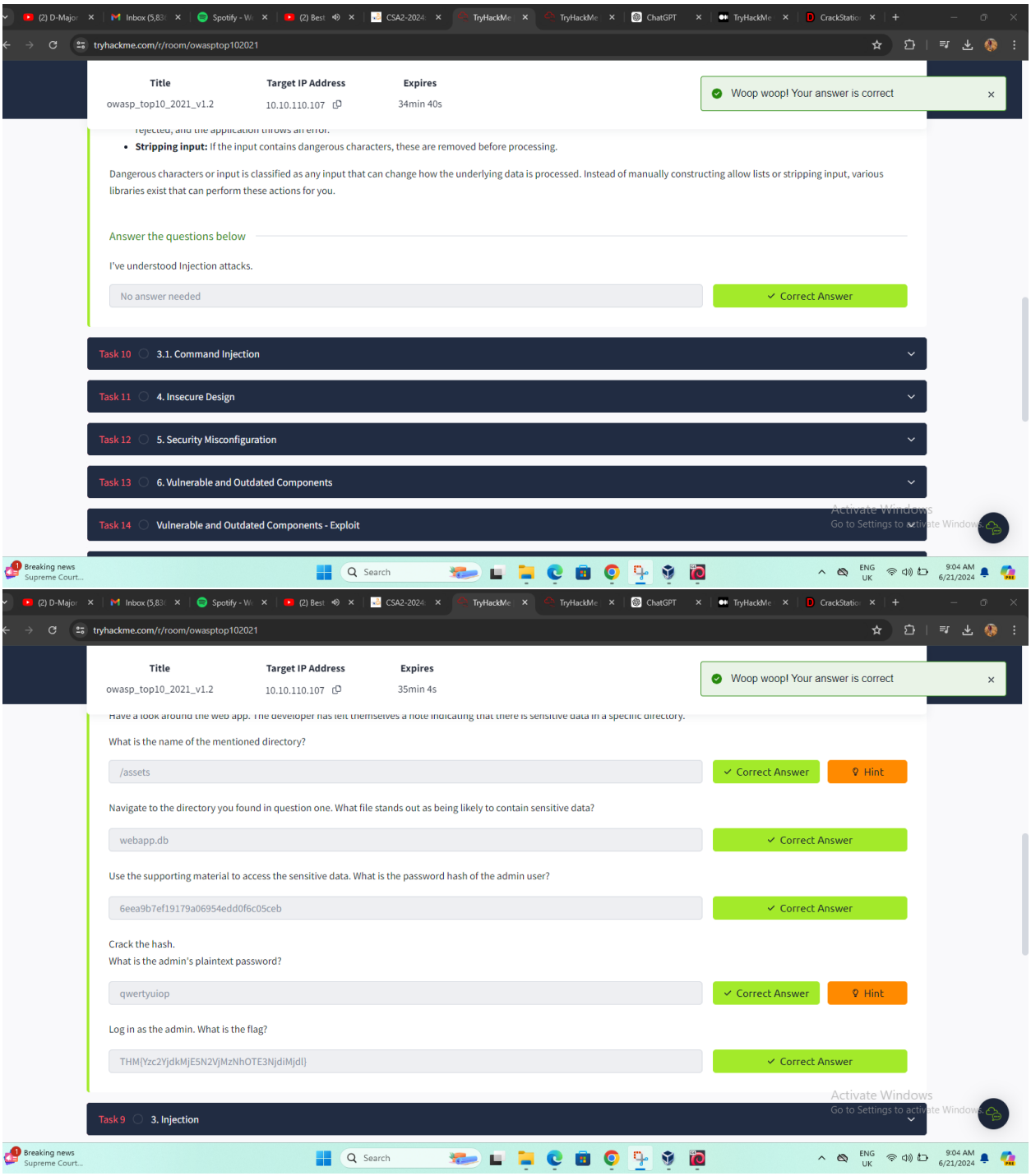
cs-sa07-24019

John_Mbithi_Mutave



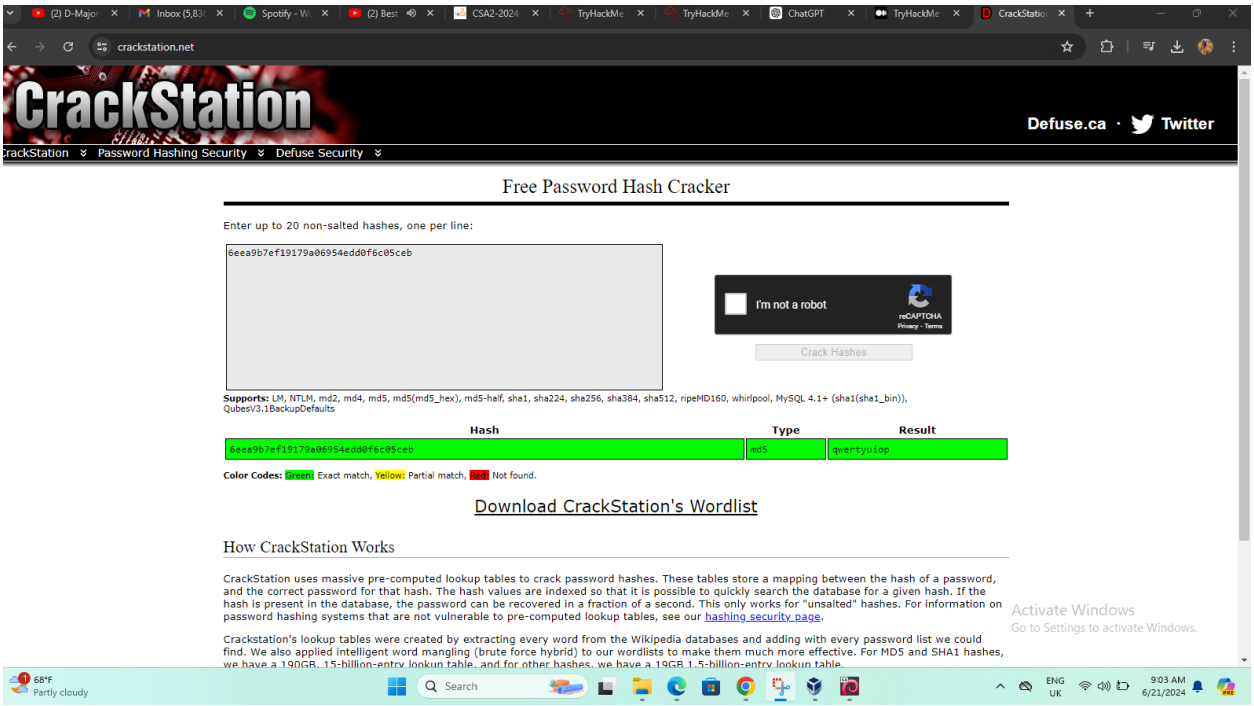
cs-sa07-24019

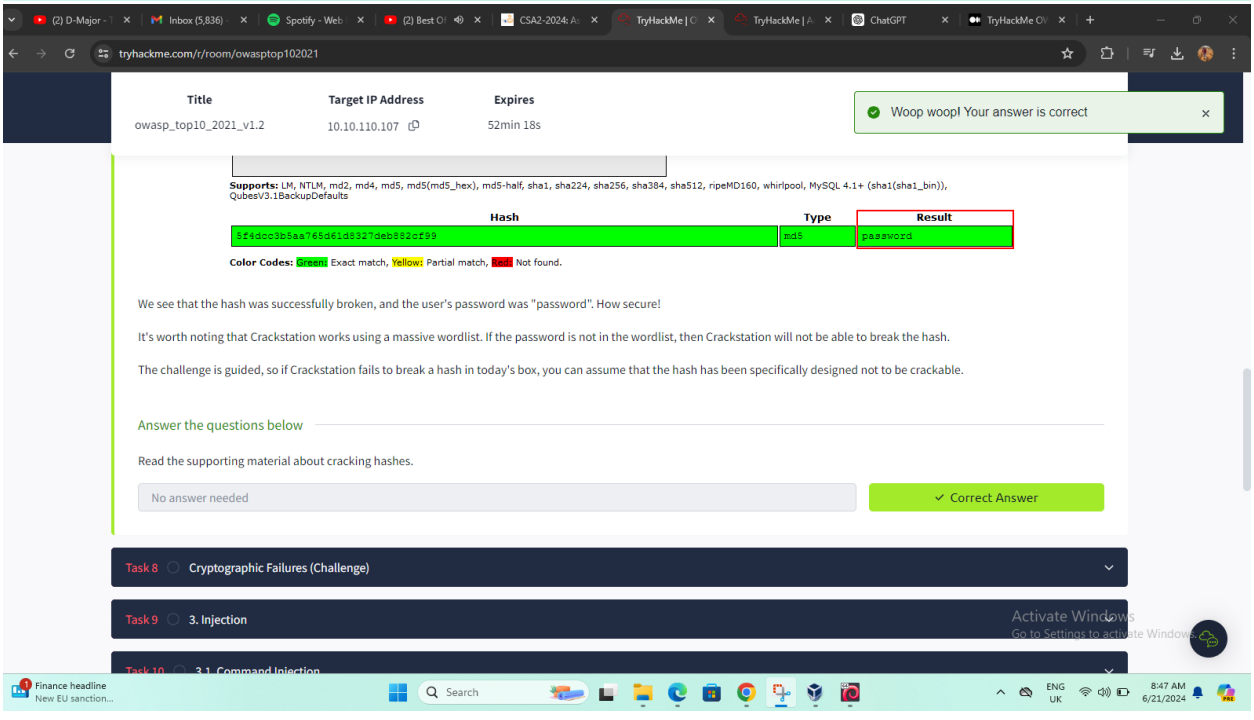
John_Mbithi_Mutave



cs-sa07-24019

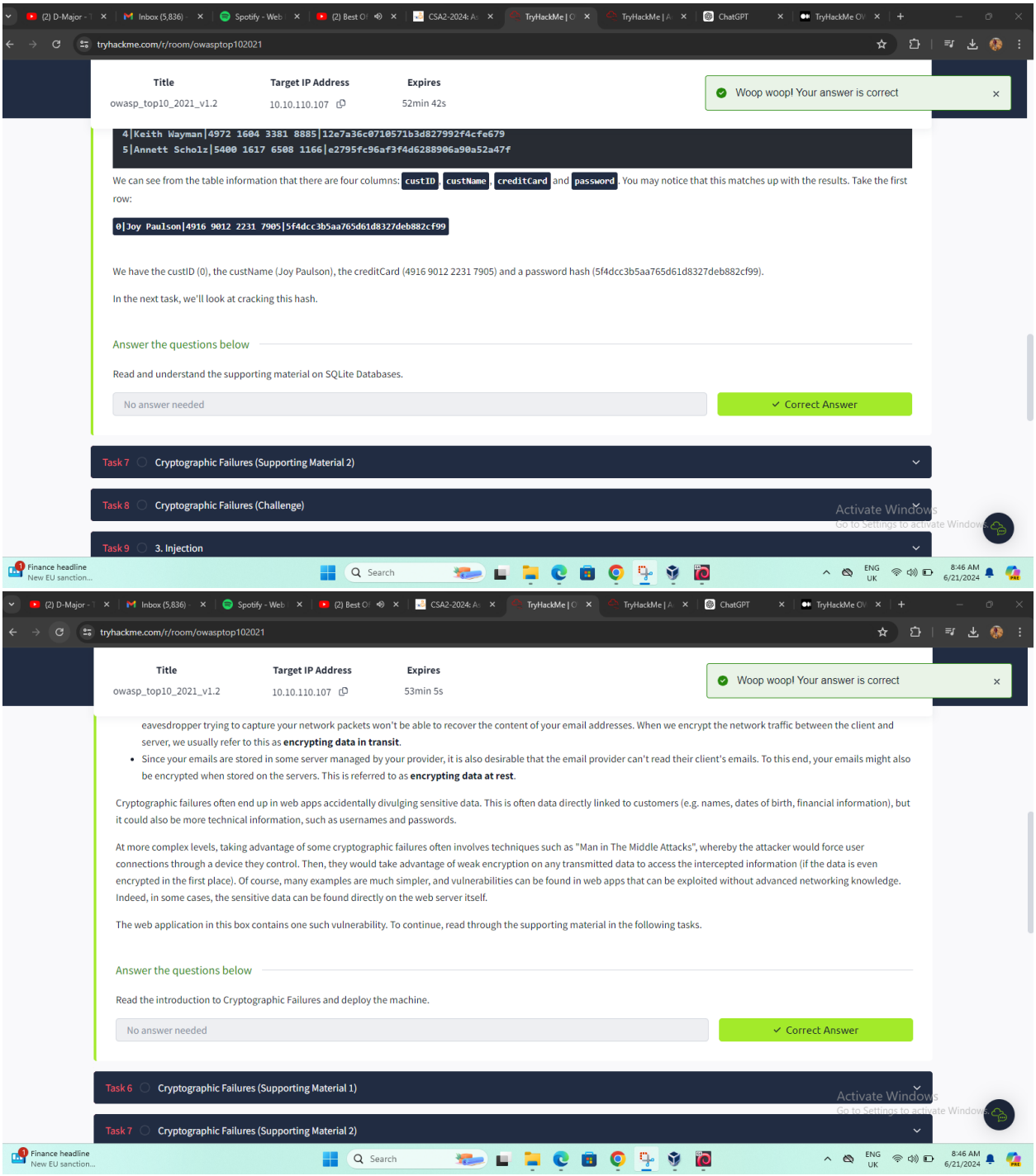
John_Mbithi_Mutave





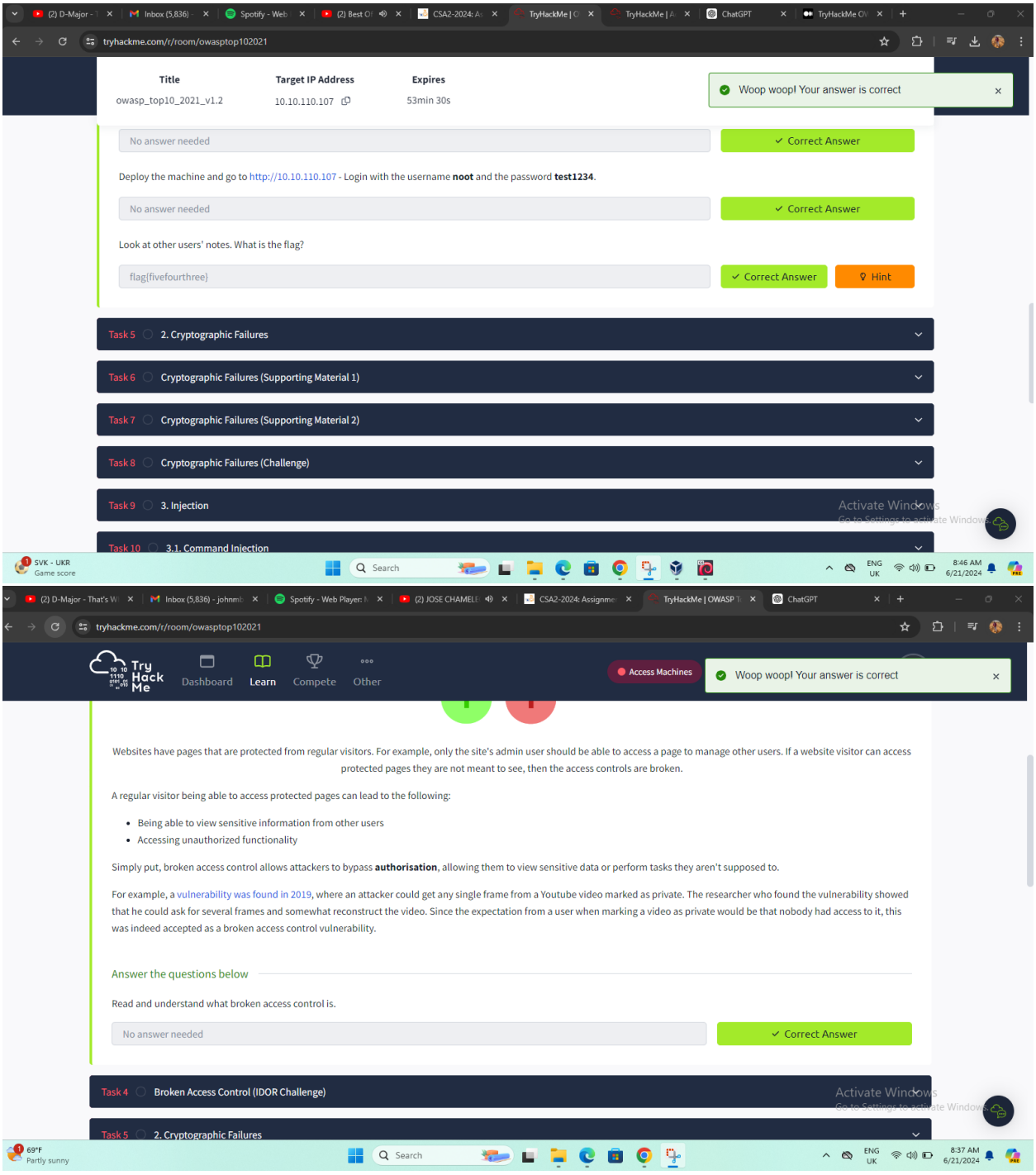
cs-sa07-24019

John_Mbithi_Mutave



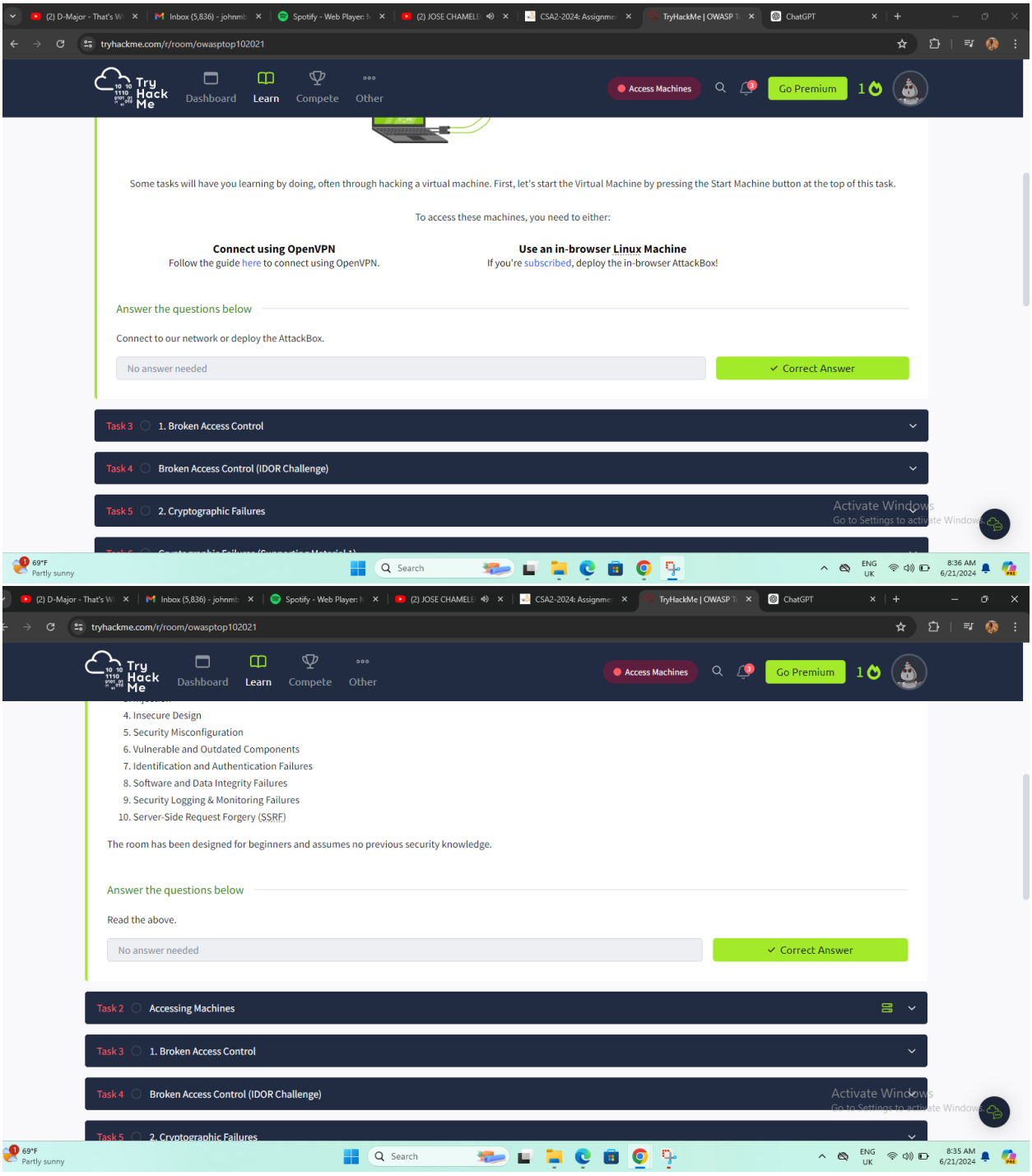
cs-sa07-24019

John_Mbithi_Mutave

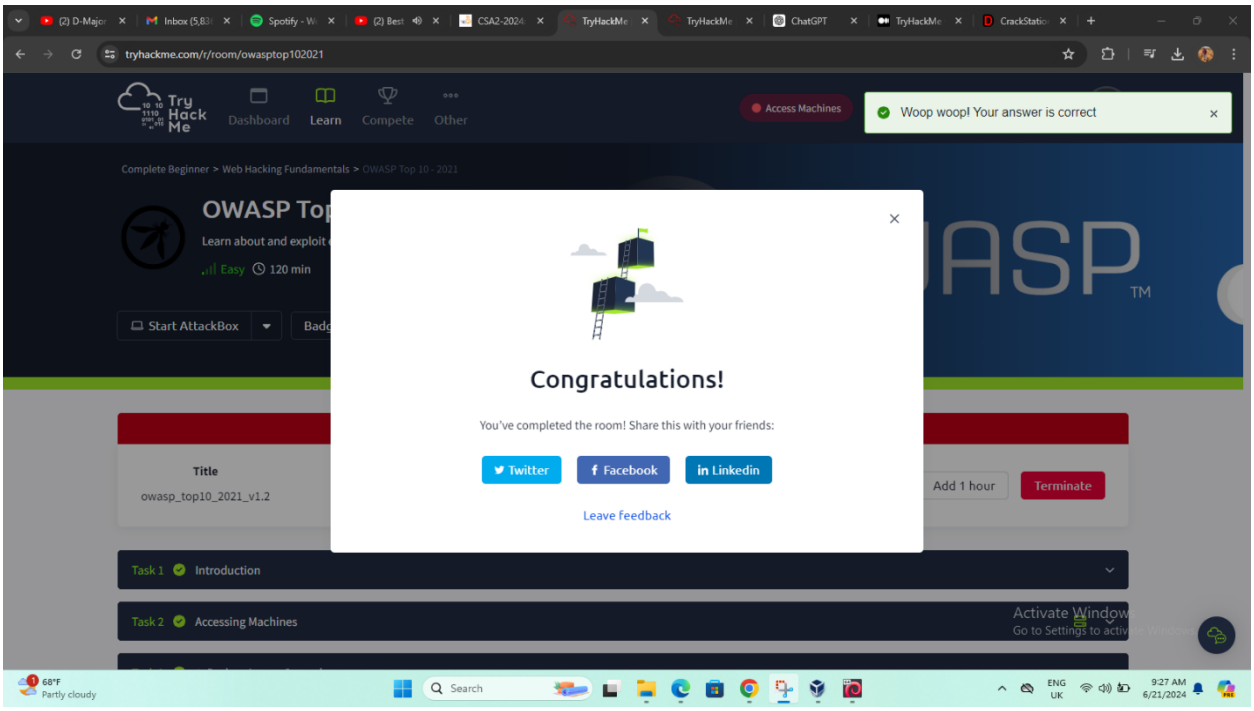


cs-sa07-24019

John_Mbithi_Mutave



cs-sa07-24019
John_Mbithi_Mutave



Shareable link - http://www.tryhackme.com/r/room/owasptop102021

Conclusion

Completing the OWASP Top 10 - 2021 course on TryHackMe provided a comprehensive understanding of the most critical web security risks. The combination of theoretical content and practical challenges allowed for the application of knowledge in real-world scenarios, enhancing both detection and mitigation skills. This training is crucial for staying current with web security practices and protecting applications from prevalent threats.

cs-sa07-24019
John_Mbithi_Mutave