**Step 3:** Cisco - Introduction to Cybersecurity

# A screenshot of a computer Description automatically generated

Reflection:

From Cisco’s Introduction to Cybersecurity, I learned how about cybersecurity is in our daily lives. I learnt a basic understanding of common cyber threats, basic security principles, and how to protect data. I learnt about how to protect personal and companys’ data.

# **Step 4: PortSwigger**

A screenshot of a computer

Description automatically generated

## 16 completed labs:

### Topic: SQL Injection

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

SQL injection vulnerability allowing login bypass

### Topic: Authentication

2FA simple bypass

Password reset broken logic

### Path traversal

File path traversal, simple case

### Topic: Access Control

Unprotected admin functionality

Unprotected admin functionality with unpredictable URL

User role controlled by request parameter

User role can be modified in user profile

User ID controlled by request parameter

User ID controlled by request parameter, with unpredictable user IDs

User ID controlled by request parameter with data leakage in redirect

User ID controlled by request parameter with password disclosure

Insecure direct object references

### HTTP Host header attacks

Basic password reset poisoning

Host header authentication bypass

### Reflection

During this topic, I learnt about hands-on experience with web vulnerabilities and how attackers exploit them. SQL injection labs showed how easily crafted inputs can manipulate queries, retrieve hidden data, or bypass login systems. These exercises taught me to always be careful about user input. From those labs, I learned how to access control and protect my password.

# **Step 5: The Booking system project**

Throughout the four phases of the Booking System project, I engaged in full-cycle penetration testing using tools like Kali Linux, Docker, Burp Suite, ZAP, Hashcat, and Hydra. In Phase 1, I tested the initial application version and identified major registration page vulnerabilities, followed by a second test round on an updated version. I documented flaws and improvements, and shared findings in the discussion forum. In the each pase, I performed advanced tests on a new application version, including password cracking and both dictionary and non-dictionary attacks via Burp and Hydra. I documented login weaknesses and conducted authorization testing using roles like Guest, Reserver, and Administrator. I also used ZAP, wfuzz, and http for broad scanning and enumeration of hidden or unlinked pages.

What worked:

ZAP automation and Burp’s attack tools gave precise insights. Docker made setup reliable across versions.

What didn’t work:

Some Hydra attacks were time-consuming without adjusted masks. Manual testing sometimes missed subtle issues without automation.

What took the most time:

Password cracking and full-page enumeration using wfuzz took the most effort due to trial-and-error and large wordlists.

What I learned:

I gained hands-on experience in structured penetration testing, web app security, and reporting. I learned to chain tools and techniques effectively to evaluate real-world systems and report findings professionally.

Reflection:

This project taught me how to apply a full pentesting workflow. I knew about from environment setup to attack execution and reporting. I learned to test not just for flaws but also how users and roles interact with the system, which is critical in real-world cybersecurity work.

# **Step 6: Logbook**

<https://github.com/ChenjingZhuang/Cybersecurity-and-data-privacy/tree/main>

Topic &Hours

Cisco - Intro to Cybersecurity - 9.0h

PortSwigger - 15.5h

Lectures / Workshops - 24.5h

Bookingsystem Project- 35.5h

**Total- 93.5h**

Reflection:

During the Cybersecurity and Data Privacy course, I gained a strong foundational understanding of key cybersecurity principles and tools. Through the Cisco modules, I explored real-world attack techniques and effective defenses. PortSwigger labs helped me apply theory in practical scenarios which are helpful for me to enhance my skills in identifying and exploiting web vulnerabilities. The Bookingsystem project allowed me to try secure coding practices and troubleshoot within real-world systems. Lectures and workshops deepened my experiences of cybersecurity's importance. Overall, this experience growed my technical skills and awareness of responsible data handling in the internet.