

Task4

As a cyber security generalist at CommBank, it's important to have a basic understanding of penetration testing. Penetration testing is a way to check the security of computer systems and networks by simulating an attack. This helps identify weaknesses in the system and evaluate the effectiveness of security measures. By regularly doing this, organisations can find and fix potential security problems before they can be exploited by bad people.

In this task, you will be completing the "Basic" web challenge from HackThisSite.org, which is an online platform that provides a safe and legal environment for students like you to improve their cyber security skills through a variety of challenges.

The challenge is divided into 11 levels and each level ranges from easy to difficult. The purpose of this challenge is to test your skills and knowledge in identifying vulnerabilities and exploiting them. By completing this challenge, you will gain a better understanding of how to identify and exploit vulnerabilities in web applications. Additionally, you will also learn how to apply this knowledge to real-world scenarios, which will help you improve your penetration testing skills. How exciting! Look at it like a game that helps you learn about web security.

After completing the challenge, you will need to create a pentest report detailing what you found and learnt, and give recommendations for how to better secure the web application. A penetration testing report is like a summary of the results of a security test. It shows any weaknesses or problems that were found during the test and suggests ways to fix them. This report is important because it helps organisations understand where they need to improve their security and how to do it. It also helps them comply with laws and regulations related to security. In simple terms, a pentest report is like a report card for a company's security and helps them pass security inspections. By having a good security posture, organisations can prevent data breaches, protect sensitive information, and maintain compliance with regulations and industry standards.