SIT182- Real World Practices for Cybersecurity T1 2019

Assessment Task 2 Problem Solving Task
Due: May 19th at 11.59pm.
Total Available Marks: 100, Weighting 20%

General Requirements

Please use the REPORT TEMPLATE provided in the assessments folder on CloudDeakin to complete this assessment.

- NO EXTENSIONS allowed without medical or other certification.
- LATE ASSIGNMENTS will automatically lose 5% per day up to a maximum of five days, including weekends and holidays. Assignments submitted 6 or more days late will not be marked and are given zero.
- You **MUST** use the SIT182 Assessment Task – *Deakin Wargames Custom Website* to complete this assessment available from http://ec2-18-191-11-183.us-east-2.compute.amazonaws.com
- NO work is saved or backed up on the Website – Make sure you keep a record of your steps and findings!
- Ensure you take screenshots of your work for evidence and that these are legible in your report.
- To complete this assessment you will need to do research, read the information provided on the Website and covered the theory and practical material for weeks 5-9.
- Your submission must be in a form readable by Microsoft Word.
- Each student is required to submit 1 problem solving task report. The report must not be more than 20 pages, each page must have margins no less than 2cm, and font size no less than 11 point. Oversized assignments will be penalised.
- Ensure you keep a backup copy of your work.
- Plagiarism is not tolerated. For information on Plagiarism and Collusion including penalties please refer to the link: http://www.deakin.edu.au/students/clouddeakin/help-guides/assessment/plagiarism
- The APA Referencing Style is to be used for this assignment where appropriate. https://www.deakin.edu.au/students/studying/study-support/referencing/apa-6

Help with the assessment

This solution for this assessment cannot be directly found using a 'Google' search. You must understand this is a challenge and need to apply your knowledge and problem solving skills to a series of cyber security concepts. Also make sure you don't share your progress or solutions with others.

It is important to understand that the assessment has been designed for everyone to pass. To achieve a higher grade is going to require a concerted effort by you.

If you require assistance please ask your instructors (Burwood students ask your practical demonstrator; Geelong and Cloud students ask Damien Hutchinson). We will **NOT** answer questions that are requesting answers or solutions. A question MUST be substantiated with evidence that work has been attempted relating to the question being asked.

Cybersecurity Scenario

Welcome to Deakin Wargames, an interactive assessment of your knowledge and understanding of vulnerabilities relating to computer security, internet security and privacy.

This challenge requires you to work through **ten levels**, each of which contains a vulnerability. In order to progress to the next level, you must exploit this vulnerability to obtain a password which will grant you access to the next level.

Marks are allocated based on your ability to progress through each level as well as your understanding of the vulnerability and the recommendations you make on how to fix the issue. That is, you are expected to fully understand how you completed each level; this will be assessed through the problem solving task report.

Problem solving task report

Each student is to submit a report of approximately 2000 words and exhibits following the rubric provided. The report **MUST** include **descriptions** and **evidence** of **results** of the **steps performed** in order to be eligible to be awarded maximum marks for each rubric criterion.

Just plainly stating the results will **NOT** be sufficient to receive full marks.

You will note that the weighting is higher for levels 0-3 to enable everyone to pass. The levels then get more complex enabling you to decide what grade you want to achieve.

You are required to identify vulnerabilities and perform associated attacks to ultimately gain access to level 10 of the website. There are 5 vulnerabilities listed below covered by the 10 levels.

The name of the vulnerability that corresponds to each level is provided for you!

- Information Leakage
- Directory Traversal
- Weak Encryption
- Cookie Manipulation
- SQL Injection

The following table provides guidelines on the information to be included for each vulnerability.

There needs to be 1 table completed per level.

	Vulnerability Name	Level No(s)	War Game Level

Affected resources:
Copy and Paste the URL here corresponding to the level.

Description of Vulnerability
Describe the *weakness or flaw* of the War game level.

Observation
This is the main section of your report; what you were able to ascertain/discover as a result of testing. You **MUST** state the steps taken to exploit the vulnerability.

Be sure to include a screenshot showing the level of the 'War Game' the vulnerability relates to. No more than 3 screenshots per vulnerability, and make sure to provide a description for the screenshots.

Focus on demonstrating your understanding of the vulnerability and importantly, your understanding of the exploit you used.

Screenshot

Level Credentials – here you list the credentials to be used to gain access to the 'War Game' level(s) relating to the vulnerability. Level 0 Password:	**Impact Analysis** What is the threat? What can an attacker do through exploiting this vulnerability? If nothing, could they use this as an entry point to pivot and perform further attacks?

Recommendation
What are your recommendation(s) to mitigate this issue?