WEEK 6 – TASK 6.2D

Distinction Task.

Release Date: 27 April, Due Date: 11 May, End Date: 17 May.

Learning Outcomes

In this task, you will learn about two new cyber security threats including SQL Injection and CSRF. You will learn both about the theory behind these threats and you will get hands dirty by trying them out using Kali Linux and Damn Vulnerable Web Application (DVWA).

Instructions

An **answer sheet template** is available on OnTrack as a `**Resources**'. Please download the answer sheet and fill it with your answers. This task must be uploaded both to OnTrack and the unit site. See the last page of this document for more information.

We are fighting the good fight. We are on the good side of the cyber world, and we are in this together. We learn together and from each other.

Help is always available in SIT182. Please go to **Discussions** and ask your questions about this task in **Task 6.2D**. All students are encouraged to participate and help peers with their questions. Helping others is a great way to learn and think about aspects you may have overlooked. You can also seek help from tutors during online and face-to-face pracs. However, please note that pracs are primarily aimed at Pass-level tasks, and tutors will only aim to provide you with suggestions about the more advanced tasks.

Note: Distinction and HD tasks are more challenging and are less guided. The only source of support for these tasks is Discussions on the unit site. Students who achieve Distinction and HD in this unit are top performers in Bachelor of Cyber. You will need to show dedication, professionalism, and ambition to complete these challenging tasks.

References: In cyber security, one of the most common referencing styles is **IEEE** – however, you can use any referencing style in this unit. Please refer to unit site > Content > Referencing - Hints & Tips for more information. *Submissions are automatically checked for plagiarism using Turnitin, and the unit staff have no authority to help if you violate academic integrity.*

In the following, you will learn about two well-known cyber security attacks that are not covered in SIT182 lectures. Both of these threats are important topics in cyber security domain and commonly referred to in job interviews. You will need to do your research to understand the nature of these threats and how they can be prevented and try them out against DVWA within your Kali VM. Word counts are **suggestions**, and you will not be penalised for extra or fewer words as long as the tutor is convinced you have understood the concepts covered. However, excessively long or short answers will not be accepted. Please ensure that you include references for your answers.

Setup

Ensure that your Kali has access to the Internet. Then, download and install Damn Vulnerable Web Application (DVWA) from the following URL on your Kali VM:

http://www.dvwa.co.uk/

Ensure that you set DVWA Security to “Low”.

Question 1 - SQL Injection

1. What does SQL stand for? How is it different compared with a DBMS?
2. In your own words, define what is an SQL injection attack and what vulnerabilities allow an SQL injection attack to occur? *(Suggested word count: up to 400 words)*
3. What are some of the recent attacks that have been initiated by SQL injection? How were they conducted? *(Suggested word count: up to 400 words)*
4. Can a firewall prevent an SQL Injection attack? Briefly discuss and support your answer. *(Suggested word count: up to 300 words)*
5. Go to the SQL Injection tab on DVWA and show a successful SQL injection attack. Include screenshots or link to a screencast confirming that you have successfully conducted an SQL injection attack.

Question 2 - CSRF

1. What does CSRF stand for? How does this attack work? *(Suggested word count: up to 300 words)*
2. How can a CSRF attack be prevented? [3 approaches are enough] *(Suggested word count: up to 300 words)*
3. Go to the CSRF tab on DVWA. Show a successful CSRF attack. Include screenshots or link to a screencast confirming that you have successfully conducted a CSRF attack.

4. What is a browser Cookie (or HTTP cookie)? What is it used for?
5. Go to the XSS reflected tab on DVWA. Type “<script>alert(document.cookie)</script>” in the textbox and click Submit. What happens? What information are your shown? Include screenshots or link to a screencast confirming that you have successfully conducted an XSS attack.

6. What is the difference between CSRF and XSS (in terms of attack and prevention)? *(Suggested word count: up to 300 words)*
7. Can an Intrusion Prevention System such as Snort prevent CSRF and XSS attacks? Briefly discuss and support your answer. *(Suggested word count: up to 300 words)*

Question 3 – Interview questions

A good practice for preparing interviews is to have your own question bank as you study different topics during your course. You can browse online and find interview questions related to the topics that you learn about whether at university or on your own. This is also useful to cross-check what you are taught about is of relevance in the real world and prepares you for your career ambitions. To give this a try: find and list 2 interview questions related to SQL Injection and 2 interview questions related to CSRF online.