# Learning Guide Unit 8

# Description

Learning Guide Unit 8

# Table of contents

# Overview

**Unit 8: Security by Design**

**Topics:**

- Common Vulnerability Scoring System (CVSS)
- Common Configuration Scoring System (CCSS)
- Common Misuse Scoring System (CMSS)

**Learning Objectives:**

By the end of this Unit, you will be able to:

1. Define Common Configuration Scoring System (CCSS)
2. Define Common Misuse Scoring System (CMSS)
3. Define Common Vulnerability Scoring System (CVSS)
4. Compare CMSS, CVSS and CCSS based on their metrics sets

**Tasks:**

- Read through the Learning Guide and the Reading Assignment
- Complete the Discussion Assignment by posting in the Discussion Forum
- Respond to three of your fellow classmates' posts in the Discussion Forum
- Make entries to the Learning Journal
- Take and submit the Self-Quiz
- Read the Unit 9 Learning Guide carefully for instructions on the Final Exam
- Take the Review Quiz
- Complete and submit the anonymous Course Evaluation

# Introduction

*Vulnerability Measurement and Scoring Systems*

To provide standardized methods for vulnerability measurement and scoring, three specifications have been created, one for each of the categories of system vulnerabilities defined in Section 1.1. The first specification, the Common Vulnerability Scoring System (CVSS), addresses software flaw  vulnerabilities. The first version of CVSS was introduced in 2004, and the second version became available in 2007. CVSS has been widely adopted by the Federal government, industry, and others. CVSS was originally intended for use in prioritizing the deployment of patches, but there has been considerable interest in applying it more broadly, such as using its measures as inputs to risk assessment methodologies.

The second vulnerability measurement and scoring specification is the Common Configuration Scoring System (CCSS). CCSS was designed for measuring and scoring software security configuration issue vulnerabilities. CCSS uses the basic components of CVSS and adjusts them to account for the differences between software flaws and security configuration issues.

The Common Misuse Scoring System (CMSS), the third of the vulnerability measurement and scoring specifications, is defined in this report. CMSS addresses software feature misuse vulnerabilities. CMSS is largely based on CVSS and CCSS, and it is intended to complement them.

# Reading Assignment

- Mell, P., Scarfone, K., & Romanosky. (2007, June). *A complete guide to the common vulnerability scoring system*. FIRST. https://www.first.org/cvss/v2/guide
  - You can read the pdf here.

**Reference as needed**

- **NIST IR 7502**: The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities. Retrieved from: http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7502.pdf
- **NIST  Interagency Report 7864**: The Common Misuse Scoring System (CMSS): Metrics for Software Feature Misuse Vulnerabilities. Retrieved from: https://www.nist.gov/publications/common-misuse-scoring-system-cmss-metrics-software-feature-misuse-vulnerabilities

# Discussion

Define CMSS and reason why CMSS and CCSS have similar sets of temporal metrics, but CVSS has a different set?

You must post your initial response (with references) before being able to review other student's responses.  Once you have made your first response, you will be able to reply to other student's posts.  You are expected to make a minimum of 3 responses to your fellow student's posts.

# Learning Journal

**Assignment instructions**

Consider the two scenarios in both the parts (A) and (B) and answer both the questions accordingly.

**Part A:**

**Scenario**: Under cross-site scripting, the attacker creates a fake site (that looks exactly like genuine bank website) with malicious URL parameters that triggers the vulnerability. A Vulnerability Assessment Specialist finds that their bank is vulnerable to reflected cross-site scripting (XSS).

If a bank user gets tricked into the fake URL, then the attack becomes successful. The malicious code is only able to access information associated with the bank's vulnerable website due to Same Origin Policy (SOP) restrictions in web browsers.

> 1) What is "Scope" metric? Will the Vulnerability Assessment Specialist set the Scope metric (CVSS metric) to 'Changed' or 'Unchanged'? Why?

> 2) What shall be considered as the impacted component here?

**Part B:**

**Scenario**: Due to a vulnerability in the database server, a remote and authenticated user can inject malicious SQL code that runs with high privileges in a way that prevents the execution of arbitrary SQL statements.

> 1) Define the purpose of "Access Vector" and "Privileges Required" CVSS metric.

> 2) For the stated scenario, what shall be the value of "Access Vector" and "Privileges Required"? Why?

**Submission instructions**

- Create a report to your supervisor answering both the questions in part A and part B.

- Your response must be 500-750 words, double spaced using Times New Roman – 12 points font.

- Use sources to support your arguments. Use APA formatting for your citation and reference list. For assistance with APA formatting, view the [Learning Resource Center: Academic Writing](#).

**This assignment will be assessed by your instructor using the rubric available on the assignment page located on the course homepage.**

# Self-Quiz

The Self-Quiz gives you an opportunity to self-assess your knowledge of what you have learned so far.

The results of the Self-Quiz do not count towards your final grade, but the quiz is an important part of the University's learning process and it is expected that you will take it to ensure understanding of the materials presented. Reviewing and analyzing your results will help you perform better on future Graded Quizzes and the Final Exam.

Please access the Self-Quiz on the main course homepage; it will be listed inside the Unit.

# Review Quiz

The Review Quiz will test your knowledge of all materials learned in this course. The results of this quiz will not count towards your final grade, but will help guide you in more thoroughly reviewing necessary topics and adequately preparing for the Final Exam.

Please access the Review Quiz under Unit 9 on the main course homepage; it will be listed inside the Unit.

# Checklist

- Read through the Learning Guide and the Reading Assignment
- Complete the Discussion Assignment by posting in the Discussion Forum
- Respond to three of your fellow classmates' posts in the Discussion Forum
- Make entries to the Learning Journal
- Take and submit the Self-Quiz
- Read the Unit 9 Learning Guide carefully for instructions on the Final Exam
- Take the Review Quiz
- Complete and submit the anonymous Course Evaluation