



Republic of the Philippines
BATANGAS STATE UNIVERSITY
The National Engineering University

Alangilan Campus

Golden Country Homes, Alangilan Batangas City, Batangas, Philippines 4200

Tel Nos.: (+63 43) 425-0139 local 2222 / 2223

E-mail Address: cics.alangilan@g.batstate-u.edu.ph | Website Address: <http://www.batstate-u.edu.ph>

College of Informatics and Computing Sciences

Name: Catalo, Francis A.

Score: /

Year and Section: 4th Year – IT 4107

Date:

Laboratory Activity 3

Using CVSS Calculator - FIRST Website

Objective:

You will use the Common Vulnerability Scoring System (CVSS) calculator from the FIRST website to assess a given security vulnerability. You will learn how to evaluate the base metric group of the CVSS and determine the appropriate vector string for the vulnerability.

Scenario:

A critical vulnerability has been discovered in a web-based payroll system used by your company. The vulnerability allows an attacker to execute arbitrary code remotely by sending a specially crafted request to the payroll server. This exploit can give the attacker complete control over the affected system, including the ability to access sensitive employee data. The company has tasked you with assessing the severity of this vulnerability using the CVSS calculator from the FIRST website.

Task:

1. Visit the CVSS calculator on the FIRST website:
CVSS Calculator – FIRST
2. Based on the provided scenario, analyze the vulnerability and determine the following base metric groups: (Provide a comprehensive explanation for your chosen values and explain how the severity score is determined.)

Attack Vector (AV): Network (N)

Explanation: The vulnerability is remotely exploitable through the network, as the attacker can send a specially crafted request to the payroll server over the network.

Attack Complexity (AC): Low (L)

Explanation: Exploitation of this vulnerability does not require any specialized conditions or advanced skills. It can be done by an attacker using readily available tools.

Privileges Required (PR): None (N)

Explanation: No privileges are required for the attacker to exploit the vulnerability. The attacker can perform the exploit without any authentication.

User Interaction (UI): None (N)

Explanation: The attacker does not need any interaction from a user. The exploit is executed directly by sending the crafted request to the server.

Scope (S): Changed (C)

Explanation: Exploitation of the vulnerability leads to control over the payroll system, affecting both the payroll system and potentially other systems connected to it.

Confidentiality (C): High (H)

Explanation: Exploiting the vulnerability gives the attacker full access to sensitive employee data, leading to a severe breach of confidentiality.

Integrity (I): High (H)

Explanation: The attacker can modify or delete critical data, potentially impacting the integrity of the payroll system's operations and records.

Availability (A): High (H)

Explanation: The attacker can disrupt the availability of the payroll system, making it unusable for an extended period.

Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



Republic of the Philippines
BATANGAS STATE UNIVERSITY
The National Engineering University
Alangilan Campus

Golden Country Homes, Alangilan Batangas City, Batangas, Philippines 4200
Tel Nos.: (+63 43) 425-0139 local 2222 / 2223

E-mail Address: cics.alangilan@g.batstate-u.edu.ph | Website Address: <http://www.batstate-u.edu.ph>

College of Informatics and Computing Sciences

3. Use the CVSS calculator to calculate the overall severity score of the vulnerability.

CVSS Score:	10.0	Rating:	Critical
-------------	------	---------	----------