Dance Registration System

Security Report

Group Number: 2

CPSC 488 Section 01

**TABLE OF CONTENTS**

**1 INTRODUCTION………………………..……………………………………………………3**

* 1. DESCRIPTION……………………………………………………………………………….3

**2 SCOPE………………………..………………………………………………………………...3**

2.1 ITEMS ADDRESSED………………………………………………………………………...3

**3 SECURITY…………………..………………………………………………………………....3**

3.1 ISSUE IDENTIFICATION…………………………………………………………………...3

*3.1.1 Weak Passwords*…………………..……………………………………………......*.*3

*3.1.2 Excel Files*……………………………………………………………………….......4

Vulnerabilities in Excel Upload...…………………………………………………4

*3.1.3 Duplicate Emails*……………..……………………………………………………...4

Account Hijacking…………………………………………………..…………….4

Data Exposure…………………………………………………..………………....4

*3.1.4 Permissions/Roles*…………………………………………………………………...4

Sensitive Information…………………………………………………….………..4

3.2 PREVENTATIVE MEASURES…...…………………………………………………………4

*3.2.1 Passwords*………………………………………………………………………......*.*4

First Logon………………………………………………………………………...4

Character Constraints……………………………………………………………...4

*3.2.2 Excel Files*……………………………………………………………………….......5

Vulnerabilities in Excel Upload………………………………...…………………5

Specific Value Checks…………………………………………………………….5

*3.2.3 Account Emails*…..………………………………………………..………………...5

*3.2.4 Permissions/Roles*…………………………………………………………………...5

Access Permissions to Data…………………………………….…………………5

1 INTRODUCTION

* 1. **Description**

The purpose of this report is to describe in detail the security vulnerabilities found in the program for the Dance Registration System. These given security vulnerabilities have been identified, processed, and handled accordingly. Throughout this document, the vulnerabilities are described where they are found and the best common practices to prevent these security concerns.

Most data contained in this program pertains to personal information or information that could be sensitive to the Dance Studio. The measures below discuss how the information given can be kept private and secure.

2 SCOPE

**2.1 Items Addressed**

This document depicts security concerns that have raised questions during testing. Below will describe the concerns themselves and how they relate to the program. Additionally, there is a description of the implementation to avoid these vulnerabilities.

3 SECURITY

**3.1 Issue Identification**

3.1.1 Passwords

Each user account holds sensitive information that only the respective user should be able to access. Passwords are the key to being able to access that information, and the security of the accounts relies on the strength of these passwords. Each user account is set up with a default password of “1234.” This is a textbook weak password and needs to be changed before the user can enter any sensitive information.

Weak passwords can expose an account to brute force attacks, dictionary attacks, and be easily exposed by password cracking tools. With any attacks, figuring out “1234” or any simple password would take less than a second to hack into the account. Because of the sophistication of tools and attacks, users need to make sure they have secure passwords, so their data stays protected.

3.1.2 Upload Excel Files

The admin user has permission to upload an admin file containing information for the admin users, manager users, and the studio location information. The user information pertains to their email, first and last names, phone number, and userID. The location data contains the addresses and phone numbers for each studio. This information is specific to the program and the administrative users. Managers will upload files pertaining to the activities, charges per class, instructor personal information, and parent/child personal information. Therefore, all the excel files uploaded into the program contain quite sensitive information and information that is specific to the program. Also, due to the format being in excel, there is a higher risk of macros and SQL injection.

3.1.3 Account Emails

Having duplicate account email addresses could pose many security concerns. Accounts hold sensitive information and duplicate emails could potentially compromise the security of them. Account hijacking could occur if two users had the same email address and one user attempted to reset the password of the other account, gaining unauthorized access. On the other hand, data exposure could also occur if the studio sent out an email to one user, but another user with a duplicate email address received the email. Emails could contain information such as name, child information, address, as well as banking and payment information. Both of these outcomes result in a breach of privacy and security.

3.1.4 Roles/Permissions

As a registration system, certain actions need to be performed by users with specific credentials. Being a user-based system, some of the user data falls under PII (Personal Identifiable Information) which should only be accessed, viewed, modified, and or deleted by users with the correct qualifications. Other data pertaining to the studio itself should also only be accessed, viewed, modified, and or deleted by administrative users of the studio company.

All data contained can be considered sensitive information – whether it be to the users, clients, employees, and studio.

**3.2 Preventative Measures**

3.2.1 Passwords

In order to best protect the users’ accounts, the system requires every user to change their password upon first logon. As mentioned above, every account is set with a default password of “1234,” which is an easily hackable password. After attempting to log in with the default password, the system will prompt the user to create a new password. The account cannot be logged into until the password is changed from the default.

Not only does the system require users to create a new password, but the password must follow specific security constraints. Passwords must be at least eight characters long, have an upper and lowercase letter, at least one number, and at least one symbol. Requiring a password with those constraints is a good practice to reduce the likelihood of an attack. Adding the bare minimum of requirements increases the time to hack into the account from less than a second up to two or more hours. The more unique characters, symbols, and numbers in a password, the stronger the password will be, further decreasing the chances of the account getting hacked.

3.2.2 Upload Excel Files

Due to high risks when uploading the Excel files, the preventative measure in place is to ensure that the correct files are being uploaded. To implement this, the first cell (A1) of each Excel sheet has a specific entry that the program checks for prior to reading and uploading the given file. For example, for the manager to upload the Parent/Child Excel file, the file must contain the value “PARENTCHILD” in the first cell. The program will check this cell first and ensure that values are equal. There is a check in place for every file prior to uploading and reading.

3.2.3 Account Emails

Duplicate email addresses are an easy way for an attacker to gain unauthorized access to someone else’s account. Because of this concern, the system does not allow two users with the same email address to register. A check is implemented that throws an error if a user tries to register with an email that already has an account associated with it. By implementing this check, the chance of account hijacking and data exposure is lessened.

3.2.4 Permissions/Roles

As mentioned previously, the data and information contained in the program and database is associated with users and the studio and can be considered sensitive information. Therefore, to ensure that the qualified personnel are the only users granted access to the given information, the WebSecurityConfig File contains rules that only permit certain users with their granted roles upon login.

This is implemented by restricting access to specific logons. Once an administrator is logged in, all mapping that follows is only accessible by the administrator. The same logic follows for Managers. These are the only two roles that have the permissions allowing them to edit, modify, and delete data and information. Users that try to access webpages that are not granted access to receive a 403 permission denied error in return.