NURSING SKILL TRACKER SYSTEM SECURITY REVIEW

Development Project

Marissa Cleroux

Winter Semester

April 14th, 2020

Table of Contents

Introduction

The Nursing Skills Tracker System (NST) will be developed using the .NET Core stack. As such, data security practices related to the stack must be followed and implemented. Data security measures must be taken to protect the data of NST users. This document will discuss the security measures implemented related to user authentication/authorization, encryption, data privacy and confidentiality, SSL, back up of data, database security, common attacks, and testing techniques.

User Authentication

User authentication into NST will be handled by the Application Management System (AMS). AMS provides a login service that authorizes and authenticates users for applications hosted by Heritage College. NST will send the user's credentials to the login service, AMS will then return if the user has been successfully authenticated.

NST will also use a cookie-based authentication service implemented by .NET Core to persists the user's session and to keep track of whether a user is still authenticated or not.

User Authorization

User authorization when logging in to NST is will be partly handled by AMS. Each user's roles are stored in AMS and can be easily configured in the AMS interface. NST will send the NST project code along with the user's username to determine if the user is authorized to use NST. This will ensure that only the specified roles (teachers, students, clinical teachers, and coordinators) can access NST. NST will then ensure the user is part of the nursing department to prevent non-nursing department users from using the application.

Specific pages will only be accessible by users with specific roles. NST will enforce specific page access by role-based authorization. When a user logs in to NST, AMS will return all roles belonging to the user. These roles are will then be added to the user's session. Before a page is accessed, the user's roles will be checked, if they do not meet the role requirements, they will be forbidden from accessing the page.

Encryption

Encryption will not be used on any data stored by NST. The data that will be stored by NST is not classified as requiring such measures. Passwords will not be stored by NST. NST will use HTTPS in the production environment

Confidentiality of Data

Protecting student's personal information will be of the utmost importance. As such, student information will be obfuscated in the dev and test environments. Developers will be unable to access real student information.

NST will also protect the confidentiality of students by only letting coordinators have access to every student's skill set. Teachers and Nursing Technicians will only be able to access their current cohort's skill set.

Use of a Security Certificate (SSL) on the Server

SSL will only be used in the test and production environment. SSL certificates are handled by the I.T. department.

SSL will be used in the test and production environments to encrypt requests and responses between the client and the server. This will enable credentials to be securely communicated between the client and server without any worry of sniffers picking up the credentials.

Backup of Data

Backups are extremely important as a fail safe in case of attacks which lock or destroy data, as is common with the evermore popular ransomware attack. Backups will be handled by the I.T. department of Heritage College. NST will not have any automatic or manual backup plan on its own.

Privacy Considerations

Ensuring user's privacy is protected is very important. Therefor NST will not store or access any data it does not require. Information like gender and birthdates are not important or required for NST's functionality so this information will not be stored in the NST database.

Database Security

The test and production databases are inaccessible from outside the Heritage College network. This adds a layer of protection for the database.

The NST database must have the most granular access possible to ensure good security practices and to protect other systems if NST is used as an attack vector into the Heritage College servers. App pools will be used so that no usernames and passwords are stored in the connection string of the NST application.

Protection Against Path Truncation and Reverse Directory Transversal

NST will not vulnerable to path truncation or reverse directory traversal. The IIS server NST will be deployed on prevents directory traversal.

NST will not serve up any files based on user input and this further protects NST from path truncation or reverse directory traversal, as this is the most common vector for those type of attacks.

Protection Against Cross-Site Scripting and SQL Injection

NST will use Entity Framework Core (EF) which protects against SQL Injection attacks. Along with EF, NST will not use any raw SQL queries and will thus be protected from SQL Injection attacks.

Cross-Site Scripting (XSS) is always a concern when it comes to web applications. NST will be particularly vulnerable to it as it will dynamically serve up content based on user input. NST should make use of HTML encoding to ensure XSS cannot take place when rendering user input on the application.

Input Validation

NST will use model validation whenever accepting input to ensure data meets the requirements. With the proper protections used for XSS and SQL injection, input is not a huge security risk, however, NST

should also cleanse input being accepted so that no malicious actors could exploit vulnerabilities in this manner.

Testing Techniques

Proper testing must be done to ensure NST has limited vulnerabilities, as security is never 100% and there is always a risk of zero-days. In the test environment and with the consent of the administrators, the system should be tested by executing common attacks. The most common attack vectors can be found here: https://owasp.org/www-project-top-ten/ with appropriate ways to test for these vulnerabilities also described.

Conclusion

The main security vulnerabilities for NST are the potential for XSS and the lack of information concerning backups. However, it is important that future NST developers guard against and ensure the system is not vulnerable to the most common attack vectors found in the OWASP top ten linked in “Testing Techniques.”