Final Project BDAT 1001 Information Encoding Standards

Professor: Nital Shah

Group 9:

- Bhavesh Waghela
- Deema Al Dogom
- Pablo Martinez

April 1st , 2023

Project Summary

- Authorization is a crucial aspect of web application development, especially when it comes to protecting user data and maintaining security.
- Role-based access control is a useful approach to authorization that allows us to define different levels of access for different user roles.
- We found that ASP.NET Core provides built-in functionality for implementing role-based access control, making it easier to develop secure web applications.
- Testing is an essential part of the development process, and in this project, launching multiple browsers to simulate different users helped us to ensure that the app was working as intended.
- By building this app, we have gained experience in developing web applications with ASP.NET Core and implementing authorization features, which can be applied to future projects to create more secure and functional web applications.

About Us

- Bhavesh Waghela
  - A software developer with robust problem-solving skills and proven experience in creating e-commerce software solutions in a test-driven environment.

- Deema Al Dogom
  - Business intelligence developer with hands on experience in implementing and delivering reports, dashboards, data warehousing, and analytics.

- Pablo Martinez
  - Bachelor, Biomedical Engineering.
    Skills: Python, Microsoft Excel and Power BI for Data Analytics.

Part 1: Demonstration

- Demonstration will be done during group meeting with Professor Nital Shah.

Part 2 Security Technologies Recommendations

A company is asking for you to act as a consultant on a project. They have some questions that they hope you can answer:

- How can we transfer personal data securely within their network?

- FTP/FTPS – Good for transferring computer files

FTP Service may provide anonymous FTP access, data transfer can be done in 3 modes: stream mode, block mode and compressed mode.

SFTP – Good for securely transferring SSN

User ID and password are required to connect to the server, the connection is encrypted and has more options than nay other file sharing system.

- HTTP/HTTPS – Good for web communication

Data communication from WWW, HTTP has functions as a request-response protocol in the client-server computing model.

Part 2 Security Technologies Recommendations - Continued

- What security protocol is best for transferring personal files?

- SFTP – SSH/secure file transfer protocol

SFTP uses encryption and cryptographic hash functions to make sure your data is no readable to anyone during file transfer, also uses a single port for connections to the server.

SSH (Secure Shell) keys or User ID and Password to connect to the server.

This can provide a secure connection to transfer files on both the local and remote system.

Security SFTP provides faster file transfer than other protocols

Provides two methods of authentication

SFTP use a single port number for communication making it firewall friendly.

Part 2 Security Technologies Recommendations - Continued

- Can we encode and encrypt images?

Yes, images can be encoded using Base64 for fast and easy way of transferring files.

- Encoding. We can encode images to Base64, the process of encoding images into base 64 is an easy method of transferring image data using plain text encoding.

- Encryption. It can be done by using AES (Advance Encryption Standard) where a single key is required and is considered as a fast encryption method, and RSA (Rivest-Shamir-Adleman) uses two keys one private and another public one, which can only be decrypted by the private one and is considered a fast encryption.

Part 2 Security Technologies Recommendations - Continued

- Our database cannot be moved from the site and we need to be able to access it externally using a secure API. Can you explain the architecture of a secure API?
- The first layer is authentication, which ensures that only authorized users can access the API. This can be achieved using techniques such as API keys or OAuth2; which is a widely-used authorization framework that is often used in the context of secure APIs. It provides a standardized way for users to grant permissions to third-party applications to access their data or perform actions on their behalf, without requiring the user to share their login credentials directly with the third-party application.
- The second layer is authorization, which determines what actions the user can perform once they are authenticated. This can be achieved by defining different levels of access based on user roles or permissions.
- The third layer is encryption, which protects data as it is transmitted between the API and the client. This can be achieved using SSL/TLS encryption.
- The fourth layer is rate limiting, which prevents users from overwhelming the API with requests. This can be achieved by setting limits on the number of requests a user can make over a given time period.

Part 2 Security Technologies Recommendations - Continued

- Can you recommend a secure framework for coding an API?

- Java Spring MVC (Model, View, Controller) is a secure framework for coding APIs that handles controllers, implementable HTTP requests, has and equivalent rest controller for building REST API, is scalable, covers an extensive ecosystem and allows decouple the framework for easier execution.
- Spring Framework, which is an open-source framework for Java. The Spring Framework includes built-in security features such as authentication, authorization, and encryption, as well as support for SSL/TLS encryption.
- Django REST framework, which is a powerful and flexible toolkit for building APIs with Python. The Django REST framework includes built-in security features such as authentication and permissions, as well as support for SSL/TLS encryption.
- For coding an API in C#, the ASP.NET Core framework is a secure and powerful choice. ASP.NET Core includes built-in security features such as authentication and authorization and also provides support for SSL/TLS encryption.

Part 2 Security Technologies Recommendations - Continued

- What data interchange format should we use while transferring data between locations?

- JSON (JavaScript Object Notation) is a popular and widely supported data interchange format that can be used for transferring data between locations. It is a lightweight format that is easy to read and write and is supported by many programming languages and frameworks.
- Another popular data interchange format is XML (Extensible Markup Language), which is a more structured format that can be used for transferring complex data. It is also widely supported and can be used in a variety of contexts.

Part 2 Security Technologies Recommendations - Continued

- How should we store our data in our many locations?

- One approach to storing data in multiple locations is to use a distributed database system such as Apache Cassandra or Amazon DynamoDB. These systems are designed to handle large volumes of data and can distribute data across multiple nodes to improve performance and scalability.

- Another approach is to use a cloud storage service such as Amazon S3 or Google Cloud Storage, which provides a simple and scalable solution for storing large amounts of data in multiple locations. These services also include built-in security features such as encryption and access control to protect data.

- A hybrid approach can also be used, where some data is stored locally on-premises and some data is stored in the cloud. This approach can provide the benefits of both local and cloud storage, such as faster access to frequently accessed data and greater scalability and flexibility for less frequently accessed data.

Part 2 Security Technologies Recommendations - Continued

- What are the ethical concerns related to the transmission of personal data?

- Maintain confidentiality. Personal data can include sensitive information such as medical records, financial information, and personal identifiers such as social security numbers, which can be used for identity theft or other malicious purposes. It is important to ensure that personal data is properly protected and secured to prevent

- Another ethical concern is transparency. Individuals have the right to know what personal data is being collected about them, how it is being used, and who it is being shared with. Transparency can help build trust between organizations and individuals and can also help individuals make informed decisions about how their personal data is being used.

Thank you