**MoneyLion Test application Project**

**Software Architecture Document**

**Version 1.0**

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 13-02-2021 | 1.0 | Software Architecture Document | Mohammedarief |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Software Architecture Document**

**1. Introduction **

#### **1.1 Purpose**

This document provides an architectural overview of the system, using a number of different architectural views to depict different aspects of the system. It is intended to capture and convey the significant architectural decisions which have been made on the system.

#### **1.2 Scope**

This Software Architecture Document provides an architectural overview of the simple web application form with authentication which includes user details such as SSN,DOB,Name and Email address. The C-Registration System is being developed using asp.net,IIS web server, MSSQL and azure for hosting.

**2. Architectural Representation **

This document presents the architecture as a series of views; use case view, There is no separate implementation view described in this document.

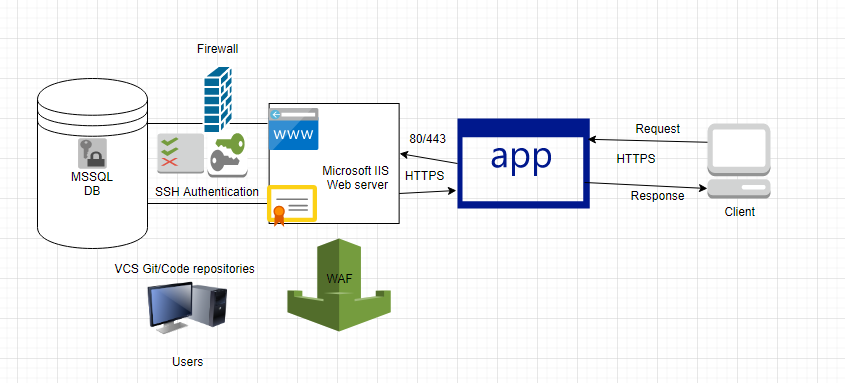
**4. Use-Case View **

A description of the use-case view of the Moneytestapplication. It also describes the set of scenarios and/or use cases that have a substantial architectural coverage (that exercise many architectural elements) or that stress or illustrate a specific, delicate point of the architecture.

* The Moneytestapplication use cases are:
* Login
* Statusmessage
* Resetpassword confirmation
* Reset password
* Register confirmation
* Register
* Logout
* Login
* Lockout
* Forgotpasswordconfirmation
* Forgotpassword
* Confirmemailchange
* Confirmemail
* Accessdenied
* Changepassword
* Email
* Index
* Manage
* Setpassword

These use cases are initiated by the user.

**4.1 Architectural Design **

****

**Webserver - IIS 10**

**Asp.net 3.1.11**

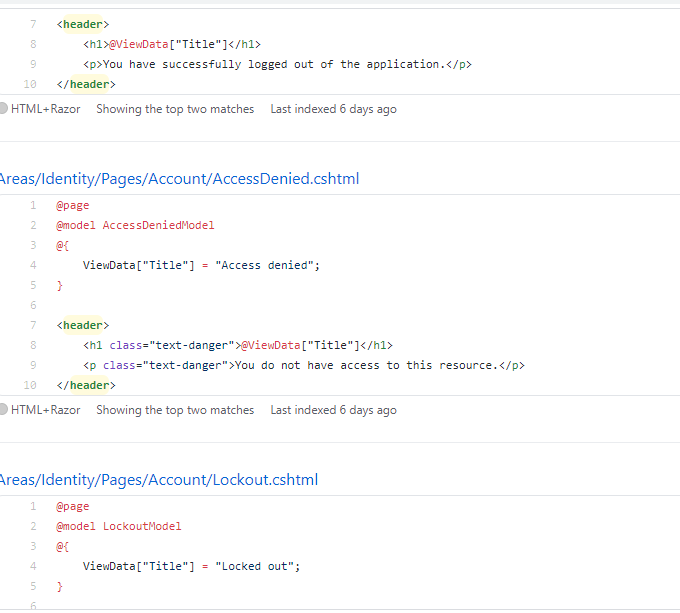
**MSSQL- 8.0.15**

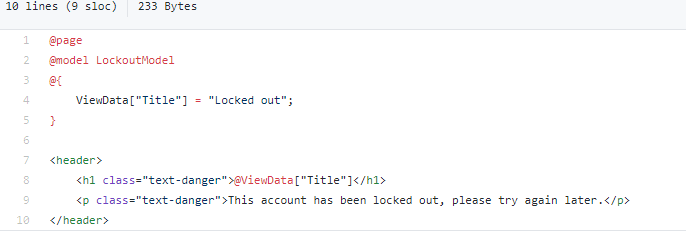
**Key Security Implementations:**

Created a contact form application using Asp.net MVC framework. Implemented access control, i.e. authentication for the application, requiring a user to authenticate first before the user is authorised to use the application.After successful authentication, the application presents a form interface to update and edit a user’s details, comprising of SSN,Name,DOB and email address.

For authentication included below security controls

1. Account lockout for burteforce attack
2. Strong password policy of using 8-14 characters includes special characters,numbers and alphabets.
3. Cookie protected using secure flag and http only flag.
4. Forgotpassword and recovery not built due to limited features but it can be configured securely by enabling flag for recovering passwords through password recovery.

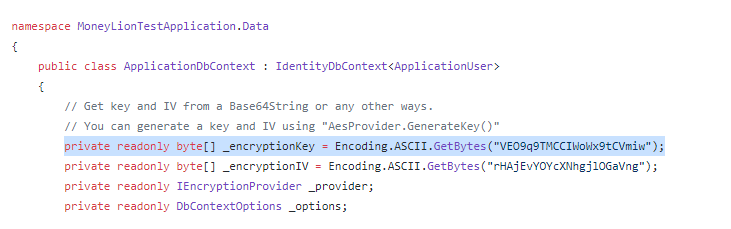
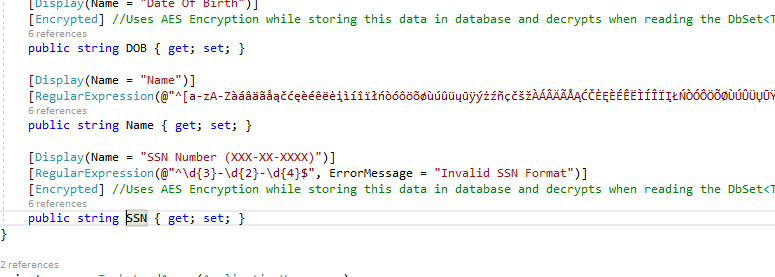






Data Validation:

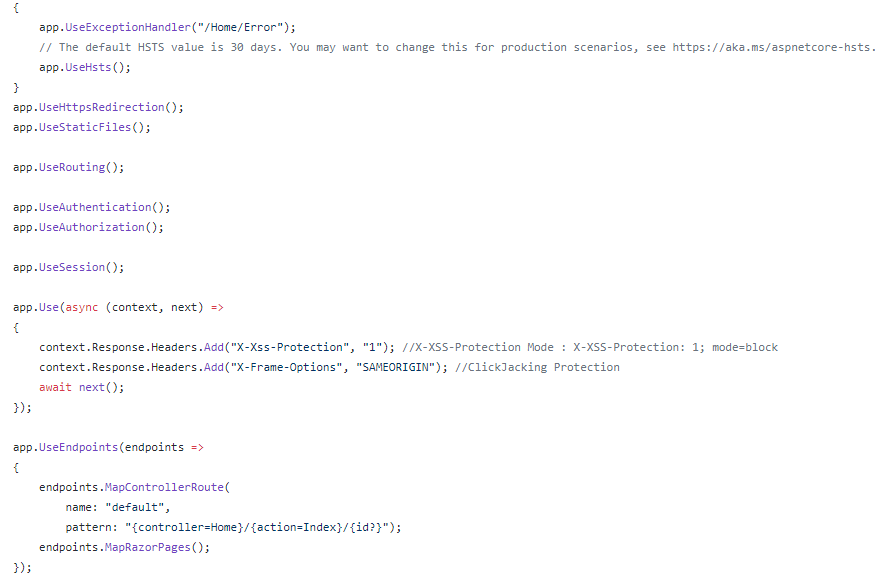
All SQL queries are constructed using parameterized queries and no wild cards used in the query construction.For avoiding SQL injection stored procedures are used along with proper input validation.



SSN,Email address,DOB,username and password are securely stored in the database using Microsoft.EntityFrameworkCore.DataEncryption.

**Header Security:**

XSS Protection mode,Xframe options and HSTS implemented for secure configurations.



I tried implementing a CSP header but it's somehow blocking the external static pages.But I can work on the improvisation part on CSP implementation.

<httpProtocol>

<customHeaders>

<add name="Content-Security-Policy" value="default-src 'self'" />

</customHeaders>

</httpProtocol>

**Azure security Hardening:**

Due to feature limitation and few services are paid not able implement secure config for azure, but below security hardenings can be followed.

*1. General Azure Security*

The list of general Azure Security Technologies are below:

Azure Security Center: It is a workload protection solution; it provides security management. Additionally, advanced threat protection across the hybrid cloud.

Azure Key Vault: It secures every sensitive detail like passwords, connection strings, and other information you need to keep your apps working.

Azure Monitor logs: A service that collects telemetry and other data and provides a query language and analytics engine to deliver operational insights for apps and resources. It can be used standalone or along with Azure Security Centre.

Azure Dev/Test Labs: A service that helps testers and developers instantly create Azure environments while minimizing waste and controlling.

*2. Operations Security*

The list of Operations Security technologies are below:

Security and Audit solution: It provides a complete view of an organization’s IT security posture

Azure Resource Manager: It enables us to work with the resources in the organization’s solution as a group. In a single coordinated operation, an organization can deploy, update, or delete all the resources.

*3. Applications Security*

List of Applications Security technologies are below:

Web Application vulnerability scanning: Azure provides one-click vulnerability scanning.

Web Application Firewall: The web application firewall (WAF) in Azure Application Gateway aims to secure web apps from rising web-based threats such as SQL injection, cross-site scripting threats, and user hijacking.

Application Insights: It is for web developers, an extendable Application Performance Management (APM) program.

*4. Storage Security*

Listed below are the Storage Security technologies:

Role-Based Access Control (RBAC): Restricting access based on the need to know and least privilege security principles is imperative for organizations that want to enforce security policies for data access.

Encryption: Encryption in transit is a mechanism of protecting data when it is transmitted across networks.

*5. Network Security*

Listed below are the Network Security technologies:

Azure Virtual Network: An Azure virtual network (VNet) represents a client’s network in the cloud. It is a logical isolation of the Azure network fabric dedicated to your subscription.

VPN Gateway: VPN gateway is a virtual network gateway that sends encrypted traffic across a public connection.

Network Layer Controls: Network access control is the act of controlling connectivity to and from individual devices or subnetworks, forming the center of network security.

*6. Backup and Disaster Recovery*

The two types of Disaster Backup Recovery are listed below:

Azure Site Recovery: It helps to orchestrate Backup, failover, and recovery of workloads and applications. Whenever the primary location goes down, they would be accessible from a secondary site.

Virtual machine backup: Azure Backup protects application data with minimal operating costs and zero capital investment.

Know about our Services in Disaster Backup Recovery here.

*7. Identity and Access Management*

There are two categories of Identity and access management:

*Azure Active Directory*: Authentication repository supports Azure’s multi-tenant, cloud-based directory, and multi-identity management services.

Azure Multi-Factor Authentication: A security provision that utilizes several authentications and verification methods before accessing protected information.

Security Checklist for Azure

Check out our Azure Security Services Checklist for better securing the data on Azure.

*The Starting Checklist*:

* Ensure that multifactor authentication is enabled for all users
* Ensure that there are no guest users.
* Use Role-Based Access Control to manage access to resources.
* Ensure that ‘enable users to memorize multi factor authentication on devices they trust’ is disabled.
* Ensure that the ‘number of processes required to reset’ is set to 2.
* Assure that ‘number of days before users are asked to re-confirm their authentication report’ is not set to 0.
* Assure that ‘caution users on password resets’ is set to yes.
* Ensure that ‘notify all admins when other admins reset their password?’ is set to yes.
* Ensure that ‘users can comply with apps obtaining company data on their account’ is set to none.
* Guarantee that ‘users can add gallery apps to their Entrance Panel’ is set to no.
* Ensure that ‘users can disclose applications’ is fixed to no.
* Guarantee that ‘guest users agreements are limited’ is set to yes.
* Ensure that ‘members can request’ is set to no.
* Guarantee that ‘guests can invite’ is set to no.
* Ensure that entrance to the Azure AD administration portal should be limited.
* The Ending Checklist
* Ensure that ‘users can create security associations’ is set to none.
* Ensure that ‘self-service group administration enabled’ is established to no.
* Make sure ‘users who can handle security groups’ is set to none.
* Ensure that ‘users can create Office 365 groups’ is set to no.
* Ensure that ‘users who can manage Office 365 groups’ is set to none.
* Make sure ‘require multi factor auth to join devices’ is set to yes.
* Ensure that ‘secure transfer required’ is arranged to enable.
* Ensure that ‘storage service encryption’ is set to enabled
* On SQL servers, ensure that ‘auditing’ is set to on.
* On SQL servers, ensure that ‘auditing type’ is set to a blob.
* Ensure on SQL servers that ‘threat detection’ is set to on.
* On SQL servers, ensure that ‘threat detection types’ is set to all.
* On SQL servers, ensure that ‘send alerts to’ is set.
* Ensure on SQL servers that’ email service and co-administrators’ is enabled.
* On SQL servers, ensure that firewall rules are set as appropriate.
* Disable RDP access on network security groups from the internet
* Disable SSH access on network security groups from the internet

**External Libraries:**

I have used Bootstrap 4.3.1,Jquery 3.5.1 and [EntityFrameworkCore.DataEncryption 2.0.0](https://github.com/Eastrall/EntityFrameworkCore.DataEncryption).

All external libraries are reviewed and verified in terms of checking CVE and vulnerable functions.

*Note:Code manually reviewed,Dynamic security testing performed on the application mapping with OWASP vulnerabilities and Threat modelling created separately.*