Vulnerability Management Tool

Design Manual

Student Name: Síne Doheny
Supervised by: Richard Butler
Student ID: C00226237

Table of Contents

Síne Doheny | C00226237

Introduction

The purpose of this design manual document is to provide detailed information regarding how the vulnerability management application will function and its relative behaviours. This document will provide an architecture overview, database design, system sequence diagrams and use cases. The document will provide the reader an enhanced understanding of the application as a system and the functionality provided by the application as mentioned in the functional specification document.

Síne Doheny | C00226237

Project Management Plan

The following plan outlines the dates for project deliverables.

Task	Start Date	End Date
Complete Research Manual	23/09/2020	13/11/2020
Complete Functional Specification	13/11/2020	26/11/2020
Complete Design Manual	26/12/2020	11/12/2020
Presentation		17/12/2020
Development	21/12/2020	05/02/2021
Testing	05/02/2021	01/03/2021
Second Presentation		15/01/2021
Complete Technical Manual	21/12/2020	19/04/2021
Final Report	21/12/2020	19/04/2021
Final Product	21/12/2020	23/04/2021
Project Demonstration		30/04/2021

Database Schema

ER Diagram
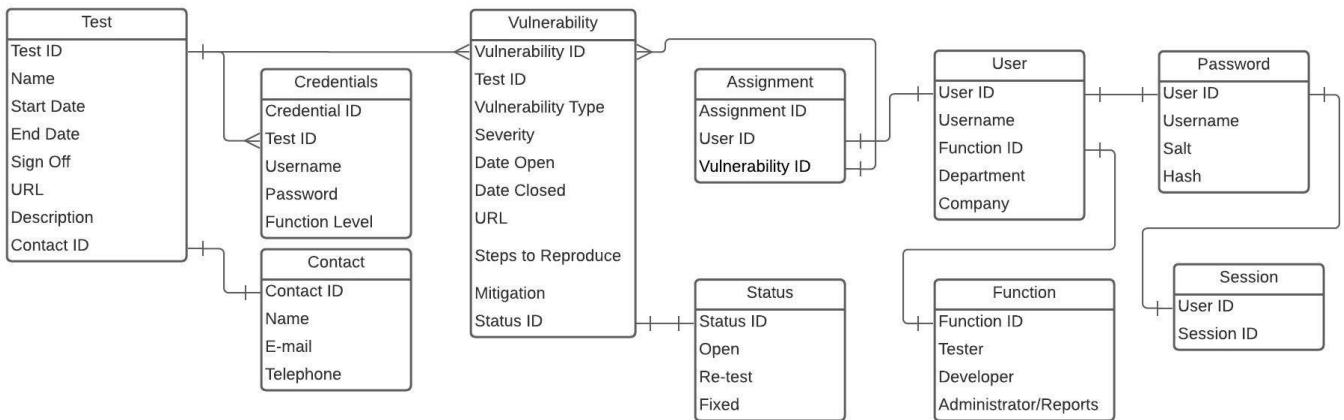
These tables may be altered during development, however this will not affect the relationships shown in the diagram.

Tables

User Table

User ID	Username	Function ID	Department	Company

Column Usage

User ID: Unique Identifier for a user's authenticated session.

Username: Unique identifier for user account.

Function ID: Functionality mode of user.

Department: Department user is working in.

Company: Company user is working with.

Password Table

User ID	Username	Salt	Hash

Column Usage

User ID: Unique identifier for a user's authenticated session.

Username: Unique identifier for user account.

Salt: Used with Hash of Password for stronger security, used to prevent brute force attacks.

Hash: Cryptographic Hash of Password use for stronger security.

5

Function Table

Function ID	Tester	Developer	Admin/Reports

Column Usage

Function ID: Unique identifier for users function.

Tester: A role which can be selected as the function of the user.

Developer: A role which can be selected as the function of the user.

Administrator/Reports: A role which can be selected as the function of the user.

Session Table

User ID	Session

Column Usage

User ID: Unique identifier for a user's authenticated session.

Session ID: Unique Session Identifier for a user's authenticated session.

Test Table

Test ID	Name	Start Date	End Date	Sign Off	URL	Description	Contact ID

Column Usage

Test ID: Unique identifier for test.

Name: Unique identifier for name of test.

Start Date: Start Date of test.

End Date: End Date of test.

Sign Off: Identifier to state whether legal requirements have been signed off before a test can proceed.

URL: URL being tested.

Description: Description of test scenario.

Contact ID: Contact of test owner.

Credentials Table

Credential ID	Test ID	Username	Password	Function Level

Column Usage

Credential ID: Unique identifier credential of user allowed to work on a test.

Test ID: Unique Identifier for test.

Username: Unique identifier for user account.

Password: Unique password for user account

Function Level: Functionality role level of user, for example the user has developer privileges.

Contact Table

Contact ID	Name	E-mail	Telephone

Column Usage

Contact ID: Unique identifier for user that is allocated as contact.

Name: Name of user that is allocated as contact.

E-mail: E-mail of user that is allocated as contact.

Telephone: Telephone number of user that is allocated as contact.

Vulnerability Table

Vulnerability ID	Test ID	Vulnerability Type	Severity	Date Open	Date Closed	URL	Steps to Reproduce	Mitigation	Status ID

Column Usage

Vulnerability ID: Unique identifier for vulnerability.
Test ID: Unique Identifier for test.

Vulnerability Type: Type of vulnerability.

Severity: Severity level of vulnerability.

Date Open: Date vulnerability was found and set to open.

Date Closed: Date vulnerability was found and set to closed.

URL: URL where vulnerability was found.

Steps to Reproduce: How to reproduce the vulnerability.

Mitigation: How to mitigate the vulnerability.

Status ID: The status of the vulnerability; open, re-test or fixed.

Status Table

Status ID	Open	Re-test	Fixed

Column Usage

Status ID: Unique identifier for vulnerability status.

Open: vulnerability can be set to the status Open.

Re-test: vulnerability can be set to the status Re-test.

Fixed: vulnerability can be set to the status Fixed.

Assignment Table

Vulnerability ID	User ID

Column Usage

Vulnerability ID: Unique identifier for vulnerability.

User ID: Unique identifier for the user assigned the vulnerability.

8

Sequence Diagrams

Login

The following sequence diagram conveys the process of authenticating with the application.
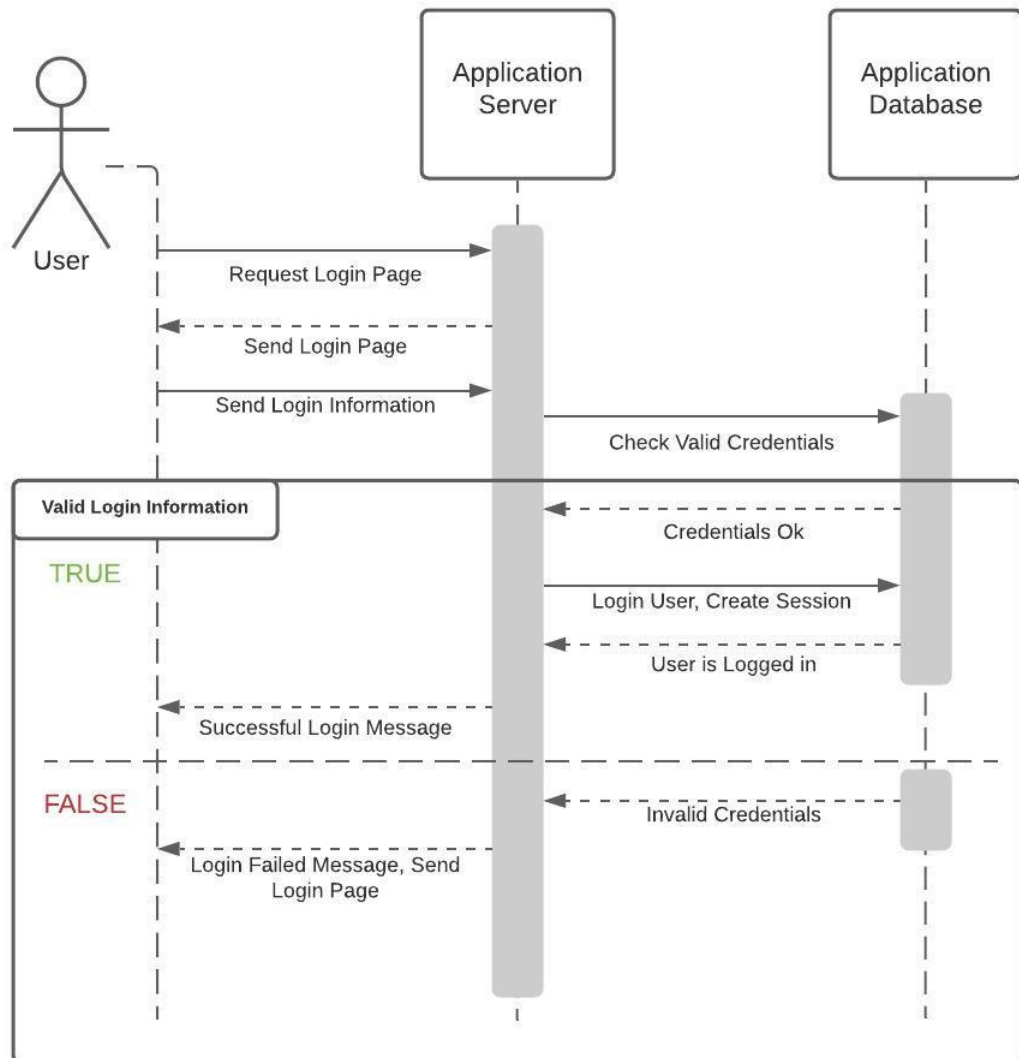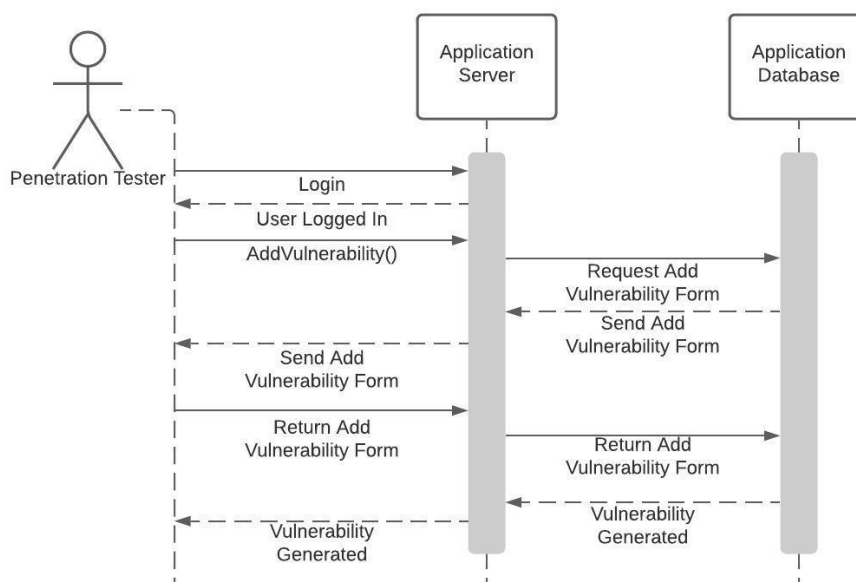
Generate Test

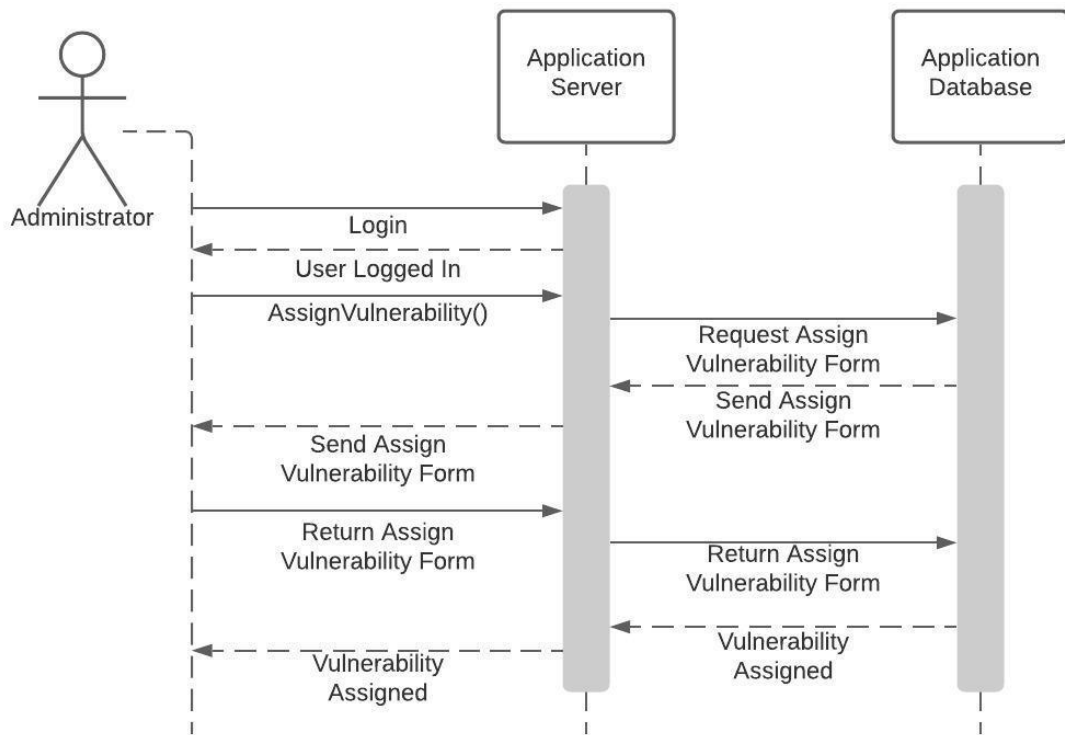The following sequence diagram conveys the process of setting up a test within the application.
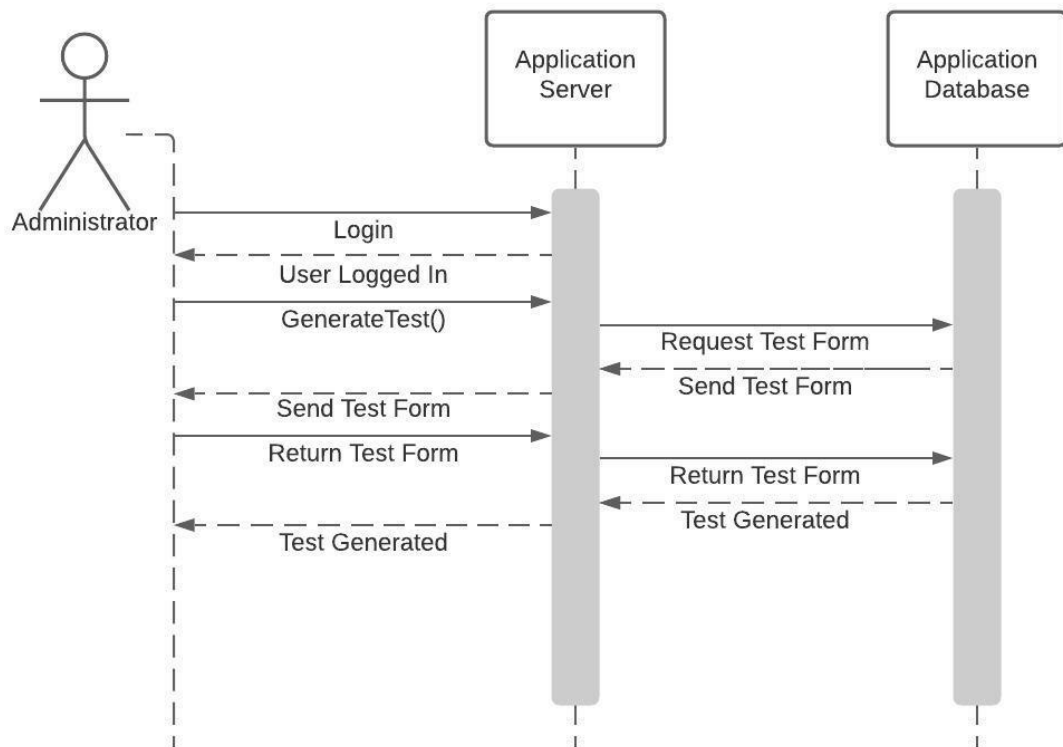
Add Vulnerability

The following sequence diagram conveys the process of adding a vulnerability within the application.
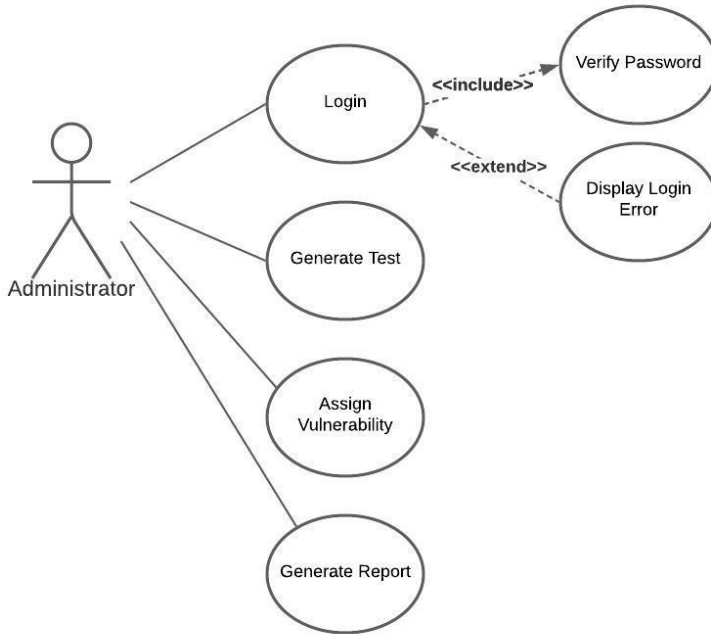
Síne Doheny | C00226237
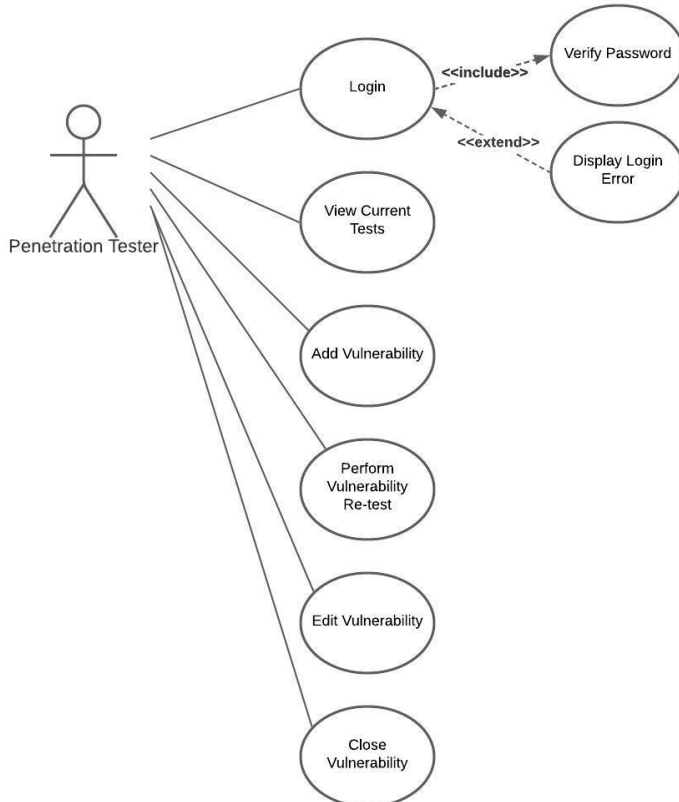
Assign Vulnerability

Síne Doheny | C00226237

Use Case Diagrams
Administrator

Penetration Tester

12

Developer

Síne Doheny | C00226237