A close up of a sign

Description automatically generated

Project 1 - Report

Secure Applications

Calin Doran – C00220175

2019

Table of Contents

[Introduction 2](#_Toc26521385)

[Test Cases 2](#_Toc26521386)

[1. Register with System 2](#_Toc26521387)

[2. Successful Authentication Attempt 2](#_Toc26521388)

[3. Successful Authentication 2](#_Toc26521389)

[4. Password Change 3](#_Toc26521390)

[5. Event Log & Admin User 3](#_Toc26521391)

# Introduction

This report will outline the development and testing of the fourth-year Project 1 for secure apps and development. Too create an authentication mechanism for a web application using XAMPP, PHP & MySQL. This application will create the underlying database on requesting the login page as a root user with no password.

# Test Cases

## 1. Register with System

|  |  |  |
| --- | --- | --- |
| Tasks | Case | Result |
| 1 | The system should allow users to register with the system using a username and password. | Pass |
| 2 | Complexity rules regarding the password should be enforced. | Pass |
| 3 | Password storage should be salted and hashed. | Pass |

## 2. Successful Authentication Attempt

|  |  |  |
| --- | --- | --- |
| Task | Case | Result |
| 1 | Reflect the supplied username provided in the above message. Ensure that this reflected parameter in not susceptible to XSS. You are to write your own sanitisation code for characters that can be utilised for XSS. | Pass |
| 2 | Lockout after 5 attempts for 3 minutes. | Pass |

## 3. Successful Authentication

|  |  |  |
| --- | --- | --- |
| Task | Case | Result |
| 1 | The system should greet the user by their username. | Pass |
| 2 | Create an active authenticated session. | Pass |
| 3 | Allow for the authenticated user to view some pages (at least two) that an unauthenticated user will not have access to. | Pass |
| 4 | Allow for the user to logout securely. | Pass |
| 5 | Lockout after 10 minutes of inactivity. | Pass |
| 6 | Max session duration of one hour irrespective of in session activity. | Pass |

## 4. Password Change

|  |  |  |
| --- | --- | --- |
| Task | Case | Result |
| 1 | Authenticated users should be capable of changing their password. | Fail |
| 2 | Complexity rules regarding the password should be enforced. | Pass |
| 3 | On password change the active session should be expired. | Fail |
| 4 | The user will have to re-authenticate using new credentials to gain access to the system. | Pass |
| 5 | No out of band communication, mechanism is required to inform the user that their credentials have been updated. | Pass |
| 6 | You are to implement Cross Site Request Forgery (CSRF) protection on this page. | Fail |

## 5. Event Log & Admin User

|  |  |  |
| --- | --- | --- |
| Task | Case | Result |
| 1 | The application should store unsuccessful and successful login attempts to an event log. This event log should accessible and viewable to the authenticated user “ADMIN” only. | Pass |
| 2 | This user’s authentication details are as follows  Username = “ADMIN”  Password = “SAD\_2019!” | Pass |
| 3 | This account is to be created, when your database is being created. | Pass |