Contents

[1 Introduction 1](#_Toc477455035)

[1.1 Summary 1](#_Toc477455036)

[1.2 Motivation 1](#_Toc477455037)

[1.3 Objectives 1](#_Toc477455038)

[2 Analysis And Design 2](#_Toc477455039)

[2.1 Web Application Attacks 2](#_Toc477455040)

2.2 Attack Prevention 6

[2.3 Manual Testing 8](#_Toc477455041)

[3 Implementation 15](#_Toc477455042)

[3.1 Automated Testing 15](#_Toc477455043)

[3.2 Report Generation 15](#_Toc477455044)

[4 Integration & Testing 16](#_Toc477455045)

[4.1 Device Integration 16](#_Toc477455046)

[4.2 Graphical Interface 16](#_Toc477455047)

[5 Conclusions 17](#_Toc477455048)

[5.1 Recommendations 17](#_Toc477455049)

[Appendix 18](#_Toc477455050)

[Bibliography 19](#_Toc477455051)

Figure Index

[1 Standard Login Form 9](#_Toc477455068)

[2 Bypassing a Login Form 9](#_Toc477455069)

[3 Succesful Login Form Bypass 9](#_Toc477455070)

[4 User Lookup Bypass 10](#_Toc477455071)

[5 Cookie Manipulation 11](#_Toc477455072)

[6 Login Error Example 11](#_Toc477455073)

[7 Reflected XSS Example 12](#_Toc477455074)

[8 Succesful Reflected XSS 12](#_Toc477455075)

[9 Stored XSS Example 13](#_Toc477455076)

[10 Succesful Stored XSS 13](#_Toc477455077)

[11 CSRF Example 14](#_Toc477455078)