Contents

[1 Introduction 1](#_Toc477531625)

[1.1 Summary 1](#_Toc477531626)

[1.2 Motivation 1](#_Toc477531627)

[1.3 Objectives 1](#_Toc477531628)

[2 Analysis And Design 2](#_Toc477531629)

2.1 Web Application Attacks 2

2.2 Attack Prevention 6

2.3 Manual Testing 8

[3 Implementation 15](#_Toc477531630)

[3.1 Automated Testing 15](#_Toc477531631)

[3.2 Report Generation 16](#_Toc477531632)

[4 Integration & Testing 17](#_Toc477531633)

[4.1 Device Integration 17](#_Toc477531634)

[4.2 Graphical Interface 17](#_Toc477531635)

[5 Conclusions 18](#_Toc477531636)

[5.1 Recommendations 18](#_Toc477531637)

[6 Appendix 19](#_Toc477531638)

[7 Bibliography 20](#_Toc477531639)

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)