

**UNIVERSIDAD DE CASTILLA - LA MANCHA**

ESCUELA DE INGENIERÍA INDUSTRIAL DE TOLEDO

TRABAJO FIN DE GRADO Nº XX-A/B-XXXXXX

*WEB HAZARD & INFRASTRUCTURE SCANNING THROUGH AUTOMATED PENTESTING AND REPORTING*

Autor:

SAMUEL VÁZQUEZ MORÓN

Director:

FRANCISCO MOYA FERNÁNDEZ

<MES y AÑO de defensa>

Contents

[1 Introduction 1](#_Toc479254566)

[1.1 Summary 1](#_Toc479254567)

[1.2 Motivation 1](#_Toc479254568)

[1.3 Objectives 1](#_Toc479254569)

[2 Antecedents 2](#_Toc479254570)

[2.1 Web Application Attacks 2](#_Toc479254571)

[2.2 Attack Prevention 7](#_Toc479254572)

[2.3 Manual Testing 9](#_Toc479254573)

[3 Implementation 16](#_Toc479254574)

[3.1 Automated Testing 16](#_Toc479254575)

[3.2 Report Generation 17](#_Toc479254576)

[4 Integration and Testing 18](#_Toc479254577)

[4.1 Device Integration 18](#_Toc479254578)

[4.2 Graphical Interface 18](#_Toc479254579)

[5 Conclusions 19](#_Toc479254580)

[5.1 Recommendations 19](#_Toc479254581)

[6 Appendix 20](#_Toc479254582)

[7 Bibliography 21](#_Toc479254583)

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)