

**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](#_Toc483496845)

[1.1 Summary 1](#_Toc483496846)

[1.2 Motivation 1](#_Toc483496847)

[1.3 Objectives 1](#_Toc483496848)

[2 Antecedents 2](#_Toc483496849)

[2.1 Web Application Attacks 2](#_Toc483496850)

[2.2 Attack Prevention 7](#_Toc483496851)

[2.3 Manual Testing 9](#_Toc483496852)

[3 Implementation 16](#_Toc483496853)

[3.1 Information Gathering 16](#_Toc483496854)

[3.2 Automated Testing 17](#_Toc483496855)

[3.3 Report Generation 21](#_Toc483496856)

[4 Integration 23](#_Toc483496857)

[4.1 Device Integration 23](#_Toc483496858)

[4.2 Dependences 23](#_Toc483496859)

[4.3 Remote Control 25](#_Toc483496860)

[5 Conclusions 30](#_Toc483496861)

[5.1 Recommendations 30](#_Toc483496862)

[6 Appendix 31](#_Toc483496863)

[7 Bibliography 32](#_Toc483496864)

Figure Index

[1 Standard Login Form 10](#_Toc483497319)

[2 Bypassing a Login Form 10](#_Toc483497320)

[3 Succesful Login Form Bypass 10](#_Toc483497321)

[4 User Lookup Bypass 11](#_Toc483497322)

[5 Cookie Manipulation 12](#_Toc483497323)

[6 Login Error Example 12](#_Toc483497324)

[7 Reflected XSS Example 13](#_Toc483497325)

[8 Succesful Reflected XSS 13](#_Toc483497326)

[9 Stored XSS Example 14](#_Toc483497327)

[10 Succesful Stored XSS 14](#_Toc483497328)

[11 CSRF Example 15](#_Toc483497329)

[12 API key configuration in OWASP ZAP 24](#_Toc483497330)

[13 Configuration to enable VNC in Raspberry Pi 26](#_Toc483497331)

[14 Locating the Raspberry Pi's IP address via "ifconfig" 26](#_Toc483497332)

[15 Security configuration for the VNC server 27](#_Toc483497333)

[16 Configuration of the dhcpcd.conf file 28](#_Toc483497334)

[17 Finding the IP address of a router 28](#_Toc483497335)