

**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](#_Toc485304125)

[1.1 Summary 1](#_Toc485304126)

[1.2 Background 1](#_Toc485304127)

[1.3 Motivation 3](#_Toc485304128)

[1.4 Objectives 4](#_Toc485304129)

[2 Antecedents 6](#_Toc485304130)

[2.1 Web Application Attacks 6](#_Toc485304131)

[2.2 Attack Prevention 11](#_Toc485304132)

[2.3 Manual Testing 13](#_Toc485304133)

[3 Implementation 20](#_Toc485304134)

[3.1 Information Gathering 20](#_Toc485304135)

[3.2 Automated Testing 22](#_Toc485304136)

[3.3 Report Generation 26](#_Toc485304137)

[4 Integration 28](#_Toc485304138)

[4.1 Device Integration 28](#_Toc485304139)

[4.2 Dependences 28](#_Toc485304140)

[4.3 Remote Control 30](#_Toc485304141)

[5 Conclusions 35](#_Toc485304142)

[5.1 Recommendations 35](#_Toc485304143)

[6 Appendix 36](#_Toc485304144)

[7 Bibliography 37](#_Toc485304145)

Figure Index

[1 Global Web Application Attack Source Countries, Q1 2017 2](#_Toc485304335)

[2 Top 10 Target Countries for Web Application Attacks, Q1 2017 3](#_Toc485304336)

[3 Web Application Attack Frequency, Q1 2017 6](#_Toc485304337)

[4 Standard Login Form 14](#_Toc485304338)

[5 Bypassing a Login Form 14](#_Toc485304339)

[6 Succesful Login Form Bypass 14](#_Toc485304340)

[7 User Lookup Bypass 15](#_Toc485304341)

[8 Cookie Manipulation 16](#_Toc485304342)

[9 Login Error Example 16](#_Toc485304343)

[10 Reflected XSS Example 17](#_Toc485304344)

[11 Succesful Reflected XSS 17](#_Toc485304345)

[12 Stored XSS Example 18](#_Toc485304346)

[13 Succesful Stored XSS 18](#_Toc485304347)

[14 CSRF Example 19](#_Toc485304348)

[15 API key configuration in OWASP ZAP 30](#_Toc485304349)

[16 Configuration to enable VNC in Raspberry Pi 31](#_Toc485304350)

[17 Locating the Raspberry Pi's IP address via "ifconfig" 31](#_Toc485304351)

[18 Security configuration for the VNC server 32](#_Toc485304352)

[19 Configuration of the dhcpcd.conf file 33](#_Toc485304353)

[20 Finding the IP address of a router 33](#_Toc485304354)