

**UNIVERSIDAD DE CASTILLA - LA MANCHA**

ESCUELA DE INGENIERÍA INDUSTRIAL DE TOLEDO

TRABAJO FIN DE GRADO Nº 17- B-225017

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

Autor:

SAMUEL VÁZQUEZ MORÓN

Director:

FRANCISCO MOYA FERNÁNDEZ

JULIO de 2017

Contents

[1 Introduction 1](#_Toc486263153)

[1.1 Summary 1](#_Toc486263154)

[1.2 Motivation 1](#_Toc486263155)

[1.3 Objectives 1](#_Toc486263156)

[2 Antecedents 2](#_Toc486263157)

[2.1 Background 2](#_Toc486263158)

[2.2 Web Application Attacks 4](#_Toc486263159)

[2.3 Attack Prevention 9](#_Toc486263160)

[2.4 Manual Testing 11](#_Toc486263161)

[3 Implementation 17](#_Toc486263162)

[3.1 Information Gathering 18](#_Toc486263163)

[3.2 Automated Testing 20](#_Toc486263164)

[3.3 Report Generation 24](#_Toc486263165)

[4 Integration 25](#_Toc486263166)

[4.1 Device Integration 25](#_Toc486263167)

[4.2 Dependences 25](#_Toc486263168)

[4.3 Remote Control 27](#_Toc486263169)

[4.4 Graphical User Interface 30](#_Toc486263170)

[5 Conclusions 31](#_Toc486263171)

[5.1 Recommendations 32](#_Toc486263172)

[6 Appendix 32](#_Toc486263173)

[7 Bibliography 33](#_Toc486263174)

Figure Index

[1 Global Web Application Attack Source Countries, Q1 2017 3](#_Toc486263373)

[2 Top 10 Target Countries for Web Application Attacks, Q1 2017 4](#_Toc486263374)

[3 Web Application Attack Frequency, Q1 2017 5](#_Toc486263375)

[4 Standard Login Form 12](#_Toc486263376)

[5 Bypassing a Login Form 12](#_Toc486263377)

[6 Succesful Login Form Bypass 12](#_Toc486263378)

[7 User Lookup Bypass 13](#_Toc486263379)

[8 Cookie Manipulation 14](#_Toc486263380)

[9 Login Error Example 14](#_Toc486263381)

[10 Reflected XSS Example 15](#_Toc486263382)

[11 Succesful Reflected XSS 15](#_Toc486263383)

[12 Stored XSS Example 16](#_Toc486263384)

[13 Succesful Stored XSS 16](#_Toc486263385)

[14 CSRF Example 17](#_Toc486263386)

[15 API key configuration in OWASP ZAP 27](#_Toc486263387)

[16 Configuration to enable VNC in Raspberry Pi 28](#_Toc486263388)

[17 Locating the Raspberry Pi's IP address via "ip addr" 28](#_Toc486263389)

[18 Security configuration for the VNC server 29](#_Toc486263390)

[19 Configuration of the dhcpcd.conf file 30](#_Toc486263391)

[20 GUI main screen 31](#_Toc486263392)

[21 Sample scan on the GUI 31](#_Toc486263393)