PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

UNIVERSITY OF FERHAT ABBAS SETIF-1



Faculty of Sciences Department of Computer Science

Master Thesis

Master's Degree in Data Engineering and Web Technology

Audit and Evaluation of Information System Security

Presented by:

ZERI Tarek & HATNNA Daoud

Supervised by:

Dr. Hadi Fairouz

Jury:

Supervisor:	Dr. Hadi Fairouz
President:	Dr. Slimani Yacine
Examiner:	Dr. Annane Boubakeur

Academic Year: 2025–2026

Abstract

Web application security auditing remains fragmented in practice, with reconnaissance results, testing evidence, vulnerability records, and final reports often distributed across multiple tools and documents. This fragmentation reduces traceability, complicates audit management, and increases the risk of overlooking security findings.

This thesis proposes a structured web security auditing methodology based on OWASP WSTG and implements it through **PentOS**, an integrated platform using React, FastAPI, PostgreSQL, and Redis. PentOS supports target scoping, reconnaissance, vulnerability assessment, findings management, CVSS-based risk evaluation, and report generation in one workflow.

The approach was validated on an authorized vulnerability disclosure program target (reconnaissance and non-intrusive analysis) and in a DVWA laboratory for confirmation of exploitable classes. The evaluation demonstrated centralized audit activities, traceable evidence, hybrid manual and automated testing, and structured reporting.

Experimental results included a **potential subdomain takeover scenario**, validation of the findings workflow, and laboratory confirmation of reflected XSS and SQL injection. Findings were evaluated through contextual risk assessment and aligned with NIST CSF 2.0 and ISO/IEC 27001:2022 controls.

The study demonstrates that a structured, reproducible web security auditing process can be supported through an integrated platform combining methodology, tooling, risk analysis, and reporting.

Keywords: Web application security, OWASP WSTG, PentOS, vulnerability assessment, risk analysis.

Résumé

L'audit de sécurité des applications web reste fragmenté en pratique : les résultats de reconnaissance, les preuves de tests, les enregistrements de vulnérabilités et les rapports finaux sont souvent répartis entre plusieurs outils et documents, ce qui réduit la traçabilité et complique la gestion de l'audit.

Ce mémoire propose une méthodologie structurée d'audit web fondée sur OWASP WSTG et la met en œuvre via **PentOS**, une plateforme intégrée (React, FastAPI, PostgreSQL, Redis) couvrant ciblage, reconnaissance, évaluation des vulnérabilités, gestion des findings, risques (CVSS) et rapports dans un même workflow.

L'approche a été validée sur une cible autorisée (programme public de signalement — reconnaissance et analyse non intrusive) et en laboratoire DVWA pour la confirmation de failles exploitables. Les résultats montrent la centralisation des activités, la traçabilité des preuves, les tests hybrides et le reporting structuré.

Les résultats incluent un **scénario potentiel de subdomain takeover**, la validation du workflow de findings, et la confirmation en laboratoire de XSS réfléchi et d'injection SQL, évalués selon une analyse contextuelle des risques et alignés sur NIST CSF 2.0 et ISO/IEC 27001:2022.

L'étude démontre qu'un audit web structuré et reproductible peut être soutenu par une plateforme intégrée combinant méthodologie, outillage, analyse des risques et reporting.

Mots-clés : Sécurité des applications web, OWASP WSTG, PentOS, évaluation des vulnérabilités, analyse des risques.

الملخص

لا يزال تدقيق أمن تطبيقات الويب يعاني في الممارسة العملية من التشتت، حيث تتوزع نتائج الاستكشاف، وأدلة الاختبار، وسجلات الثغرات، والتقارير النهائية بين أدوات ووثائق متعددة. هذا التشتت يقلّص قابلية التتبع، ويُعقّد إدارة عملية التدقيق، ويزيد من خطر تجاهل بعض النتائج الأمنية المهمة.

تقترح هذه الرسالة منهجية منظمة لتدقيق أمن تطبيقات الويب تستند إلى دليل OWASP WSTG، وتنفّذها عبر منصة PentOS، وهي منصة متكاملة مبنية باستخدام React وFastAPI وPostgreSQL وRedis. تدعم هذه المنصة تحديد نطاق الهدف، والاستكشاف، وتقييم الثغرات، وإدارة النتائج، وتقييم المخاطر وفق نظام CVSS، وإنتاج التقارير، ضمن مسار عمل واحد متكامل.

جرى التحقق من المنهجية على هدف مصرَّح به ضمن برنامج علني للإبلاغ عن الثغرات (استكشاف وتحليل غير تدخّلي)، وكذلك في بيئة مخبرية قائمة على DVWA لتأكيد فئات الثغرات القابلة للاستغلال. أظهر التقييم مركزية أنشطة التدقيق، وقابلية تتبع الأدلة، والدمج بين الاختبار اليدوي والآلي، إضافة إلى إعداد تقارير منظمة.

شملت النتائج التجريبية سيناريو محتملاً للاستيلاء على نطاق فرعي (subdomain takeover)، والتحقق من سلامة مسار إدارة النتائج، وتأكيداً مخبرياً لثغرتي البرمجة النصية العاكسة عبر المواقع (Reflected XSS) وحقن SQL. قُيّمت هذه النتائج عبر تحليل سياقي للمخاطر، وجرت مواءمتها مع ضوابط إطار NIST CSF 2.0 ومعيار ISO/IEC 27001:2022.

تُبيّن هذه الدراسة أن عملية تدقيق منظمة وقابلة للتكرار لأمن تطبيقات الويب يمكن دعمها عبر منصة متكاملة تجمع بين المنهجية والأدوات التقنية وتحليل المخاطر وإعداد التقارير.

الكلمات المفتاحية: أمن تطبيقات الويب، دليل OWASP WSTG، منصة PentOS، تقييم الثغرات، تحليل المخاطر.

Contents

Dedication 1

Acknowledgements 2

Abstract 3

Résumé 4

List of Figures 9

List of Tables 11

List of Acronyms 12

General Introduction 13

1 Foundations of Information Systems Security and Auditing 18

1.1 Introduction 18

1.2 Information Systems Security Fundamentals 18

1.2.1 Information Systems 18

1.2.2 Information Security 19

1.2.3 The CIA Triad 20

1.2.4 Security Objectives: Authentication, Authorization, and Traceability . . . 20

1.3 Security Threats and Vulnerabilities 21

1.3.1 Threats and Threat Actors 21

1.3.2 Attack Types 21

1.3.3 Vulnerabilities and Common Vulnerability Categories 22

1.3.4 CVE and CVSS Overview 22

1.4 Security Auditing Concepts and Methodologies 23

1.4.1 Definition and Objectives of a Security Audit 23

1.4.2 The Security Audit Process 24

1.4.3 Types of Security Audits 24

1.4.4 Vulnerability Assessment versus Penetration Testing 25

1.5 Security Standards and Frameworks 25

1.5.1 NIST Cybersecurity Framework 25

1.5.2 ISO/IEC 27001 26

1.5.3 OWASP Methodology . . . 26
1.6 Vulnerability Assessment and Risk Analysis . . . 27
1.6.1 Vulnerability Identification . . . 27
1.6.2 Risk Assessment Process . . . 27
1.6.3 Risk Classification . . . 27
1.6.4 Risk Prioritisation . . . 27
1.7 Comparative Discussion . . . 28
1.7.1 Comparison of Security Frameworks . . . 28
1.7.2 Advantages, Limitations, and Methodological Choices . . . 28
1.8 Conclusion . . . 29
2 Related Work and Research Background . . . 30
2.1 Introduction . . . 30
2.2 Related Work . . . 30
2.2.1 Information Systems Security Auditing . . . 31
2.2.2 Vulnerability Assessment and Risk Analysis . . . 31
2.2.3 Security Audit Automation Platforms . . . 32
2.3 Comparative Analysis of Existing Approaches . . . 33
2.4 Research Gap . . . 34
2.5 Positioning of the Thesis . . . 35
2.6 Conclusion . . . 36
3 Proposed Methodology and System Architecture . . . 37
3.1 Introduction . . . 37
3.2 Overview of the Proposed Approach . . . 38
3.2.1 Practical Illustration of Each Workflow Stage . . . 38
3.3 Requirements Analysis . . . 39
3.3.1 Functional Requirements . . . 39
3.3.2 Non-Functional Requirements . . . 40
3.4 Proposed Audit Methodology . . . 40
3.4.1 Methodology Principles . . . 41
3.4.2 Audit Phases and PentOS Mapping . . . 41
3.5 General Architecture of PentOS . . . 42
3.5.1 Logical Architecture . . . 42
3.5.2 Backend Services . . . 42
3.5.3 Frontend Application . . . 43
3.5.4 Data Model Overview . . . 43
3.6 Functional Modules of the System . . . 44
3.6.1 Target Manager . . . 44

3.6.2 Recon Engine . . . 44
3.6.3 Vulnerability Assessment Modules . . . 46
3.6.4 Findings Register . . . 47
3.6.5 Reports Module . . . 48
3.6.6 Dashboard and Documentation . . . 48
3.7 System Workflow . . . 48
3.8 Conclusion . . . 50

4 Experimental Validation of the Proposed Methodology . . . 51
4.1 Introduction . . . 51
4.2 Deployment Environment . . . 52
4.2.1 Audit Workstation and PentOS Stack . . . 52
4.2.2 Authorized Program Target . . . 52
4.2.3 Laboratory Target (DVWA) . . . 52
4.3 Target Registration and Validation Plan . . . 53
4.4 Reconnaissance on the Authorized Target . . . 54
4.5 Information Disclosure Module . . . 56
4.5.1 URL Hunter Execution . . . 56
4.6 Security Misconfiguration Module . . . 58
4.6.1 Takeover Scan Results . . . 58
4.6.2 Confirmed Finding: Smartling Subdomain Takeover Candidate . . . 58
4.7 Laboratory Hybrid Testing (DVWA) . . . 59
4.7.1 Reflected XSS via PentOS Reflection Tester . . . 59
4.7.2 SQL Injection: Manual Verification Outside PentOS . . . 60
4.8 Findings Consolidation and Report Generation . . . 61
4.9 Experimental Results Summary . . . 64
4.10 Conclusion . . . 64

5 Risk Evaluation and Security Recommendations . . . 65
5.1 Introduction . . . 65
5.2 Risk Evaluation Methodology . . . 65
5.2.1 Risk Scoring Framework . . . 65
5.2.2 Contextual Adjustments . . . 66
5.2.3 Probability and Impact Scales . . . 66
5.2.4 Risk Scoring for All Findings . . . 67
5.3 Risk Matrix . . . 68
5.4 Remediation Roadmap . . . 68
5.4.1 Immediate Actions (Week 1) . . . 68

5.4.2 Short-Term Actions (Weeks 2–4) 69
5.4.3 Medium-Term Actions (Month 2+) 69
5.5 Alignment with International Security Standards 70
5.5.1 Mapping to NIST Cybersecurity Framework 2.0 70
5.5.2 Mapping to ISO/IEC 27001:2022 Annex A 71
5.5.3 Compliance Gap Analysis 71
5.6 Limitations and Future Work 72
5.6.1 Limitations 72
5.6.2 Future Work 73
5.7 Conclusion 73
General Conclusion **74**
Bibliography **78**