MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___" _____ 2025

EVALUAREA ȘI MITIGAREA VULNERABILITĂȚILOR APLICAȚIILOR WEB PRIN TESTE DE PENETRARE

Proiect de master

Student: _____ **Magdei Octavian, SI-231M**

Coordonator: _____ **Alexei Arina, lect. univ.**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chişinău, 2025

REZUMAT

În prezent, aplicațiile web sunt o componentă de bază în o mulțime de instituții și domenii, de la servicii financiare și comerț electronic la educație și managementul datelor personale. Cu creșterea utilizării și a complexității acestor aplicații, vulnerabilitățile de securitate au devenit tot mai frecvente, sofisticate și complexe, ce pune în pericol confidențialitatea, integritatea și disponibilitatea informațiilor. Teza ține să abordeze în detaliu problemele securității aplicațiilor web, concentrându-se pe evaluarea și mitigarea vulnerabilităților prin teste de penetrare. Studiul analizează vulnerabilitățile comune, cum ar fi Cross-Site Scripting (XSS), SQL Injection, Broken Access Control și Server-Side Request Forgery (SSRF), analizând cum acestea se propagă și soluțiile de remediere. Totodată, lucrarea subliniază importanța testelor de penetrare, atât manuale, cât și automatizate, pentru detectarea vulnerabilităților și prevenirea atacurilor aplicațiilor web. De asemenea, oferă o metodologie pentru evaluarea riscurilor și implementarea măsurilor de protecție. Pentru a atinge acest scop, cercetarea abordează următoarele aspecte, ca investigarea celor mai frecvente vulnerabilități din aplicațiile web menționate anterior. Propunerea de soluții de mitigare și bune practici, în conformitate cu reglementările și standardele existente, pentru reducerea riscurilor și îmbunătățirea securității. Cercetarea implică utilizarea unor instrumente asociate testării de penetrare, cum ar fi Burp Suite, OWASP ZAP și Nessus, pentru identificarea vulnerabilităților și evaluarea eficienței măsurilor de securitate aprobate.

ABSTRACT

Nowadays, web applications are a core component in a wide range of institutions and domains, from financial services and e-commerce to education and personal data management. With the increasing use and complexity of these applications, security vulnerabilities have become more frequent, sophisticated and complex, which endangers the confidentiality, integrity and availability of information. The thesis aims to address in detail the security issues of web applications, focusing on the assessment and mitigation of vulnerabilities through penetration testing. The study analyzes common vulnerabilities, such as Cross-Site Scripting (XSS), SQL Injection, Broken Access Control and Server-Side Request Forgery (SSRF), analyzing how they propagate and remediation solutions. At the same time, the paper emphasizes the importance of penetration testing, both manual and automated, for detecting vulnerabilities and preventing web application attacks. It also provides a methodology for assessing risks and implementing protective measures. To achieve this goal, the research addresses the following aspects, such as investigating the most common vulnerabilities in the aforementioned web applications. Proposing mitigation solutions and best practices, in accordance with regulations and standards, to reduce risks and ensure security. The research involves the use of penetration testing tools, such as Burp Suite, OWASP ZAP and Nessus, to identify vulnerabilities in the measures and evaluate the effectiveness of the approved security.

CUPRINS

INTRODUCERE

În prezent, aplicațiile web joacă un rol decesiv în viața contemporană. Aplicațiile web permit utilizatorilor să acceseze o gamă largă de servicii, de la tranzacții bancare la gestionarea datelor personale. În timp ce popularitatea și interesul utilizatorilor față de aplicațiile web au început să crească, dar și dependența față de aplicațiile web, a devenit evidentă necesitatea de a oferi un nivel avansat de securitate cibernetică.

Vulnerabilitățile aplicațiilor web reprezintă breșe și deficiențe care pot fi exploatate de catre atacatori pentru a compromite integritatea, confidențialitatea și disponibilitatea informațiilor ce pot fi stocate în acest sistem. Vulnerabilitățile nu sunt numai erori in codul programului, dar și neconcordanțe în arhitectura aplicației sau în procesele de dezvoltare și implementare a unor funcționalități noi.

Printre vulnerabilitățile des întâlnite sunt cele de injectare, cum ar fi SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), care permit atacatorilor să compromită aplicațiile prin injectarea de comenzi malețioase, redirecționarea utilizatorului sau chiar accesul neautorizat la datele din sistem, referitor la utilizatori sau informații despre sistemul gazda atacat. În contextul dezvoltării non stop a aplicațiilor web, este esențial de înțeles natura acestor vulnerabilități, catalogizarea din perspectiva documentelor și reglementărilor existente, care la urma lor, stabilesc metode și standarte pentru evaluarea securității aplicațiilor web.

Securitatea aplicațiilor web este un domeniu complex și în continuă evoluție. Într-o lume digitală interconectată, amenințările cibernetice devin din ce în ce mai sofisticate, iar atacatorii identifică mereu noi metode pentru a exploata vulnerabilitățile existente. Evaluarea securității aplicațiilor web, în special prin identificarea și analiza vulnerabilităților, devine o componentă crucială pentru protejarea infrastructurilor digitale.

O evaluare adecvată a vulnerabilităților presupune o înțelegere profundă a tehnologiilor și arhitecturilor utilizate, precum și a metodelor de atac care pot compromite aceste sisteme. Documentele și standardele internaționale, precum OWASP (Open Web Application Security Project), NIST (National Institute of Standards and Technology) sau ISO/IEC 27001, oferă ghiduri detaliate și bune practici pentru identificarea și gestionarea vulnerabilităților aplicațiilor web.

Evaluarea vulnerabilităților nu este doar un proces tehnic, dar și unul de conformitate. În multe industrii, organizațiile sunt obligate să respecte standarde stricte de securitate pentru a proteja datele utilizatorilor și pentru a evita penalizările legale. De exemplu, reglementările precum GDPR (General Data Protection Regulation) impun obligații clare în ceea ce privește securitatea datelor personale procesate de aplicațiile web. Evaluarea vulnerabilităților și implementarea unor măsuri adecvate de securitate contribuie la conformitatea cu aceste reglementări și la prevenirea potențialelor breșe de securitate.

BIBLIOGRAFIE

[1] "What is a CVE?" Accessed: Jan. 1, 2025. [Online]. Available: https://www.redhat.com/en/topics/security/what-is-cve

[2] "Number of common vulnerabilities and exposures 2024," Statista. Accessed: Jan. 1, 2025. [Online]. Available: https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/

[3] "Top 10 web application vulnerabilities in 2021–2023." Accessed: Jan. 1, 2025. [Online]. Available: https://securelist.com/top-10-web-app-vulnerabilities/112144/

[4] M. Liu, B. Zhang, W. Chen, and X. Zhang, "A Survey of Exploitation and Detection Methods of XSS Vulnerabilities," *IEEE Access*, vol. 7, pp. 182004–182016, 2019, doi: 10.1109/ACCESS.2019.2960449.

[5] L. Erdodi, Å. Å. Sommervoll, and F. M. Zennaro, "Simulating SQL Injection Vulnerability Exploitation Using Q-Learning Reinforcement Learning Agents," May 22, 2021, *arXiv*: arXiv:2101.03118. doi: 10.48550/arXiv.2101.03118.

[6] M. M. Hassan, M. A. Ali, T. Bhuiyan, M. H. Sharif, and S. Biswas, "Quantitative Assessment on Broken Access Control Vulnerability in Web Applications".

[7] K. Al-talak and O. Abbass, "Detecting Server-Side Request Forgery (SSRF) Attack by using Deep Learning Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 12, 2021, doi: 10.14569/IJACSA.2021.0121230.

[8] S. K. Lala, A. Kumar, and S. T., "Secure Web development using OWASP Guidelines," in *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, May 2021, pp. 323–332. doi: 10.1109/ICICCS51141.2021.9432179.

[9] I. M, M. Kaur, M. Raj, S. R, and H.-N. Lee, "Cross Channel Scripting and Code Injection Attacks on Web and Cloud-Based Applications: A Comprehensive Review," *Sensors*, vol. 22, no. 5, Art. no. 5, Jan. 2022, doi: 10.3390/s22051959.

[10] E. R. Harold, *XML 1.1 Bible*. John Wiley & Sons, 2004.

[11] R. Shahid, S. N. K. Marwat, A. Al-Fuqaha, and G. B. Brahim, "A Study of XXE Attacks Prevention Using XML Parser Configuration," in *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)*, Dec. 2022, pp. 830–835. doi: 10.1109/CICN56167.2022.10008276.

[12] H. Li, L. Yu, and W. He, "The Impact of GDPR on Global Technology Development," *J. Glob. Inf. Technol. Manag.*, vol. 22, no. 1, pp. 1–6, Jan. 2019, doi: 10.1080/1097198X.2019.1569186.

[13] S. O. Sadjadi, C. Greenberg, E. Singer, L. Mason, and D. Reynolds, "The 2021 NIST Speaker Recognition Evaluation," Apr. 21, 2022, *arXiv*: arXiv:2204.10242. doi: 10.48550/arXiv.2204.10242.

[14] Technical University of Moldova and A. Alexei, "ENSURING INFORMATION SECURITY IN PUBLIC ORGANIZATIONS IN THE REPUBLIC OF MOLDOVA THROUGH THE ISO 27001 STANDARD," *J. Soc. Sci.*, vol. IV(1), Mar. 2021, doi: 10.52326/jss.utm.2021.4(1).11.

[15] Z. Hu, R. Beuran, and Y. Tan, "Automated Penetration Testing Using Deep Reinforcement Learning," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Sep. 2020, pp. 2–10. doi: 10.1109/EuroSPW51379.2020.00010.

[16] Assistant professor, Department of IT, Sri Krishna College of Engineering and Technology. *et al.*, "Web Application Penetration Testing," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 10, pp. 1029–1035, Aug. 2019, doi: 10.35940/ijitee.J9173.0881019.