Digital Health and Informatics Innovations for Sustainable Health Care Systems
J. Mantas et al. (Eds.)

doi:10.3233/SHTI240628

Developing an Open-Source, User-Friendly, OWASP-Compliant Architecture for Healthcare Web Application Testing

Ylenia MURGIA [a,1], Jaime DELGADO [b] and Mauro GIACOMINI [a]
[a] *Department of Informatics, Bioengineering, Robotics and System Engineering (DIBRIS), University of Genoa, Genoa, Italy*
[b] *Departament d'Arquitectura de Computadors (DAC), Universitat Politècnica de Catalunya - BarcelonaTech (UPC), Spain*
ORCiD ID: Ylenia Murgia https://orcid.org/0009-0009-3303-3160
Jaime Delgado https://orcid.org/0000-0003-1366-663X
Mauro Giacomini http://orcid.org/0000-0001-5646-2034

Abstract. Nowadays, web applications are fundamental in the healthcare sector. However, with the widespread use of this technology, risks related to cybersecurity attacks also increase. To mitigate this phenomenon, every 3-4 years, the nonprofit foundation Open Worldwide Application Security Project (OWASP) compiles a top 10 ranking of the most critical web application security risks. Along with the top 10 Web Application Security Risks, OWASP also provides the Web Security Testing Guide, which offers comprehensive guidelines for conducting security tests. This guide includes suggestions for specific tools to use when performing different tests, among other valuable insights. However, the use of these recommended tools can be costly and can require advanced technical skills and a deep understanding of security best practices and web technologies. In addition, since the OWASP work on web security is generic, it would be useful to restrict and adapt it to the healthcare area. This would help in reducing the overhead when dealing with the needed tools. The goal of this study is to make web application security assessment in healthcare more accessible by developing tools that simplify the process and makes it user-friendly. Before developing such tools, an in-depth feasibility study must be conducted to verify the existence of open-source libraries to carry out the necessary testing procedures. It will be also necessary to identify how tools could be simplified and enhanced when focusing on healthcare.

Keywords. Healthcare Web Application, Security, OWASP Top 10 Web Application Security Risks

1. Introduction

Advances in technology are essential to enhance the healthcare sector and, as a result, to improve the well-being of society. Health systems are adopting digital solutions to enhance services and manage medical problems more effectively. Web applications for healthcare have played a crucial role in this transformation, making services more

[1] Corresponding Author: Ylenia Murgia; Department of Informatics, Bioengineering, Robotics and System Engineering (DIBRIS) - University of Genoa, Via all'Opera Pia 13, 16145 Genoa, Italy; E-mail: ylenia.murgia@edu.unige.it.

accessible and efficient. These applications, available through web browsers or mobile devices, manage activities such as appointment scheduling, medical record management, and telemedicine [1]. While technologies applied to healthcare continue to advance, the downside is that security threats are increasing, posing a risk to healthcare institutions and patients [2]. Established in 2004, the European Union Agency for Cybersecurity (ENISA) aimed primarily to promote a common level of cybersecurity across all European Union countries [3]. In particular, the ENISA Threat Landscape (ETL) report is meant to explore the current state of cybersecurity, by identifying the main threats, attack techniques, and motivations of actors. The latest published report [4] covers the observation period from July 2022 to June 2023: globally, a significant increase in both the diversity and amount of cyber attacks and their consequences is reported. Moreover, an in-depth examination of threats, considering various sectors and geographic regions, indicates that public administration (16.19%), targeted individuals (15.44%), and the healthcare sector (10.22%) remain the primary focal points for data leaks and breaches. In addition, in July 2023, ENISA released an additional report [5], focused specifically on the healthcare sector, covering the observation period from January 2021 to March 2023. ENISA emphasizes that, within the healthcare sector, attacks primarily target public-facing infrastructure, such as websites or portals, leading to disruptions and potential issues in healthcare service delivery. Drawing on these insights, the aim of this study is to enhance accessibility to web application security assessment in the healthcare sector. This will be achieved by creating user-friendly tools that streamline the process and aim to protect various category of sensitive healthcare data, including medical history, clinical and diagnostic data and any Personal Identifiable Information (PII) in general. Preserving these data helps patients maintain trust, ensure regulatory compliance, prevent identity theft, and provide higher quality care. The main target audience of this project consists of healthcare IT developers, such as computer scientists, biomedical engineering, and technical experts, with a high level of computer literacy [6], but who may not necessarily have a background in cybersecurity.

2. Materials and Methods

2.1. OWASP Top 10 Web Application Security Risks

The Open Worldwide Application Security Project (OWASP) is a nonprofit organization dedicated to enhancing software security, and it provides projects, tools, documents, forums, freely available to the community. Among all the resources made available, OWASP periodically releases a report describing the Top 10 Web Application Security Risks. Initially introduced in 2003, this list has been regularly updated and republished every 3-4 years. The latest version, dated 2021, can be accessed on the OWASP website [7]. Figure 1 shows the current list of OWASP Top 10 Web Application Security Risks. It is worth mentioning that the web applications that OWASP is considering are not health-specific. Identifying the impact of such specificities is part of our research work.

Figure 1. OWASP Top 10 Web Application Security Risks

2.2. OWASP Web Security Testing Guide

Related to OWASP Top 10 Web Application Security Risks, a Web Security Testing Guide (WSTG) is also developed by OWASP. The WSTG project is the leading cybersecurity testing resource for web application developers and security professionals. The purpose of this project is to gather all possible testing techniques, explain them, and keep the guide up-to-date. The current stable version of WSTG is v4.2 and it is available at [8]. The following are the primary OWASP WSTG subcategories in which the tests are categorized: Information Gathering, Configuration and Deployment Management Testing, Identify Management Testing, Authentication Testing, Authorization Testing, Session Management Testing, Input Validation Testing, Testing for Error Handling, Testing for Weak Cryptography, Business Logic Testing, Client-side Testing, API Testing. In addition, OWASP also provides an Appendix [9], containing different tools, both open and commercial, that can be used to perform the tests. Among several web application security testing tools, the most widely used [10] are Burp Suite and Zed Attack Proxy (ZAP). Burp Suite [11] provides both a free version, with significant limitations, and a paid version, which offers advanced elements useful to professionals in the fields. Its paid version provides an intuitive interface and a broad range of tools for web application security analysis [12]. ZAP [13] is a free and open-source tool for web application security analysis. It was created by the OWASP foundation, but, since August 2023, it has joined the Software Security Project (SSP). ZAP is currently maintained by an international team of volunteers. It is an alternative to Burp Suite, but, to perform more in-depth tests, its interface is less intuitive and has fewer features [12].

3. Results

We aim to create open-source tools that focus on web application security analysis, adhering to the OWASP Top 10 Web Application Security Risks standard. These tools will prioritize ease of use, ensuring accessibility to people outside the cybersecurity world. In addition, our goal remains to customize these tools specifically for web application analysis in the healthcare sector, recognizing the unique security challenges in this environment. In this scenario, the first step will involve a feasibility analysis and then on the development of the architecture of the tools.

3.1. Feasibility Assessment

The first point is to conduct a feasibility assessment to verify the existence of open-source libraries suitable for performing the necessary testing procedures in web applications. This involves a deep investigation of the resources available, assessing their suitability and alignment with the specific requirements for web application security testing in the healthcare context. Therefore, it will be necessary to understand the features of the available resources, such as open-source libraries, APIs, REST solutions, and figure out how to integrate them together to create a unified suite that incorporates these various tools. This analysis will provide a fundamental basis for the next phase of developing the tools needed to simplify and make accessible the security assessment of web applications in the health care sector.

3.2. Architectural Prototype

The second point concerns the architectural proposal for the new tools. These tools will be designed to simplify the process of security assessment of web applications in the healthcare sector. Several aspects need to be considered in the architecture prototype:

- Intuitive and user-friendly interface to allow users to easily navigate through the suite's functionality without requiring advanced technical skills.
- Simplified test management: these tools should simplify the process of conducting web application security tests, allowing users to perform different types of tests without having to manually configure each individual parameter.
- Clear and comprehensive reporting: the architecture must include a system for generating clear and comprehensive reports that summarize the results of the tests performed. Additionally, we will have to ensure the security of the reports themselves, as they contain potential vulnerabilities of the web applications.
- Open-source, but secure: the architecture we are going to implement will have the task of finding potential vulnerabilities in a healthcare-related web application. Thus, before performing the analysis and unveiling the results, it will be necessary to verify that it is the owner of the application who is requesting such tests. This could be achieved by going to implement a system similar to the Domain Name System (DNS) verification.
- Data security: it is essential to incorporate robust mechanisms to ensure data security during the testing process, avoiding any risk of breach of patient privacy or loss of sensitive data.

4. Discussion and Conclusions

As healthcare-related web applications become more widespread, the risks and threats in terms of cybersecurity are increasing. For this reason, this study proposes the development of user-friendly tools, aimed at healthcare IT developers, to assess the security of web applications. OWASP Top 10 Web Application Security Risks is regarded as a standard for what concerns web application security analysis, although it is not mandatory and it is not specific to the healthcare sector. Therefore, a study will be needed to understand which of the top 10 Web Application Security Risks are the most critical in healthcare by submitting a questionnaire to security professionals in Italian

hospitals and clinics. In addition, as we recognize the value of other organizations, such as CERT (Computer Emergency Response Team) [14], we will be considering other valuable resources in the future. After this initial research, the next step will be the feasibility assessment phase, which is necessary to determine the availability of existing open-source tools for conducting web application security testing and to understand how to use them to develop a unified suite. Next, the design and development phase of the architectural prototype will aim to prioritize simplicity and usability. Indeed, the development of intuitive and user-friendly web application security analysis tools, specific to the healthcare industry, can simplify the testing process for healthcare IT developers. By integrating cybersecurity best practices and ensuring compliance with healthcare regulations, this suite could help mitigate risks related to cyber attacks and the protection of sensitive patient data. It is essential to recognize that the development of this architecture will require substantial resources, such as dedicated teams of developers and cybersecurity experts, time to research the necessary materials for tools development, and time for broad testing and refinement.

Acknowledgements

Hub Life Science - Digital Health (LSH-DH) PNC-E3-2022-23683267 - DHEAL-COM Project - CUP: D33C22001980001, funded by the Ministry of Health under the National Plan Complementary to the PNRR Innovative Health Ecosystem - UIC: PNC-E.3

References

[1] Stoumpos AI, Kitsios F, Talias MA. Digital Transformation in Healthcare: Technology Acceptance and Its Applications. *Int J Environ Res Public Health*; 20. Epub ahead of print 1 February 2023. DOI: 10.3390/ijerph20043407.
[2] Kelly B, Quinn C, Lawlor A, et al. Cybersecurity in Healthcare. In: Sakly H, Yeom K, Halabi S, et al. (eds) *Trends of Artificial Intelligence and Big Data for E-Health*, pp. 213–232.
[3] About ENISA - The European Union Agency for Cybersecurity. *https://www.enisa.europa.eu/about-enisa*.
[4] Lella I, Tsekmezoglou E, Theocharidou M, et al. ENISA Threat Landscape 2023. DOI: 10.2824/782573.
[5] Theocharidou M, Lella I. ENISA Threat Landscape: Health Sector. Epub ahead of print 2023. DOI: 10.2824/163953.
[6] Marceglia S, Balestra G, Bottrighi A, et al. Developing the Digital Healthcare Workforce in Italy: The SIBIM Experience. In: *Studies in Health Technology and Informatics*. IOS Press BV, 2022, pp. 46–50.
[7] OWASP Top 10. *https://owasp.org/www-project-top-ten/*.
[8] OWASP Web Security Testing Guide. *https://owasp.org/www-project-web-security-testing-guide/*.
[9] OWASP - Testing Tools Resource. *https://owasp.org/www-project-web-security-testing-guide/v42/6-Appendix/A-Testing_Tools_Resource*.
[10] Aydos M, Aldan Ç, Coşkun E, et al. Security testing of web applications: A systematic mapping of the literature. *Journal of King Saud University - Computer and Information Sciences* 2022; 34: 6775–6792.
[11] Burp Suite. *https://portswigger.net/burp*.
[12] Kashyap T. The Ultimate Testing Toolkit - 11 Essential Tools for Website Security Testing. *https://www.bugraptors.com/blog/security-testing-tools*.
[13] Zed Attack Proxy (ZAP). *https://www.zaproxy.org/*.
[14] Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU). *https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/computer-emergency-response-team-eu-institutions-bodies-and-agencies-cert-eu_en*.