CHAPTER V
CONCLUSION AND RECOMMENDATIONS

This chapter presents the conclusions from the research conducted on a comparative analysis of two scanning tools OWASP ZAP and Nessus against four websites: bWAPP, Metasploitable 3, Zero Bank, and Website X. The findings are presented based on each tools ability to detect vulnerabilities, a comparison of the scanning results provided, and their effectiveness in detecting website vulnerabilities. The objective of this study is to provide an overview of the capabilities or performance of these tools in detecting website vulnerabilities. Ultimately, it is hoped that the results of this study will provide appropriate recommendations for penetration testers on which scanning tools to use to detect website vulnerabilities.

5.1. Conclusion

Based on research conducted on a comparative analysis of OWASP ZAP and Nessus using vulnerability scanning methods on the four websites, the following conclusions were reached:

1. OWASP ZAP was able to detect vulnerabilities on all four websites under study. The scans conducted on these four websites focused on detecting vulnerabilities related to website structure, information leaks via HTTP headers, and vulnerabilities in publicly exposed components. On bWAPP, OWASP ZAP successfully detected 24 vulnerabilities, with 20 valid and 4 invalid. On Metasploitable 3, OWASP ZAP successfully detected 26 vulnerabilities, with 18 valid and 8 invalid. On Zero Bank, OWASP ZAP successfully detected 11 vulnerabilities, with 10 valid and 1 invalid. On Website X, OWASP ZAP successfully detected 13 vulnerabilities, with 11 valid and 2 invalid. Overall, OWASP ZAP outperformed in detecting structural vulnerabilities at the web application layer.
2. Nessus was able to detect vulnerabilities on all four websites under study, though with a different focus than OWASP ZAP. The scans conducted on the four websites focused on detecting vulnerabilities related to the software used as well as vulnerabilities at the network layer. On bWAPP, OWASP ZAP successfully detected 23 vulnerabilities, with 14 valid and

9 invalid. On Metasploitable 3, OWASP ZAP successfully detected 10 vulnerabilities, with 9 valid and 1 invalid. On Zero Bank, OWASP ZAP successfully detected 8 vulnerabilities, all of which were valid. On website X, OWASP ZAP successfully detected 7 vulnerabilities, with 6 valid and 1 invalid. Overall, Nessus outperformed OWASP ZAP in detecting vulnerabilities in the website's system and infrastructure components.

3. There are significant differences in the scan results between OWASP ZAP and Nessus. In terms of vulnerability types, OWASP ZAP detects more vulnerabilities at the web application layer, such as HTTP header configuration errors, the absence of Anti-CSRF tokens, XSS vulnerabilities, and the disclosure of information via response headers. Meanwhile, Nessus detects more vulnerabilities in infrastructure and server components, such as vulnerable Nginx versions, exposed Git repositories, and system information leaks. In terms of ease of use, OWASP ZAP requires proxy configuration and two scanning processes—Automatic and Manual Scanning—to obtain comprehensive results, whereas Nessus only requires a single feature, the Web Application Test, without any proxy configuration. In terms of limitations, OWASP ZAP can be used for free with no limit on the number of websites scanned, while Nessus has a limit on the number of websites in its free version but offers more extensive capabilities in its paid version.
4. Quantitatively, the effectiveness of the two tools was evaluated based on three priority scenarios. In the first scenario, which prioritized detection accuracy and completeness, Nessus performed better on average (Mean Effectiveness 0.32 vs. 0.31). In the second scenario, which prioritizes the detection of vulnerabilities with the highest severity, OWASP ZAP outperformed Nessus (0.41 vs. 0.40). In the third scenario, which prioritizes scanning speed, Nessus once again outperformed OWASP ZAP (0.38 vs. 0.34). Qualitatively, OWASP ZAP is more effective at detecting structural vulnerabilities in web applications, while Nessus is more effective at detecting infrastructure and system component vulnerabilities. Therefore, using both tools in combination is highly recommended to

achieve more comprehensive vulnerability scanning coverage across various aspects of website security.

5.2. Recommendations

Based on the research conducted, several recommendations can be made for future research as well as for the administrators of the relevant websites. The recommendations are as follows:

1. Administrators of website X are advised to immediately address the identified critical vulnerabilities, particularly the “Git Repository Served by Web Server” and “Hidden File Found” vulnerabilities, which have a CVSS score of 7.5 (High), and to promptly implement security headers such as Content Security Policy (CSP), Strict-Transport-Security (HSTS), and X-Content-Type-Options. Furthermore, vulnerability scans should be conducted periodically using both tools simultaneously so that security gaps in both the application and infrastructure can be identified and addressed promptly.
2. For future researchers, it is recommended to use a combination of OWASP ZAP and Nessus simultaneously during the vulnerability scanning process, as the two tools complement each other in terms of vulnerability detection coverage, resulting in more comprehensive findings.
3. Future research is recommended to explore the use of other tools, such as Acunetix or OpenVAS, as additional points of comparison, thereby providing a broader perspective on the effectiveness of various vulnerability scanning tools in the context of web application security. Additionally, the scope of the research could be expanded by including other vulnerable web applications or real-world websites.