CHAPTER V
CONCLUSION

5.1 Conclusion

Based on the results of the security testing research conducted on the PT. XYZ e-commerce website using the PTES method with reference to NIST SP 800-115 and OWASP Top 10, the following conclusions can be drawn:

1. Vulnerability identification was carried out through a combination of automated scanning using OWASP ZAP with the Active Scan feature configured with Laravel CSRF token-based authentication context, and manual scanning using Burp Suite. The automated scan produced 48 alerts, while the manual scan of the /back-auth directory discovered through wfuzz enumeration added 3 findings that were not detected by the automated scan. All findings were verified to eliminate false positives and then mapped to OWASP Top 10 2021 categories, resulting in 37 valid findings consisting of 1 High, 16 Medium, and 20 Low. Of these 37 findings, six vulnerabilities were successfully exploited actively, namely Clickjacking, CSP Header Not Set, Vulnerable JS Library, Cross-Domain Misconfiguration, Source Code Disclosure, and Username Enumeration & Brute Force, with five carrying a Medium risk level and one carrying a High risk level.
2. Security testing of the PT. XYZ e-commerce website was carried out through seven PTES phases with reference to NIST SP 800-115 guidelines at each stage. The Pre-engagement phase produced three foundational testing documents, namely the official authorization letter, NDA, and Rules of Engagement. The Intelligence Gathering phase, using Google Dorking, WHOIS, wfuzz, Wappalyzer, Nmap, and Burp Suite in accordance with NIST SP 800-115 sub-section 4.1, successfully identified technologies, directories, open ports, as well as weaknesses in the header configuration and cookies of the target system. The Threat Modeling phase identified 5 critical assets, 4 threat actors, and 10 attack surfaces. The Vulnerability Analysis phase, through a combination of automated and manual scanning, produced 37 findings that were all mapped to OWASP Top 10 2021, with a dominance of A05 Security Misconfiguration at 18 findings and A01 Broken Access Control at 8 findings. The Exploitation phase successfully proved six vulnerabilities in a controlled manner in accordance with NIST SP 800-115 Section

5.2. The Post Exploitation phase identified four potential follow-up attacks that could not be executed due to Rules of Engagement restrictions. The Reporting phase documented all findings along with Laravel-based remediation recommendations in accordance with NIST SP 800-115 reporting guidelines.

5.2 Recommendations

Based on the research results and conclusions that have been outlined, the following recommendations can be considered by the relevant parties:

1. PT. XYZ is advised to immediately follow up on the remediation recommendations in this research, prioritizing the handling of the Username Enumeration & Brute Force vulnerability through the implementation of rate limiting, unification of login error messages, and the addition of CAPTCHA on the administrator page. In addition, the addition of security headers, updating of JavaScript libraries, restriction of CORS configuration, and disabling of debug mode in the production environment need to be addressed in the near term. PT. XYZ is also advised to schedule regular security testing at least once a year or whenever there are significant system updates.
2. Future researchers are advised to expand the testing scope by including network security and mobile application security aspects if PT. XYZ develops a mobile-based application. The combinative use of black box, grey box, and white box testing methods can also provide more comprehensive vulnerability identification results. Furthermore, the integration of the PCI-DSS (Payment Card Industry Data Security Standard) can be considered given that the e-commerce website processes financial transaction data, so that the security aspects of the payment gateway can be tested more thoroughly.