CHAPTER V
CONCLUSION

5.1. Conclusion

This study aimed to comprehensively evaluate the security of the MAJADIGI web application owned by the East Java Provincial Communication and Informatics Office using a Vulnerability Assessment and Penetration Testing (VAPT) approach integrated with the OWASP Top 10:2021 framework, MITRE ATT&CK, and CVSS v3.1 assessment. Based on all testing stages that were conducted, starting from planning, information gathering, vulnerability scanning, validation, and controlled exploitation, this study produced the following conclusions:

1. Of the 12 indications of vulnerability detected in the scanning phase, manual validation confirmed 9 of the findings as True Positive. The nine vulnerabilities are distributed into three OWASP Top 10:2021 categories, including in category A05:2021 - Security Misconfiguration includes six findings, namely CSP: Failure to Define Directive with No Fallback, CSP: Wildcard Directive, CSP: script-src unsafe-inline, CSP: style-src unsafe-inline, Content Security Policy Header Not Set, and Missing Anti-Clickjacking Header, then in category A01:2021 - Broken Access Control includes two findings, namely Absence of Anti-CSRF Tokens and Cross-Domain Misconfiguration, and category A07:2021 - Identification and Authentication Failures includes one finding, namely Information Disclosure - JWT in Browser localStorage. The dominance of the vulnerability category in Security Misconfiguration indicates that the main security problem in MAJADIGI stems from the configuration of browser-side security mechanisms that have not been fully and consistently implemented, both on the main domain of the portal and the SSO domain of MAJADIGI.
2. Mapping to the MITRE ATT&CK Enterprise Matrix shows that 9 True Positive findings are distributed into four attack tactics. Execution tactics are mapped to CSP Findings: Failure to Define Directive with No Fallback (Score 6.1), CSP: Wildcard Directive (Score 6.1), CSP: script-src unsafe-inline (Score 6.1), Content Security Policy Header Not Set (Score 6.1), via the T1059.007 (Command and Scripting Interpreter: JavaScript) technique, which means that

the absence or weakness of CSP configurations on both domains opens the path for unhindered execution of malicious scripts. Furthermore, the Impact tactic is mapped to CSP: style-src unsafe-inline (Score 6.1), via technique T1491.001 (Defacement: Internal Defacement), which means that its weakness in style-src restriction allows manipulation of interface views that have the potential to mislead users, and the Collection tactic is mapped to Absence of Anti-CSRF Tokens (Score 5.4) and Missing Anti-Clickjacking Headers (Score 4.7) through technique T1185 (Browser Session Hijacking), which illustrates potential abuse User sessions are authenticated through cross-domain requests or iframe-based interface manipulation. The Credential Access tactic is mapped to Information Disclosure - JWT in Browser localStorage (Score 6.9) via the T1539 (Steal Web Session Cookie) technique, which reflects the risk of theft of authentication tokens from localStorage, and then, the Cross-Domain Misconfiguration findings (Score 4.3) are mapped to the Reconnaissance and Collection tactics through the T1590 and T1213 techniques, as the overly permissive CORS configuration allows for cross-domain reading of internal structural data. From this mapping, two interconnected attack chains were identified, with Content Security Policy Header Not Set Findings as the entry point and Information Disclosure Findings - JWT in Browser localStorage as the end target of authentication token theft. The CVSS v3.1 assessment resulted in scores in the range of 4.3 to 6.9, with all findings being in the Medium risk category. Information Disclosure - JWT in Browser localStorage earned the highest score of 6.9 with a value of Confidentiality:High, making it a finding that has the potential to directly expose users' personal data.

3. Mitigation recommendations are compiled based on three priority levels established from the results of the CVSS v3.1 assessment integrated with the strategic position of each finding in the attack chain. At High Priority, the Information Disclosure Finding - JWT in Browser localStorage is recommended to be fixed by moving the authentication token from localStorage to the HttpOnly cookie and removing the token delivery pattern over the URL. In Medium Priority, there are seven findings recommended to be addressed in order, starting from Content Security Policy Header Not Set Findings prioritized because remediation can simultaneously close the gap in

Missing Anti-Clickjacking Header Findings, followed by CSP Findings: script-src unsafe-inline through migration to nonce-based CSP, then CSP Findings: style-src unsafe-inline by moving inline styles to external CSS files, then CSP: Failure to Define Directive with No Fallback with the addition of form-action and default-src directives to Keycloak configurations, CSP: Wildcard Directive findings with allowlist definitions on all CSP directives, Findings of Absence of Anti-CSRF Tokens with implementation of Synchronizer Token Pattern and changes to SameSite attributes on session cookies, and Finding Missing Anti-Clickjacking Headers that are automatically closed along with Content Security Findings remediation Policy Header Not Set. Furthermore, at Normal Priority, Cross-Domain Misconfiguration Findings are recommended to be addressed by overriding the wildcard CORS configuration using a trusted domain allowlist explicitly defined through Cloudflare Transform Rules.

Overall, this study demonstrates that integrating the four frameworks, namely VAPT, OWASP Top 10:2021, MITRE ATT&CK, and CVSS v3.1, can produce a more comprehensive security evaluation compared to the single-framework approaches commonly used in previous studies. This integrated approach is not only capable of identifying vulnerabilities technically, but also of explaining how those vulnerabilities may be exploited in real-world attack scenarios, measuring their impact quantitatively, and determining mitigation priorities systematically.

5.2. Recommendations for Future Development

This study successfully identified and analyzed vulnerabilities within the MAJADIGI web application. However, several aspects remain outside the scope of this research due to the limitations of the defined methodology and testing boundaries. The following recommendations may serve as considerations for future researchers as well as for the East Java Provincial Communication and Informatics Office as the system administrator:

1. Expansion of the testing approach from grey-box to white-box. This study was limited to grey-box testing using public access and registered user credentials without access to source code or server configurations. Future studies are recommended to adopt a white-box testing approach that provides broader access, thereby enabling the identification of vulnerabilities that cannot be

reached through grey-box testing, such as business logic weaknesses and deeper backend-layer vulnerabilities.

2. Periodic security testing by the East Java Provincial Communication and Informatics Office. The results of this study only reflect the security condition of MAJADIGI during the defined testing period. Therefore, the Communication and Informatics Office is advised to conduct regular security testing after each system modification or update so that newly emerging vulnerabilities can be identified and addressed promptly.
3. Follow-up implementation of mitigation recommendations based on the established priority order. The East Java Provincial Communication and Informatics Office, as the administrator of MAJADIGI, is advised to follow up on the nine True Positive findings according to the mitigation priority order presented in Table 4.27. Primary attention should be given to Finding #10 (JWT in Browser localStorage) because it is the only finding with the potential to expose users' personal data protected under Law No. 27 of 2022. In addition, Finding #8 (CSP Header Not Set) should also be addressed as early as possible due to its role as the root cause that directly facilitates the most critical attack chain.

The results of this study are expected to serve as a reference for future researchers in the field of public-sector web application security and as a consideration for the East Java Provincial Communication and Informatics Office in continuously strengthening the security of the MAJADIGI portal.