

CHAPTER 5. CONCLUSION AND RECOMENDATIONS

5.1. Conclusion

This thesis has demonstrated the effectiveness of a threat modelling based risk management approach to secure PT XYZ's Content Management System (CMS). By integrating the STRIDE and LINDDUN methodologies with a DREAD assessment and a comprehensive vulnerability and security gap analysis, this study provides a structured framework for identifying, analyzing, and mitigating technical and privacy threats.

The results indicate that the CMS used by PT XYZ is vulnerable to several critical attack vectors, with 31 threats identified in the journalist process and 41 in the editor process. The most common and high-profile threats include SQL injection, authentication bypass, brute-force login attacks, unauthorized API access, and denial of service (DoS). These risks, if left unchecked, could significantly compromise the confidentiality, integrity, and availability of the platform.

The vulnerability analysis phase, supported by both automated tools and manual assessment, identified common vulnerabilities aligned with OWASP Top 10 categories such as injection flaws, broken access control, and insecure design. The security gap analysis further revealed weaknesses in PT XYZ's existing security posture, particularly in areas such as access control, session management, and secure coding practices. These insights reinforced the necessity for an integrated risk management framework that is proactive, adaptable, and continuously updated to match the evolving threat landscape.

The DREAD model serves as an effective tool for assessing risks by offering a structured and systematic approach to evaluating potential threats. It takes into account multiple dimensions, including potential damage, ease of reproduction, exploitability, the number of users impacted, and how easily the threat can be discovered. Despite its strengths, the model can be influenced by subjectivity, as the assessment outcomes often rely on the evaluator's expertise and personal judgment.

In conclusion, this thesis lays the foundation for a threat aware and risk based security strategy for content management systems in media organizations. It not only offers an actionable framework for risk mitigation but also contributes to the academic body of

knowledge on combining various threat modeling techniques with measurable risk analysis. Proposed future directions aim to advance this foundation toward a more intelligent, automated, and adaptive security posture for digital content systems like PT XYZ's.

5.2.Recomendations

According to the research result in this thesis work, the author will provide recommendations to organizations:

1. For future development involves creating collaborative threat modeling environments where cross functional team including developers, security analysts, product managers, and legal advisors can contribute to and validate threat models in real-time. This would foster a more inclusive and accurate risk analysis process, improving both technical and organizational preparedness. Lastly, future research can explore the economic and organizational impact of implementing threat modeling-driven risk management, providing quantitative analysis on cost savings, incident reduction, and return on security investment (ROSI) to support executive level decision making and budget allocation.
2. To strengthen the security posture of PT XYZ's Content Management System (CMS), it is essential to implement a multi faceted strategy that integrates both policy and technical controls. First, establishing a secure development lifecycle (SDLC) policy is critical to ensure that security is embedded throughout the software development process from design and implementation to testing and deployment. This policy should define security checkpoints, threat modeling stages, code review practices, and continuous integration of security tools, promoting a culture of security by design across the organization.
3. In parallel, mandatory OWASP training for developers must be enforced to raise awareness and build competence in identifying and mitigating common vulnerabilities such as those outlined in the OWASP Top 10. This training should be regularly updated and tailored to the development context of the CMS to ensure that all engineering teams are equipped with up-to-date secure coding practices.

4. To enhance access control, PT XYZ should implement a centralized Identity and Access Management (IAM) system. This would allow for unified control over authentication, authorization, and user provisioning across all CMS components. Centralized IAM not only improves operational efficiency but also supports compliance with ISO/IEC 27001:2022 by enforcing the principle of least privilege and enabling audit logging and monitoring.
5. The organization should enforce peer reviews on all code and configuration changes, especially those affecting security critical components. Peer reviews not only help identify logical flaws and overlooked vulnerabilities but also promote accountability and shared knowledge among developers.
6. Future work in this area is expected to focus on developing more adaptive and automated methods, leveraging artificial intelligence and machine learning to detect new attack patterns in real time. This approach will become even more relevant when integrated with DevSecOps practices, where security is no longer a last resort but is embedded early in the software development cycle.(Nagasundari *et al.*, 2025) By connecting threat modeling automation and the DevSecOps pipeline, organizations can conduct continuous risk assessments, dynamically update threat scenarios, and implement mitigations more quickly and effectively.
7. It is recommended that management develop a cybersecurity awareness program that emphasizes data protection obligations under UU PDP 2022 in Content Management System (CMS) management. This program should include regular training, security incident simulations, and the dissemination of internal policies to increase employee understanding of data breach risks and their legal consequences. This way, organizations can strengthen CMS security while maintaining compliance with national regulations and building a sustainable security culture.

8. Providing a Virtual Private Network (VPN) for every Content Management System (CMS) user can be a strategic step in strengthening security. By requiring all access to the CMS to be conducted solely through a VPN, organizations can ensure that data communications are protected by end-to-end encryption, thus preventing the risk of credential theft and man-in-the-middle attacks. Furthermore, according to (Thakur *et al.*, 2015), using a VPN limits access to only authenticated devices and users, thereby reducing the possibility of unauthorized access from outside parties. VPNs are also effective in protecting journalists and editors working remotely or using vulnerable public networks, as all traffic is routed through a secure channel. From a monitoring perspective, VPNs provide greater visibility through user activity logging, enabling early detection of suspicious behavior. Thus, implementing a VPN not only adds a layer of technical protection but also strengthens access control, compliance, and the overall integrity of the CMS system.

5.3.Future Works.

For future works, This research can be expanded by developing a dynamic threat modeling dashboard that integrates real-time risk data with vulnerability scanning results. Such a dashboard could facilitate continuous monitoring, risk scoring, and automated recommendations, enhancing PT XYZ's ability to respond to emerging threats. The integration of artificial intelligence or machine learning for threat pattern recognition and anomaly detection could also improve the predictive capabilities of the system.

Future research could explore the integration of this threat modeling framework into CI/CD (Continuous Integration/Continuous Deployment) pipelines, thereby enabling automated risk evaluation during code commits and releases. This DevSecOps integration would ensure that security checks become a seamless part of agile software development practices, reducing time-to-mitigation and improving security maturity.

Cybersecurity awareness programs focused on UU PDP 2022 Personal Data Protection Law play a crucial role in increasing the understanding of Content Management System (CMS) users and administrators regarding privacy and data security risks. CMS, as

digital content management platforms, are often targeted by attacks such as unauthorized access, SQL injection, and API misuse, which, if left unaddressed, can lead to personal data leaks. Through security awareness programs, management can educate employees on the basic principles of data protection stipulated in the PDP Law, including data controller obligations (Pasal 35), access restrictions (Pasal 39), and data subjects' rights to transparency and information security (Pasal 6 and 55). This program can be implemented through **regular training, cyber incident simulations, and policy briefings** to ensure all stakeholders understand the legal, ethical, and reputational consequences of personal data breaches. Thus, cybersecurity awareness not only strengthens the CMS security posture but also ensures the organization's compliance with national regulations while building a sustainable security culture.

According to (Shinde and Ardhapurkar, 2016), penetration testing on an application is one way to verify its security. However, given that penetration testing cannot validate all threat scenarios, a layered security approach is needed to provide additional protection through the integration of static and dynamic code analysis, vulnerability scanning, continuous monitoring, and incident response procedures. Furthermore, a risk-based strategy enables organizations to focus security resources on threats with the highest impact and probability, thereby maximizing mitigation effectiveness. Integrating continuous testing into the DevSecOps pipeline further strengthens this approach, as every change in code, configuration, and infrastructure can be tested automatically and consistently. (Nagasundari *et al.*, 2025)

By combining threat modeling with a layered security approach (defense in depth), risk-based security, and continuous testing within the DevSecOps framework, threat modeling serves as the initial step in systematically identifying potential threats from the design phase, providing the basis for risk prioritization and mitigation planning. Thus, the limitations of penetration testing do not diminish the overall effectiveness of the security framework; instead, it is complemented by proactive and adaptive mechanisms that can increase the system's resilience to dynamic cyberthreats.