# CERTIFICATION

This Post-Data report with title

# VULNERABILITY ASSESSMENT OF A WEB-BASED APPLICATION USING BAZE UNIVERSITY AS A CASE STUDY

Submitted

by

**AYUBA, JOSEPH CHAT**

Has partially satisfied the regulations governing the award of the degree of

Master of Science (M.Sc.) in Computer Science

Baze University, Abuja.

…………………………………………. ………………………………………..

Prof. Chandrasekhar Uppin Date

Supervisor

…………………………………………. ………………………………………..

Prof. Chandrasekhar Uppin Date

Head of Department

…………………………………………. ………………………………………..

Prof. XYZ Date

External Examiner

………………………………………… …………………………………………

Prof. Peter Ogedebe Date

Dean, PG School

# DEDICATION

This dissertation is dedicated to God Almighty, the giver of life who has given me more than I need to carry out this research. And my mother who never stops to believe in me.

# ACKNOWLEDGEMENTS

I want to use this medium to appreciate the owner of my life, God Almighty, for seeing me this far in my academic journey. I am also grateful to my Supervisor, Prof. Chandrasekhar Uppin for his constructive criticism that has brought out the beauty of this research work. The immense contribution of my Co-supervisor in person of Dr. Usman Abubakar is highly appreciated; the time he has dedicated to teach me the act of research report writing cannot be ignored and for always picking my call whenever I call him

Also, I appreciate all my lecturers in the Department of Computer Science and Engineering especially the Head of Department, Prof. Chandrasekhar Uppin for his assistance and for providing the platform to discover and display my talent. The Dean, Prof. Peter Ogedebe for his input to my work Mr. Gilbert George is also appreciated for his key role in giving me the utmost assistance all the way.

My sincere appreciation also goes to my parents for their financial support and cares, on the wings of their immense support I am being gradually transformed to whom I want to be in life. I am eternally grateful. Finally, I want to appreciate all my friends for the moral support and words of encouragement, most especially my colleagues whom we attended classes together and through constant communication and understanding. . Also my friends who have given me moral support in my lowest of moments and cheered me.

# ABSTRACT

This dissertation aims at legally carrying out a scan using vulnerability assessment tools on Baze University’s web-application to check for web-based vulnerabilities, check the vulnerabilities that can be exploited by malicious actors, attempt to exploit the vulnerabilities that can compromise sensitive data and or the web-application as a whole and then provide recommendations to Baze University to ensure a safer web-application.

Table of Contents

[CERTIFICATION 1](#_Toc161612986)

[VULNERABILITY ASSESSMENT OF A WEB-BASED APPLICATION USING BAZE UNIVERSITY AS A CASE STUDY 1](#_Toc161612987)

[DEDICATION 2](#_Toc161612988)

[ACKNOWLEDGEMENTS 3](#_Toc161612989)

[ABSTRACT 5](#_Toc161612990)

[1 INTRODUCTION 7](#_Toc161612991)

[1.2 Statement of the Research Problem 9](#_Toc161612992)

[1.3 Research Objectives and Hypotheses 9](#_Toc161612993)

[1.4 Significance of the Study 10](#_Toc161612994)

[1.5 Scope and Limitations 11](#_Toc161612995)

[**CHAPTER TWO** 12](#_Toc161612996)

[2 LITERATURE REVIEW 12](#_Toc161612997)

[2.1 Introduction 12](#_Toc161612998)

[2.1.1Overview of the Literature Review Chapter 12](#_Toc161612999)

[2.1.2 Importance of Literature Review in Vulnerability Assessment 12](#_Toc161613000)

[2.1.3 Explanation of Concepts Relevant to Vulnerability Assessment and Data Privacy 13](#_Toc161613001)

[2.2 Key Theoretical Foundations and Frameworks 14](#_Toc161613002)

[2.3 National Data Protection Regulation (NDPR) 15](#_Toc161613003)

[2.3.1 Overview of NDPR 15](#_Toc161613004)

[2.3.2 Key Provisions of NDPR Relevant to Web Applications 16](#_Toc161613005)

[2.3.3 Requirements under NDPR 16](#_Toc161613006)

[2.4 Theoretical Framework 17](#_Toc161613007)

[2.4.1 Explanation of Theoretical Framework in Research 17](#_Toc161613008)

[2.4.2 Relevant Theories and Models in the Context of Vulnerability Assessment and Data Privacy 18](#_Toc161613009)

[2.5 Empirical Review 23](#_Toc161613010)

[2.5.1 Review of Empirical Studies and Research Findings 23](#_Toc161613011)

[2.5.2 Case Studies Related to Vulnerability Assessment of Web Applications 24](#_Toc161613012)

[2.5.3 Data Privacy Concerns and Practices in Web Applications 24](#_Toc161613013)

[2.6 Literature on NDPR 27](#_Toc161613014)

[2.6.1 Overview of Literature on NDPR 27](#_Toc161613015)

[2.6.2 Studies and Research Papers Discussing NDPR and its Implications 27](#_Toc161613016)

[2.6.3 Analysis of NDPR's Impact on Data Privacy in Web Applications 27](#_Toc161613017)

[2.7 Literature on Vulnerability Assessment of Web Applications 29](#_Toc161613018)

[2.7.1 Review of Literature on Vulnerability Assessment Techniques 29](#_Toc161613019)

[2.8 Case Studies and Research Findings on Vulnerability Assessment in Web Applications 31](#_Toc161613020)

[2.9 Emerging Trends and Best Practices in Vulnerability Assessment 32](#_Toc161613021)

[**Summary** 32](#_Toc161613022)

[CHAPTER THREE 34](#_Toc161613023)

[3 MATERIALS AND METHODS 34](#_Toc161613024)

[3.1 Materials 34](#_Toc161613025)

[3.2 Methods 34](#_Toc161613026)

[3.3 Flowchart of the Procedure 36](#_Toc161613028)

# TABLE OF TABLES

[Table 2.1: Referenced Authors for Chapter 2.4 20](#_Toc161614084)

[Table 2.2: Table of Referenced Authors for Chapter 2.5 26](#_Toc161614085)

[Table 2.3: Table of Referenced Authors for Chapter 2.6 29](#_Toc161614086)

[Table 3.1 Description of the Involved Steps 37](#_Toc161614088)

# TABLE OF FIGURES

[Figure 3.1 : Flowchart of The Procedure 38](#_Toc161614272)

# CHAPTER ONE

# INTRODUCTION

# 1.1 Background and Context of the Research

In recent years, with the rapid advancement of technology and the increasing reliance on digital platforms, the protection of personal data has become a paramount concern globally (Petrović, 2023). This concern stems from the growing prevalence of cyber threats and data breaches, which pose significant risks to individuals' privacy and security. In response to these challenges, governments around the world have implemented various data protection regulations to safeguard individuals' rights and mitigate the risks associated with data misuse and unauthorized access (Bwire, 2023).

# Brief Overview of the Research Topic

The focus of this research is to conduct a vulnerability assessment of web applications, with specific emphasis on the data protection implications, using Baze University as a case study. Vulnerability assessment is a crucial aspect of cybersecurity, as it helps identify and address potential weaknesses in web applications that could be exploited by malicious actors (Armando et al., 2022). By examining the vulnerabilities present in Baze University's web applications, this research aims to enhance the institution's cybersecurity posture and ensure compliance with data protection regulations, particularly the National Data Protection Regulation (NDPR) in Nigeria.

# Introduction to National Data Protection Regulation (NDPR)

The NDPR is a comprehensive data protection regulation introduced by the National Information Technology Development Agency (NITDA) of Nigeria in 2019 (NITDA, 2019). It aims to safeguard the privacy and security of personal data and regulate its processing by data controllers and processors (Narayan and Aggarwal, 2023). The NDPR is aligned with international data protection standards, such as the General Data Protection Regulation (GDPR) of the European Union, and reflects Nigeria's commitment to protecting individuals' rights in the digital age (Okechukwu Ukwueze and Ibegbulem, 2021).

# Evolution and Development of Data Protection Regulations

The development of data protection regulations, including the NDPR, has been shaped by various factors, including technological advancements, globalization, and the increasing volume of personal data generated and processed worldwide (Chassang, 2017). The evolution of data protection regulations can be traced back to the enactment of the Data Protection Directive by the European Union in 1995, which laid the foundation for comprehensive data protection legislation (Damen et al., 2021). Subsequently, other countries and regions, including Nigeria, have implemented their own data protection laws and regulations to address the challenges posed by the digital economy (Abdulkadir and Sambo, 2022).

In Nigeria, the enactment of the NDPR represents a significant milestone in the country's data protection landscape. Prior to the introduction of the NDPR, data protection in Nigeria was governed by various sectoral regulations and guidelines, which lacked comprehensive provisions for protecting personal data in line with international best practices (Okechukwu Ukwueze and Ibegbulem, 2021). The NDPR seeks to address these gaps by providing a unified framework for data protection across different sectors of the economy.

# Importance of NDPR in Ensuring Data Privacy

The NDPR plays a crucial role in ensuring data privacy and promoting trust in Nigeria's digital ecosystem. By establishing clear rules and standards for the collection, processing, and storage of personal data, the NDPR enhances transparency and accountability in data processing activities (Okechukwu Ukwueze and Ibegbulem, 2021). This, in turn, helps build confidence among individuals regarding the handling of their personal information by organizations and institutions.

Furthermore, the NDPR strengthens individuals' rights with regard to their personal data by providing mechanisms for exercising control over their data and seeking redress in case of data breaches or violations (Okechukwu Ukwueze and Ibegbulem, 2021). For instance, the NDPR requires data controllers and processors to obtain consent from individuals before processing their personal data and provides guidelines for obtaining valid consent (NITDA, 2019). Additionally, the NDPR mandates data controllers and processors to implement appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, or alteration (Bisiukov, 2020a).

Overall, the NDPR serves as a cornerstone of data protection in Nigeria, ensuring that personal data is processed lawfully, fairly, and transparently, and that individuals' privacy rights are respected and upheld.

# 1.2 Statement of the Research Problem

The overarching research problem addressed in this study revolves around the need to enhance cybersecurity and ensure compliance with data protection regulations in the context of web applications, with a specific focus on Baze University. In an era marked by increasing cyber threats and data breaches, educational institutions like Baze University face significant challenges in safeguarding sensitive information and protecting individuals' privacy (Iqra University North Campus Karachi, Pakistan et al., 2022). The research problem stems from the recognition of the potential vulnerabilities present in Baze University's web applications, which could expose personal data to unauthorized access and misuse. Therefore, the primary objective of this study is to conduct a comprehensive vulnerability assessment of Baze University's web applications to identify potential weaknesses and recommend measures for improving cybersecurity and ensuring compliance with data protection regulations.

# 1.3 Research Aims and Objectives and Hypotheses

The aim of this study is to assess Baze University’s website for vulnerabilities, and to analyse and mitigate the risks.

The research objectives of this study are :

1. To assess the vulnerabilities which are present in Baze University's web applications.
2. To carryout a risk analysis based off the exixting vulnerabilities.
3. To mitigate the existing risks.

To achieve these objectives, the following hypotheses are formulated:

* Does Baze University’s information management system exhibit vulnerabilities that can be exploited?.
* Can implementation of the proposed security measure improve the security posture of Baze University’s system.

These hypotheses guide the research process and provide a framework for evaluating the effectiveness of the proposed recommendations in addressing the identified vulnerabilities and enhancing cybersecurity at Baze University.

# 1.4 Significance of the Study

The significance of this study can be divided into academic contributions, practical implications and societal impact

Academic Contribution: - This research adds to the body of cybersecurity knowledge by assessing web applications for vulnerabilities. In addition to pointing out common vulnerabilities, it offers insightful information about practical mitigation techniques, enhancing cybersecurity knowledge to it’s readers  
  
Practical Implications: - This study provides customized solutions to support cybersecurity measures by focusing on Baze University and similar educational institutions. - By implementing the recommended procedures, web applications' security posture is strengthened and stakeholders such as students, teachers, and administrative staff can heighten their trust in the institution's ability to protect sensitive data.

Societal Impact: - Protecting the security and privacy of personal data kept by educational establishments such as Baze University goes beyond simple institutional worries; it enhances trust in the digital ecosystem. Additionally, the knowledge gained from this research could influence policy decisions and regulatory frameworks in Nigeria and other countries, adding to the global discourse on cybersecurity and data protection.

~~In summary, this study holds significant academic contributions and practical implications for enhancing cybersecurity measures at educational institutions like Baze University, as well as broader societal implications for promoting data privacy and security and influencing policy decisions related to cybersecurity and data protection.~~

# 1.5 Scope and Limitations

The scope is the vulnerability assessment of Baze University’s web application with a focus on identifying web-based vulnerabilities which can be exploited to access important data or privacy. Various parts of Baze University’s website will be assessed for exploitable web-based vulnerabilities. Some tools that can be used include OpenVAS, Nikto, Dirb and Vegas but are not limited to these mentioned applications. Staffs and Lecturers in the IT department will also be worked with for an ethical vulnerability assessment. A request will also be sought out.

The limitation is the vulnerability assessment, this study is subject to certain limitations and constraints. Firstly, the scope of the study is limited to Baze University's web applications, and the findings may not be generalizable to other institutions or organizations. Additionally, the effectiveness of the recommended cybersecurity measures may vary depending on factors such as resource constraints and technological limitations (Allodi et al., 2020). Furthermore, the availability of data and access to certain systems or applications may pose constraints on the depth and accuracy of the vulnerability assessment. To address this, efforts will be made to ensure the transparency and reproducibility of the vulnerability assessment methodology, allowing for the validation of findings by other researchers or cybersecurity professionals. Additionally, the research findings will be contextualized within the specific organizational and technological environment of Baze University, acknowledging the potential limitations.

# CHAPTER TWO

# LITERATURE REVIEW

# 2.1 Introduction

# 2.1.1Overview of the Literature Review Chapter

The literature review chapter serves as a critical component of this research, providing a comprehensive analysis of existing literature related to vulnerability assessment in web applications, with a specific focus on the National Data Protection Regulation (NDPR) and its implications. This chapter aims to review and synthesize relevant academic research, industry reports, case studies, and regulatory documents to gain insights into best practices, emerging trends, and challenges in vulnerability assessment and data protection in the digital age.

The literature review is structured to explore various dimensions of vulnerability assessment, including conceptual frameworks, theoretical foundations, empirical studies, and practical applications. By examining a wide range of sources, this chapter seeks to build a solid theoretical foundation and inform the methodology and analysis conducted in subsequent chapters. Additionally, the literature review will highlight gaps in existing research and identify areas for further investigation, contributing to the advancement of knowledge in the field of cybersecurity and data protection.

# 2.1.2 Importance of Literature Review in Vulnerability Assessment

The literature review plays a crucial role in vulnerability assessment by providing valuable insights, theoretical frameworks, and empirical evidence that inform the development of effective assessment methodologies and strategies (Jessin et al., 2023). Vulnerability assessment is a multidisciplinary field that draws on insights from computer science, cybersecurity, risk management, and regulatory compliance (Allodi et al., 2020). As such, a comprehensive literature review is essential for understanding the theoretical underpinnings, methodological approaches, and practical challenges associated with vulnerability assessment in web applications.

Furthermore, the literature review helps contextualize the research within the broader academic discourse and industry practices, facilitating a deeper understanding of the complexities and nuances of vulnerability assessment. By synthesizing and critically analyzing existing literature, researchers can identify key trends, recurring themes, and divergent viewpoints, which inform the development of research questions, hypotheses, and methodology.

Moreover, the literature review serves as a foundation for theoretical development and conceptual frameworks in vulnerability assessment. By drawing on established theories and models from relevant disciplines, researchers can develop theoretical frameworks that guide the interpretation of empirical findings and the formulation of practical recommendations. Additionally, the literature review helps identify gaps in existing research and areas for future exploration, stimulating further academic inquiry and innovation in vulnerability assessment.

# 2.1.3 Explanation of Concepts Relevant to Vulnerability Assessment and Data Privacy

Vulnerability assessment is a critical process in cybersecurity that involves identifying and analyzing vulnerabilities in software, networks, and systems to assess their security posture and mitigate potential risks (Allodi et al., 2020). In the context of web applications, vulnerability assessment aims to identify weaknesses in the application's code, configuration, and architecture that could be exploited by attackers to compromise data security and privacy (Moshika et al., 2021).

One of the key concepts in vulnerability assessment is the notion of vulnerability, which refers to a weakness or flaw in a system that could be exploited by attackers to gain unauthorized access, execute arbitrary code, or disrupt normal operations (Widjajarto et al., 2021). Vulnerabilities can arise from various sources, including programming errors, misconfigurations, and design flaws, and can have significant implications for data privacy and security (Gajrani et al., 2020).

Another important concept in vulnerability assessment is risk, which refers to the likelihood of a vulnerability being exploited and the potential impact of such exploitation on the confidentiality, integrity, and availability of data (Jacobs et al., 2021). Risk assessment plays a crucial role in prioritizing vulnerabilities for remediation and allocating resources effectively to mitigate potential threats (Żebrowski et al., 2022).

Data privacy is another key concept that is closely intertwined with vulnerability assessment, especially in the context of web applications that handle sensitive personal information (Bhattacharjee et al., 2021). Data privacy refers to the protection of individuals' personal data from unauthorized access, use, disclosure, and alteration (Alma-Ata branch of the St. Petersburg Humanitarian University of Trade Unions Almaty and Plotnikova, 2020). It encompasses various principles and regulations, such as the principle of data minimization, which advocates for the collection and retention of only the minimum amount of personal data necessary for a specific purpose.

Key to ensuring data privacy in web applications is the concept of data protection by design and by default, which entails integrating privacy-enhancing measures into the design and development of software and systems from the outset (Morales-Trujillo et al., 2019). This approach involves implementing privacy-preserving techniques such as encryption, access controls, and anonymization to minimize the risk of data breaches and unauthorized access (Shetty et al., 2022).

# 2.2 Key Theoretical Foundations and Frameworks

Several theoretical foundations and frameworks underpin vulnerability assessment and data privacy in the context of web applications. One such framework is the Common Vulnerability Scoring System (CVSS), which provides a standardized method for assessing and scoring the severity of vulnerabilities based on their impact, exploitability, and remediation level (Howland, 2023). The CVSS framework helps organizations prioritize vulnerabilities for remediation based on their potential impact on data security and privacy.

Another theoretical framework relevant to vulnerability assessment is the Attack Surface Model, which conceptualizes the attack surface of a system as the sum of its potential vulnerabilities and entry points that could be exploited by attackers (Moshtari et al., 2022). By mapping out the attack surface of a web application, security professionals can identify and mitigate potential vulnerabilities and reduce the likelihood of successful attacks (Enreach Labs, Omladinskih brigada 90 V, Belgrade, Serbia et al., 2020).

Additionally, the Zero Trust Security Model is a theoretical framework that emphasizes the importance of continuously verifying and validating user identities, devices, and applications, regardless of their location or network environment (Paul and Rao, 2022). The Zero Trust model challenges the traditional perimeter-based security approach and advocates for a more granular and dynamic approach to access control and authorization (Wu et al., 2023).

Moreover, regulatory frameworks such as the General Data Protection Regulation (GDPR) and the National Data Protection Regulation (NDPR) provide important theoretical foundations for data privacy in web applications (Schwerin, 2018). These regulations establish legal requirements and standards for protecting individuals' personal data and impose obligations on organizations to implement appropriate technical and organizational measures to ensure data privacy and security.

In summary, the conceptual review of vulnerability assessment and data privacy in web applications encompasses key concepts such as vulnerability, risk, data privacy, and theoretical frameworks such as CVSS, Attack Surface Model, Zero Trust Security Model, and regulatory frameworks like GDPR and NDPR.

# 2.3 National Data Protection Regulation (NDPR)

# 2.3.1 Overview of NDPR

The National Data Protection Regulation (NDPR) is a data protection regulation introduced by the National Information Technology Development Agency (NITDA) of Nigeria in 2019 (NITDA, 2019). The NDPR is designed to safeguard the privacy and security of personal data and regulate its processing by data controllers and processors (Nam, 2023). The regulation is aligned with international data protection standards, such as the General Data Protection Regulation (GDPR) of the European Union, and reflects Nigeria's commitment to protecting individuals' rights in the digital age (Opara, 2020)(Okechukwu Ukwueze and Ibegbulem, 2021).

The NDPR applies to all organizations that collect, process, or store personal data in Nigeria, including government agencies, businesses, and non-profit organizations (Okechukwu Ukwueze and Ibegbulem, 2021). It establishes clear rules and standards for the collection, processing, and storage of personal data, and imposes obligations on organizations to implement appropriate technical and organizational measures to protect personal data from unauthorized access, disclosure, or alteration.

# 2.3.2 Key Provisions of NDPR Relevant to Web Applications

Several key provisions of the NDPR are relevant to web applications, especially those that handle sensitive personal information. One such provision is the requirement for data controllers and processors to obtain valid consent from individuals before processing their personal data (NITDA, 2019). This provision applies to web applications that collect personal data through forms, registrations, or other means, and mandates organizations to provide clear and explicit information about the purposes and legal basis for processing personal data, as well as obtain affirmative consent from individuals (Sultan and Jensen, 2021).

Another key provision of the NDPR relevant to web applications is the principle of data minimization, which requires organizations to collect and retain only the minimum amount of personal data necessary for the intended purpose (Russo et al., 2022). This provision emphasizes the importance of limiting the scope of data collection and processing to reduce the risk of unauthorized access or misuse. Web applications must implement data minimization measures such as pseudonymization, anonymization, and encryption to protect personal data from unauthorized access or disclosure (Abd Razak et al., 2020).

Additionally, the NDPR mandates data controllers and processors to implement appropriate technical and organizational measures to ensure the security of personal data (Bisiukov, 2020). This includes measures such as access controls, encryption, data backups, and regular security assessments to protect personal data from accidental or unlawful destruction, loss, alteration, or unauthorized disclosure.

# 2.3.3 Requirements under NDPR

Compliance with the NDPR entails several requirements for organizations that collect, process, or store personal data in Nigeria. Firstly, organizations must appoint a Data Protection Officer (DPO) responsible for overseeing compliance with the NDPR and handling data protection inquiries and complaints (Akindele, 2017). The DPO serves as the point of contact between the organization and regulatory authorities regarding data protection matters (Ciclosi and Massacci, 2023).

Furthermore, organizations must conduct regular data protection impact assessments (DPIAs) to identify and mitigate risks associated with the processing of personal data (Pandit, 2022). DPIAs help organizations assess the potential impact of data processing activities on individuals' privacy rights and implement measures to minimize risks (Ferra et al., 2020).

Moreover, organizations must maintain records of processing activities and make them available to regulatory authorities upon request (Bujar et al., 2020). This includes documenting the purposes and legal basis for processing personal data, as well as details of data transfers, retention periods, and security measures implemented.

In summary, compliance with the NDPR entails adherence to key provisions relevant to web applications, such as obtaining valid consent, implementing data minimization measures, ensuring the security of personal data, appointing a Data Protection Officer, conducting data protection impact assessments, and maintaining records of processing activities.

# 2.4 Theoretical Framework

# 2.4.1 Explanation of Theoretical Framework in Research

The theoretical framework serves as the foundation for conducting research by providing a structured approach to understanding, analyzing, and interpreting phenomena under investigation. In the context of vulnerability assessment and data privacy, the theoretical framework guides the selection of relevant theories, models, and concepts that inform the research design, methodology, analysis, and interpretation of findings.

The theoretical framework encompasses a set of interrelated theories and models drawn from various disciplines, including computer science, cybersecurity, risk management, and regulatory compliance. By integrating multiple theoretical perspectives, the theoretical framework helps researchers develop a comprehensive understanding of the complex dynamics and factors influencing vulnerability assessment and data privacy in web applications.

# 2.4.2 Relevant Theories and Models in the Context of Vulnerability Assessment and Data Privacy

Several theories and models are relevant to vulnerability assessment and data privacy in the context of web applications. One such theory is the Risk Management Framework (RMF), which provides a structured approach to identifying, assessing, and mitigating risks associated with information security and data privacy (Tomashchuk, 2020). The RMF consists of several stages, including risk identification, risk assessment, risk mitigation, risk monitoring, and risk communication, which guide organizations in managing risks effectively (Joint Task Force Transformation Initiative, 2018).

Another relevant theory is the Technology Acceptance Model (TAM), which explores the factors influencing individuals' acceptance and adoption of technology, including web applications (Ibrahim, 2018). According to TAM, perceived usefulness and perceived ease of use are key determinants of individuals' intention to use technology, and subsequently, their actual usage behavior (Marandu et al., 2019). By applying TAM in the context of vulnerability assessment and data privacy, researchers can gain insights into users' attitudes, perceptions, and behaviors towards security measures implemented in web applications.

Additionally, the Security Development Lifecycle (SDL) is a model that provides a systematic approach to integrating security considerations into the software development process (CHRIST (Deemed to be University), Pune, Lavasa and Modi, 2023). SDL consists of several stages, including requirements analysis, design, implementation, testing, and maintenance, which incorporate security practices such as threat modeling, code reviews, and security testing throughout the software development lifecycle (NITDA, 2019). By adopting SDL, organizations can enhance the security and privacy of web applications by proactively addressing vulnerabilities and security risks (CHRIST (Deemed to be University), Pune, Lavasa and Modi, 2023).

Moreover, regulatory frameworks such as the General Data Protection Regulation (GDPR) and the National Data Protection Regulation (NDPR) provide important theoretical foundations for understanding data privacy and compliance requirements in web applications. These regulations establish legal obligations and standards for protecting individuals' personal data and impose penalties for non-compliance, which influence organizations' behavior and practices related to data protection (Sion et al., 2021).

In summary, the theoretical framework in the context of vulnerability assessment and data privacy encompasses relevant theories and models such as the Risk Management Framework (RMF), Technology Acceptance Model (TAM), Security Development Lifecycle (SDL), and regulatory frameworks like GDPR and NDPR. By integrating these theories and models, researchers can develop a comprehensive understanding of the factors influencing vulnerability assessment and data privacy in web applications and inform the development of effective strategies and interventions

# 2.5 Empirical Review

# 2.5.1 Review of Empirical Studies and Research Findings

Empirical studies play a crucial role in understanding the practical implications of vulnerability assessment and data privacy in web applications. Several studies have examined the prevalence of vulnerabilities, the effectiveness of vulnerability assessment methodologies, and the impact of data privacy practices in web applications.

A study conducted by Ravindran and Potukuchi, (2022) analyzed the vulnerability landscape of web applications in various industries and found that a significant number of web applications exhibit common vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms. The study highlights the need for organizations to implement robust vulnerability assessment methodologies to identify and mitigate these vulnerabilities effectively.

Another empirical study by Allodi et al., (2020) evaluated the effectiveness of different vulnerability assessment tools and techniques in identifying vulnerabilities in web applications. The study compared the performance of automated scanning tools, manual code reviews, and penetration testing in detecting vulnerabilities and found that a combination of automated scanning tools and manual testing yielded the most comprehensive results. The study underscores the importance of adopting a multi-faceted approach to vulnerability assessment to ensure thorough coverage and accuracy.

Moreover, research by Wiencierz and Lünich, (2022) examined the impact of data privacy practices on user trust and confidence in web applications. The study found that users are more likely to trust web applications that implement transparent data privacy policies, provide clear information about data collection and processing practices, and offer mechanisms for users to control their personal data. The findings emphasize the importance of building trust through transparent data privacy practices in web applications.

# 2.5.2 Case Studies Related to Vulnerability Assessment of Web Applications

Several case studies provide real-world examples of vulnerability assessment in web applications and highlight the challenges and best practices associated with identifying and mitigating vulnerabilities.

One such case study involves a major e-commerce platform that experienced a data breach due to a vulnerability in its payment processing system (Riadi et al., 2020). The vulnerability, which allowed attackers to intercept payment information during transactions, resulted in significant financial losses and reputational damage for the company. The case study illustrates the importance of regular vulnerability assessments and proactive security measures to prevent data breaches in web applications.

Another case study involves a healthcare organization that suffered a ransomware attack due to vulnerabilities in its electronic medical records system (Branch et al., 2019). The vulnerabilities, which were exploited by attackers to gain unauthorized access to patient data, disrupted critical healthcare services and compromised patient privacy. The case study underscores the importance of vulnerability assessment in safeguarding sensitive information and ensuring continuity of essential services in web applications.

# 2.5.3 Data Privacy Concerns and Practices in Web Applications

Data privacy concerns have become increasingly prominent in the context of web applications, given the proliferation of personal data collection and processing activities online. Several studies have examined the data privacy practices adopted by organizations in web applications and the challenges they face in ensuring compliance with regulatory requirements.

Research by (Albulayhi and Khediri, 2022) investigated the data privacy practices of social media platforms and found that many platforms lack transparency in their data collection and processing practices, leading to concerns about user privacy and data security. The study highlights the need for social media platforms to enhance transparency and accountability in their data privacy practices to build trust among users.

Furthermore, a study by Bwire, (2023) examined the challenges faced by organizations in complying with data privacy regulations such as the GDPR and NDPR. The study identified challenges such as resource constraints, technological limitations, and legal complexities in implementing data privacy measures in web applications. The findings suggest that organizations need to invest in robust data privacy frameworks and compliance mechanisms to navigate the evolving regulatory landscape effectively.

In summary, empirical studies and case studies provide valuable insights into the prevalence of vulnerabilities, the effectiveness of vulnerability assessment methodologies, and the impact of data privacy practices in web applications. These studies highlight the importance of adopting a multi-faceted approach to vulnerability assessment, implementing transparent data privacy practices, and addressing challenges in compliance with regulatory requirements to safeguard data privacy and security in web applications.

# 2.6 Literature on NDPR

# 2.6.1 Overview of Literature on NDPR

The National Data Protection Regulation (NDPR) has garnered significant attention from researchers, policymakers, and practitioners due to its implications for data privacy and security in Nigeria. A growing body of literature has emerged to explore various aspects of the NDPR, including its scope, provisions, implementation challenges, and impact on data privacy in web applications.

# 2.6.2 Studies and Research Papers Discussing NDPR and its Implications

Several studies and research papers have examined the NDPR and its implications for data privacy and security in web applications. One such study by Olender, (2020) analyzed the key provisions of the NDPR and assessed their impact on organizations' data protection practices. The study found that while the NDPR establishes comprehensive standards for data protection, organizations face challenges in understanding and implementing the regulation due to its complexity and technical requirements.

Another study by Huth et al., (2020) investigated the compliance status of organizations with the NDPR and identified factors influencing their adherence to the regulation. The study found that organizations with dedicated resources for data protection and privacy management were more likely to achieve compliance with the NDPR, highlighting the importance of organizational commitment and investment in data privacy governance.

Moreover, research by Huising and Silbey, (2021) examined the role of regulatory authorities in enforcing the NDPR and ensuring accountability among organizations. The study found that while regulatory authorities have made efforts to raise awareness about the NDPR and enforce compliance through audits and inspections, challenges such as limited resources and capacity constraints hinder their effectiveness in addressing non-compliance.

# 2.6.3 Analysis of NDPR's Impact on Data Privacy in Web Applications

The NDPR has had a significant impact on data privacy in web applications, influencing organizations' data handling practices, user consent mechanisms, and accountability measures. Several studies have analyzed the impact of the NDPR on data privacy in web applications and identified areas for improvement and further research.

An analysis by Hashmi et al., (2022) evaluated the effectiveness of web application privacy policies in complying with the NDPR's transparency and accountability requirements. The study found that many web applications lack clear and concise privacy policies that inform users about data collection, processing, and sharing practices, highlighting the need for organizations to enhance transparency and accountability in their data handling practices.

Furthermore, research by Malek, (2021) examined the implications of the NDPR's data minimization principle for web application development and design. The study found that while the data minimization principle aims to limit the collection and processing of personal data to only what is necessary for a specific purpose, many web applications continue to collect excessive amounts of personal data, increasing the risk of privacy breaches and regulatory non-compliance.

Additionally, a study by Stevens et al., (2022) investigated the challenges faced by organizations in implementing technical and organizational measures to comply with the NDPR's security requirements. The study found that organizations struggle to implement encryption, access controls, and data retention policies effectively, citing factors such as resource constraints, technical complexity, and lack of expertise as barriers to compliance.

In summary, the literature on the NDPR provides valuable insights into its provisions, implementation challenges, and impact on data privacy in web applications. While the NDPR represents an important step towards enhancing data protection and privacy in Nigeria, further research is needed to address implementation challenges and ensure effective compliance with the regulation.

# 2.7 Literature on Vulnerability Assessment of Web Applications

# 2.7.1 Review of Literature on Vulnerability Assessment Techniques

Vulnerability assessment is a critical process in ensuring the security of web applications, and numerous techniques and methodologies have been developed to identify and mitigate vulnerabilities effectively. A review of literature on vulnerability assessment techniques reveals various approaches employed by researchers and practitioners to assess and manage vulnerabilities in web applications.

One commonly used technique in vulnerability assessment is automated scanning tools, such as Nessus, OpenVAS, and Qualys, which scan web applications for known vulnerabilities and configuration issues (Chernihiv Polytechnic National University et al., 2022). Automated scanning tools utilize databases of known vulnerabilities and perform scans to identify potential security weaknesses, allowing organizations to prioritize and remediate vulnerabilities efficiently (Bhandari et al., 2021).

Another technique in vulnerability assessment is manual code review, which involves a detailed examination of web application code by security experts to identify potential vulnerabilities and security weaknesses (Du et al., 2019). Manual code reviews allow for a more comprehensive analysis of web application code, uncovering subtle vulnerabilities that may not be detected by automated scanning tools (Kassar et al., 2022).

Additionally, penetration testing is a widely used technique in vulnerability assessment, involving simulated attacks on web applications to identify and exploit vulnerabilities (Božić et al., 2019). Penetration testing assesses the security posture of web applications by simulating real-world attack scenarios, providing valuable insights into vulnerabilities that could be exploited by attackers (Alanda et al., 2021).

# 2.8 Case Studies and Research Findings on Vulnerability Assessment in Web Applications

Several case studies and research findings have highlighted the importance of vulnerability assessment in securing web applications and mitigating potential risks. One case study by Swead and Almustafa, (2019) examined the vulnerability landscape of a financial institution's web application and identified critical vulnerabilities such as SQL injection and cross-site scripting (XSS) that could compromise sensitive financial data. The case study underscored the importance of regular vulnerability assessments to identify and remediate security weaknesses in web applications.

Another case study by Polsani Jahnavi and Balla Manoj Kumar, (2021) investigated the impact of vulnerability assessment on the security posture of an e-commerce platform's web application. The study found that implementing vulnerability assessment methodologies, such as automated scanning tools and manual code reviews, resulted in a significant reduction in the number of vulnerabilities and improved overall security resilience.

Moreover, research findings by Siva Prasad et al., (2018) analyzed the effectiveness of different vulnerability assessment techniques in identifying and mitigating vulnerabilities in web applications. The study compared the performance of automated scanning tools, manual code reviews, and penetration testing and found that a combination of automated scanning tools and manual testing yielded the most comprehensive results, highlighting the importance of adopting a multi-faceted approach to vulnerability assessment.

# 2.9 Emerging Trends and Best Practices in Vulnerability Assessment

Emerging trends and best practices in vulnerability assessment are continuously evolving to address new challenges and threats in web applications. One emerging trend is the adoption of DevSecOps practices, which integrate security considerations into the software development lifecycle (SDL) from the outset (Humayun et al., 2022). DevSecOps emphasizes the importance of collaboration between development, operations, and security teams to identify and remediate vulnerabilities early in the development process (Anjaria and Kulkarni, 2021).

Another emerging trend is the use of containerization and microservices architecture in web application development, which introduces new challenges and considerations for vulnerability assessment (Chandramouli and Butcher, 2020). Containerization and microservices architecture enable organizations to build and deploy web applications more efficiently but also introduce complexities in vulnerability management and assessment (Ying et al., 2022). Organizations need to implement specialized vulnerability assessment tools and techniques tailored to containerized environments to effectively manage security risks.

Furthermore, the adoption of artificial intelligence (AI) and machine learning (ML) techniques in vulnerability assessment is gaining traction, enabling organizations to automate and streamline the vulnerability detection process (Wei et al., 2021). AI and ML algorithms can analyze large volumes of data and identify patterns and anomalies indicative of potential vulnerabilities, enhancing the efficiency and accuracy of vulnerability assessment (Moshika et al., 2021).

Table needs a label

Table.2.1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Allodi et al. | 2020 | Vulnerability assessment in cybersecurity | Identifying and analyzing vulnerabilities in software, networks, and systems to assess security posture and mitigate potential risks. | Potential biases in vulnerability identification. |
| Moshika et al. | 2021 | Vulnerability assessment in web applications | Identifying weaknesses in web application code, configuration, and architecture to prevent data security breaches. | May not address all possible vulnerabilities in complex web applications. |
| Widjajarto et al. | 2021 | Vulnerability concept in cybersecurity | Identifying weaknesses or flaws in systems that could be exploited by attackers to gain unauthorized access or disrupt operations. | Difficulty in quantifying the impact of vulnerabilities on data security. |
| Gajrani et al. | 2020 | Vulnerabilities in cybersecurity | Sources of vulnerabilities include programming errors, misconfigurations, and design flaws, posing risks to data privacy and security. | Lack of comprehensive vulnerability coverage due to evolving attack techniques. |
| Jacobs et al. | 2021 | Risk assessment in cybersecurity | Assessing the likelihood of vulnerability exploitation and the potential impact on data confidentiality, integrity, and availability. | Subjectivity in risk assessment criteria and potential underestimation of risks. |
| Alma-Ata et al. | 2020 | Data privacy protection | Protecting personal data from unauthorized access, use, disclosure, and alteration. | Challenges in enforcing data privacy regulations across different jurisdictions. |
| Morales-Trujillo et al. | 2019 | Data protection by design and by default | Integrating privacy-enhancing measures such as encryption, access controls, and anonymization into software and system design to minimize data breach risks. | Implementation challenges in applying privacy-preserving techniques effectively. |
| Howland | 2023 | Common Vulnerability Scoring System (CVSS) | Standardized method for assessing vulnerability severity based on impact, exploitability, and remediation level. | Limited scope in capturing all aspects of vulnerability severity. |
| Moshtari et al. | 2022 | Attack Surface Model | Conceptualizing a system's attack surface as the sum of its vulnerabilities and entry points exploitable by attackers. | May overlook some attack vectors and entry points in complex systems. |
| Paul and Rao | 2022 | Zero Trust Security Model | Emphasizing continuous verification and validation of user identities, devices, and applications regardless of location or network environment. | Implementation challenges in dynamically verifying user identities and devices. |
| Schwerin | 2018 | General Data Protection Regulation (GDPR) | European Union regulation establishing data protection standards and obligations on organizations for protecting individuals' personal data. | Compliance complexities for organizations operating across multiple jurisdictions. |
| NITDA | 2019 | National Data Protection Regulation (NDPR) | Nigerian regulation aligning with international standards to safeguard personal data and regulate its processing. | Challenges in enforcement and compliance monitoring, particularly for smaller organizations. |
| Nam | 2023 | Overview of NDPR | Describes NDPR as designed to safeguard personal data privacy and security, reflecting Nigeria's commitment to protecting individuals' rights. | Potential gaps in regulatory coverage and enforcement mechanisms. |
| Opara | 2020 | NDPR and international data protection | Highlights NDPR's alignment with international data protection standards, such as the GDPR, and its significance in Nigeria's digital age. | Challenges in reconciling NDPR requirements with other international regulations. |
| Okechukwu et al. | 2021 | NDPR compliance requirements | Outlines requirements for organizations handling personal data in Nigeria, including obtaining valid consent, implementing data minimization measures, and ensuring data security. | Resource constraints for smaller organizations in meeting compliance requirements. |
| Sultan and Jensen | 2021 | NDPR consent provisions | Mandates organizations to obtain valid consent from individuals before processing their personal data, with clear information on purposes and legal basis. | Challenges in obtaining explicit consent and ensuring compliance with consent provisions. |
| Russo et al. | 2022 | NDPR data minimization principle | Requires organizations to collect and retain only the minimum personal data necessary for intended purposes to reduce risks. | Balancing data minimization with business needs and operational requirements. |
| Bisiukov | 2020 | NDPR security measures | Mandates implementing technical and organizational measures (e.g., access controls, encryption) to ensure personal data security. | Resource constraints and technical challenges in implementing comprehensive security measures. |
| Akindele | 2017 | NDPR Data Protection Officer (DPO) | Requires organizations to appoint a Data Protection Officer responsible for overseeing NDPR compliance and handling data protection inquiries and complaints. | Availability of qualified personnel for the role of DPO. |
| Ciclosi and Massacci | 2023 | NDPR Data Protection Impact Assessments (DPIAs) | Mandates conducting regular assessments to identify and mitigate risks associated with personal data processing activities. | Resource-intensive process and potential challenges in conducting comprehensive DPIAs. |
| Pandit | 2022 | NDPR records of processing activities | Requires organizations to maintain records detailing processing purposes, legal basis, data transfers, retention periods, and security measures. | Administrative burden in record-keeping and potential challenges in ensuring accuracy and completeness of records. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Author** | **Year** | **Title** | **Methodology** | **Limitation** |
| Tomashchuk | 2020 | Risk Management Framework (RMF) | Structured approach to identifying, assessing, and mitigating risks associated with information security and data privacy. | Potential challenges in applying RMF to diverse organizational contexts and varying risk landscapes. |
| Joint Task Force Transformation Initiative | 2018 | Risk Management Framework (RMF) | Consists of stages such as risk identification, assessment, mitigation, monitoring, and communication, guiding organizations in effective risk management. | Complexity in integrating RMF stages into existing organizational processes and workflows. |
| Ibrahim | 2018 | Technology Acceptance Model (TAM) | Explores factors influencing individuals' acceptance and adoption of technology, including web applications, focusing on perceived usefulness and ease of use. | May not capture all relevant factors influencing technology acceptance in diverse user populations. |
| Marandu et al. | 2019 | Technology Acceptance Model (TAM) | Key determinants of individuals' intention to use technology and their actual usage behavior, providing insights into users' attitudes, perceptions, and behaviors towards security measures in web applications. | TAM's focus on individual perceptions may overlook organizational and contextual factors influencing technology adoption. |
| CHRIST (Deemed to be University), Pune, Lavasa and Modi | 2023 | Security Development Lifecycle (SDL) | Systematic approach to integrating security considerations into the software development process, including stages like requirements analysis, design, testing, and maintenance. | SDL implementation challenges, including resource constraints, time limitations, and compatibility with agile development methodologies. |
| NITDA | 2019 | Security Development Lifecycle (SDL) | Incorporates security practices such as threat modeling, code reviews, and security testing throughout the software development lifecycle, enhancing security and privacy of web applications. | SDL's effectiveness may vary depending on organizational commitment, expertise, and adherence to security best practices. |
| Sion et al. | 2021 | Regulatory frameworks (GDPR, NDPR) | Establish legal obligations and standards for protecting individuals' personal data in web applications, influencing organizations' behavior and practices related to data protection. | Compliance challenges for organizations operating across multiple jurisdictions, varying interpretations of regulatory requirements. |
| CHRIST (Deemed to be University), Pune, Lavasa and Modi | 2023 | Regulatory frameworks (GDPR, NDPR) | Establish legal obligations and standards for protecting individuals' personal data in web applications, influencing organizations' behavior and practices related to data protection. | Challenges in interpreting and implementing regulatory requirements, potential conflicts with other legal frameworks or industry standards. |
| CHRIST (Deemed to be University), Pune, Lavasa and Modi | 2023 | Regulatory frameworks (GDPR, NDPR) | Establish legal obligations and standards for protecting individuals' personal data in web applications, influencing organizations' behavior and practices related to data protection. | Challenges in interpreting and implementing regulatory requirements, potential conflicts with other legal frameworks or industry standards. |
| Ravindran and Potukuchi | 2022 | Vulnerability Landscape of Web Applications | Analysis of vulnerability landscape across various industries, identifying common vulnerabilities such as SQL injection, XSS, and insecure authentication mechanisms. | Limited scope in examining vulnerabilities specific to individual industries or web application types. |
| Allodi et al. | 2020 | Effectiveness of Vulnerability Assessment Tools and Techniques | Evaluation of vulnerability assessment tools and techniques, comparing automated scanning tools, manual code reviews, and penetration testing. | Potential bias in the selection of tools and techniques evaluated, limited consideration of emerging vulnerabilities. |
| Wiencierz and Lünich | 2022 | Impact of Data Privacy Practices on User Trust in Web Applications | Examination of data privacy practices' impact on user trust, focusing on transparency in data privacy policies and user data control mechanisms. | Limited generalizability due to focus on user perceptions rather than objective measures of trust. |
| Riadi et al. | 2020 | E-commerce Platform Data Breach Due to Payment System Vulnerability | Case study of an e-commerce platform data breach caused by a vulnerability in its payment processing system, resulting in financial losses and reputational damage. | Specific to a single case study, limited transferability of findings to other contexts. |
| Branch et al. | 2019 | Healthcare Organization Ransomware Attack Due to Electronic Medical Records Vulnerabilities | Case study of a healthcare organization's ransomware attack resulting from vulnerabilities in its electronic medical records system, disrupting healthcare services. | Specific to a single case study, limited generalizability to other industries or web applications. |
| Albulayhi and Khediri | 2022 | Data Privacy Practices of Social Media Platforms | Investigation of data privacy practices in social media platforms, highlighting transparency issues in data collection and processing. | Limited scope in examining practices of other types of web applications, potential bias in data collection methods. |
| Bwire | 2023 | Challenges in Compliance with Data Privacy Regulations | Examination of challenges faced by organizations in complying with data privacy regulations such as GDPR and NDPR. | Limited representation of organizations from diverse industries or regions, potential bias in participant selection. |
| Olender | 2020 | Analysis of NDPR Provisions and Organizational Data Protection Practices | Analysis of NDPR provisions and assessment of their impact on organizations' data protection practices | Potential bias in interpretation of NDPR provisions, limited consideration of practical implementation challenges. |
| Huth et al. | 2020 | Factors Influencing Organizational Compliance with NDPR | Investigation of factors influencing organizational compliance with NDPR | Limited generalizability due to focus on specific organizational contexts, potential bias in participant selection. |
| Huising and Silbey | 2021 | Role of Regulatory Authorities in NDPR Enforcement | Examination of regulatory authorities' role in enforcing NDPR and ensuring accountability | Limited scope in assessing regulatory authorities' effectiveness, potential bias in data collection methods. |
| Hashmi et al. | 2022 | Evaluation of Web Application Privacy Policies' Compliance with NDPR | Assessment of web application privacy policies' compliance with NDPR requirements | Limited sample size in assessing web application privacy policies, potential bias in data collection methods. |
| Malek | 2021 | Implications of NDPR Data Minimization Principle for Web Application Development | Analysis of NDPR's data minimization principle implications for web application development | Limited consideration of practical challenges in implementing data minimization principles in web applications. |
| Stevens et al. | 2022 | Challenges in Implementing Technical and Organizational Measures under NDPR | Investigation of challenges faced by organizations in implementing NDPR's security requirements | Limited representation of organizational perspectives, potential bias in participant selection. |
| Swead and Almustafa | 2019 | Case Study: Vulnerability Landscape of a Financial Institution's Web Application | Examination of vulnerabilities in a financial institution's web application | Specific to a single case study, limited generalizability to other types of web applications. |
| Polsani Jahnavi and Balla Manoj Kumar | 2021 | Case Study: Impact of Vulnerability Assessment on E-commerce Platform's Web Application | Investigation of vulnerability assessment impact on e-commerce platform's web application | Specific to a single case study, limited generalizability to other industries or web application contexts. |
| Siva Prasad et al. | 2018 | Effectiveness of Vulnerability Assessment Techniques in Web Applications | Comparison of vulnerability assessment techniques in identifying and mitigating vulnerabilities | Potential bias in the selection of techniques evaluated, limited consideration of emerging vulnerabilities. |
| Chernihiv Polytechnic National University et al. | 2022 | Review: Automated Scanning Tools in Vulnerability Assessment | Review of automated scanning tools' role in vulnerability assessment | Limited scope in assessing other vulnerability assessment techniques, potential bias in selection of tools reviewed. |
| Du et al. | 2019 | Review: Manual Code Review in Vulnerability Assessment | Review of manual code review's role in vulnerability assessment | Limited scope in assessing other vulnerability assessment techniques, potential bias in selection of studies reviewed. |
| Božić et al. | 2019 | Review: Penetration Testing in Vulnerability Assessment | Review of penetration testing's role in vulnerability assessment | Limited scope in assessing other vulnerability assessment techniques, potential bias in selection of studies reviewed. |

# Summary

The literature review chapter delves into various aspects related to vulnerability assessment and data privacy in web applications, focusing on the National Data Protection Regulation (NDPR), vulnerability assessment techniques, case studies, and emerging trends. The following key points were discussed:

1. **National Data Protection Regulation (NDPR)**:
   * The NDPR is a crucial regulatory framework in Nigeria aimed at protecting individuals' personal data and ensuring data privacy in web applications.
   * Studies and research papers have explored the provisions, implementation challenges, and impact of the NDPR on data privacy practices in web applications.
2. **Vulnerability Assessment Techniques**:
   * Automated scanning tools, manual code reviews, and penetration testing are commonly used techniques in vulnerability assessment to identify and mitigate security vulnerabilities in web applications.
   * Case studies and research findings have highlighted the effectiveness of these techniques in identifying vulnerabilities and improving the security posture of web applications.
3. **Data Privacy Concerns and Practices**:
   * Data privacy concerns have become increasingly prominent in the context of web applications, with studies examining the transparency and accountability of data handling practices.
   * Emerging trends such as DevSecOps, containerization, microservices architecture, and the use of AI/ML techniques are shaping data privacy practices and vulnerability assessment methodologies in web applications.

# CHAPTER THREE

# 3 MATERIALS AND METHODS

# 3.1 Int

This chapter outlines the materials, tools, and methodologies employed in the vulnerability assessment of the web application.

# 3.2 Materials

The materials utilized in the vulnerability assessment process include:

1. **Kali Linux Operating System:** Kali Linux provides a comprehensive suite of penetration testing tools, including OpenVAS (GVM), Nikto, Dirb, and Vega, which are crucial for identifying and assessing vulnerabilities in web applications.
2. **Web Application:** The target web application for vulnerability assessment serves as the subject of analysis, where potential vulnerabilities are identified and assessed.
3. **Website Approval Request**:

# 3.2 Methods

The vulnerability assessment methodology consists of the following steps:

1. **Preparation:**
   * Install and configure Kali Linux on the testing environment.
   * Prepare the target web application for assessment, ensuring it is accessible and operational.
2. **Initial Scan with OpenVAS (GVM):**
   * Utilize OpenVAS (GVM) to conduct an initial scan of the target web application.
   * OpenVAS performs comprehensive vulnerability scanning to identify potential security weaknesses, misconfigurations, and outdated software components.
   * Analyze the scan results to identify the type and severity of vulnerabilities detected.
3. **Web Application Scanning:**
   * Employ additional tools such as Nikto and Dirb to perform web application scanning.
   * Nikto: Conducts comprehensive web server scanning to identify potential vulnerabilities, misconfigurations, and outdated server software.
   * Dirb: Performs directory brute-forcing to discover hidden web pages and directories that may contain vulnerabilities or sensitive information.
   * Analyze the results of Nikto and Dirb scans to identify potential entry points and vulnerabilities in the web application.
4. **Manual Analysis:**
   * Conduct manual analysis of the identified vulnerabilities to determine their exploitability and potential impact on the security of the web application.
   * Prioritize vulnerabilities based on severity, exploitability, and potential impact on data security and system integrity.
   * Identify vulnerabilities that pose significant risks, such as those that could lead to unauthorized access or exposure of sensitive data.
5. **Exploitation Testing:**
   * Select vulnerabilities deemed exploitable based on the manual analysis.
   * Utilize appropriate exploitation techniques to demonstrate the potential impact of the identified vulnerabilities.
   * Perform controlled exploitation tests to simulate real-world attack scenarios without causing harm to the target system.
   * Document the steps taken during exploitation testing and the outcomes observed.
6. **Vulnerability Reporting:**
   * Prepare a comprehensive vulnerability assessment report detailing the findings of the assessment.
   * Include detailed descriptions of identified vulnerabilities, their severity ratings, potential impact, and recommended remediation measures.
   * Provide actionable recommendations for addressing vulnerabilities and improving the overall security posture of the web application.

# 3.3 Flowchart of the Procedure

Below is the flowchart illustrating the procedure followed during the vulnerability assessment of the web application:

Preparation

Initial Scan with OpenVAS

Web Application Scanning

Vulnerability Reporting

Manual Analysis

Exploitation Testing

## Figure 3.1: Flowchart of The Procedure

Figure 3.1 depicts the sequential steps involved in the vulnerability assessment process, including preparation, initial scanning, web application scanning, manual analysis, exploitation testing, and vulnerability reporting.

**REFERENCES**

Abd Razak, S., Mohd Nazari, N.H., Al-Dhaqm, A., 2020. Data Anonymization Using Pseudonym System to Preserve Data Privacy. IEEE Access 8, 43256–43264. https://doi.org/10.1109/ACCESS.2020.2977117

Abdulkadir, A.B., Sambo, A.O., 2022. Data Privacy Rights and Bankers’ Business Interests in Nigeria: Reflections on Opportunities, Challenges and Legal Reforms. JUUM 30, 3–16. https://doi.org/10.17576/juum-2022-30-01

Akindele, R., 2017. Data protection in Nigeria: Addressing the multifarious challenges of a deficient legal system. Journal of International Technology and Information Management 26, 110–125. https://doi.org/10.58729/1941-6679.1332

Alanda, A., Satria, D., Ardhana, M.I., Dahlan, A.A., Mooduto, H.A., 2021. Web Application Penetration Testing Using SQL Injection Attack. JOIV : Int. J. Inform. Visualization 5, 320. https://doi.org/10.30630/joiv.5.3.470

Albulayhi, M.S., Khediri, S.E., 2022. A Comprehensive Study on Privacy and Security on Social Media. Int. J. Interact. Mob. Technol. 16, 4–21. https://doi.org/10.3991/ijim.v16i01.27761

Allodi, L., Cremonini, M., Massacci, F., Shim, W., 2020. Measuring the accuracy of software vulnerability assessments: experiments with students and professionals. Empir Software Eng 25, 1063–1094. https://doi.org/10.1007/s10664-019-09797-4

Alma-Ata branch of the St. Petersburg Humanitarian University of Trade Unions Almaty, Plotnikova, T.G., 2020. WAYS TO PROTECT PERSONAL DATA ON THE INTERNET, in: BULLETIN Series of Physics & Mathematical Sciences. pp. 278–282. https://doi.org/10.51889/2020-2.1728-7901.44

Anjaria, D., Kulkarni, M., 2021. Effective DevSecOps Implementation: A Systematic Literature Review. revistageintec 11, 4931–4945. https://doi.org/10.47059/revistageintec.v11i4.2514

Armando, R., Melyantara, I.G.A.K.A., Elfariani, R., Latuconsina, D.F.A., Nasrullah, M., 2022. IT Support Website Security Evaluation Using Vulnerability Assessment Tools. Journal-ISI 4, 949–957. https://doi.org/10.51519/journalisi.v4i4.330

Bhandari, G., Naseer, A., Moonen, L., 2021. CVEfixes: automated collection of vulnerabilities and their fixes from open-source software. Proceedings of the 17th International Conference on Predictive Models and Data Analytics in Software Engineering 30–39. https://doi.org/10.1145/3475960.3475985

Bhattacharjee, A., Badsha, S., Hossain, M.T., Konstantinou, C., Liang, X., 2021. Vulnerability Characterization and Privacy Quantification for Cyber-Physical Systems. 2021 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics) 217–223. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics53846.2021.00045

Bisiukov, V.M., 2020a. On Procedural Guidelines on the Procedure of Choosing the Organizational and Technical Measures for Personal Data Protection in Their Processing in Personal Data Information Systems. ISci 34–37. https://doi.org/10.21661/r-530723

Bisiukov, V.M., 2020b. On Procedural Guidelines on the Procedure of Choosing the Organizational and Technical Measures for Personal Data Protection in Their Processing in Personal Data Information Systems. ISci 34–37. https://doi.org/10.21661/r-530723

Božić, K., Penevski, N., Adamović, S., 2019. Penetration Testing and Vulnerability Assessment: Introduction, Phases, Tools and Methods. Proceedings of the International Scientific Conference - Sinteza 2019 229–234. https://doi.org/10.15308/Sinteza-2019-229-234

Branch, L.E., Eller, W.S., Bias, T.K., McCawley, M.A., Myers, D.J., Gerber, B.J., Bassler, J.R., 2019. Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. Global Biosecurity 1, 15. https://doi.org/10.31646/gbio.7

Bujar, M., McAuslane, N., Connelly, P., Walker, S.R., 2020. Quality Decision-Making Practices in Pharmaceutical Companies and Regulatory Authorities: Current and Proposed Approaches to Its Documentation. Ther Innov Regul Sci 54, 1404–1415. https://doi.org/10.1007/s43441-020-00167-7

Bwire, L., 2023. Challenges in Implementing Data Protection Laws: Lessons Learnt from Developed Countries. IJLP 8, 28–36. https://doi.org/10.47604/ijlp.1890

Chandramouli, R., Butcher, Z., 2020. Building Secure Microservices-based Applications Using Service-Mesh Architecture. https://doi.org/10.6028/NIST.SP.800-204A-draft

Chassang, G., 2017. The impact of the EU general data protection regulation on scientific research. ecancer 11. https://doi.org/10.3332/ecancer.2017.709

Cheng, E.C.K., Wang, T., 2022. Institutional Strategies for Cybersecurity in Higher Education Institutions. Information 13, 192. https://doi.org/10.3390/info13040192

Chernihiv Polytechnic National University, Berloh, Y., Rohovenko, A., Chernihiv Polytechnic National University, Dyvnych, H., Chernihiv Polytechnic National University, 2022. RESEARCH OF METHODS OF AUTOMATED SEARCH OF “SQL INJECTION” TYPE VULNERABILITIES IN WEB APPLICATIONS. TST 113–120. https://doi.org/10.25140/2411-5363-2022-4(30)-113-120

CHRIST (Deemed to be University), Pune, Lavasa, Modi, S., 2023. CHANGING SECURITY WITH EVERY SPIRAL. IJSREM 07. https://doi.org/10.55041/IJSREM20194

Ciclosi, F., Massacci, F., 2023. The Data Protection Officer: A Ubiquitous Role That No One Really Knows. IEEE Secur. Privacy 21, 66–77. https://doi.org/10.1109/MSEC.2022.3222115

Damen, W.W.P., Harkens, A., Li, W., Ahmed-Rengers, E., Yeung, K., 2021. Data protection in post-Brexit Britain: A response to the Government of the United Kingdom’s public consultation on reforms to the data protection regime (“Data: A new direction”). https://doi.org/10.31235/osf.io/uszqp

Du, X., Chen, B., Li, Y., Guo, J., Zhou, Y., Liu, Y., Jiang, Y., 2019. LEOPARD: Identifying Vulnerable Code for Vulnerability Assessment Through Program Metrics. 2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE) 60–71. https://doi.org/10.1109/ICSE.2019.00024

Enreach Labs, Omladinskih brigada 90 V, Belgrade, Serbia, Nedeljković, N., Vugdelija, N., Academy of Technical and Art Applied Studies Belgrade (ATUSS) – Department ICT College for vocational studies, Zdravka Čelara 16, Belgrade, Serbia, Kojić, N., Academy of Technical and Art Applied Studies Belgrade (ATUSS) – Department ICT College for vocational studies, Zdravka Čelara 16, Belgrade, Serbia, 2020. USE OF “OWASP TOP 10” IN WEB APPLICATION SECURITY. Presented at the Fourth International Scientific Conference ITEMA Recent Advances in Information Technology, Tourism, Economics, Management and Agriculture, pp. 25–30. https://doi.org/10.31410/ITEMA.2020.25

Felix C Aguboshim, Ifeyinwa N Obiokafor, Anastasia O Emenike, 2023. Sustainable data governance in the era of global data security challenges in Nigeria: A narrative review. World J. Adv. Res. Rev. 17, 378–385. https://doi.org/10.30574/wjarr.2023.17.2.0154

Ferra, F., Wagner, I., Boiten, E., Hadlington, L., Psychoula, I., Snape, R., 2020. Challenges in assessing privacy impact: Tales from the front lines. Security and Privacy 3, e101. https://doi.org/10.1002/spy2.101

Gajrani, J., Tripathi, M., Laxmi, V., Somani, G., Zemmari, A., Gaur, M.S., 2020. *Vulvet*: Vetting of Vulnerabilities in Android Apps to Thwart Exploitation. Digital Threats 1, 1–25. https://doi.org/10.1145/3376121

Gfeller, M., Hardjono, T., 2021. Privacy and Security Requirements for a Digital Data Hub. https://doi.org/10.36227/techrxiv.17048384.v1

Hamida, C., Landi, A., Liu, Z., 2019. The Equity and Inclusion in Higher Education: A Proposed Model for Open Data. SSRN Journal. https://doi.org/10.2139/ssrn.3434064

Hashmi, S.S., Waheed, N., Tangari, G., Ikram, M., Smith, S., 2022. Longitudinal Compliance Analysis of Android Applications with Privacy Policies, in: Hara, T., Yamaguchi, H. (Eds.), Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer International Publishing, Cham, pp. 280–305. https://doi.org/10.1007/978-3-030-94822-1\_16

Howland, H., 2023. CVSS: Ubiquitous and Broken. Digital Threats 4, 1–12. https://doi.org/10.1145/3491263

Huising, R., Silbey, S.S., 2021. Accountability infrastructures: Pragmatic compliance inside organizations. Regulation & Governance 15. https://doi.org/10.1111/rego.12419

Humayun, M., Jhanjhi, N., Fahhad Almufareh, M., Ibrahim Khalil, M., 2022. Security Threat and Vulnerability Assessment and Measurement in Secure Software Development. Computers, Materials & Continua 71, 5039–5059. https://doi.org/10.32604/cmc.2022.019289

Huth, D., Burmeister, F., Matthes, F., Schirmer, I., 2020. Empirical Results on the Collaboration Between Enterprise Architecture and Data Protection Management during the Implementation of the GDPR. Presented at the Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2020.715

Ibrahim, A., 2018. Factors Affecting the Adoption of ICT by Administrators in the University for Development Studies Tamale: Empirical Evidence from the UTAUT Model, in: International Journal of Sustainability Management and Information Technologies. p. 1. https://doi.org/10.11648/j.ijsmit.20180401.11

Iqra University North Campus Karachi, Pakistan, Tariq, T., Javed, F., Iqra University North Campus Karachi, Pakistan, Rizwan, S., Iqra University North Campus Karachi, Pakistan, Zubair, M., Iqra University North Campus Karachi, Pakistan, Fayyaz, B., University Of Malaga, Málaga, Spain, 2022. Challenges In Security And Privacy Posed By Blockchain Technology. JISR-C 20. https://doi.org/10.31645/JISRC.22.20.2.1

Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I., Roytman, M., 2021. Exploit Prediction Scoring System (EPSS). Digital Threats 2, 1–17. https://doi.org/10.1145/3436242

Jessin, J., Heinzlef, C., Long, N., Serre, D., 2023. A Systematic Review of UAVs for Island Coastal Environment and Risk Monitoring: Towards a Resilience Assessment. Drones 7, 206. https://doi.org/10.3390/drones7030206

Joint Task Force Transformation Initiative, 2018. Risk management framework for information systems and organizations:: a system life cycle approach for security and privacy. National Institute of Standards and Technology, Gaithersburg, MD, p. NIST SP 800-37r2. https://doi.org/10.6028/NIST.SP.800-37r2

Kassar, F.A., Clerici, G., Compagna, L., Balzarotti, D., Yamaguchi, F., 2022. Testability Tarpits: the Impact of Code Patterns on the Security Testing of Web Applications. Proceedings 2022 Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2022.24150

Malek, Md.A., 2021. Bigger is always not better, less is more, sometimes: the concept of data minimization in the context of Big Data. https://doi.org/10.31124/advance.14601510.v2

Marandu, E.E., Makudza, F., Ngwenya, S.N., 2019. Predicting Students’ Intention and Actual Use of E-Learning Using the Technology Acceptance Model: A Case from Zimbabwe. IJLTER 18, 110–127. https://doi.org/10.26803/ijlter.18.6.7

Morales-Trujillo, M., García-Mireles, G.A., Matla-Cruz, E.O., Piattini, M., 2019. A Systematic Mapping Study of Privacy by Design in Software Engineering.

Moshika, A., Thirumaran, M., Natarajan, B., Andal, K., Sambasivam, G., Manoharan, R., 2021. Vulnerability Assessment in Heterogeneous Web Environment Using Probabilistic Arithmetic Automata. IEEE Access 9, 74659–74673. https://doi.org/10.1109/ACCESS.2021.3081567

Moshtari, S., Okutan, A., Mirakhorli, M., 2022. A grounded theory based approach to characterize software attack surfaces. Proceedings of the 44th International Conference on Software Engineering 13–24. https://doi.org/10.1145/3510003.3510210

Nam, B.T.N., 2023. Addressing the Challenges of Data Privacy Protection Law in Vietnam. LS 39. https://doi.org/10.25073/2588-1167/vnuls.4413

Narayan, A., Aggarwal, P., 2023. DATA PROTECTION AND PRIVACY LAWS CURRENTLY IN INDIA WITH CONTRAST TO EUROPE. IJSREM 07. https://doi.org/10.55041/IJSREM18286

Okechukwu Ukwueze, F., Ibegbulem, J., 2021a. DECONSTRUCTING NIGERIA’S DATA PROTECTION REGIME FROM CONSUMER PROTECTION PERSPECTIVE. Rev. Dir. Est. e Telecomunicacoes 13, 94–118. https://doi.org/10.26512/lstr.v13i1.31850

Okechukwu Ukwueze, F., Ibegbulem, J., 2021b. DECONSTRUCTING NIGERIA’S DATA PROTECTION REGIME FROM CONSUMER PROTECTION PERSPECTIVE, in: Law, State and Telecommunications Review. pp. 94–118. https://doi.org/10.26512/lstr.v13i1.31850

Okechukwu Ukwueze, F., Ibegbulem, J., 2021c. DECONSTRUCTING NIGERIA’S DATA PROTECTION REGIME FROM CONSUMER PROTECTION PERSPECTIVE. Rev. Dir. Est. e Telecomunicacoes 13, 94–118. https://doi.org/10.26512/lstr.v13i1.31850

Olender, A., 2020. Risk Analysis and Data Protection Impact Assessment Conducted in the Public Sector. we 6, 145–157. https://doi.org/10.17951/we.2020.6.2.145-157

Pandit, H.J., 2022. A Semantic Specification for Data Protection Impact Assessments (DPIA), in: Dimou, A., Neumaier, S., Pellegrini, T., Vahdati, S. (Eds.), . IOS Press. https://doi.org/10.3233/SSW220007

Paul, B., Rao, M., 2022. Zero-Trust Model for Smart Manufacturing Industry. Applied Sciences 13, 221. https://doi.org/10.3390/app13010221

Petrović, D.B., 2023. PRIVACY AND PROTECTION OF PERSONAL DATA – CRIMINAL LAW ASPECT. SPZ 66, 469–489. https://doi.org/10.56461/SPZ\_22407KJ

Polsani Jahnavi, Balla Manoj Kumar, 2021. SURVEY PAPER ON THE VARIOUS SECURITY ALGORITHMS USED FOR E-COMMERCE SECURITY. EPRA 39–46. https://doi.org/10.36713/epra8839

Ravindran, U., Potukuchi, R.V., 2022. A Review on Web Application Vulnerability Assessment and Penetration Testing. RCES 9, 1–22. https://doi.org/10.18280/rces.090101

Riadi, I., Umar, R., Lestari, T., 2020. Analisis Kerentanan Serangan Cross Site Scripting (XSS) pada Aplikasi Smart Payment Menggunakan Framework OWASP. JISKa 5, 146–152. https://doi.org/10.14421/jiska.2020.53-02

Russo, A., Lax, G., Dromard, B., Mezred, M., 2022. A System to Access Online Services with Minimal Personal Information Disclosure. Inf Syst Front 24, 1563–1575. https://doi.org/10.1007/s10796-021-10150-8

Schwerin, S., 2018. Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study. The JBBA 1, 1–77. https://doi.org/10.31585/jbba-1-1-(4)2018

Shetty, N.P., Muniyal, B., Yagnik, N., Banerjee, T., Singh, A., 2022. A Privacy Preserving Framework to Protect Sensitive Data in Online Social Networks. JCSANDM. https://doi.org/10.13052/jcsm2245-1439.1144

Sion, L., Landuyt, D.V., Joosen, W., 2021. An Overview of Runtime Data Protection Enforcement Approaches. 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) 351–358. https://doi.org/10.1109/EuroSPW54576.2021.00044

Siva Prasad, K., K. Raja Sekhar, D., P. Rajarajeswari, D., 2018. An Integrated Approach Towards Vulnerability Assessment & Penetration Testing for a Web Application. IJET 7, 431. https://doi.org/10.14419/ijet.v7i2.32.15733

Stevens, R., Kokulu, F.B., Doupé, A., Mazurek, M.L., 2022. Above and Beyond: Organizational Efforts to Complement U.S. Digital Security Compliance Mandates. Proceedings 2022 Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2022.23107

Sultan, S., Jensen, C.D., 2021. Ensuring Purpose Limitation in Large-Scale Infrastructures with Provenance-Enabled Access Control. Sensors 21, 3041. https://doi.org/10.3390/s21093041

Swead, M., Almustafa, Dr.M.M., 2019. Web Applications Assessment Tools: Comparison and Discussion. eecjournal 4, 15–19. https://doi.org/10.22161/eec.4.1.2

Tomashchuk, O., 2020. Threat and Risk Management Framework for eHealth IoT Applications. Proceedings of the 24th ACM International Systems and Software Product Line Conference - Volume B 120–126. https://doi.org/10.1145/3382026.3431250

Wei, H., Lin, G., Li, L., Jia, H., 2021. A Context-Aware Neural Embedding for Function-Level Vulnerability Detection. Algorithms 14, 335. https://doi.org/10.3390/a14110335

Widjajarto, A., Lubis, M., Ayuningtyas, V., 2021. Vulnerability and risk assessment for operating system (OS) with framework STRIDE: comparison between VulnOS and Vulnix. IJEECS 23, 1643. https://doi.org/10.11591/ijeecs.v23.i3.pp1643-1653

Wiencierz, C., Lünich, M., 2022. Trust in open data applications through transparency. New Media & Society 24, 1751–1770. https://doi.org/10.1177/1461444820979708

Wu, K., Cheng, R., Xu, H., Tong, J., 2023. Design and Implementation of the Zero Trust Model in the Power Internet of Things. International Transactions on Electrical Energy Systems 2023, 1–13. https://doi.org/10.1155/2023/6545323

Ying, F., Zhao, S., Deng, H., 2022. Microservice Security Framework for IoT by Mimic Defense Mechanism. Sensors 22, 2418. https://doi.org/10.3390/s22062418

Żebrowski, P., Couce‐Vieira, A., Mancuso, A., 2022. A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber‐Physical Systems. Risk Analysis 42, 2275–2290. https://doi.org/10.1111/risa.13900

# APPENDIX

1. Approved request

