CHAPTER II
LITERATURE REVIEW

1.6 Theoretical Foundations

The theoretical foundations used in this research are as follows:

2.1.1. Odoo ERP (On-Demand Open Object Enterprise Resource Planning)

Odoo ERP, formerly known as Open ERP, has a long history rooted in the development of open-source software. The project was first introduced in 2005 by Fabien Pinckaers in Belgium. Its initial aim was to provide an affordable and customizable ERP solution for small and medium-sized businesses. Initially, Odoo ERP included only a few basic modules such as sales, purchasing, and inventory.

Over time, the Odoo ERP project expanded rapidly and gained strong community support. Additional modules were developed by the community, and the platform began to encompass various business aspects, including manufacturing, accounting, human resources, and more. With the transition to a subscription-based open-source business model to support further development and maintenance, Odoo has become one of the most popular and successful open-source ERP platforms globally.

The development history of Odoo ERP reflects a push towards the use of open-source software in business environments and a significant contribution to developing affordable, adaptive, and customizable ERP solutions. It has become an attractive choice for many organizations seeking comprehensive enterprise management solutions.

In Odoo 17.0 documentation, it is detailed that Odoo is an integrated suite of business applications effectively designed to automate and simplify various business processes. Its main features include modularity and customization, allowing businesses to select and configure modules according to their specific needs, offering the much-needed scalability and

flexibility to adapt to changing business environments. The documentation also provides deep insights into how Odoo manages diverse business processes, such as sales, accounting, inventory management, and human resources, and details its technical framework, including the use of databases, server architecture, and programming language. Furthermore, this documentation includes case studies and practical application examples of Odoo, giving a real-world view of how these theories are applied in daily business practice.

Odoo ERP uses the Python programming language as its main language. Python was chosen for building Odoo due to its advantages. Python is known for being easy to read and understand, making it easier for developers to quickly comprehend and develop Odoo code. In addition, Python has a rich library of libraries that can be used to develop various features and functions required in an ERP application like Odoo. Python's syntactic clarity also helps in easy maintenance and code development. The use of Python in Odoo not only makes it easier to develop but also allows developers to access various third-party libraries available in the Python community to extend Odoo's functionality. This makes Odoo one of the popular and customizable open-source ERP solutions.

Odoo uses Django as one of the frameworks for web development. Django is a powerful Python web framework that simplifies the process of developing web applications. It helps Odoo in building responsive user interfaces, robust security, and efficient user session management, and also uses XML to define user interface views and the relationships between various data objects. JavaScript is used to control client-side interactivity in Odoo's web interface. Furthermore, Odoo uses the PostgreSQL database management system to store and manage data. PostgreSQL is a reliable and powerful open-source database suitable for large-scale business applications like Odoo.

An Odoo/Open ERP system offers many applications, including accounting, sales management, purchasing management, inventory

management, MRP, dashboards, point of sale, project management, and CRM modules. Additionally, many applications can be found on the Odoo Apps site (Wu & Chen, 2020). The Odoo/Open ERP system can offer various business scenarios by adjusting several parameter settings of each applied module. Odoo/Open ERP has a three-tier architecture, such as the database layer, application layer, and client layer (Almugadam et al., 2017).

ERP systems are the backbone of e-business, encompassing many systems like supply chain management, customer relationship management (CRM), knowledge management, and business intelligence (BI). Industry 4.0 is an industrialization concept using various new technologies consisting of the internet of things, wireless sensor networks, big data, and cyber-physical systems. The first phase of this concept is a well-integrated ERP system (Ganesh et al., 2016).

ERP systems can be divided into two categories: commercial (proprietary code) and free (open-source code). In the last decade, open-source ERP systems have developed rapidly. Al-Saleem compared three open-source ERP systems (such as SQL Ledger, Odoo (formerly OpenERP), and ERP5) with many criteria, showing that ERP5 can be used for medium and large enterprises, and that Odoo/Open ERP and ERP5 can be applied to small and medium-sized enterprises (SMEs). Bajaj and Ojha compared six open-source ERP systems (such as webERP, Compiere, Postbooks, OpenBravo, Opentabs, and ERP5) with several evaluation criteria, showing that open-source ERP systems are highly recommended for SMEs, and that webERP seems to be the best. Ganesh et al., (Safira Aziza, Rahayu, 2019) compared Odoo/Open ERP with other commercial and open-source ERP systems in several aspects, showing that Odoo/Open ERP has competitive potential against market leaders. In addition, the Odoo/Open ERP system has been implemented in many SMEs. For example, (Murnawan, 2017) applied the material requirements planning (MRP) and purchasing modules of the Odoo ERP system to a manufacturing company and identified characteristics and configurations.

2.1.2. OS Linux

Operating systems are a vital component in computer systems. They are responsible for managing the usage of computer hardware such as processors, memory, I/O devices, storage media, etc. Additionally, operating systems also function as a layer connecting computer hardware with software (Wahid, 2019).

Dynamic analysis of embedded firmware is a necessary capability for many security tasks, for example, vulnerability detection. Rehosting is a technique that enables dynamic analysis by facilitating the execution of firmware in a host environment detached from the actual hardware. Current rehosting techniques focus on high-fidelity execution of the entire firmware. As a result, these techniques attempt to run firmware in an emulation environment, with accurate modeling of hardware interactions (for instance, peripherals). However, these techniques are difficult to scale and have various limitations. We propose a new approach to rehosting by focusing on application components and their interactions with firmware without the need to model hardware dependencies (Ayesha & Yethiraj, 2018).

2.1.3. Cyber Learning

Education has undergone significant transformation with the advancement of information and communication technology (ICT). Cyber Learning, also known as distance learning or online learning, has become a key element in delivering education in this digital era.

The development of information and communication technology (ICT) has brought about fundamental changes in education. Cyber Learning, involving the use of digital devices and online platforms, has enabled education to take place without physical boundaries (Matkovic et al., 2018). This brings a change in the learning paradigm, opening new opportunities for educational access, and stimulating global collaboration.

The common terminology "Cyber Learning System" refers to a learning approach that utilizes digital technology and the internet to support,

enrich, and facilitate the teaching-learning process. This system allows interaction, collaboration, and access to learning resources from anywhere and at any time. Cyber Learning encompasses various methods, such as online courses, video lectures, forum discussions, interactive learning content, and more. This concept allows for flexible time- and place-based learning, enabling learners to schedule their learning according to their needs and convenience.

Cyber Learning offers several benefits, including wider and more inclusive educational access, flexibility in learning, the use of diverse learning materials, and the development of relevant technological skills. Despite its many benefits, cyber learning also faces challenges such as social isolation, difficulty in maintaining motivation, and lack of direct interaction (Wijaya & Sensuse, 2011). Solutions such as the use of collaborative platforms, online mentoring, and the integration of social activities can help address these challenges.

Cyber Learning relies on various technologies, including online learning platforms, web-based applications, and collaboration tools. The use of video conferencing, simulations, interactive content, and online examinations are also strategies used to enhance learning effectiveness.

Recent trends in cyber learning include the use of artificial intelligence (AI) for personalized learning, project-based learning, and the integration of virtual reality (VR) and augmented reality (AR) into the learning experience (Radianti et al., 2020). Cyber Learning has significantly changed the educational landscape. Despite ongoing challenges, the potential of cyber learning to deliver high-quality education to everyone is immense (Alicia & Rani, 2022). With wise use of technology, cyber learning can continue to be a major driver of educational transformation in the future.

2.1.4. Cyber Learning System Concepts

The significance of cyber education in the digital era cannot be ignored. In the efforts to prepare the young generation with relevant skills,

the Cyber Learning System emerges as a key concept that brings significant changes in education. Concepts such as e-learning that utilize digital technology, flexibility in access to learning, and interactivity that enables online collaboration, all play a role in creating a more inclusive and adaptive learning environment. Personalization of learning integrated into this system allows each student to learn in the most effective way for them, while broad access to various learning resources completes their learning experience. With these concepts, the Cyber Learning System opens doors to more dynamic and relevant learning that can meet the challenges and demands of learning in today's digital world.

2.1.5. Common Components of Cyber Learning System Concept

The common components in Cyber Learning System concepts play a key role in forming an effective and technology-oriented learning environment. E-learning platforms, serving as the hub, provide access to a variety of learning materials which can be texts, videos, or other digital learning tools. Online interaction through discussion forums and collaboration tools enables students to actively participate in discussions and share thoughts with fellow students and teachers. Evaluation and assessment tools are used to measure students' progress, while personalization ensures that the material delivered matches each student's level of understanding. The Learning Management System (LMS) acts as the central management hub, and multi-platform access allows learning from various devices. Security and privacy of student data are meticulously maintained, and technical support is available to address technical issues. With these components, the Cyber Learning System is capable of creating a learning environment that adapts to technological developments and meets the needs of students in the ever-changing digital era.

The Cyber Learning System concepts build a complex foundation for the transformation of education in the digital era. Various components, such as e-learning platforms, learning content, online interaction, and evaluation

tools, interact harmoniously to create a diverse and effective learning experience. The use of digital technology allows students to learn from anywhere and at any time, making flexibility a main pillar of this approach. The system's ability to tailor learning material to individual understanding levels through personalization makes each learning experience unique. In addition, the central role of the Learning Management System (LMS) in managing all aspects of online learning provides necessary control and efficiency in organizing learning programs. Data security and privacy of students are primary concerns, and reliable technical support is a pillar for smooth learning processes. In this way, the Cyber Learning System presents a complex and integrated learning ecosystem that can respond to the demands of modern education increasingly connected with technology.

2.1.6. Cyber Learning at Military Academy

Based on the Decision of the Chief of Staff of the Army Number Kep/372/VII/2023 dated July 10, 2023, regarding the 2023 Defense Electronics Engineering Education Curriculum at the Military Academy, the subject "Basic Technology Knowledge" is assigned the code EP2212. This subject consists of 2 credits for theory and 1 credit for practical work. The content covers essential aspects of basic cyber knowledge, highly relevant in the context of modern defense. The emphasis on cyber fundamentals in this curriculum reflects the need to prepare Cadets with a strong understanding of technology and cybersecurity, which is crucial in current military operations and national defense strategies.

The Semester Learning Plan (RPS) for the Basic Technology Knowledge course at the Department of Military Technology at the Military Academy includes topics such as cyber law and data security. The primary teaching methods are lectures and presentations, supplemented by assignments and discussions as supporting methods. Media used include computers, LCD screens, and whiteboards. Each session lasts for 2 x 50 minutes. Cadets are encouraged to study the material, participate in

discussions, seek additional references, and create summaries related to the material being taught. Assessment includes the accuracy and depth of the material, attendance, and mastery of the subject matter.

2.1.7. SQL Injection

SQL Injection is one of the types of cyberattacks that involves the insertion of malicious SQL code into input received by a web application. The goal of this attack is to manipulate or damage the database used by the application. SQL Injection attacks can result in unauthorized access to sensitive data, data destruction or alteration, and in extreme cases, the takeover of control over the system (Ceccato et al., 2016).

Essentially, SQL Injection occurs when a web application does not adequately validate or protect user inputs before executing SQL commands (Andrzejak et al., 2017). An attacker can exploit this vulnerability by inserting malicious SQL code as input. This SQL code will be executed by the database, resulting in unintended actions.

Example: Suppose a website has a search box that allows users to search for products by name. If the site does not properly validate input, an attacker could input malicious input such as ' OR '1'='1' --, which would make the SQL statement true and return all products in the database, not just the ones being searched for.

The impact of SQL Injection includes Unauthorized Access, where attackers can access sensitive data that they should not have access to, such as credit card information, personal data, or company secrets. Data Manipulation allows attackers to damage or alter data in the database, disrupting the integrity and reliability of information. Furthermore, Takeover of Control, if an attacker successfully executes certain SQL commands, they can take control of the system or database.

Preventing SQL Injection attacks can be done through several steps, including:

a. Input Validation: Ensuring that all input received by the application is properly validated, including cleaning out harmful characters.
b. Parameterized Statements: Using parameterized statements in code to separate data from SQL commands.
c. Escaping Input: Avoiding direct user input into SQL commands. Escape or sanitize input before using it in SQL queries.
d. Web Application Firewall (WAF): Using a WAF to monitor and prevent SQL Injection attacks as well as other web attacks.
e. Layered Security Principles: Implementing layered security principles by encrypting sensitive data and applying proper authorization.

SQL Injection attacks are a serious threat to the security of web applications and databases. It is important for developers and cybersecurity professionals to understand how these attacks work and to implement best practices in securing their applications and systems (Akbar et al., 2022). Education and awareness about SQL Injection are crucial for protecting sensitive information and preventing potential significant losses.

SQL stands for "Structured Query Language," which is used to interact with relational databases such as MySQL, PostgreSQL, SQL Server, and others. SQL allows users to create, manage, and access data in a structured manner (Reformat et al., 2003).

SQL is widely used for various tasks related to relational databases, including retrieving, inserting, updating, and deleting data. This language is also used to create, modify, and manage table structures, indexes, and constraints in databases (Azhary et al., 2019).

One crucial aspect of SQL is its ability to manipulate data using queries. Queries are statements or instructions used to perform operations on data (Pamungkas, 2018). In the context of data manipulation, queries are used to insert new data into the database, modify existing data, and retrieve the required data.

The concept of injection in the context of SQL refers to a technique in which an attacker exploits vulnerabilities in an application to insert

malicious SQL code into queries executed by the database. This can happen when the application does not properly validate or protect user input before incorporating it into SQL queries (Fanissa et al., 2018). SQL injection can lead to damaging attacks, such as unauthorized access to sensitive data or even the takeover of control over the system.

1.7 Previous Research Results

A deep understanding of previous research in the relevant field of study is a crucial foundation for the development of knowledge and significant problem-solving. In this context, previous research has helped establish a strong theoretical basis and has depicted findings discovered by researchers before. By understanding previous studies, we can observe developments and existing trends and assess how our research contributes to a broader understanding in the field. In this introduction, we will summarize the relevant findings of previous research. To provide a more detailed explanation of previous research, we have compiled the following table:

Table 2.1 Previous research

No	Researcher's Name & Year	Research Title	Research Method	Previous Research Findings	Relevance	Differences
1	Puji Dwi Gustiani, Rina Trisminingsih, and Lufty Abdillah (2018)	Documentation Module of Web-Based Odoo Point Of Sale Application at PT Belant Persada	Prototype Method	Lack of information on the use of Odoo POS application in Indonesia and the absence of a download function in the documentation	The documentation of the Odoo POS application for retail and restaurants can be downloaded in PDF format and video format.	Provides visual documentation and a download function different from the original documentation
2	Supriyono, S., & Sutiah, S. (2019)	Implementation of the Accelerated SAP Method in the Odoo ERP Project Module	Accelerated SAP Method	-	Project management implementation in ICT-based learning media using the ASAP method	The accuracy of the Accelerated SAP method reaches 85% in software project management implementation
3	Fitri Purwaningtias, Chairul Mukmim (2019)	ERP Modeling at Z-Tech Computers	Using UML	Conventional system	Addresses the issue of inaccurate stock information.	Focuses on computer sales.
4	Perdanakusuma, D., Puspitasari,	Implementation of Odoo ERP	Field Interview and Observation	Manual business processes and the	Integrates business	Implementation of an ERP system to

No	Researcher's Name & Year	Research Title	Research Method	Previous Research Findings	Relevance	Differences
	W., & Saputra, M. (2020)	System at PT.X to Improve Business Efficiency in Digital Printing		use of Microsoft Excel for reporting	processes in Odoo modules such as sales, accounting, purchasing, and inventory	maximize the business strategy of PT.X
5	Basma Alharbi (2021)	Development of an ERP System Design Course to Improve Students' Learning Outcomes	This research uses Kolb's Experiential Learning Theory, combining theory and practice through case discussions, system demos, interactive labs, and group projects.	Focus on improving student learning outcomes through practical experience with open-source ERP systems, different from traditional theoretical approaches.	This research is relevant to developing practical and theoretical skills of students in ERP system design, using open-source ERP systems like Odoo.	Different from other research in terms of utilizing open-source ERP systems and experiential learning-based approaches to deepen students' understanding of ERP
6	Arief Fahmie, Annisaa Miranty Nurendra (2022)	Evaluation of the Use of Odoo for HRIS Learning for Psychology Students at the Islamic University of Indonesia	CIPP Model (context, input, process, product)	Previous use of SAP HCM for HRIS learning	Evaluation of the implementation of the use of ODOO in an educational context	Focuses on HRIS learning for psychology students at the Islamic University of Indonesia using Odoo

No	Researcher's Name & Year	Research Title	Research Method	Previous Research Findings	Relevance	Differences
7	Saeful Jamal, Kusnadi Kusnadi, (2022)	Design of Odoo-Based HR-Training ERP Menu	SDLC Method	Not mentioned	Assists in managing employee training.	Focuses on employee training.
8	Vivian Chin, Hendro Lukman (2022)	Evaluation of Financial Reporting in Odoo Community ERP System	Qualitative Descriptive	Not mentioned	Evaluates financial reporting for performance management.	Focuses on financial reporting.
9	Agung Terminanto, Muhammad Fajar Ismail (2022)	Implementation of ERP-based Accounting Module using Odoo at LSP MUI	RAD (Rapid Application Development)	Not mentioned	Improvement of work efficiency in the LSP MUI accounting team.	Focuses on the use of information technology to improve the work efficiency of the accounting team at LSP MUI
10	Muhammad Fahrezha (2022)	Implementation of open-source ERP system for MSMEs (case study: 7 Rasa Cake and Catering)	Action Design Research	Not mentioned	Empowerment of MSMEs through the implementation of ERP technology to improve operational efficiency.	Focuses on improving the business system of MSMEs that were previously done manually

No	Researcher's Name & Year	Research Title	Research Method	Previous Research Findings	Relevance	Differences
11	Yohanes Eko Hadi Santuso, Addin Aditya (2022)	Business Process Analysis And Implementation Of Odoo ERP In Sales, Purchasing And Accounting	Value Chain Analysis and Conference Room Pilot	Not mentioned	Improvement of business process effectiveness and efficiency using information technology.	Focuses on identifying business processes related to Sales and Finance & Accounting at CV. Mitra Perkasa
12	Cindy Himawan (2023)	Project-Based Learning using Open Source Odoo Application in the Enterprise Resources Planning Course	This research involves curriculum surveys and analysis with the use of the Odoo application in the ERP context.	Previous research is not specifically mentioned, but there is a reference to the importance of ERP and challenges in its implementation.	This research explores the use of information technology in education, especially through the use of open-source ERP systems, to enrich the ERP curriculum.	This research shows how Odoo, as an ERP system, can be effectively used in project-based learning and is suitable for educational purposes

From the research title to be addressed, "Designing Cyber Learning Systems Using Odoo Enterprise Resource Planning at the Military Academy," the researcher draws inspiration to enrich the literature study from relevant previous researchers as follows:

a. Cindy Himawan (2023) explains research focused on project-based learning using Odoo. The proposed research adopts a similar method but with a focus on cybersecurity training.
b. Basma Alharbi (2021) describes the use of Kolb's Experiential Learning Theory in ERP course design, highlighting the importance of practical experience, which can be applied in the context of cyber learning.
c. Muhammad Fahrezha (2022) discusses the implementation of ERP systems in MSMEs, demonstrating the flexibility of Odoo in various contexts, including military education.
d. Yohanes Eko Hadi Santuso, Addin Aditya (2022) explains business process analysis and Odoo ERP implementation, offering insights into how ERP can be integrated into complex organizational structures like the military.

This research brings a new perspective by integrating ERP technology into cybersecurity education in a military environment, with the hope of providing innovative solutions to future cybersecurity education challenges.

1.8 Framework of Thought

The framework of thought presented provides a visualization of the process applied in the context of practical cyber learning for Cadets at the Military Academy. The initiation point establishes the background for the entire scenario. It begins with an understanding of the fundamental concepts and the importance of practical cyber learning.

a. Introduction to Odoo ERP: Cadets are introduced to Odoo ERP as an open-source platform to be used for the learning process.

b. Module Design: After grasping the basics of Odoo, the next step is to design modules to support the curriculum. Determining the functions and features needed to facilitate the learning process.
c. Website Design: Creating a website using Odoo ERP as an interactive learning medium. The website serves as a container for learning modules accessible by Cadets.
d. Homepage: Functions as the entry point and central navigation hub. Cadets can access various sections of the learning system.
e. Learning: From the Homepage, Cadets can navigate to the Learning area. It is divided into several sections:
    1) Theory: Theoretical learning material is presented.
    2) Pre-Test: Initial evaluation to measure Cadets' initial understanding.
    3) Post-Test: Evaluation after the theoretical material to measure improvement in understanding.
    4) Practice: Practical sessions where Cadets apply theoretical knowledge.
f. Web SQL Injection: As part of the cybersecurity curriculum, Cadets are introduced to techniques such as SQL Injection attacks. This imparts knowledge about web vulnerabilities and how to protect applications from such attacks.
g. Login Page: Cadets use the login page to access the system. This page is also used as a practice point to understand and simulate SQL Injection attacks.
h. Attack Analysis: After simulating attacks, Cadets are encouraged to analyze the attacks conducted. Understanding the impact and strategies to counter potential similar attacks.

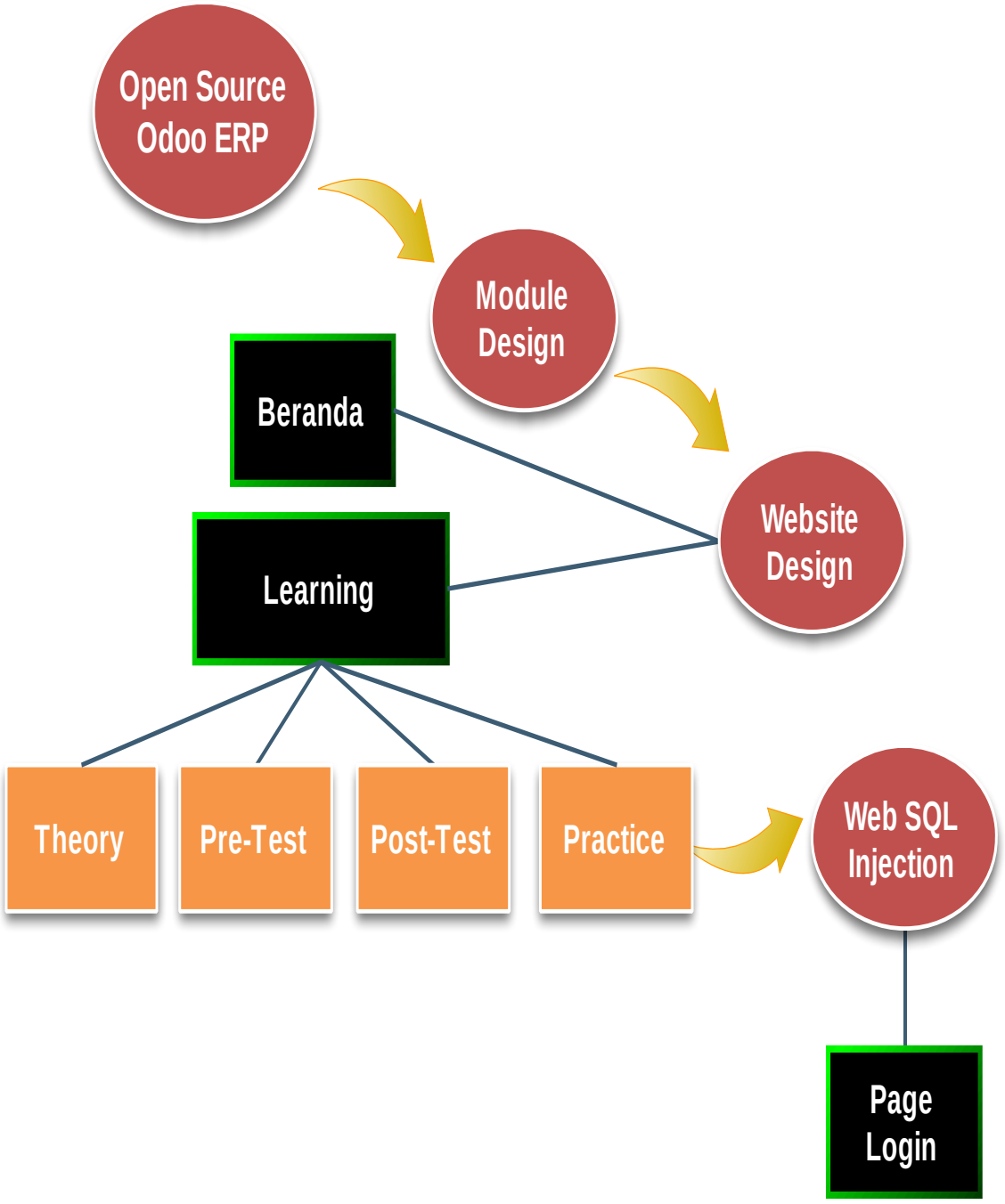

Figure 2.1 Framework of Thought