SINTECHCOM: Science, Technology and Communication Journal
Vol. 6, No. 3, June 2026, pp. 189-198, DOI: 10.59190/stc.v6i3.370

Security audit of a pharmacy information system using blackbox testing and CIA triad: A case study

Rahmalia Syahputri, M Rivaldi Arwin Hadi Wijaya*
Computer Engineering, Faculty of Computer Science, Institute of Information Technology and Business Darmajaya, Bandar Lampung 35141, Indonesia

ABSTRACT

Pharmacy information systems are essential for managing drug inventory, sales, financial reports, and user administration, yet they are exposed to security risks like data manipulation, account misuse, and information leakage. This study integrates Blackbox Testing and the CIA Triad (Confidentiality, Integrity, Availability) to audit a pharmacy application. Testing employed 19 security scenarios, supported by tools such as SQLmap, Burp Suite, OWASP ZAP, and Apache JMeter to detect vulnerabilities without accessing source code. Results show that the system meets availability requirements and provides audit logging for user activity monitoring. However, confidentiality and integrity weaknesses were identified: input validation allowed illogical data like negative stock, potential SQL Injection existed on the login page, and password encryption was insufficient. Strengthening input sanitization, adopting strong encryption, and enhancing authentication are necessary to close security gaps and improve system reliability.

ARTICLE INFO

Article history:

Received May 13, 2026
Revised May 23, 2026
Accepted May 24, 2026

Keywords:

Blackbox Testing
CIA Triad
Pharmacy Application
Security Audit

* **Corresponding Author**
E-mail address: rivaldiar.2211010077@mail.darmajaya.ac.id

1. INTRODUCTION

The rapid adoption of information systems has accelerated digital transformation across multiple sectors, including healthcare and pharmacy. Digitalization enhances operational efficiency while ensuring accuracy, speed, and transparency in data management [1, 2]. In the pharmaceutical domain, pharmacy applications serve as strategic solutions for managing drug inventory, sales transactions, financial reporting, and user administration in a computerized environment. Integrated systems enable more effective business processes compared to manual methods and minimize recording errors and data loss [3-5]. Nevertheless, the growing complexity of these systems introduces new challenges, particularly concerning data security and information protection.

A pharmacy application stores various critical and sensitive data, including drug stock, pricing, transactions, and user activities, all of which are directly tied to business operations. Without adequate security mechanisms, such systems are vulnerable to data manipulation, unauthorized modifications, account misuse, and information leakage. These risks can cause financial losses and erode trust in the system [6-9]. Therefore, a security audit is essential to ensure that the system operates in accordance with information security standards.

Security issues in information systems commonly stem from weaknesses in input validation that may trigger attacks such as SQL Injection, along with inadequate authentication and authorization mechanisms that can lead to broken authentication and access control vulnerabilities [10-12]. Moreover, storing passwords without sufficient encryption, lack of session management, and the absence of audit logging and data backup mechanisms can increase risks to confidentiality, integrity, and availability of information [13-15]. Within the context of a pharmacy application, internal fraud threats such as stock manipulation without official transactions, concurrent session misuse, and privilege escalation are also real concerns [16, 17]. A systematic, measurable, and standards-based

security evaluation approach is needed to comprehensively identify system vulnerabilities and prevent potential exploitation that could harm the organization.

Prior research has demonstrated that the Blackbox Testing method is effective for examining system functionality and identifying input validation weaknesses without requiring access to the application's source code. This approach adopts a user perspective, making it capable of detecting logic errors, validation gaps, and mismatches between outputs and system requirements [18, 19]. Meanwhile, the CIA Triad concept, comprising Confidentiality, Integrity, and Availability, has been widely used as a foundational framework for evaluating information security, as it provides a comprehensive view of a system's level of protection against security threats [20]. However, existing studies generally have limitations. Research employing Blackbox Testing often focuses solely on functional testing without linking findings to structured security impact analysis. Conversely, studies adopting the CIA Triad approach tend to be more conceptual and have not directly integrated vulnerability testing [21, 22]. The present study addresses this gap by integrating Blackbox Testing and CIA Triad analysis in a comprehensive security audit of a pharmacy application. This integration produces a more measurable, applicable evaluation oriented toward the direct identification of system vulnerabilities [23, 24].

Based on this background, the problem addressed in this study is the assessment of the security level of the pharmacy application through Blackbox Testing and evaluation of its security posture using CIA Triad analysis [25]. The objectives of this research are to conduct a security audit of the application, identify potential vulnerabilities in the login feature, drug data management, transactions, and reporting, and evaluate the implementation of confidentiality, integrity, and availability principles within the system. The scope of the study is limited to functional testing of the system using the Blackbox Testing method and security analysis based on the CIA Triad, without performing source code analysis or advanced penetration testing [26]. The findings are expected to provide theoretical contributions to the field of information system security auditing, practical benefits for pharmacy managers in enhancing system control and transparency, and serve as an academic reference for future research related to the security of information-system-based applications.

2. RESEARCH METHODS

This study adopts a systematic and measurable security audit framework. The main approach combines Blackbox Testing with the CIA Triad (Confidentiality, Integrity, Availability) risk analysis framework. The integration of these two methods allows the identification of vulnerabilities from an external user or attacker perspective without requiring access to the source code, while also evaluating the extent to which the system protects sensitive pharmacy operational data.

2.1. Planning and Scoping

This initial stage maps the architecture of the pharmacy application and defines the attack surface. Since a black-box approach is used, testing is conducted purely from an external user perspective without access to the source code or database. The scope of features to be audited is limited to critical points for pharmacy operations, namely:

- Authentication module: login form and session management mechanism.
- Data management module: forms for adding, editing, and deleting drug and stock data.
- Transaction & report module: sales processing and financial report generation features.
- Audit log module: user activity history feature.

2.2. Blackbox Testing Execution

At this stage, attack simulations and input manipulations are performed to identify security gaps within the defined scope. Unlike ordinary functional testing, this testing focuses on the system’s response to anomalous inputs. The planned security test scenarios are presented in Table 1.

2.3. Security Audit Tools

To support the Blackbox Testing scenarios and facilitate evaluation aligned with the CIA Triad, several open-source security testing tools were utilized. Each tool was selected to specifically assess one or more CIA aspects without accessing the application’s source code.

Table 1. Security test scenarios (Test cases).

Target module	Attack vector / testing technique	Security audit objective
Authentication	SQL injection (Authentication bypass)	Test whether an attacker can log in without valid credentials using SQL queries.
Authentication	Brute force / dictionary attack	Test for the presence or absence of rate limiting (temporary account lockout) after multiple incorrect passwords.
Drug data input	Stored cross-site scripting (XSS)	Test whether the system sanitizes dangerous script input in the drug name form.
Stock management	Boundary value analysis (Negative input)	Test business logic: whether the system accepts stock value manipulation to a negative (-) value.
Reports & logs	Broken access control (Privilege escalation)	Test whether a regular user (Employee) can access report URLs reserved for the Pharmacist.

- Confidentiality Testing:
  SQLmap (for automated SQL Injection detection) and Burp Suite Community Edition (for intercepting and manipulating login requests) were used to evaluate authentication bypass possibilities and session management weaknesses. These tools helped verify that sensitive data such as user credentials could not be accessed without authorization.
- Integrity Testing:
  OWASP ZAP (Zed Attack Proxy) was employed to perform input validation fuzzing on drug data forms and stock management fields. Manual boundary value analysis with ZAP's active scanner allowed the detection of illogical input acceptance, such as negative stock values. Additionally, the built-in XSS scanner was used to check for stored Cross-Site Scripting vulnerabilities in drug name fields.
- Availability Testing:
  Apache JMeter was configured to simulate concurrent user transactions, including login sessions and repeated report generation, ensuring the system remained responsive under load. The Presence System's real-time status updates were also monitored during connectivity interruptions to confirm service continuity.

All tools were operated strictly from an external user perspective, consistent with the black-box approach. Their outputs were correlated with manual observation to form the basis for vulnerability classification in the subsequent CIA Triad analysis.

2.4. CIA Triad Analysis and Risk Evaluation

After collecting vulnerability data from the Blackbox Testing phase, the findings are classified using the CIA Triad security framework parameters:

- Confidentiality: Evaluates whether the discovered gaps allow unauthorized parties to access sensitive data (e.g., password leakage, exploitation of financial data).
- Integrity: Analyzes whether validation weaknesses enable users to manipulate data without a trace (e.g., illegally changing stock levels, deleting audit logs).
- Availability: Identifies whether abnormal actions can cause the system to crash or become inaccessible to the pharmacist.

2.5. Reporting and Mitigation

The final stage involves compiling an audit report document containing a list of discovered vulnerabilities, their risk levels (based on the CIA Triad), and technical mitigation recommendations such as input sanitization, password encryption using hashing algorithms (e.g., Bcrypt), and the reinforcement of Prepared Statements in SQL queries.

3. RESULTS AND DISCUSSIONS

This section presents the findings from the Blackbox Testing and CIA Triad analysis conducted on the pharmacy application. The system description, test results, security analysis, illustrative case studies, and identified limitations are discussed sequentially.

Table 2. Drug data in the pharmacy application.

Drug name	Drug code	Price (Rp)	Drug type	Stock
Paracetamol 500mg	OBX-7A9K2	5,000	Tablet	120
Amoxicillin 500mg	OBX-3L8P1	12,000	Capsule	85
Ibuprofen 400mg	OBX-9Q2W4	8,000	Tablet	100
Cetirizine 10mg	OBX-5M7Z1	6,000	Tablet	75
Antimo	OBX-2B6N8	4,000	Tablet	150
Bodrex	OBX-8X1C3	3,500	Tablet	200
OBH Combi	OBX-4V9T6	18,000	Syrup	60
Promag	OBX-6R3H7	7,000	Chewable tablet	110
Diapet	OBX-1K5J9	6,500	Capsule	95
Betadine 60ml	OBX-7D4F2	20,000	Antiseptic solution	40

Table 3. Blackbox testing results.

Tested feature	Test scenario	Expected result	Actual result	Status
Login	Input valid username & password	Dashboard is displayed	Dashboard successfully shown	Valid
Login	Input incorrect password	System shows error "Wrong password"	Error message appears	Valid
Login	Empty username or password	System rejects login, shows validation	Validation appears	Valid
Register	New user registers with complete data	Account created, enters system	Account stored in database	Valid
Register	User registers with already registered email	System rejects, shows error message	Error message appears	Valid
Single device login	Login on device B while account active on A	Device A auto-logout, notification shown	Auto-logout succeeded	Valid
Add drug	Employee adds new drug with complete data	Data saved and displayed in drug list	Data added successfully	Valid
Add drug	Employee inputs drug data without name	System rejects, shows validation	Validation appears	Valid
Edit stock	Employee changes stock quantity	Stock updated as input	Stock updated	Valid
Restock item	Employee adds stock quantity	Stock increases by restock amount	Stock increased	Vulnerable
Drop/reduce stock	Employee reduces stock quantity	Stock decreases as input	Stock decreased	Valid
Delete drug	Employee deletes drug data	Data removed from system	Data deleted	Valid
Audit log	Employee adds/edits/deletes drug	System records activity in log (user, time, action)	Activity logged completely	Valid
Audit log	Owner opens activity history menu	System displays all user activities	Log displayed completely	Valid
Auto calculation	Drop drug transaction occurs	System calculates drop × price, updates finance	Financial report updated	Vulnerable
Financial report	Owner opens report menu	System shows total revenue based on transactions	Report displayed correctly	Needs improvement
Presence system	User logs in	Status changes to "Online"	Online status shown	Valid
Presence system	User logs out	Status changes to "Offline"	Offline status shown	Valid
Logout	User presses logout button	System returns to login page	Logout succeeded	Valid

3.1. System Description

The Pharmacy Application is a mobile-based information system designed to manage:

1. User login and authentication.
2. Drug data management.
3. Sales transactions.
4. Sales reports.
5. User activity logs.

The application stores essential drug inventory data, as listed in Table 2.

3.2. Blackbox Testing Results

Blackbox Testing was performed on the main features of the application using 19 predefined security test scenarios. The execution of these scenarios was assisted by security tools detailed in Section 2.3, which helped automate the detection of SQL Injection, XSS, and input validation flaws. The tests aimed to identify potential vulnerabilities related to Confidentiality, Integrity, and Availability. The detailed results are presented in Table 3.

Out of the 19 test scenarios, 16 returned a Valid status, indicating that most basic security functionalities performed as expected. The system successfully blocked unauthorized login attempts, enforced single-device login, and consistently recorded activity in the audit log. However, two scenarios were marked Vulnerable, namely the Restock Item and Auto Calculation features, while the Financial Report feature required improvement. These findings highlight weaknesses primarily in the Integrity pillar, concerning input validation of stock quantities and automated calculations, as well as in the Confidentiality pillar related to access control of financial data.

3.3. CIA Triad Analysis

The vulnerabilities and security postures identified during Blackbox Testing were further evaluated using the CIA Triad framework. Table 4 summarizes the relationship between each test scenario and the relevant CIA aspects.

Table 4. CIA triad evaluation.

Feature	Test scenario	CIA aspect	Security rationale
Login	Input valid	Confidentiality	Ensures only legitimate users access the system
Login	Password wrong	Confidentiality	Prevents unauthorized access
Login	Empty fields	Integrity	Validation prevents non-conforming data
Register	Complete data	Integrity	Ensures user data stored correctly
Register	Email already registered	Integrity	Prevents duplication and inconsistency
Single device login	Login on another device	Confidentiality	Prevents session sharing and account hijacking
Add drug	Complete input	Integrity	Ensures accurate drug data storage
Add drug	Without drug name	Integrity	Validation maintains database consistency
Edit stock	Change stock	Integrity	Ensures stock changes are recorded correctly
Restock item	Add stock	Integrity	Maintains inventory accuracy
Drop/reduce stock	Reduce stock	Integrity	Prevents stock manipulation
Delete drug	Delete data	Integrity	Only valid data can be deleted
Audit log	Record activity	Integrity	Activities cannot be altered without trace
Audit log	Owner views log	Confidentiality	Only authorized roles can view logs
Auto calculation	Calculate transaction	Integrity	Ensures accurate financial calculations
Financial report	Open report	Confidentiality	Financial data is sensitive
Presence system	Status online	Availability	System must be real-time and available
Presence system	Status offline	Availability	Status update must be consistent
Logout	User logout	Confidentiality	Terminates session to prevent misuse
Internet connection	Internet disconnected	Availability	System must handle connection disruptions

3.3.1. Confidentiality Analysis

The absence of a strong password encryption mechanism, as confirmed by manual inspection and Burp Suite's request analysis, presents a high risk to confidentiality. This situation exposes user credentials to potential disclosure if the database is compromised. Furthermore, the potential SQL Injection vulnerability on the login form, detected using sqlmap, significantly worsens the security

posture of this pillar, as it could lead to massive data leakage, unauthorized access, and even full account takeover.

3.3.2. Integrity Analysis

The integrity aspect exhibits medium risk due to weak server-side input validation. OWASP ZAP's fuzzing engine revealed that the system accepts illogical boundary values, such as negative stock input, which can cause inventory record inconsistencies and illegal stock manipulation. Additionally, the lack of character length restriction on input forms, also observed during ZAP passive scanning, poses a low-to-medium risk, potentially disrupting database formatting and consistency over time.

3.3.3. Availability Analysis

The availability aspect shows very satisfactory performance with low risk. Throughout the testing simulations, all main features remained consistently accessible. Functionalities such as financial report generation based on specific periods operated optimally. The system demonstrated stability without any crashes or denial-of-service incidents, even under simultaneous multi-transaction loads. The absence of significant vulnerabilities in this pillar confirms that the system architecture is robust and ready to support daily pharmacy operations without interruption.

3.4. Case Studies

To further illustrate the practical implications of the audit findings, three real-world case studies are presented.

- Case Study 1: Inventory Discrepancy Investigation
  A discrepancy occurred between the physical stock of Paracetamol and system records. While sales transactions accounted for a reduction of only 10 units, the physical count showed 30 units missing. Examination of the audit log (Figure 1) revealed that a specific user had manually executed a "drop stock" of 30 units outside the regular sales transaction mechanism. The system's detailed log, including user ID, timestamp, and action type, proved the non-repudiation capability and accurately identified the fraudulent action, thus enhancing internal transparency and asset protection.

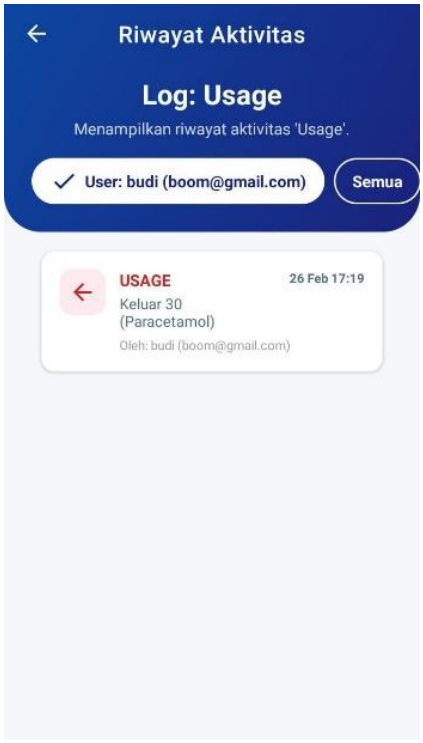

Figure 1. User activity history log.

- Case Study 2: Prevention and Detection of Illegal Access to Narcotics Data
  An attempt was made by a regular employee to access the narcotics inventory management module, which should only be accessible to the responsible pharmacist. The system immediately blocked the interface and displayed an "Access Denied" pop-up (Figure 2). Simultaneously, a hidden back-end log recorded the event as UNAUTHORIZED ACCESS (Figure 3), complete with user identity and timestamp.

Figure 2. Access denied pop-up and user activity recording.

Figure 3. Unauthorized access log in drug management module.

This demonstrates the effective implementation of Role-Based Access Control (RBAC) as a preventive control and the audit log as a detective control, reflecting a defense-in-depth approach that safeguards the confidentiality of highly regulated data.

- Case Study 3: Traceability and Recovery from Price Update Anomaly
  A drastic price anomaly was found for "Amoxicillin Syrup," which had been changed from Rp15,000 to Rp150,000. Using the deep edit logging feature, the system displayed the old value, new value, user who made the change, and the exact timestamp (Figure 4).

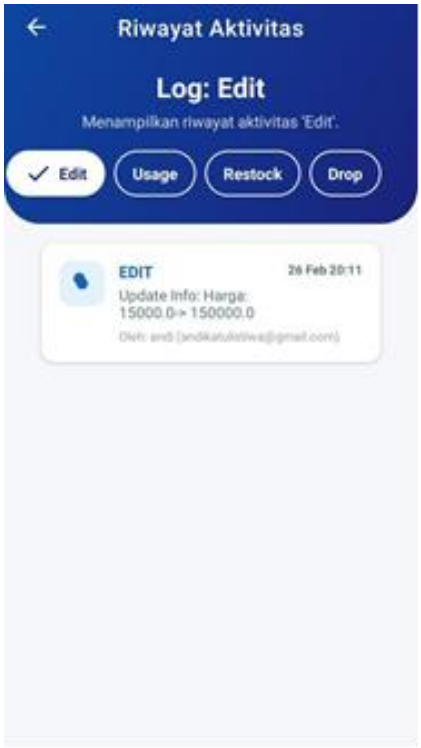

Figure 4. Edit history log – price change detail.

This granular data traceability enabled the pharmacist to quickly restore the correct price without manual estimation. The mechanism preserves data integrity by recording complete transition history, mitigating damage from human error, and strengthening data accountability.

3.5. Limitations of the Audit System

Although the applied audit mechanisms have demonstrated effective capabilities in recording user activities and supporting data traceability, several limitations should be acknowledged. First, the Blackbox Testing method can only identify vulnerabilities from an external perspective without access to source code; consequently, architectural flaws such as hardcoded credentials, backdoors, or insecure cryptographic implementations remain undetected. Second, testing was confined to 19 predefined scenarios and did not explore all attack vectors, such as race conditions or side-channel attacks. Third, the current audit system lacks real-time alerting and automated incident response, making the detection of suspicious activities still reactive and dependent on manual administrator review. Fourth, no in-depth penetration testing was performed on supporting infrastructure like databases and servers. These limitations present opportunities for future enhancements to strengthen the overall resilience of the pharmacy information system.

4. CONCLUSION

Based on the results of the research and testing conducted, it can be concluded that the pharmacy application fulfills the functional requirements and a portion of the security requirements as evaluated through Blackbox Testing and CIA Triad analysis. The system is capable of real-time drug

stock monitoring, displaying critical stock notifications, and recording user activities through an audit trail feature, thereby enabling traceability of every data change. The implementation of single-device login strengthens the Confidentiality aspect by restricting account access, while the logging of activities supports Integrity as all data modifications are recorded in the system. Furthermore, in terms of Availability, the system proved to be consistently accessible throughout the testing period without service disruptions, thereby supporting the smooth operation of the pharmacy.

Nevertheless, several weaknesses require attention. The system lacks an optimal input validation mechanism, as evidenced by its acceptance of illogical values such as negative stock quantities. In addition, the absence of strong password encryption and the potential SQL Injection vulnerability on the login feature indicate that the Confidentiality and Integrity aspects are not yet fully assured. Therefore, further development is necessary, including the implementation of stricter input sanitization, the adoption of hash-based encryption, and the enhancement of authentication mechanisms. These improvements are expected to elevate the overall security level, protect sensitive data, and strengthen the reliability of the pharmacy information system as a whole. Future work may also incorporate automated real-time threat detection and periodic penetration testing to maintain a resilient security posture.

REFERENCES

[1] Pawar, O. Y., Patil, S. L., Redekar, R. S., Patil, S. B., Lim, S., & Tarwal, N. L. (2023). Strategic development of piezoelectric nanogenerator and biomedical applications. *Applied Sciences*, **13**(5), 2891.

[2] Zancanaro, A., Cisotto, G., & Badia, L. (2023). Tackling age of information in access policies for sensing ecosystems. *Sensors*, **23**(7), 3456.

[3] Bagies, T. (2024). Classifying software security requirements into confidentiality, integrity, and availability using machine learning approaches. *PeerJ Computer Science*, **10**, e2554.

[4] Black, P., Guttman, B., & Okun, V. (2021). *Guidelines on Minimum Standards for Developer Verification of Software*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8397.

[5] Hermawan, A., Hartati, T., & Wijaya, Y. A. (2022). Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad. *Jurnal Informatika: Jurnal Pengembangan IT*, **7**(3), 125–130.

[6] Maspupah, A. (2024). Literature review: Advantages and disadvantages of black box and white box testing methods. *Jurnal Techno Nusa Mandiri*, **21**(2), 151–162.

[7] Mulyati, S., Kusyadi, I., Akbar, S. A. A., Saputra, A., & Hidayat, H. (2022). Pengujian Aplikasi Sistem Informasi Absensi Karyawan PT Prakarsa Mitra Andalan Menggunakan Metode Black Box. *Jurnal Teknologi Sistem Informasi dan Aplikasi*, **5**(2).

[8] Pratasik, S. (2020). Pengembangan Aplikasi E-DUK Dalam Pengelolaan SDM Menggunakan Metode Agile Development The Development Of E-DUK Application in HR Management Using Agile Development Method. *CogITo Smart Journal*, **6**(2), 204–216.

[9] Rahman, R., Rannu, Y., & Muchtar, M. D. (2026). Pengujian keamanan aplikasi berbasis web terhadap serangan parameter tampering. *Jurnal Riset Sistem Informasi*, **3**(2), 72–76.

[10] Bimandaru, A., Alamsyah, A., & Nugroho, A. (2023). Analisis Pengujian Penetrasi Pada Layanan Hosting Menggunakan Metode Black Box (Studi kasus: Blogspot, Wordpress dan Shared Hosting). *Foristek*, **13**(1).

[11] Harahap, A. H. H., Andani, C. D., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *Jurnal Manajemen dan Pemasaran Digital*, **1**(2), 73–83.

[12] Pribadi, D. A. & Winarti, W. (2026). Evaluasi keamanan sistem informasi keuangan sekolah paud berbasis laravel filament 3 menggunakan penetration testing. *Jurnal Informatika dan Teknik Elektro Terapan*, **14**(1).

[13] Syahroni, A. W., Dewi, N. P., Ramadhani, N., & Said, B. (2024). Uji Keamanan Back end Aplikasi Berbasis Website Menggunakan Metode Black Box Testing. *Jurnal PROCESSOR*, **19**(2).

[14] Rachman, R. & Patty, J. S. (2024). Penetration Testing of a Computerized Psychological Assessment Website Using Seven Attack Vectors for Corporation Website Security. *Jurnal Teknik Informatika (Jutif)*, **5**(3), 831–842.
[15] Rahman, M. M., Kshetri, N., Sayeed, S. A., & Rana, M. M. (2024). AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and Cybersecurity risk assessment. *Journal of Information Security*, **15**(4).
[16] Islam, K., Edwards, A. L., Shi, D., Lim, J. R., Sheppard, R., Liu, B. F., & Seeger, M. W. (2022). Crisis communication and learning: The US higher education's response to a global pandemic. *The Learning Organization*, **29**(4), 357–376.
[17] Lukmasari, A., Trialimas, J., Taqwim, W. K., & Pramana, C. (2021). Massive Pleural Effusion as a Rare Manifestation in Severe Neonatal Sepsis. *Open Access Macedonian Journal of Medical Sciences*, **9**(C), 263–266.
[18] Jia, B., Sun, L., Liu, X., Xu, S., Tan, W., & Jiao, J. (2023). Carrier aircraft flight controller design by synthesizing preview and nonlinear control laws. *Drones*, **7**(3), 200.
[19] Novianto, E., Ujianto, E. H. H., & Rianto, R. (2023). Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Sumber Daya Manusia. *Rabit: Jurnal Teknologi dan Sistem Informasi Univrab*, **8**(1), 10–15.
[20] Anggraeni, D. P., Zen, B. P., & Pranata, M. (2022). Security analysis on websites using the information system assessment framework (ISSAF) and open web application security version 4 (OWASPv4) using the penetration testing method. *Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity*, **8**(3), 497–506.
[21] Lestari, S., Yulmaini, Y., Aswin, A., Ma'ruf, S., Sulyono, S., & Fikri, R. (2024). Alleviating cold start and sparsity problems in the micro, small, and medium enterprises marketplace using clustering and imputation techniques. *International Journal of Electrical and Computer Engineering (Ijece)*, **14**(3), 3220.
[22] Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis keamanan sistem informasi berdasarkan framework COBIT 5 menggunakan Capability Maturity Model Integration (CMMI). *Jurnal Sistem Informasi Bisnis*, **9**(1), 47–53.
[23] Devitasari, D., Wati, T., & Sarika, S. (2021). Analisis Kualitas Website Tokome Menggunakan Metode Webqual 4.0 dan Importance Performance Analysis. *Jurnal Informatika Universitas Pamulang*, **6**(1), 57–66.
[24] Dianta, I. A. & Zusrony, E. (2019). Analisis Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking. *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, **3**(1), 1–9.
[25] Ardiansah, T. (2022). Perancangan Sistem Persediaan Menggunakan Metode Extreme Programming. *Jurnal Ilmiah Informatika Dan Ilmu Komputer (JIMA-ILKOM)*, **1**(1), 1–6.
[26] Heng, Z., Yang, S., Li, X., & Shang, L. (2023). The phenomenological research on Higgs and dark matter in the next-to-minimal supersymmetric standard model. *Symmetry*, **15**(2), 456.