PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8267

# SECURITY ANALYSIS OF PAYROLL SYSTEM USING THE PENETRATION TESTING EXECUTION STANDARD (PTES) AND OWASP TOP 10 2021

**Monas Tarigan**

Informatics Study Program, Faculty of Information Technology
Universitas Nusa Mandiri, Jakarta, Indonesia
https://nusamandiri.ac.id/
monastarigan@gmail.com
(*) Corresponding Author



***Abstract***— *The payroll system plays a critical role in human resource management as it processes and stores sensitive employee data, including personal identity, salary information, financial records, and employment history. The increasing reliance on web-based applications has significantly improved operational efficiency; however, it also increases exposure to cybersecurity threats when security controls are not optimally implemented. This study aims to analyze security vulnerabilities in the payroll system of PT. Vidira Eshan Abadi using the Penetration Testing Execution Standard (PTES) methodology, with OWASP Top 10 2021 used as a vulnerability classification framework. The research stages include pre-engagement interactions, reconnaissance, scanning, enumeration, exploitation, post-exploitation analysis, and reporting. Security testing was conducted using tools such as Nuclei, Gobuster, Dirsearch, Burp Suite, and SQLMap. The results indicate the presence of several vulnerabilities with low to high severity levels, including security misconfiguration, absence of authentication rate limiting, potential SQL injection, and stored Cross-Site Scripting (XSS) vulnerabilities across multiple system modules. This study recommends implementing strict input validation mechanisms, consistent output encoding, improved server configuration, and enhanced authentication protection to strengthen the security posture of the payroll system.*

***Keywords:*** *OWASP Top 10, payroll system, penetration testing, PTES, web application security.*

***Abstrak***— *Sistem penggajian memiliki peran krusial dalam manajemen sumber daya manusia karena memproses dan menyimpan data karyawan yang bersifat sensitif, termasuk identitas pribadi, informasi gaji, catatan keuangan, dan riwayat pekerjaan. Peningkatan penggunaan aplikasi berbasis web telah secara signifikan meningkatkan efisiensi operasional; namun, hal ini juga meningkatkan paparan terhadap ancaman keamanan siber apabila kontrol keamanan tidak diterapkan secara optimal. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan pada sistem penggajian PT. Vidira Eshan Abadi menggunakan metodologi Penetration Testing Execution Standard (PTES), dengan OWASP Top 10 2021 sebagai kerangka klasifikasi kerentanan. Tahapan penelitian meliputi pre-engagement interactions, reconnaissance, scanning, enumeration, exploitation, post-exploitation analysis, dan reporting. Pengujian keamanan dilakukan menggunakan alat seperti Nuclei, Gobuster, Dirsearch, Burp Suite, dan SQLMap. Hasil penelitian menunjukkan adanya beberapa kerentanan dengan tingkat keparahan rendah hingga tinggi, termasuk kesalahan konfigurasi keamanan (security misconfiguration), tidak adanya pembatasan tingkat autentikasi (authentication rate limiting), potensi SQL injection, serta kerentanan stored Cross-Site Scripting (XSS) pada beberapa modul sistem. Penelitian ini merekomendasikan penerapan mekanisme validasi input yang ketat, pengkodean output yang konsisten, peningkatan konfigurasi server, serta penguatan perlindungan autentikasi untuk memperkuat postur keamanan sistem penggajian.*

***Kata Kunci****: OWASP Top 10, sistem penggajian, penetration testing, PTES, keamanan aplikasi web.*

## INTRODUCTION

The rapid development of information technology has encouraged organizations to digitize various business processes, including payroll management systems. Web-based payroll systems provide efficiency in managing employee data, salary calculations, allowances, deductions, attendance records, and financial reporting

(Tandrio & Fianty, 2026). Despite these benefits, payroll systems store highly sensitive information such as personal identity data, financial details, and employment records that must be protected from unauthorized access, and cyber threats.

Payroll data is categorized as high-value strategic information because it directly relates to employee financial rights and organizational operational stability (Lubis, Devi, & Donargo, 2024). A breach involving payroll data may result in financial losses, legal consequences, and reputational damage. Therefore, ensuring the security of payroll systems is a fundamental organizational responsibility.

Threats to web-based payroll systems may originate from external attackers exploiting vulnerabilities such as SQL Injection (Zairina, Huwae, & Jatmika, 2025), Cross-Site Scripting (XSS) (Widianto, Wijaya, Harjono, & Wicaksono, 2025), brute force attacks (Utama et al., 2022), and server misconfigurations. Additionally, insider threats, including misuse of access privileges, may pose significant security risks if proper access controls are not enforced.

To proactively identify and mitigate such vulnerabilities, a structured and systematic security assessment is required. This research employs the Penetration Testing Execution Standard (PTES) as the primary testing framework and OWASP Top 10 2021 as the vulnerability classification reference to ensure standardized and comprehensive security evaluation.

Based on this background, this research aims to evaluate the security level of the payroll system at PT. Vidira Eshan Abadi using the PTES methodology, identify vulnerabilities based on the OWASP Top 10 2021 classification, and propose appropriate mitigation strategies to enhance the system's security posture. The specific objectives are to analyze security vulnerabilities, classify them according to OWASP Top 10 2021, and provide technical recommendations for improving system security.

This study is expected to provide an objective assessment of the payroll system's security, assist organizations in strengthening their web application security mechanisms, and contribute to academic references in the field of penetration testing and information security.

Although previous studies have applied the OWASP Top 10 framework and penetration testing approaches to evaluate web application security, most have focused on general web applications or educational systems (Bardian & Sutanto, 2025). Research specifically addressing payroll systems despite their highly sensitive financial and personal data remains limited, particularly those employing a structured methodology such as PTES combined with OWASP Top 10 2021.

Moreover, prior studies often emphasize vulnerability identification without conducting structured post-exploitation impact analysis based on the CIA triad. Therefore, this study addresses this gap by implementing a comprehensive PTES-based penetration testing approach and systematically classifying findings using OWASP Top 10 2021 within the context of a web-based payroll system.

## MATERIALS AND METHODS

### Information Security

Information security refers to the protection of data and information systems from unauthorized access, disclosure, alteration, or destruction. The fundamental concept of information security is based on the CIA triad: Confidentiality, Integrity, and Availability (Huda, 2020). Confidentiality ensures that information is accessible only to authorized individuals. Integrity guarantees that data remains accurate and unaltered without authorization. Availability ensures that systems and data remain accessible when needed by legitimate users.

In payroll systems, all three principles are critically important because the system handles sensitive financial and personal data that must be securely maintained.

### Web-Based Payroll Systems

A web-based payroll system is an application used to manage payroll processes through internet or intranet networks (Lubis et al., 2024). It integrates modules such as employee management, salary computation, allowances, deductions, attendance tracking, and financial reporting.

Because it operates over network infrastructure, web-based systems face higher security risks compared to standalone systems. Common risks include injection attacks, authentication weaknesses, session hijacking, and server configuration errors.

### Penetration Testing

Penetration testing is a security testing method that simulates cyberattacks to identify system vulnerabilities before malicious actors exploit them (Widianto et al., 2025). The primary objectives of penetration testing are vulnerability identification, risk assessment, and mitigation recommendation.

Penetration testing must be conducted within a defined scope and authorized environment to avoid operational disruption and legal implications.

PILAR Nusa Mandiri: Journal of Computing and Information System
Vol. 22, No. 1 March 2026 | DOI: 10.33480/pilar.v22i1.8267

Penetration testing is widely implemented to evaluate organizational security controls and identify exploitable weaknesses (Saputra, Dione, & Uluputty, 2023).

**Penetration Testing Execution Standard (PTES)**

The PTES framework provides a comprehensive and systematic structure for penetration testing (Widianto et al., 2025). The stages include:

1. Pre-Engagement Interactions – defining scope, objectives and legal agreements.
2. Intelligence Gathering (Reconnaissance) – collecting initial information about the target system.
3. Threat Modeling – identifying potential threats based on gathered information.
4. Vulnerability Analysis – scanning and enumerating potential vulnerabilities.
5. Exploitation – controlled validation of identified vulnerabilities.
6. Post-Exploitation – evaluating the impact on system security.
7. Reporting – documenting findings and mitigation recommendations.

The structured approach ensures accountability and reproducibility in security assessments (Widianto et al., 2025).

The scope of testing in this study was limited to the web-based payroll system of PT. Vidira Eshan Abadi, specifically covering authentication mechanisms, user access control, salary processing modules, employee data management, and database interaction components. Testing was conducted within an authorized and controlled environment to prevent disruption of operational services.

Each phase of the Penetration Testing Execution Standard (PTES) was implemented systematically. The Pre-Engagement phase included formal authorization and scope limitation agreements (Safitra, Lubis, & Widjajarto, 2023). Intelligence Gathering applied passive and controlled active reconnaissance techniques (Astrida, Saputra, & Assaufi, 2022). Threat Modeling identified potential attack vectors based on exposed assets and system architecture (Ridwan, 2024). Vulnerability Analysis combined automated tools and manual validation to reduce false positives. Exploitation was conducted strictly for proof-of-concept validation without modifying production data. Post-Exploitation assessed business impact using CIA triad principles. The Reporting phase documented reproducible findings and prioritized mitigation strategies.

## RESULTS AND DISCUSSION

The findings presented in this section reflect the systematic implementation of the PTES methodology described in the Materials and Methods section.

**Overview of Security Testing Process**

The security assessment of the payroll system at PT. Vidira Eshan Abadi was conducted within a defined and authorized testing scope. The evaluation focused on web application security, particularly on authentication mechanisms, employee data management modules, and administrative functionalities.

Recent global security analyses highlight that injection and authentication failures remain dominant attack vectors in financial web applications (Theocharidou, Lella, Naydenov, & Malatras, 2025).

**Implementation of PTES Phases**

The penetration testing process followed the structured phases of the PTES framework. The assessment began with reconnaissance to collect publicly accessible information related to system structure, accessible directories, and exposed services. Automated scanning and manual verification were then performed to identify potential vulnerabilities. Controlled exploitation was conducted solely to validate the presence of vulnerabilities without disrupting system operations.

**Tools Used in Testing**

The tools utilized during testing included:

1. Nuclei for automated vulnerability scanning.
2. Dirsearch and Gobuster for directory and endpoint enumeration.
3. Burp Suite for HTTP request and response analysis.
4. SQLMap for controlled SQL injection testing (Adinata, Putra, Juliantari, & Sutrisna, 2022).

Testing was conducted ethically and did not result in service interruption or data modification.

**Identified Vulnerabilities**

1. Security Misconfiguration (A05)

Several directories and endpoints were found to be accessible without proper authentication controls. This condition indicates incomplete or improper security configuration within the web application or server environment. Potential Impact:

a. Exposure of application structure information
b. Facilitation of further reconnaissance activities
c. Increased attack surface for exploitation

The security testing identified several vulnerabilities categorized according to the official OWASP Top 10 2021 classification (A01–A10) (Bardian & Sutanto, 2025). The identified findings are mapped as follows:

a. A03:2021 – Injection (SQL Injection and Stored Cross-Site Scripting)
b. A05:2021 – Security Misconfiguration
c. A07:2021 – Identification and Authentication Failures

This classification ensures standardized vulnerability categorization aligned with internationally recognized web application security standards. +Although this vulnerability did not directly expose sensitive data during testing, it increases the likelihood of successful subsequent attacks. Therefore, it is classified as a medium-risk vulnerability.

2. Missing Rate Limiting on Authentication (A07)
The authentication module did not implement rate limiting mechanisms to restrict repeated login attempts. This allows attackers to perform brute force attacks to guess valid credentials. Potential Impact:

a. Unauthorized account access
b. Privilege escalation
c. Manipulation of payroll data

Since authentication controls are critical for system protection, this vulnerability directly threatens confidentiality and integrity. It is classified as a medium-risk vulnerability.

3. Potential SQL Injection (A03: Injection**)**
Testing indicated insufficient input validation within authentication parameters. Although full exploitation was not executed to preserve system integrity, response patterns suggested possible SQL injection vulnerabilities. If successfully exploited, SQL injection could allow attackers to:

a. Access the database without valid credentials
b. Retrieve sensitive employee data
c. Modify salary records
d. Delete or corrupt database tables

Due to its potential impact on confidentiality, integrity, and availability simultaneously, this vulnerability is categorized as a high-risk vulnerability.

4. Stored Cross-Site Scripting (XSS) (A03: Injection)
Stored XSS vulnerabilities were identified in several system modules, including employee management, department, position, branch, leave, holidays, working hours and allowances modules. Malicious scripts inserted into input fields were stored in the database and executed when the affected page was accessed by other users. Potential Impact**:**

a. Session hijacking
b. Account takeover (including administrative accounts)
c. User interface manipulation
d. Persistent malicious script injection

Stored XSS presents a serious security concern due to its persistent nature. Depending on the affected user privileges, the risk ranges from medium to high severity.

**Impact Analysis Based on the CIA Triad**

The identified vulnerabilities affect the three fundamental principles of information security:

1. Confidentiality: Potential SQL Injection and Stored XSS vulnerabilities may allow unauthorized access to employee salary and personal data.
2. Integrity: Attackers may manipulate payroll data, modify salary records, or alter system configurations.
3. Availability: Exploitation of injection vulnerabilities could lead to database crashes, deletion of records, or service disruption.

Therefore, the payroll system's overall security posture requires immediate improvement to prevent exploitation that may compromise all three security principles. Similar findings regarding injection-based vulnerabilities have been reported in comparative security studies (Susanto et al., 2020).

**Risk Classification Summary**

Based on the vulnerability assessment results, four main security issues were identified in the payroll system. Security Misconfiguration and Missing Rate Limiting were categorized as medium-risk vulnerabilities because they increase the likelihood of unauthorized access and facilitate further exploitation attempts.

The identified SQL Injection vulnerability was classified as high risk due to its potential impact on confidentiality, integrity, and availability (Adinata et al., 2022). Successful exploitation could allow attackers to access, modify, or delete sensitive payroll data.

Stored Cross-Site Scripting (XSS) was categorized as medium to high risk depending on the affected user privilege level. This vulnerability may enable session hijacking, account takeover, and persistent malicious script execution.

Risk assessment was conducted qualitatively based on impact severity and exploitation feasibility following OWASP risk evaluation guidelines

(Zairina et al., 2025). In addition to qualitative classification, risk levels were further analyzed using impact and likelihood indicators. Injection vulnerabilities (A03:2021) were categorized as **High Risk** due to their direct impact on database confidentiality, integrity, and availability. Authentication weaknesses (A07:2021) were reclassified as **High Risk** because payroll systems manage financial assets and sensitive employee information, making brute-force exploitation potentially critical.

Security misconfiguration issues (A05:2021) were categorized as **Medium Risk**, but may escalate to High Risk if combined with other exploitable weaknesses. The cumulative risk exposure indicates that the payroll system is positioned within a **moderate-to-high overall risk level**, requiring immediate remediation prioritization.

**Mitigation Recommendations**

To enhance system security, the following technical improvements are recommended:

1. Implement prepared statements and parameterized queries to prevent SQL injection attacks.
2. Apply strict input validation using a whitelist approach across all modules.
3. Implement consistent output encoding to mitigate XSS vulnerabilities.
4. Introduce rate limiting and CAPTCHA mechanisms for authentication endpoints.
5. Use SSL certificates issued by trusted Certificate Authorities.
6. Deploy a Web Application Firewall (WAF) to detect and block malicious traffic.
7. Conduct periodic security testing as part of organizational security policy.
8. Implement Multi-Factor Authentication (MFA) to mitigate A07:2021 authentication risks.
9. Apply Content Security Policy (CSP) headers and X-Content-Type-Options to reduce A03:2021 XSS exploitation vectors.
10. Enforce secure session management using HTTPOnly, Secure, and SameSite cookie attributes.
11. Integrate secure code review and DevSecOps practices within the software development lifecycle.

## CONCLUSION

This study analyzed the security posture of the payroll system at PT. Vidira Eshan Abadi using the PTES methodology combined with OWASP Top 10 2021 classification. The findings reveal multiple vulnerabilities ranging from medium to high severity levels, particularly related to injection flaws and authentication weaknesses.

The PTES framework proved effective in systematically identifying and validating vulnerabilities, while OWASP Top 10 facilitated standardized categorization of security risks. Among the identified issues, SQL injection presents the highest risk due to its potential to compromise confidentiality, integrity, and availability simultaneously.

Overall, although the payroll system demonstrates functional operational capability, significant improvements in security controls are necessary to ensure adequate protection of sensitive employee data.

This study contributes to the academic field by demonstrating a structured integration between PTES execution phases and the official OWASP A01–A10 classification within a payroll system environment. Unlike prior general web security assessments, this research provides contextualized risk evaluation for financial-data-intensive applications, strengthening both methodological rigor and applied cybersecurity governance practices (Budiyanto, 2025).

Future research may explore the integration of DevSecOps practices to enable continuous security monitoring and proactive vulnerability management. In addition, the combination of black-box and white-box testing approaches could provide a more comprehensive evaluation of system security by examining both external attack surfaces and internal code structures. Further studies may also assess compliance with ISO/IEC 27001 standards to strengthen information security governance frameworks. Moreover, the implementation of automated continuous vulnerability scanning mechanisms would support real-time detection and mitigation of emerging threats. Expanding the research scope in these directions would provide deeper insight into long-term security governance and sustainable risk management strategies within financial-data-intensive systems.

## REFERENCE

Adinata, P. G. S., Putra, I. P. W. P., Juliantari, N. P. A. I., & Sutrisna, K. D. A. (2022). Analisis Perbandingan Tools SQL Injection Menggunakan SQLmap , SQLsus dan The Mole. *JURNAL INFORMATIK*, *18*(3), 286–292. https://doi.org/10.52958/iftk.v18i3.5373

Astrida, D. N., Saputra, A. R., & Assaufi, A. I. (2022). Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES). *Sinkron*, *7*(1), 147–154. https://doi.org/10.33395/sinkron.v7i1.11249

Bardian, H. A., & Sutanto, I. (2025). PENGEMBANGAN APLIKASI VULNERABILITY SCANNER UNTUK MENDETEKSI CELAH KEAMANAN SIBER PADA WEBSITE. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(3), 4404–4411.

Budiyanto, B. (2025). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia* (A. Iftitah, ed.). Retrieved from https://books.google.co.id/books?id=QSc9EQAAQBAJ

Huda, M. (2020). *Keamanan Informasi*. Retrieved from https://books.google.co.id/books?id=CcjZDwAAQBAJ

Lubis, D. S., Devi, S., & Donargo, M. (2024). Implementasi Transaksi Sistem Penggajian Dengan Metode Payroll ( Studi Kasus : PT . Diva Abadi ). *Majalah Ilmiah Warta Dharmawangsa*, *18*(4), 1440–1450. https://doi.org/10.46576/wdw.v18i4.5340

Ridwan, R. (2024). Using the Penetration Testing Execution Standard Method (PTES) for Wireless Network Security Analysis. *Greenation Computer and Information Review*, *1*(1), 25–32. https://doi.org/10.38035/gcir.v1i1.336

Safitra, M. F., Lubis, M., & Widjajarto, A. (2023). Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website. *Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering*, 139–145. https://doi.org/10.1145/3592307.3592329

Saputra, A. D., Dione, F., & Uluputty, I. (2023). Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan dan Informatika Provinsi Kalimantan Timur. *Jurnal Teknologi Dan Komunikasi Pemerintahan*, *5*(2), 159–187. https://doi.org/10.33701/jtkp.v5i2.3735

Susanto, B., Hadianto, A., Chariri, F. N., Rochman, M., Syaukani, M. M., & Daniswara, A. A. (2020). Penggunaan Digital Marketing untuk Memperluas Pasar dan Meningkatkan Daya Saing UMKM. *Community Empowerment*, *6*(1), 42–47. https://doi.org/10.31603/ce.4244

Tandrio, F., & Fianty, M. I. (2026). WEB-BASED PAYROLL SYSTEM DEVELOPMENT USING THE PROTOTYPING METHOD AND STRUCTURED DATABASE DESIGN. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, *11*(3), 851–863. https://doi.org/10.33480/jitk.v11i3.7044.WEB-BASED

Theocharidou, M., Lella, I., Naydenov, R., & Malatras, A. (2025). *Enisa Threat Landscape: Finance Sector*. https://doi.org/10.2824/5410466

Utama, I. M. P., Putri, K. R., Wirayuda, A. A. E., Herlambang, V. A. T. P., Listartha, I. M. E., & Saskara, G. A. J. (2022). Analisis Perbandingan Kinerja Tool Website Directory Brute Force dengan Target Website DVWA. *JURNAL INFORMATIK*, *18*(3), 278–285. https://doi.org/10.52958/iftk.v18i3.5256

Widianto, F., Wijaya, E. S., Harjono, H., & Wicaksono, A. P. (2025). Analisis Kerentanan Pada Aplikasi Web Menggunakan Metode PTES. *Jurnal Pendidikan Dan Teknologi Indonesia (JPTI)*, *5*(1), 155–166. https://doi.org/10.52436/1.jpti.609

Zairina, Z., Huwae, R. B., & Jatmika, A. H. (2025). IMPLEMENTASI OWASP TOP 10 DALAM PENGUJIAN PENETRASI WEBSITE : MENGIDENTIFIKASI CELAH KEAMANAN DALAM SISTEM PENGELOLAAN VOTING INDONESIA. *Jurnal Teknologi Informasi, Komputer, Dan Aplikasinya (JTIKA )*. Retrieved from https://api.semanticscholar.org/CorpusID:278116413