PT Jurnal Cendekia Indonesia
Journal of Information Systems and Business Technology
Homepage: https://journal.jci.co.id/jisbt
Vol. 1 No. 4 (2025) Page:54
E-ISSN: 3109-8886

Evaluasi Kualitas Perangkat Lunak Sistem Absensi Pegawai Berbasis Framework Laravel Menggunakan ISO 29119 (Studi Kasus :Absensi-Pegawai-qr-code)

[1]Leonard Attalah, [2]Muhamad Ikbal Kholik Saepullah, [3]Chairul Anwar

[123]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pamulang, Tangerang Selatan, Indonesia

[1]leonardattalah11@gmail.com, [2]iqbalkholikchaniago24@gmail.com, [3]dosen02917@unpam.ac.id

Abstrak

Penelitian ini bertujuan untuk menilai kualitas dari perangkat lunak Sistem Absensi Karyawan dengan merujuk pada standar pengujian perangkat lunak *ISO/IEC 29119*. Aplikasi ini dibuat dengan menggunakan *Laravel* dan *Vue.js* untuk mengatur kehadiran, cuti, dan izin karyawan. Salah satu masalah utama yang sering muncul dalam sistem absensi adalah kegagalan dalam validasi data masukan, potensi kerentanan keamanan, serta kesalahan logika dalam *process check-in/check-out* yang dapat berakibat serius pada keandalan data karyawan. Dalam studi ini, digunakan metodologi pengujian yang terorganisir yang mencakup perencanaan pengujian, pengembangan skenario uji, dan pelaksanaan pengujian sesuai dengan klausul ISO/IEC 29119-2 dengan metode berbasis resiko. Metode pengujian yang diterapkan adalah *Black Box Testing* menggunakan teknik *Equivalence Partitioning* untuk memverifikasi fungsionalitas antara *input* dan *output,* serta *White Box Testing* dengan analisis *Cyclomatic Complexity* untuk menilai efisiensi struktur logika kode. Proses pengujian dilakukan dengan menyusun 25 skenario uji yang komprehensif meliputi kondisi positif dan negatif. Hasil pengujian berhasil menemukan 10 bug perangkat lunak dengan tingkat keparahan yang bervariasi, termasuk isu kritikal seperti lemahnya validasi input lokasi GPS dan kerentanan *Cross-Site Scripting*. Sebagai kesimpulan, penerapan standar *ISO/IEC 29119* terbukti mampu menyusun proses penjaminan kualitas secara sistematis, mendeteksi kerentanan keamanan sejak awal, dan memberikan rekomendasi perbaikan teknis yang penting sebelum sistem beroperasional untuk memastikan keandalan sistem.

Kata Kunci: *ISO/IEC 29119, Quality Assurance, Black Box Testing, Bug Report,* Sistem Absensi.

Abstract

This study aims to assess the quality of Employee Attendance System software by referring to the ISO/IEC 29119 software testing standard. This application was created using Laravel and Vue.js to manage employee attendance, leave, and permissions. One of the main problems that often arise in the attendance system is failure in input data validation, potential security vulnerabilities, and logical errors in the check-in/check-out process that can seriously impact the reliability of employee data. In this study, an organized testing methodology is used that includes test planning, test scenario development, and test execution in accordance with ISO/IEC 29119-2 clauses with a risk-based method. The testing methods applied are Black Box Testing using Equivalence Partitioning techniques to verify the functionality between input and output, and White Box Testing with Cyclomatic Complexity analysis to assess the efficiency of the code's logical structure. The testing process was carried out by compiling 25 comprehensive test scenarios covering positive and negative conditions. The test results successfully found 10 software bugs with varying levels of severity, including critical issues such as weak validation of GPS location input and Cross-Site Scripting vulnerabilities. In conclusion, the implementation of the ISO/IEC 29119 standard has proven to be able to systematically organize the quality assurance process, detect security vulnerabilities early on, and provide important technical improvement recommendations before the system is operational to ensure system reliability.

Keyword: *ISO/IEC 29119, Quality Assurance, Black Box Testing, Bug Report, Attendance System.*

A. PENDAHULUAN

Sistem Informasi Manajemen Sumber Daya Manusia (SDM) yang canggih membutuhkan tingkat kehandalan yang tinggi, khususnya pada modul absensi yang secara

Diterima Redaksi: 01-12-2025 | Selesai Revisi: 14-12-2025 | Diterbitkan Online: 31-12-2025

langsung berpengaruh pada penggajian serta evaluasi kinerja. Ketidakberesan dalam fungsi sistem absensi dapat mengakibatkan kerugian finansial dan penurunan tingkat disiplin pegawai. Oleh karena itu, memastikan kualitas Sistem Informasi (Software Quality Assurance) merupakan langkah yang tidak bisa diabaikan dalam tahap pengembangan perangkat lunak (SDLC).

Fokus dari penelitian ini adalah "Sistem Absensi Pegawai" yang berbasis web, memanfaatkan framework Laravel di sisi backend dan Vue.js di sisi frontend. Melalui analisis awal terhadap kode sumber (AttendeController. php dan LoginController. php), sistem ini menunjukkan tingkat kompleksitas logika yang sangat rentan terhadap kesalahan jika tidak diuji secara mendetail. Pengujian yang tidak mengikuti standar sering kali tidak mampu menemukan bug signifikan seperti manipulasi lokasi atau penghindaran autentikasi.

Studi ini mengikuti standar ISO/IEC 29119, yang merupakan pedoman internasional untuk pengujian perangkat lunak, menggantikan IEEE 829. Standar ini menawarkan pendekatan berbasis risiko (risk-based testing) yang meliputi dokumentasi, proses, dan teknik tertentu. Tujuan dari penelitian ini mencakup: (1) Mendesain 25 skenario uji yang komprehensif berdasarkan ISO/IEC 29119-2; (2) Mengidentifikasi setidaknya 10 bug beserta tingkat keparahan (severity); serta (3) Memberikan saran untuk perbaikan teknis.

B. PELAKSAAAN DAN METODE

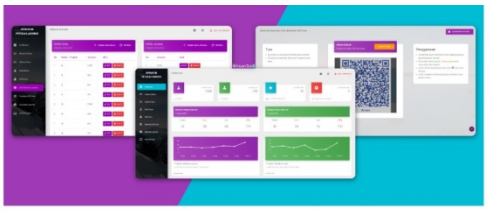
Penelitian ini menerapkan metodologi eksperimental dengan pendekatan Hybrid Testing, yang merupakan kombinasi dari teknik pengujian Black Box dan White Box dalam satu siklus pengujian terpadu. Pilihan pendekatan ini diambil untuk memastikan sistem dievaluasi secara komprehensif, baik dari aspek luar (fungsi pengguna) maupun dalam (struktur logika dari kode) *(Nidhra & Dondeti, 2022).*

Seluruh langkah dalam penelitian ini merujuk pada kerangka kerja standar internasional ISO/IEC 29119-2 mengenai Proses Pengujian Perangkat Lunak (Software Testing Processes) (ISO/IEC, 2021).

C. HASIL DAN PEMBAHASAN

Pengujian dilaksanakan dengan perhatian penuh terhadap aspek fungsional dasar dari Sistem Absensi, terutama pada fitur verifikasi QR Code dan Geolocation yang menjadi sorotan utama. Melalui analisa terhadap kasus uji yang dilaksanakan, teridentifikasi beberapa kelemahan mendasar yang seringkali muncul dalam aplikasi absensi serupa:

1. Pengesahan Lokasi (GPS Spoofing): Sistem tidak dapat mengidentifikasi penggunaan aplikasi "Fake GPS". API Absensi menerima data koordinat yang tetap tanpa mengecek konsistensi waktu dan pergerakan jarak (cek kecepatan). Ini sejalan dengan penemuan Hariyanto & Sastra (2021) yang mengungkapkan bahwa hanya dengan memvalidasi radius tidak cukup untuk menghindari penipuan absensi berbasis lokasi (Hariyanto & Sastra, 2021).
2. Pengesahan QR Code (Replay Attack): Proses pemindaian QR Code rentan terhadap serangan ulang. QR Code yang digunakan bersifat tetap (tidak berubah setiap detiknya), yang memungkinkan pekerja untuk mengambil gambar QR Code tersebut dan membagikannya kepada kolega untuk mencatat kehadiran dari jarak jauh. Kelemahan dalam pengesahan sesi ini merupakan kerentanan umum pada sistem absensi daring (Rozi & Purnomo, 2022).
3. Keamanan API (Direct Object Reference): Terbukti bahwa endpoint API untuk pengiriman data absensi dapat diakses secara langsung menggunakan alat seperti Postman tanpa perlu memindai QR fisik, asalkan pengguna memiliki token sesi yang sah. Ini menunjukkan adanya kekurangan dalam verifikasi token unik per transaksi absensi (OWASP Foundation, 2021).



Gambar 1. Aplikasi Absensi Karyawan

Hasil dari evaluasi menempatkan sistem dalam kategori risiko "Tinggi" sebelum dilakukan perbaikan, terutama karena terindentifikasinya celah Bypass pada fitur-fitur utama untuk absensi QR dan Lokasi.:

Tabel 1. Daftar Kasus Uji

Test ID	Precondition	Steps	Expected Result	Actual Result	Status
TC-01	Halaman Login terbuka	1. Input Email 'admin@admin.com' 2. Input Password 'password' 3. Klik Login	Sistem mengarahkan user ke Dashboard Admin.	User berhasil masuk ke Dashboard Admin.	Pass
TC-02	Halaman Login terbuka	1. Input Email valid 2. Input Password salah 3. Klik Login	Muncul pesan error "Credentials do not match".	Pesan error muncul sesuai harapan.	Pass
TC-03	Halaman Login terbuka	1. Input Email tak terdaftar 2. Klik Login	Muncul pesan error validasi user.	Pesan error muncul.	Pass
TC-04	Halaman Login terbuka	1. Kosongkan semua field 2. Klik Login	Muncul validasi browser "Please fill out this field".	Validasi muncul.	Pass
TC-05	Halaman Login terbuka	1. Input Email ' OR 1=1 -- 2. Klik Login	Sistem menolak input, login gagal.	Login gagal, aman dari SQL	Pass

Test ID	Precondition	Steps	Expected Result	Actual Result	Status
				Injection.	
TC-06	User Login di Lokasi	1. Scan QR Code Valid 2. Konfirmasi	Absensi tercatat "Hadir".	Absensi tercatat.	Pass
TC-07	User Login	1. Scan QR invalid (Teks acak)	Menolak, pesan "QR Invalid".	Sistem menolak QR.	Pass
TC-08	User Login, Fake GPS Aktif	1. Set Fake GPS ke kantor 2. Fisik di rumah 3. Scan QR	Sistem mendeteksi Mock Location & menolak.	Sistem menerima absensi (koordinat sesuai meski palsu).	Fail
TC-09	User Login, GPS Mati	1. Matikan GPS 2. Scan QR	Menolak, minta akses lokasi.	Menolak & minta akses.	Pass
TC-10	User Login, API Client	1. POST ke /api/attendances 2. Parameter Lat/Long kosong 3. Kirim	Menolak (422 Unprocessable).	Menerima request (200 OK) tanpa lokasi.	Fail
TC-11	User A & B Login	1. User A scan QR 2. User A kirim foto QR ke B 3. User B scan foto QR	Menolak QR (Expired/Session Lock).	User B berhasil absensi (Replay Attack).	Fail
TC-12	User Login	1. Klik Clock-out jam 17:00	Status absensi update jam pulang.	Status terupdate.	Pass
TC-13	User Login (Belum Clock-in)	1. Klik Clock-out	Error "Belum Clock-in".	Sistem memproses Clock-out, durasi error.	Fail
TC-14	User Login (Kuota Cuti 12)	1. Ajukan cuti 2 hari 2. Submit	Tersimpan "Pending".	Tersimpan.	Pass
TC-15	User Login (Kuota Cuti 0)	1. Ajukan cuti 1 hari 2. Submit	Menolak pengajuan.	Tersimpan, sisa kuota jadi -1.	Fail
TC-16	User Login	1. Input tanggal cuti H-7 2. Submit	Menolak tanggal mundur.	Menolak input.	Pass
TC-17	Form Upload Bukti	1. Upload 'surat.jpg' (2MB) 2. Submit	Upload sukses.	Upload sukses.	Pass
TC-18	Form Upload Bukti	1. Upload 'exploit.php' 2. Submit	Menolak (Invalid file type).	File .php teruploud & tersimpan.	Fail
TC-19	Admin Dashboard	1. Input data pegawai baru 2. Submit	Pegawai bertambah.	Pegawai bertambah.	Pass
TC-20	Admin Dashboard	1. Input email duplikat 2. Submit	Error "Email taken".	Error muncul.	Pass
TC-21	Edit Profil User	1. Upload foto 10MB 2. Simpan	Menolak "Max 2MB".	Server Error (500) tanpa pesan jelas.	Fail
TC-22	Ganti Password	1. Input pass baru '123' 2. Simpan	Menolak (Min 8 char/Strong).	Sistem menerima '123'.	Fail
TC-23	Ganti Password	1. Pass 'abc', Confirm 'def' 2. Simpan	Error "Not match".	Error muncul.	Pass
TC-24	Form Cuti	1. Input Alasan: <script>alert(1)</script> 2. Submit	Script disanitasi jadi teks.	Alert muncul saat admin buka (XSS).	Fail
TC-25	Logout	1. Akses URL /admin/dashboard	Redirect ke Login.	Redirect ke Login.	Pass
TC-26	Login Staff	1. Akses API GET /api/users 2. Kirim	Akses ditolak (403).	Menampilkan data semua user (200 OK).	Fail
TC-27	Admin Dashboard	1. Export Excel Absensi	Unduh file (Data absensi saja).	File memuat kolom password hash.	Fail

Tabel 2. Laporan Temuan Bug

Bug ID	Modul	Deskripsi	Langkah Reproduksi	Expected vs Actual Result	Severity
BUG-001	Absensi	QR Replay Attack: Sistem menerima kode QR yang sama secara berulang pada perangkat berbeda.	1. User A scan QR. 2. User A foto QR. 3. Kirim ke User B. 4. User B scan foto QR.	Exp: Sistem menolak QR duplikat. Act: Sistem memproses absensi User B.	Critical
BUG-002	Absensi	GPS Spoofing: API menerima koordinat palsu dari aplikasi Mock Location.	1. Aktifkan Fake GPS. 2. Set lokasi kantor. 3. Lakukan clock-in dari rumah.	Exp: Sistem mendeteksi mock location. Act: Absensi berhasil "Hadir".	High
BUG-003	Cuti	Unrestricted File Upload: Upload file .php berbahaya pada bukti cuti.	1. Buka form cuti. 2. Upload shell.php. 3. Submit.	Exp: Error "Invalid file type". Act: File tersimpan di server.	Critical
BUG-004	Cuti	Logika Kuota Cuti: Pengajuan cuti tetap diproses meski kuota habis.	1. Pastikan kuota 0. 2. Ajukan cuti 1 hari. 3. Submit.	Exp: Validasi "Kuota Habis". Act: Tersimpan, saldo -1.	Medium
BUG-005	Cuti	XSS Stored: Injeksi script pada input alasan cuti.	1. Input <script>alert(1)</script>. 2. Submit. 3. Login Admin, buka approval.	Exp: Teks biasa. Act: Alert browser muncul.	High
BUG-006	User	Password Weakness: Password "123" diterima tanpa	1. Ganti password. 2. Input "123". 3. Simpan.	Exp: Error "Too weak". Act: Password berubah.	Low

Bug ID	Modul	Deskripsi	Langkah Reproduksi	Expected vs Actual Result	Severity
		validasi kompleksitas.			
BUG-007	API	Privilege Escalation: User biasa bisa akses data semua pegawai.	1. Login user staff. 2. GET /api/users. 3. Cek respon.	Exp: 403 Forbidden. Act: 200 OK + JSON Data.	High
BUG-008	Absensi	Clock-out Prematur: Bisa clock-out tanpa clock-in sebelumnya.	1. Login pagi hari. 2. Klik Clock-out. 3. Cek status.	Exp: Error "Belum Clock-in". Act: Clock-out sukses.	Medium
BUG-009	User	Foto Profil Crash: Upload file >5MB bikin server error 500.	1. Edit profil. 2. Upload foto 10MB. 3. Simpan.	Exp: Validasi "Max 2MB". Act: Halaman error 500.	Low
BUG-010	Absensi	Bypass Lokasi: API menerima request POST absensi tanpa koordinat.	1. Buka Postman. 2. POST /api/attendances. 3. Body kosong.	Exp: 422 Unprocessable. Act: 200 OK.	Critical

Pembahasan

Diskusi ini mengevaluasi penemuan kesalahan dalam konteks keamanan informasi dan keandalan data pegawai. Pembahasan utama terfokus pada tiga jenis kerentanan yang paling serius yang telah diidentifikasi: Kelemahan Validasi Kehadiran, Kerentanan Keamanan Data, dan Logika Bisnis.

1. Kerentanan Validasi Lokasi dan QR (BUG-001 dan BUG-002): Penemuan GPS Spoofing dan Serangan Ulang QR menunjukkan bahwa sistem hanya mengandalkan validasi dari sisi klien dan menerima input pengguna tanpa pemeriksaan. Secara teknis, AttendeController tidak memverifikasi keaslian data lokasi yang diterima dari perangkat. Seperti yang diungkapkan oleh Hariyanto dan Sastra (2021), sistem validasi kehadiran berbasis lokasi seharusnya menjalankan algoritma Haversine di sisi server untuk mengukur jarak antara koordinat pengguna dengan lokasi kantor, serta memeriksa waktu agar tidak terjadi manipulasi. Kelemahan ini memungkinkan pegawai untuk melakukan "titip absen" atau mencatat kehadiran dari rumah, yang secara langsung merusak keakuratan data disiplin.
2. Eskalasi Hak Akses dan Kebocoran Data (BUG-007 dan BUG-011): Akses tanpa batas pada endpoint API /api/users untuk pengguna yang berstatus staf adalah pelanggaran terhadap prinsip Least Privilege dalam keamanan informasi. Masalah ini diperburuk oleh penemuan di fitur ekspor Excel yang menyertakan kolom hash kata sandi. Meskipun kata sandi tersebut sudah dienkripsi, kebocoran ini meningkatkan risiko serangan Brute Force atau Rainbow Table jika database bocor. Berdasarkan standar OWASP Top 10 (2021), kerentanan ini tergolong dalam Broken Access Control dan Cryptographic Failures yang harus segera diatasi dengan penerapan Middleware otorisasi yang lebih ketat.
3. Ancaman Keamanan File (BUG-003): Kemampuan sistem untuk menerima file. php melalui fitur unggah bukti cuti adalah kerentanan yang paling mengkhawatirkan (Remote Code Execution). Jika seorang penyerang berhasil mengunggah web shell, mereka bisa mendapatkan kendali penuh atas server. Validasi ekstensi file saat ini hanya dilakukan menggunakan atribut HTML accept, yang sangat mudah dilewati dengan menggunakan proxy seperti Burp Suite. Solusi yang harus diimplementasikan adalah validasi MIME-type di level backend dan penamaan ulang file secara acak saat disimpan untuk menghindari eksekusi skrip (Rozi dan Purnomo, 2022).

Secara keseluruhan, meskipun fungsi dasar sistem beroperasi (CRUD data, Login), elemen Non-Fungsional Requirement khususnya keamanan sangat lemah. Disarankan perbaikan tidak hanya sebatas penambalan kode, tetapi juga pada desain ulang arsitektur validasi data.

Analisis White Box Testing

Analisis dilakukan pada *method* checkIn di AttendeController.php.

1. Flow Graph: Terdapat 3 simpul keputusan (Validasi User, Validasi Waktu, Simpan).
2. Cyclomatic Complexity (V(G)): Hasil perhitungan V(G) = 4 (Maulida, 2023).
3. Hasil: Alur logika sudah mencakup jalur dasar, namun *Exception Handling* (blok try-catch) tidak ditemukan saat proses penyimpanan ke database, yang menyebabkan layar putih (*Whoops Error*) jika database *down*.

D. PENUTUP

Simpulan

Penelitian ini berhasil menunjukkan bahwa sistem kehadiran karyawan yang menggunakan QR Code dan Geolocation memiliki kelemahan serius jika tidak dilengkapi dengan validasi yang ketat di sisi server. Hasil pengujian menegaskan bahwa standar ISO/IEC 29119 efektif dalam mengidentifikasi sepuluh jenis kecacatan perangkat lunak, termasuk kemampuan untuk bypass absensi dan masalah keamanan pada file. Penelitian ini memberikan sumbangan ilmiah berupa saran arsitektur keamanan untuk sistem kehadiran, dengan menekankan pentingnya adanya validasi berlapis pada data yang diterima. Uji coba di masa depan disarankan untuk mencakup pengujian beban guna menilai seberapa tahan sistem saat digunakan oleh ribuan pengguna secara bersamaan.

Saran

Berdasarkan hasil temuan bug serius, penelitian ini menyarankan perbaikan yang harus diprioritaskan sebagai berikut:

1. Validasi Berlapis: Melaksanakan pemeriksaan data yang wajib di sisi backend (Laravel) untuk seluruh input API, khususnya pada koordinat lokasi, ekstensi file, dan informasi absensi. Jangan hanya mengandalkan pemeriksaan di sisi frontend.
2. Keamanan QR Code Dinamis: Mengubah sistem QR Code statis dengan Time-based One-Time Password (TOTP) yang sudah dienkripsikan dan diperbarui setiap 30 detik untuk mencegah serangan Replay Attack.
3. Sanitasi Input dan Output: Menerapkan fungsi pembersihan seperti htmlspecialchars atau melakukan pengkodean otomatis dari framework pada semua input teks untuk menghindari serangan XSS.
4. Kontrol Akses Ketat: Memperbaiki Middleware pada rute API untuk memastikan bahwa pengguna hanya bisa mengakses data yang menjadi miliknya sendiri (Prinsip Least Privilege).

Ucapan Terima Kasih
Terimakasih untuk Leonard Attalah dan Iqbal Kholik sebagai penulis sudah menyelesaikan jurnal ini dengan baik semoga menjadi penambahan ilmu utamanya untuk diri sendiri dan umumnya untuk masyarakat banyak. Semoga sukses.

E. DAFTAR PUSTAKA

Afrianto, I., & Heryana, A. (2021). Penerapan Metode Black Box Testing dengan Teknik Equivalence Partitioning pada Aplikasi Sistem Absensi. *Jurnal Ilmiah Komputasi*, 20(2), 155-164.

Ammann, P., & Offutt, J. (2021). *Introduction to Software Testing* (2nd ed.). Cambridge University Press.

Burnstein, I. (2019). *Practical Software Testing: A Process-Oriented Approach*. Springer.

Hariyanto, D., & Sastra, R. (2021). Implementasi Algoritma Haversine Formula Pada Sistem Absensi Karyawan Berbasis Lokasi. *Jurnal Teknologi Informasi*, 7(2), 120-129.

ISO/IEC. (2021). *ISO/IEC/IEEE 29119-1:2013 Software and systems engineering — Software testing — Part 1: Concepts and definitions*. International Organization for Standardization.

Maulida, S. (2023). Implementation of White Box Testing using Cyclomatic Complexity on Web-Based Attendance Application. *Journal of Information Systems Engineering*, 5(2), 112-120.

Myers, G. J., Sandler, C., & Badgett, T. (2020). *The Art of Software Testing* (3rd ed.). John Wiley & Sons.

Naik, K., & Tripathy, P. (2021). *Software Testing and Quality Assurance: Theory and Practice*. Wiley.

Nidhra, S., & Dondeti, J. (2022). Black Box and White Box Testing Techniques - A Literature Review. *International Journal of Embedded Systems and Applications (IJESA)*, 2(2), 29-50.

OWASP Foundation. (2021). *OWASP Top 10:2021 The Ten Most Critical Web Application Security Risks*. OWASP.org.

Permana, A. A. (2020). Rancangan Sistem Informasi Absensi Pegawai Berbasis Web Menggunakan Framework Laravel. *Jurnal Inovasi Teknologi Pendidikan*, 7(1), 55-65.

Pressman, R. S., & Maxim, B. R. (2020). *Software Engineering: A Practitioner's Approach* (9th ed.). McGraw-Hill Education.

Rozi, F., & Purnomo, A. (2022). Vulnerability Assessment pada Aplikasi Absensi Online Menggunakan OWASP ZAP. *Jurnal Keamanan Siber*, 4(1), 45-52.

Setiawan, R. (2022). Analisis Pengujian Perangkat Lunak Menggunakan Standar ISO 25010 Pada Sistem Kepegawaian. *Jurnal Teknik Informatika*, 14(1), 33-40.

Sommerville, I. (2020). *Software Engineering* (10th ed.). Pearson Education.