

## Aplikasi Sistem Pencatatan Pengaduan Masyarakat Berbasis Standar ISO/IEC 29119:2022

<sup>1</sup>Achmad Irvan Zidny, <sup>2</sup>Nazilah Marzukoh, <sup>3</sup>Chairul Anwar

<sup>123</sup>Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pamulang, Tangerang Selatan, Indonesia

<sup>1</sup>[zidnyi647@gmail.com](mailto:zidnyi647@gmail.com), <sup>2</sup>[nazilah.zukoh2002@gmail.com](mailto:nazilah.zukoh2002@gmail.com), <sup>3</sup>[dosen02917@unpam.ac.id](mailto:dosen02917@unpam.ac.id)

### Abstract

*The Public Complaint Recording System is a web-based application developed using PHP Native and Bootstrap 5. This study aims to evaluate the quality of the application through systematic testing based on the ISO/IEC 29119:2022 standard using the Black Box Testing approach. The testing focuses on core functionalities, including user authentication, complaint data management (CRUD), report generation, and the logout feature. A total of 25 test scenarios were executed, resulting in a success rate of 40%, with 10 test cases passing, 14 failing, and 1 partially successful. Additionally, 10 defects were identified with varying severity levels, five of which were classified as critical due to their impact on application security. The critical issues include vulnerabilities related to SQL Injection, Cross-Site Scripting (XSS), improper authorization, insecure file uploads, and unrestricted direct URL access. The findings indicate that the application is exposed to significant security risks that require immediate improvement. This study recommends prioritizing input validation, session management, authorization control, and the use of prepared statements to enhance application security and reliability.*

**Keywords:** Software Testing, ISO/IEC 29119:2022, Black Box Testing, Complaint System, Application Security.

### Abstrak

Aplikasi Pencatatan Pengaduan Masyarakat merupakan aplikasi berbasis web yang dikembangkan menggunakan PHP Native dan Bootstrap 5. Penelitian ini bertujuan untuk mengevaluasi kualitas aplikasi melalui pengujian sistematis berdasarkan standar ISO/IEC 29119:2022 dengan metode Black Box Testing. Pengujian difokuskan pada fitur utama, meliputi autentikasi pengguna, pengelolaan data pengaduan (CRUD), pencetakan laporan, dan fitur logout. Sebanyak 25 skenario pengujian dilakukan dengan tingkat keberhasilan sebesar 40%, terdiri dari 10 skenario berhasil, 14 gagal, dan 1 skenario sebagian berhasil. Selain itu, ditemukan 10 bug dengan tingkat keparahan berbeda, di mana lima di antaranya dikategorikan sebagai bug kritis karena berdampak langsung pada keamanan aplikasi. Bug kritis tersebut meliputi kerentanan SQL Injection, serangan XSS, kelemahan otorisasi, keamanan unggah file, dan akses URL tanpa autentikasi. Hasil penelitian menunjukkan bahwa aplikasi masih memiliki risiko keamanan yang perlu segera diperbaiki. Rekomendasi utama meliputi penerapan validasi input, manajemen sesi, kontrol otorisasi, serta penggunaan prepared statement untuk meningkatkan keamanan dan keandalan aplikasi.

**Kata Kunci:** Pengujian Perangkat Lunak, ISO/IEC 29119:2022, Black Box Testing, Sistem Pengaduan, Keamanan Aplikasi.

### A. PENDAHULUAN

Perkembangan dalam teknologi informasi telah mendorong perubahan digital di berbagai bidang pelayanan publik, termasuk dalam sistem pengaduan masyarakat. Aplikasi berbasis web untuk Pencatatan Pengaduan Masyarakat merupakan alternatif yang memudahkan warga untuk menyampaikan keluhan, aspirasi, atau laporan yang berkaitan dengan pelayanan publik dengan cara yang cepat, terstruktur, dan digital.

Aplikasi ini dibuat dengan menggunakan PHP Native serta database MySQL, dan menerapkan framework Bootstrap

5 untuk desain antarmuka pengguna. Fitur-fitur utama yang disediakan mencakup pendaftaran pengguna, autentikasi, pengelolaan data pengaduan (Buat, Baca, Perbarui, Hapus), pencetakan laporan, dan keluar aplikasi.

Namun, aplikasi yang tidak melewati proses pengujian yang menyeluruh dapat memiliki risiko seperti masalah keamanan, kesalahan fungsi, dan kualitas pengalaman pengguna yang rendah. Oleh karena itu, diperlukan pengujian kualitas perangkat lunak yang sesuai standar untuk memastikan aplikasi dapat berfungsi dengan baik dan aman.

## B. METODE

Standar ISO/IEC 29119:2022

ISO/IEC 29119:2022 adalah standar internasional yang mengatur proses pengujian perangkat lunak secara menyeluruh. Standar ini mencakup:

- Bagian 1: Konsep dan Definisi - Terminologi pengujian
- Bagian 2: Proses Pengujian - Tahapan dari perencanaan hingga penutupan
- Bagian 3: Dokumentasi Pengujian - Format dan konten dokumen
- Bagian 4: Teknik Pengujian - Metode dan teknik pengujian

Software Testing Life Cycle (STLC)

Pengujian mengikuti tahapan STLC yang sesuai dengan ISO/IEC 29119:2022:

### 1. Requirement Analysis

- Menganalisis fitur aplikasi berdasarkan dokumentasi
- Mengidentifikasi fungsi yang perlu diuji
- Menentukan kriteria keberhasilan

### 2. Test Planning

- Menyusun strategi pengujianMenentukan teknik Black Box Testing
- Menetapkan jadwal dan resource

### 3. Test Case Development

- Merancang test case untuk setiap modul
- Menentukan input data dan expected result
- Membuat skenario pengujian positif dan negatif

### 4. Test Environment Setup

- Menyiapkan server lokal (XAMPP)
- Mengonfigurasi database MySQL
- Memastikan environment sesuai requirement

### 5. Test Execution

- Menjalankan test case secara sistematis
- Merekam hasil pengujian
- Mendokumentasikan bug yang ditemukan

### 6. Test Cycle Closure

- Menganalisis hasil pengujian
- Menghitung metrik pengujian

Metode Black Box Testing

Black Box Testing dipilih karena fokus pada pengujian fungsional tanpa perlu mengetahui struktur internal kode.

Teknik yang digunakan:

- Equivalence Partitioning: Membagi input menjadi kelas valid dan invalid
- Boundary Value Analysis: Menguji nilai batas input
- Error Guessing: Menguji skenario error yang mungkin terjadi
- Security Testing: Menguji vulnerability (SQL Injection, XSS, dll)

## C. HASIL DAN PENGUJIAN

Hasil Test Case Pengujian Fungsional

Pengujian fungsional dilakukan terhadap seluruh fitur utama aplikasi Pengaduan Masyarakat. Berikut adalah hasil pengujian yang telah dilakukan:

### Test Login Case

| ID     | Deskripsi                     | Langkah Pengujian                                                                                       | Expected Result                               | Actual Result                        | Status |
|--------|-------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------|--------------------------------------|--------|
| TC-001 | Login dengan kredensial valid | 1. Buka halaman login2. Input username: "masyarakat"3. Input password: "masyarakat"4. Klik tombol Login | Berhasil login dan masuk ke dashboard         | Sesuai dengan expected result        | PASS   |
| TC-002 | Login dengan password salah   | 1. Input username: "masyarakat"2. Input password: "salah123"3. Klik tombol Login                        | Muncul pesan "Username atau Password salah"   | Tidak ada validasi error yang muncul | FAIL   |
| TC-003 | Username kosong               | 1. Kosongkan field username2. Input password3. Klik tombol Login                                        | Muncul validasi "Username tidak boleh kosong" | Form tetap dapat disubmit            | FAIL   |

### Test Case – Modul Register

| ID     | Deskripsi                       | Langkah Pengujian                                                | Expected Result                               | Actual Result                  | Status |
|--------|---------------------------------|------------------------------------------------------------------|-----------------------------------------------|--------------------------------|--------|
| TC-004 | Register data lengkap           | 1. Isi seluruh field pada form registrasi2. Klik tombol Register | User berhasil terdaftar                       | Sesuai dengan expected result  | PASS   |
| TC-005 | Username sudah terdaftar        | 1. Input username yang sudah terdaftar2. Klik tombol Register    | Muncul validasi "Username sudah terdaftar"    | Tidak ada validasi yang muncul | FAIL   |
| TC-006 | Password kurang dari 6 karakter | 1. Input password "123"2. Klik tombol Register                   | Muncul validasi "Password minimal 6 karakter" | Form tetap dapat disubmit      | FAIL   |

### Test Case – Edit Pengaduan

| ID     | Deskripsi      | Expected Result          | Actual Result                 | Status |
|--------|----------------|--------------------------|-------------------------------|--------|
| TC-010 | Edit pengaduan | Data berhasil diperbarui | Sesuai dengan expected result | PASS   |

| ID     | Deskripsi                          | Expected Result           | Actual Result                       | Status |
|--------|------------------------------------|---------------------------|-------------------------------------|--------|
| TC-011 | Edit field kosong                  | Muncul validasi input     | Form tetap dapat disimpan           | FAIL   |
| TC-012 | Edit pengaduan milik pengguna lain | Akses ditolak oleh sistem | Pengguna tetap dapat melakukan edit | FAIL   |

#### Summary Test Case

| Status  | Jumlah | Persentase |
|---------|--------|------------|
| PASS    | 10     | 40%        |
| FAIL    | 14     | 56%        |
| PARTIAL | 1      | 4%         |
| TOTAL   | 25     | 100%       |

#### Bug Report

##### Test Case – Hapus Pengaduan

| ID     | Deskripsi                           | Expected Result                      | Actual Result                           | Status |
|--------|-------------------------------------|--------------------------------------|-----------------------------------------|--------|
| TC-013 | Hapus pengaduan milik sendiri       | Data pengaduan berhasil dihapus      | Sesuai dengan expected result           | PASS   |
| TC-014 | Hapus pengaduan tanpa konfirmasi    | Sistem menampilkan dialog konfirmasi | Data langsung terhapus tanpa konfirmasi | FAIL   |
| TC-015 | Hapus pengaduan milik pengguna lain | Akses ditolak oleh sistem            | Pengguna tetap dapat menghapus data     | FAIL   |

##### Test Case – Cetak / Print

| ID     | Deskripsi                   | Expected Result                                       | Actual Result                           | Status |
|--------|-----------------------------|-------------------------------------------------------|-----------------------------------------|--------|
| TC-016 | Cetak detail pengaduan      | Sistem menampilkan preview cetak dengan tampilan rapi | Sesuai dengan expected result           | PASS   |
| TC-017 | Cetak pengaduan tanpa login | Sistem mengarahkan pengguna ke halaman login          | Halaman cetak dapat diakses tanpa login | FAIL   |

##### Test Case – Logout

| ID     | Deskripsi                    | Expected Result                                                   | Actual Result                                 | Status |
|--------|------------------------------|-------------------------------------------------------------------|-----------------------------------------------|--------|
| TC-018 | Logout dari sistem           | Session pengguna terhapus dan sistem mengarahkan ke halaman login | Sesuai dengan expected result                 | PASS   |
| TC-019 | Akses halaman setelah logout | Sistem mengarahkan pengguna ke halaman login                      | Pengguna masih dapat mengakses halaman sistem | FAIL   |

##### Test Case – Database

| ID     | Deskripsi                          | Expected Result             | Actual Result                      | Status |
|--------|------------------------------------|-----------------------------|------------------------------------|--------|
| TC-020 | Koneksi database                   | Database berhasil terhubung | Sesuai dengan expected result      | PASS   |
| TC-021 | Pengujian SQL Injection pada login | Proses login gagal          | Sistem dapat melewati proses login | FAIL   |

| ID      | Deskripsi                            | Expected Result             | Actual Result            | Severity | Priority |
|---------|--------------------------------------|-----------------------------|--------------------------|----------|----------|
| BUG-001 | Form login bisa disubmit tanpa input | Validasi input muncul       | Form tetap tersubmit     | Major    | P1       |
| BUG-002 | Rentan SQL Injection                 | Login gagal                 | Berhasil bypass login    | Critical | P1       |
| BUG-003 | Rentan XSS                           | Disimpan sebagai teks biasa | Script tereksekusi       | Critical | P1       |
| BUG-004 | Tidak ada authorization check        | Akses ditolak               | Data berhasil diedit     | Critical | P1       |
| BUG-005 | Session masih aktif setelah logout   | Redirect ke login           | Dashboar d tetap terbuka | Major    | P1       |
| BUG-006 | Tidak ada validasi tipe file         | Upload ditolak              | File berbahaya terupload | Critical | P1       |
| BUG-007 | Tidak ada batas ukuran file          | Ditolak (maks. 2MB)         | File tetap terupload     | Medium   | P2       |
| BUG-008 | Tidak ada konfirmasi delete          | Muncul dialog konfirmasi    | Data langsung terhapus   | Medium   | P2       |
| BUG-009 | Username duplikat bisa dibuat        | Registrasi ditolak          | Data duplikat tersimpan  | Major    | P1       |
| BUG-010 | Akses URL langsung tanpa login       | Redirect ke login           | Halaman terbuka          | Critical | P1       |
| BUG-011 | Tidak ada CSRF protection            | Request ditolak             | Request diproses         | Critical | P1       |
| BUG-012 | HTML Injection                       | Karakter di-escape          | HTML dirender            | Medium   | P2       |
| BUG-013 | Password tanpa validasi              | Ditolak (min. 6 karakter)   | Registrasi berhasil      | Medium   | P2       |
| BUG-014 | Email tidak divalidasi               | Ditolak                     | Data diterima            | Minor    | P3       |
| BUG-015 | Error tidak ditangani                | Pesan error tampil          | Halaman blank            | Major    | P1       |
| BUG-016 | Sorting tidak berfungsi              | Data tersortir              | Tidak ada perubahan      | Minor    | P3       |

#### Rekapitulasi Hasil Test Case



| ID      | Deskripsi                           | Expected Result    | Actual Result  | Severity | Priority |
|---------|-------------------------------------|--------------------|----------------|----------|----------|
| BUG-017 | Tidak ada limit login (brute force) | Akun diblokir      | Tetap diproses | Critical | P1       |
| BUG-018 | Tidak ada log aktivitas             | Aktivitas tercatat | Tidak ada log  | Medium   | P2       |

#### Rekapitulasi Bug

| Severity | Jumlah | Persentase | Deskripsi                          |
|----------|--------|------------|------------------------------------|
| Critical | 5      | 50%        | Bug yang mengancam keamanan sistem |
| Major    | 3      | 30%        | Bug yang mengganggu fungsi utama   |
| Medium   | 2      | 20%        | Bug yang mengganggu fungsi minor   |
| Total    | 10     | 100%       | -                                  |

#### Bug Berdasarkan Modul

| Modul            | Jumlah Bug | Persentase |
|------------------|------------|------------|
| Login/Auth       | 3          | 30%        |
| Pengaduan (CRUD) | 4          | 40%        |
| Upload File      | 2          | 20%        |
| Logout/Session   | 1          | 10%        |

#### Bug Berdasarkan Priority

| Priority    | Jumlah | Deskripsi                    |
|-------------|--------|------------------------------|
| P1 (High)   | 8      | Harus diperbaiki segera      |
| P2 (Medium) | 2      | Diperbaiki sprint berikutnya |

## D. PEMBAHASAN

Hasil pengujian yang dilakukan berdasarkan standar ISO/IEC 29119:2022 menunjukkan bahwa sebagian fitur aplikasi berfungsi dengan baik; namun, masih ada beberapa masalah yang berdampak pada keamanan serta kualitas sistem secara keseluruhan. Dari total 25 skenario pengujian yang dilakukan, hanya 10 skenario yang berhasil (40%), sedangkan 14 skenario mengalami kegagalan (56%) dan 1 skenario menghasilkan hasil sebagian. Persentase ini menunjukkan bahwa aplikasi memerlukan perbaikan besar, terutama dalam hal validasi, keamanan, dan pengelolaan data.

Modul autentikasi (login dan registrasi) menunjukkan beberapa kegagalan yang berkaitan dengan validasi data masukan dan manajemen sesi. Sebagai contoh, sistem tidak selalu memblokir masukan kosong atau email yang tidak valid, dan sesi pengguna tidak tertutup dengan baik setelah melakukan logout.

Pada modul pengelolaan pengaduan (CRUD), ditemukan beberapa bug kritis seperti akses instan ke URL tanpa autentikasi, celah SQL Injection, serta validasi masukan

yang kurang memadai yang dapat menimbulkan ketidaksesuaian data. Modul ini juga tercatat sebagai modul dengan jumlah bug terbanyak (40%).

Modul untuk mengunggah file memiliki dua bug keamanan utama yang memungkinkan pengguna untuk mengunggah file berbahaya, dikarenakan tidak adanya penyaringan jenis file dan pemeriksaan MIME type. Sementara itu, modul logout mengalami masalah terkait pengelolaan sesi, di mana token sesi tidak dihapus sepenuhnya, sehingga memungkinkan akses kembali tanpa login.

Secara keseluruhan, temuan ini menunjukkan bahwa aplikasi telah memenuhi beberapa kebutuhan fungsional dasar, tetapi aspek keamanan adalah bagian paling kritis yang memerlukan perhatian khusus untuk perbaikan. Disarankan untuk menerapkan prepared statements, validasi masukan, kontrol otorisasi, dan peningkatan manajemen sesi untuk memperkuat keandalan dan keamanan aplikasi.

## Kesimpulan

Berdasarkan pengujian yang telah dilakukan pada Aplikasi Sistem Pencatatan Pengaduan Masyarakat dengan mengikuti standar ISO/IEC 29119:2022 serta menggunakan metode Black Box Testing, kita bisa menarik kesimpulan bahwa kualitas aplikasi ini belum sepenuhnya memenuhi standar fungsionalitas dan keamanan dengan baik. Dari 25 skenario pengujian yang dilakukan, hanya 10 skenario yang berhasil diuji (40%), sedangkan 14 skenario mengalami kegagalan (56%) dan 1 skenario menunjukkan hasil yang tidak lengkap. Ini menunjukkan bahwa aplikasi masih memerlukan perbaikan yang signifikan untuk ditingkatkan.

Jumlah bug yang terdeteksi adalah 10, dengan 5 di antaranya termasuk dalam kategori kritis, terutama yang berkaitan dengan masalah keamanan seperti SQL Injection, XSS, akses tidak sah, kelemahan dalam mengupload file, dan manajemen sesi. Temuan ini menunjukkan bahwa sistem sangat rentan terhadap serangan yang bisa mengancam data pengguna serta integritas aplikasi.

Secara keseluruhan, aplikasi ini telah bisa menjalankan beberapa fungsi dasar, seperti meng-input dan mengelola data pengaduan, namun keamanannya belum bisa diandalkan tanpa adanya perbaikan yang menyeluruh. Maka dari itu, pengembang perlu fokus untuk memperbaiki aspek validasi input, manajemen sesi, otorisasi akses, serta penerapan prepared statement demi mengurangi kemungkinan terjadinya serangan.

Dengan melaksanakan perbaikan sesuai dengan rekomendasi yang ada, diharapkan aplikasi ini dapat mencapai kualitas yang lebih baik, baik dalam hal keamanan maupun kenyamanan pengguna, sehingga dapat berfungsi secara efektif sebagai platform pengaduan masyarakat yang berbasis web.

## E. DAFTAR PUSTAKA

- Sari, R. (2021). Pengujian sistem informasi akademik menggunakan ISO/IEC 29119. *Jurnal TEKNO SI*.
- Winata, W. (2021). Pengujian website EPOS dengan black box dan equivalence partitioning. *Jurnal Informatika*.  
<https://ojs.uaaj.ac.id/index.php/jiaj/article/view/6780>
- (2025). *Analisis kerentanan keamanan website menggunakan OWASP Top-10: Studi kasus Web BNPB*. Indonesian Journal of Education And Computer Science.  
PDF:  
<https://jurnal.intekom.id/index.php/indotech/article/view/1411>
- Yusuf, M. F., Hikmah, I. R., & Amiruddin. (2025). *Security testing of XYZ website application using ISSAF and OWASP WSTG v4.2 methods*. *Teknika*, 14(1), 66–77.  
PDF:  
<https://ejournal.ikado.ac.id/index.php/teknika/article/view/1156>
- Sugara, V. I., & Sriyasa, I. W. (2024). *Analisis keamanan web menggunakan OWASP*. *The Indonesian Journal of Computer Science*, 13(2).  
PDF:  
<https://ijcs.net/ijcs/index.php/ijcs/article/view/3736>
- Rafeli, A. I., Seta, H. B., & Widi, I. W. (2025). Pengujian celah keamanan website menggunakan OWASP WSTG. *Informatik*.  
PDF:  
<https://ejournal.upnvj.ac.id/informatik/article/view/4632>
- Widianto, F., Wijaya, E. S., Harjono, H., & Wicaksono, A. P. (2025). Analisis kerentanan aplikasi web menggunakan metode PTES. *Jurnal Pendidikan dan Teknologi Indonesia*, 5(1), 155–166.  
PDF:  
<https://www.jpti.journals.id/index.php/jpti/article/view/609>
- Herman, H., Riadi, I., Kurniawan, Y., & Rafiq, I. A. (2023). Analisis keamanan website menggunakan ISSAF. *Jurnal Teknologi Informatika dan Komputer*, 9(1).  
PDF:  
<https://journal.thamrin.ac.id/index.php/jtik/article/view/1439>
- Febrian, D. W., Huwae, R. B., & Mardiansyah, A. Z. (2025). Security analysis of university websites against SQLi, XSS & IDOR attacks. *BITe*, 7(1), 25–38.  
PDF:  
<https://journal.universitasbumigora.ac.id/bite/article/view/5032>
- Siddiq, M., & Subandri, M. A. (2025). Pengujian kualitas website Kelurahan Rimba Sekampung berdasarkan ISO 29119:2022. *SABER*, 3(4), 29–39.  
PDF:  
<https://jurnal.stikes-ibnusina.ac.id/index.php/SABER/article/view/3213>
- Fachrurrozi, M., & Widodo, W. (2021). *Pengujian aplikasi web menggunakan metode Black Box Testing*. *Jurnal Teknologi dan Sistem Informasi*, 8(3).  
PDF:  
<https://ojs.trigunadharma.ac.id/index.php/jtsi/article/view/1044>
- Utami, D., & Hidayat, T. (2022). *Implementasi Black Box Testing pada aplikasi layanan masyarakat*. *Jurnal Sisfokom*, 11(2), 178–189.  
PDF:  
<https://jurnal.stmikroyal.ac.id/index.php/sisfokom/article/view/1917>
- Romadhoni, R., & Nuryasin, I. (2023). *Analisis kondisi keamanan aplikasi web menggunakan OpenVAS*. *Jurnal Teknik Informatika Unika*, 12(1).  
PDF:  
<https://ejournal.unika.ac.id/index.php/jti/article/view/6574>
- Putra, R. A., & Rahmatullah, A. (2020). *Penerapan metode Black Box pada sistem informasi aduan masyarakat*. *Jurnal Teknologi Informasi*, 9(2).  
PDF:  
<https://journal.amikom.ac.id/index.php/ijcit/article/view/1205>
- Aldiansyah, H., & Kurniawan, D. (2021). *Analisis keamanan web berbasis PHP menggunakan teknik security testing*. *Jurnal Ilmiah Teknologi Informasi*, 15(1).  
PDF:  
<https://jurnal.polsri.ac.id/index.php/sinkron/article/view/2319>
- Sembiring, A., & Hutabarat, D. (2023). *Pengujian kerentanan aplikasi dengan BurpSuite*. *Jurnal Rekayasa Sistem & Teknologi Informasi*, 7(4).  
PDF:  
<https://jim.teknokrat.ac.id/index.php/JIRSTI/article/view/2763>
- Amalia, N., & Rohman, M. (2024). *Security testing pada aplikasi e-government*. *Jurnal Sistem Informasi dan Keamanan*, 10(1).  
PDF:  
<https://journal.unisayogya.ac.id/index.php/jsik/article/view/3941>
- Fathoni, A., & Saputra, Y. (2023). *Evaluasi keamanan web UMKM menggunakan OWASP ZAP*. *Jurnal*

Teknologi Komputer, 1).  
PDF:  
<https://journal.itk.ac.id/index.php/jtk/article/view/1847>

Rizqi, M., & Satria, A. (2020). *Testing dan analisis kualitas software berbasis web*. Jurnal Informatika Polinema, 4(2).  
PDF:  
<https://jurnal.polinema.ac.id/index.php/inf/article/view/2240>

Damanik, R., & Ginting, R. (2022). *Uji keamanan website menggunakan OWASP dan SQLMap*. Jurnal Teknik Informatika UNIMED, 11(2).  
PDF:  
<https://jurnal.unimed.ac.id/202/index.php/jti/article/view/30923>

Fajri, H., & Rafiudin. (2024). *Analisis kelemahan autentikasi pada platform pengaduan publik berbasis web*. Jurnal Informasi & Teknologi, 6(1).  
PDF:  
<https://ejournal.unib.ac.id/index.php/infortech/article/view/3879>

Mahendra, Y. S., & Arfianto, N. (2019). *Pengujian fungsional sistem layanan publik menggunakan Black Box Testing*. Jurnal Sains dan Teknologi Komputer, 4(3).  
PDF:  
<https://jurnal.stkipsimbah.ac.id/index.php/jstk/article/view/1331>