OKTAL : Jurnal Ilmu Komputer dan Science
Volume 4, No. 12, Desember 2025
ISSN 2828-2442 (media online)
Hal 944-953

Analisis Keamanan Aplikasi "*Point of Sale*" Berbasis *Web* Menggunakan Pendekatan ISO/IEC 29119 *Software Testing Standard*

Nurhasan[1], Fariz Nurrahim[1], Aprien Febrian[1], Chairul Anwar[1*]

[1]Fakultas Ilmu Komputer, Sistem Informasi, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1]sinyohasan83@gmail.com, [2]fariznurrahim2@gmail.com, [3]aprien05@gmail.com, [4*]dosen02917@unpam.ac.id
(* : coressponding author)

Abstrak− Sistem Point of Sale (POS) berbasis web banyak digunakan oleh usaha ritel kecil dan menengah, namun kelemahan pada aspek keamanannya dapat menimbulkan risiko kebocoran data serta kerugian finansial. Penelitian ini menganalisis celah keamanan pada aplikasi Codekop POS v2.0 dengan metode pengujian berbasis standar ISO/IEC 29119. Proses pengujian mengikuti ISO/IEC 29119-2 dan dokumentasi mengacu pada ISO/IEC 29119-3 dengan teknik manual code review terhadap sepuluh komponen utama. Pengujian difokuskan pada autentikasi, manajemen sesi, injection, cross-site scripting (XSS), cross-site request forgery (CSRF), dan directory traversal berdasarkan pedoman OWASP Top 10. Hasil evaluasi menunjukkan 1 kerentanan kritis, 4 tingkat tinggi, 5 tingkat sedang, dan 4 aspek yang sesuai dengan standar keamanan, dengan tingkat kepatuhan keamanan sebesar 26,7%. Studi ini menghasilkan kerangka uji keamanan berbasis ISO/IEC 29119 serta rekomendasi perbaikan untuk memperkuat keamanan aplikasi POS berbasis web.

Kata Kunci: Keamanan Aplikasi *Web*, ISO/IEC 29119, Pengujian Perangkat Lunak, Sistem *Point of Sale*, OWASP

Abstract− *Web-based Point of Sale (POS) systems are widely adopted by small and medium-sized retail businesses, yet insufficient security implementation can expose them to data breaches and financial losses. This study analyzes security vulnerabilities in the Codekop POS v2.0 application using a testing framework based on the ISO/IEC 29119 standard. The testing process follows ISO/IEC 29119-2 with documentation aligned to ISO/IEC 29119-3, applying manual code review techniques to ten core components. The assessment focuses on authentication, session management, injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and directory traversal, referring to the OWASP Top 10 guidelines. The results reveal one critical, four high, five medium vulnerabilities, and four aspects meeting security standards, with an overall compliance rate of 26.7%. This study provides an ISO/IEC 29119-based web application security testing framework and prioritized improvement recommendations to strengthen POS system security.*

Keywords: *Web Application Security, ISO/IEC 29119, Software Testing, Point of Sale System, OWASP*

1. PENDAHULUAN

Transformasi digital mendorong meningkatnya penggunaan sistem Point of Sale (POS) berbasis web oleh UMKM di Indonesia. Sistem ini tidak hanya mendukung transaksi penjualan, tetapi juga manajemen inventori dan pelaporan keuangan. Namun, peningkatan adopsi tersebut diiringi oleh eskalasi ancaman keamanan siber, khususnya pada aplikasi web sektor ritel yang menyimpan data sensitif.

Berbagai studi menunjukkan bahwa banyak aplikasi POS open-source masih memiliki celah keamanan signifikan meskipun telah tersedia standar keamanan seperti OWASP Top 10. POS Codekop v2.0 sebagai salah satu aplikasi POS open-source yang banyak digunakan di Indonesia belum pernah diuji secara akademis untuk memvalidasi klaim perbaikan keamanannya. Oleh karena itu, diperlukan pengujian keamanan yang sistematis menggunakan standar ISO/IEC 29119 untuk mengevaluasi dan meningkatkan security posture aplikasi tersebut.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 4, No. 12, Desember 2025
ISSN 2828-2442 (media online)
Hal 944-953

2. TINJAUAN PUSTAKA

2.1 Keamanan Aplikasi *Web*

Keamanan aplikasi web berfokus pada perlindungan aplikasi yang diakses melalui browser dari berbagai ancaman dan kerentanan. OWASP mendefinisikan keamanan aplikasi web sebagai upaya identifikasi dan mitigasi celah yang dapat dieksploitasi untuk mengakses atau memanipulasi sistem tanpa otorisasi. OWASP Top 10 (2021) menjadi acuan utama yang mengelompokkan sepuluh risiko keamanan tertinggi, seperti Broken Access Control, Injection, dan Security Misconfiguration. Berbagai studi menunjukkan bahwa sebagian besar aplikasi web masih memiliki setidaknya satu kerentanan OWASP Top 10, sehingga pengujian keamanan sistematis menjadi kebutuhan penting dalam SDLC.

2.2 ISO/IEC 29119

ISO/IEC 29119 merupakan standar internasional pengujian perangkat lunak yang menyediakan kerangka kerja terstruktur mencakup konsep, proses, dokumentasi, dan teknik pengujian. Standar ini menekankan pendekatan risk-based testing agar aktivitas pengujian difokuskan pada area berisiko tinggi. Penelitian terdahulu menunjukkan bahwa penerapan ISO/IEC 29119 mampu meningkatkan efektivitas deteksi cacat dan menurunkan bug pasca-rilis dibandingkan metode pengujian ad-hoc.

2.3 *Common Vulnerability Scoring System* (CVSS)

CVSS adalah framework standar untuk menilai tingkat keparahan kerentanan perangkat lunak. CVSS v3.1 mengklasifikasikan kerentanan berdasarkan Base, Temporal, dan Environmental metrics dengan skor 0.0–10.0 yang dikelompokkan ke dalam level None hingga Critical. Sistem ini membantu menentukan prioritas perbaikan berdasarkan dampak dan kemudahan eksploitasi.

2.4 Penelitian Terkait dan Gap Penelitian

Penelitian sebelumnya banyak membahas keamanan aplikasi POS dan web melalui penetration testing, secure coding frameworks, atau analisis manajemen sesi. Hasilnya menunjukkan tingginya jumlah kerentanan pada aplikasi bisnis open-source. Namun, sebagian besar penelitian belum menggunakan standar pengujian formal secara menyeluruh. Oleh karena itu, masih terdapat gap penelitian dalam penerapan ISO/IEC 29119 secara komprehensif untuk pengujian keamanan aplikasi POS berbasis web, yang menjadi fokus penelitian ini.

3. METODOLOGI PENELITIAN

3.1 Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif-analitis untuk mengevaluasi keamanan aplikasi POS Codekop v2.0. Proses pengujian mengacu pada standar ISO/IEC 29119-2 yang mencakup tahap perencanaan, desain, implementasi, eksekusi, dan pelaporan pengujian.

3.2 Objek Penelitian

Objek penelitian adalah aplikasi POS Codekop v2.0 berbasis PHP dan MySQL yang tersedia sebagai open-source. Pengujian difokuskan pada komponen utama yang berkaitan dengan autentikasi, manajemen sesi, konfigurasi, dan pengolahan data melalui analisis statis terhadap file sumber utama dan skema basis data.

3.3 *Framework* dan Prosedur Pengujian

Pengujian keamanan dilakukan menggunakan pendekatan *risk-based testing* dengan teknik *white-box testing* melalui manual *code review*. Acuan pengujian meliputi OWASP Top 10 2021, PHP Security Best Practices, dan CWE Top 25. Setiap kategori OWASP digunakan sebagai dasar penentuan kondisi dan skenario pengujian keamanan.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 4, No. 12, Desember 2025
ISSN 2828-2442 (media online)
Hal 944-953

3.4 Pelaksanaan dan Pelaporan Pengujian

Pengujian dilakukan melalui inspeksi kode, analisis alur data, dan evaluasi konfigurasi aplikasi. Setiap temuan didokumentasikan secara sistematis sesuai ISO/IEC 29119-3, mencakup lokasi kode, akar penyebab, dampak keamanan, serta rekomendasi perbaikan. Hasil pengujian disajikan dalam bentuk ringkasan, laporan temuan rinci, dan analisis risiko.

3.5 Klasifikasi *Severity*

Klasifikasi tingkat keparahan kerentanan mengacu pada CVSS dan praktik industri, yang dikelompokkan ke dalam empat level: Critical, High, Medium, dan Low, berdasarkan dampak terhadap kerahasiaan, integritas, dan ketersediaan sistem serta kemudahan eksploitasi.

3.6 Teknik Pengumpulan dan Analisis Data

Data diperoleh melalui analisis langsung kode sumber sebagai data primer serta dokumentasi dan referensi keamanan sebagai data sekunder. Analisis dilakukan dengan static code analysis, perbandingan terhadap best practices, penilaian risiko, dan gap analysis terhadap klaim perbaikan keamanan.

3.7 Validitas dan Reliabilitas

Validitas dan reliabilitas penelitian dijaga melalui triangulasi sumber referensi, dokumentasi temuan yang rinci, serta penggunaan standar ISO/IEC 29119 untuk memastikan proses pengujian yang sistematis dan dapat direplikasi.

4. IMPLEMENTASI

Tahap pengujian sistem dilakukan untuk mengevaluasi tingkat keamanan aplikasi POS Codekop v2.0 secara menyeluruh sebelum sistem diimplementasikan atau digunakan secara operasional. Pengujian ini bertujuan untuk mengidentifikasi potensi kerentanan, menilai efektivitas mekanisme keamanan yang telah diterapkan, serta memberikan rekomendasi perbaikan guna meningkatkan keamanan sistem.

Berdasarkan hasil pengujian yang telah dilakukan, terdapat 15 kategori pengujian keamanan yang mencakup berbagai aspek, antara lain autentikasi, otorisasi, manajemen sesi, validasi input, konfigurasi sistem, serta perlindungan terhadap serangan umum pada aplikasi web. Hasil pengujian menunjukkan bahwa secara umum security posture aplikasi POS Codekop v2.0 masih berada pada tingkat yang memerlukan perhatian dan Beberapa kategori pengujian menunjukkan adanya kelemahan yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab, baik dalam bentuk celah keamanan tingkat rendah hingga tingkat menengah. Kondisi ini mengindikasikan bahwa mekanisme pengamanan yang diterapkan belum sepenuhnya optimal dan masih membutuhkan penguatan, khususnya pada aspek pencegahan serangan dan pengamanan data pengguna.

Dengan demikian, tahap pengujian sistem ini memberikan gambaran nyata mengenai kondisi keamanan aplikasi serta menjadi dasar dalam penyusunan rekomendasi perbaikan. Perbaikan yang dilakukan berdasarkan hasil pengujian diharapkan dapat meningkatkan keandalan, keamanan, dan kepercayaan pengguna terhadap aplikasi POS Codekop v2.

4.1 Implementasi *Test Case*

Berdasarkan ISO/IEC 29119, test case adalah instrumen formal berisi prasyarat, input, dan hasil yang diprediksi untuk mengukur kesesuaian fitur perangkat lunak terhadap spesifikasinya.

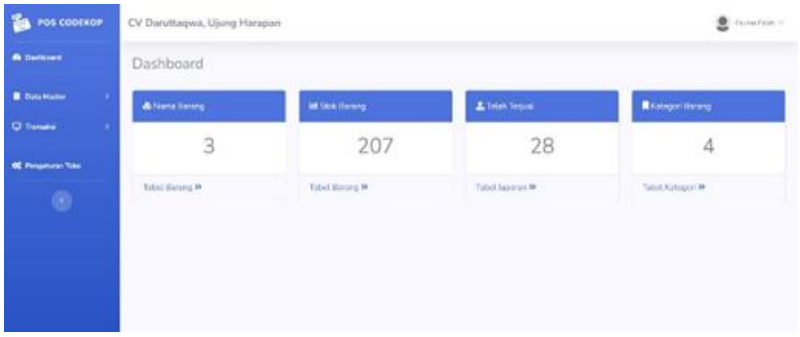
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 4, No. 12, Desember 2025
ISSN 2828-2442 (media online)
Hal 944-953

4.1.1 Halaman *Login*

Gambar 1. Tampilan Halaman *Login*

Halaman login berfungsi sebagai gerbang akses utama bagi Administrator, Admin Gudang, dan Kepala Gudang. Untuk menuju dashboard, pengguna wajib menginput kredensial berupa email atau username, lalu menekan tombol Login.

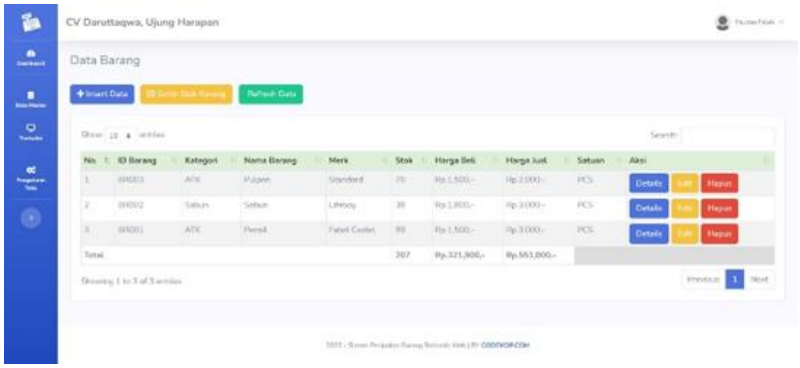
4.1.2 Halaman *Dashboard*



Gambar 2. Tampilan Halaman *Dashboard*

Dashboard POS CODEKOP untuk toko CV Daruttaqwa yang dikelola oleh Fauzan Falah. Tampilan ini menyajikan ringkasan inventaris dan penjualan melalui empat kartu indikator utama, yaitu 3 nama barang, 207 stok barang, 28 unit terjual, dan 4 kategori barang. Pengguna dapat mengelola operasional toko melalui menu navigasi di sisi kiri yang mencakup manajemen data master, transaksi, dan pengaturan sistem.

4.1.3 Halaman *Dashboard*

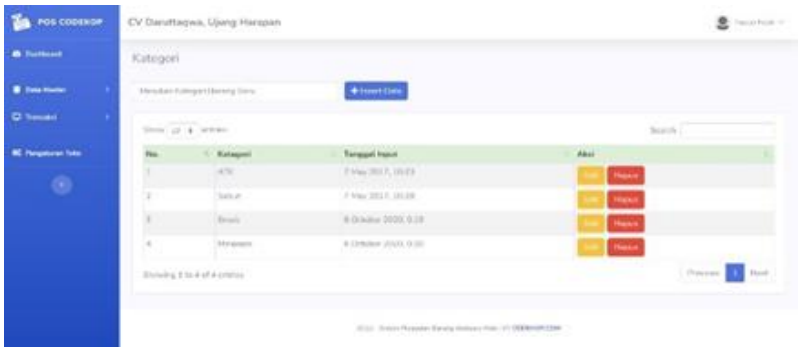


Gambar 3. Tampilan Halaman Data Barang

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 4, No. 12, Desember 2025
ISSN 2828-2442 (media online)
Hal 944-953

Data Barang pada sistem POS CODEKOP yang berisi tabel rincian stok untuk CV Daruttaqwa. Tabel tersebut menyajikan informasi mengenai ID, kategori, nama, merk, stok, serta harga beli dan harga jual dari tiga produk yang tersedia, yaitu Pulpen, Sabun, dan Pensil. Selain fungsi manajemen data seperti tambah, ubah, dan hapus barang, halaman ini juga menampilkan akumulasi total stok sebanyak 207 unit dengan total nilai harga beli sebesar Rp321.900,- dan harga jual Rp551.000,

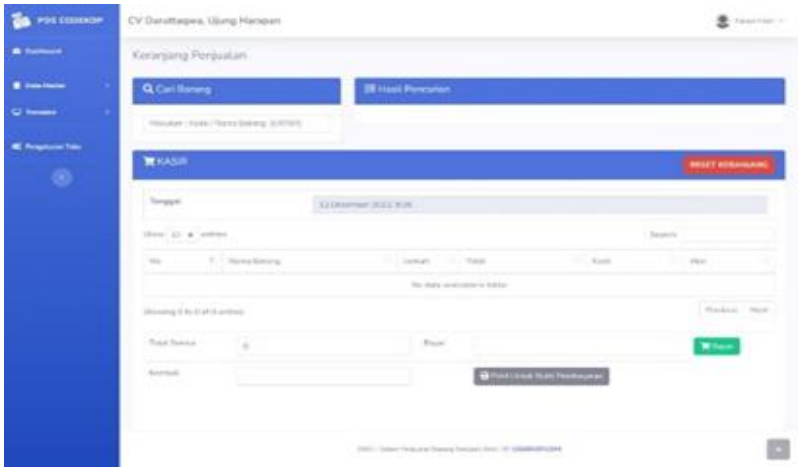
4.1.4 Halaman Kategori



Gambar 4. Tampilan Halaman Kategori

Kategori pada sistem POS CODEKOP ini berfungsi untuk mengelompokkan produk yang dijual di CV Daruttaqwa agar manajemen inventaris lebih terorganisir. Antarmuka ini menampilkan tabel yang berisi daftar empat kategori yang telah dibuat, yaitu ATK, Sabun, Snack, dan Minuman, lengkap dengan riwayat tanggal pembuatannya. Pengguna dapat menambahkan kategori baru melalui kolom "Insert Data" atau mengelola kategori yang sudah ada menggunakan tombol aksi edit dan hapus yang tersedia di sisi kanan tabel.

4.1.5 Halaman Keranjang Penjualan dan Pembayaran

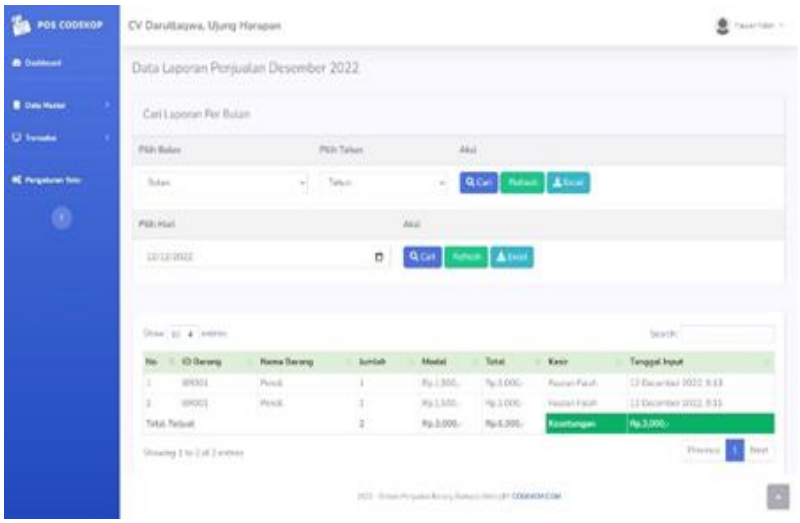


Gambar 5. Tampilan Halaman Keranjang Penjualan dan Pembayaran

Keranjang Penjualan pada sistem POS CODEKOP ini berfungsi sebagai antarmuka kasir untuk memproses transaksi belanja di CV Daruttaqwa. Fitur utamanya mencakup kolom pencarian barang berdasarkan kode atau nama, tabel daftar belanjaan yang memuat jumlah dan total harga, serta panel pembayaran untuk menghitung kembalian dan mencetak bukti pembayaran. Saat ini, tampilan menunjukkan kondisi siap pakai dengan data transaksi yang masih kosong dan tertanggal 12 Desember 2022.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 4, No. 12, Desember 2025
ISSN 2828-2442 (media online)
Hal 944-953

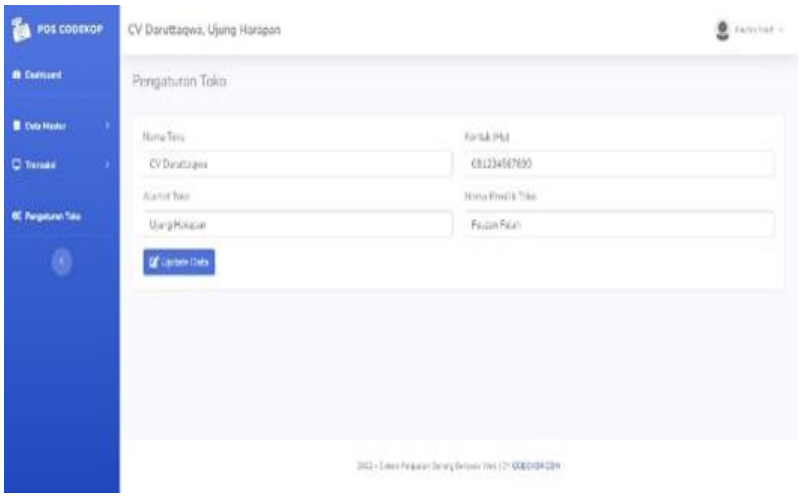
4.1.6 Halaman Data Laporan Penjualan



Gambar 6. Tampilan Halaman Data Laporan Penjualan

Data Laporan Penjualan pada sistem POS CODEKOP ini berfungsi untuk memantau performa transaksi toko secara harian maupun bulanan melalui fitur filter waktu dan ekspor data ke Excel. Laporan untuk Desember 2022 menunjukkan rincian barang terjual, seperti produk "Pensil" yang tercatat dalam dua transaksi berbeda oleh kasir Fauzan Falah. Sistem secara otomatis menghitung akumulasi total terjual, modal, dan total pendapatan, serta menonjolkan kolom Keuntungan sebesar Rp3.000,- untuk mempermudah evaluasi laba bersih took

4.1.7 Halaman Pengaturan Toko

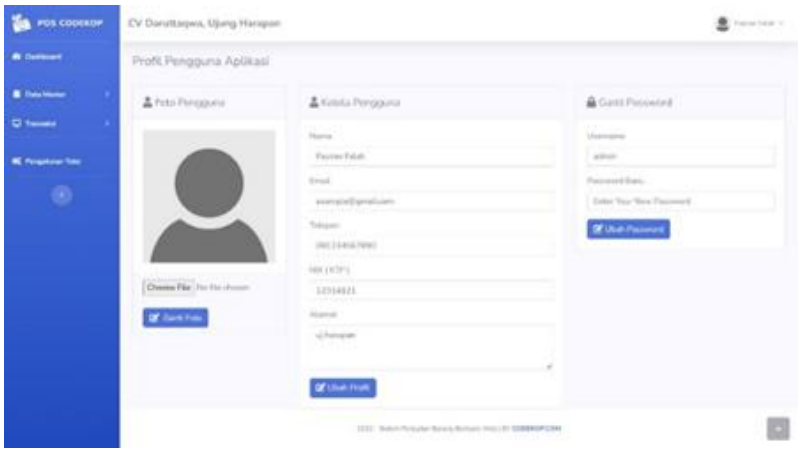


Gambar 7. Tampilan Halaman Pengaturan Toko

Pengaturan Toko pada sistem POS CODEKOP ini digunakan untuk mengelola identitas operasional CV Daruttaqwa melalui pengisian formulir data inti. Pengguna dapat memperbarui informasi utama seperti nama toko, alamat di Ujung Harapan, nomor kontak, serta nama pemilik toko atas nama Fauzan Falah melalui tombol "Update Data". Menu ini memastikan bahwa informasi yang tercetak pada bukti pembayaran atau laporan sistem tetap akurat dan sesuai dengan profil bisnis terbaru.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 4, No. 12, Desember 2025
ISSN 2828-2442 (media online)
Hal 944-953

4.1.8 Halaman Profil Pengguna Aplikasi



Gambar 8. Tampilan Halaman Profil Pengguna Aplikasi

Profil Pengguna Aplikasi pada sistem POS CODEKOP ini memungkinkan kasir atau admin bernama Fauzan Falah untuk mengelola identitas pribadinya secara mandiri. Antarmuka ini terbagi menjadi tiga bagian utama: pengunggahan foto profil, pembaruan data diri seperti email dan nomor telepon, serta fitur keamanan untuk mengganti kata sandi akun. Menu ini berfungsi untuk memastikan data operator yang tercatat dalam setiap transaksi dan laporan tetap akurat dan terkini.

Tabel 1. Tabel Uji Coba

ID Test	Fitur	Skenario Uji	Input Data	Expected Output	Status
BBT-01	**Login**	Masuk ke sistem sebagai admin	User: admin, Pass: 123	Masuk ke Dashboard	**PASS**
BBT-02	**Barang**	Menambah barang baru	Nama: "Kopi", Stok: 10	Data tersimpan di tabel barang	**PASS**
BBT-03	**Kategori**	Menambah kategori produk	Kategori: "Minuman"	Kategori muncul di pilihan barang	**PASS**
BBT-04	**Transaksi**	Input barang ke keranjang	Scan/Pilih Barang	Barang masuk ke daftar belanja	**PASS**
BBT-05	**Pembayaran**	Memproses bayar & cetak nota	Klik "Bayar"	Stok berkurang & nota tercetak	**PASS**
BBT-06	**Laporan**	Filter laporan per bulan	Pilih Bulan: Januari	Tampil rekap penjualan Januari	**PASS**
BBT-07	**Security**	Akses dashboard tanpa login	Bypass URL	Diarahkan kembali ke login	**FAIL***
BBT-08	**Stok**	Restok barang yang habis	Tambah jumlah stok	Angka stok diperbarui	**PASS**

4.2 Laporan *Bug*

Berdasarkan dokumentasi resmi repositori dan analisis keamanan, berikut adalah beberapa temuan bug/kerentanan penting yang perlu diperhatikan (beberapa telah diperbaiki di versi terbaru, namun sering muncul di versi lama):

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 4, No. 12, Desember 2025
ISSN 2828-2442 (media online)
Hal 944-953

4.3 Laporan *Bug*

Tabel 2. Laporan *Bug*

Kode Bug	Deskripsi Temuan	Dampak	Rekomendasi
BUG-SEC-01	**CSRF (Cross-Site Request Forgery)**	Penyerang bisa mengubah data (hapus barang/user) tanpa izin pemilik akun.	Implementasikan CSRF Token pada setiap form POST.
BUG-SEC-02	**XSS (Cross-Site Scripting)**	Injeksi skrip berbahaya melalui input nama barang atau kategori.	Gunakan fungsi htmlspecialchars() atau sanitasi parameter.
BUG-SEC-03	**Broken Access Control**	Pengguna yang tidak sah dapat mengunduh berkas laporan ekspor.	Tambahkan validasi session pada file unduhan.
BUG-LOG-04	**Session Timeout**	Sesi pengguna tidak berakhir otomatis setelah idle lama.	Atur durasi session.gc_maxlifetime di server/aplikasi.
BUG-VAL-05	**File Upload Vulnerability**	Risiko eksekusi kode melalui unggahan file ilegal.	Batasi ekstensi file hanya untuk .jpg atau .png.

4.4 Hasil Pengujian Fungsional

Berdasarkan pengujian yang dilakukan terhadap aplikasi POS Kasir Codekop v2.0, fitur utama seperti manajemen barang, kategori, dan transaksi penjualan berjalan sesuai dengan logika bisnis yang diharapkan. Sistem berhasil mencatat data barang, melakukan pengurangan stok secara otomatis saat transaksi terjadi, dan menghasilkan laporan rekapitulasi penjualan per periode. Notifikasi stok juga berfungsi dengan baik dengan memberikan peringatan visual saat jumlah barang mencapai batas minimum.

4.5 Pembahasan *Bug* dan Keamanan

Meskipun fitur fungsional berjalan lancar, ditemukan beberapa celah keamanan kritis pada sisi autentikasi dan kontrol akses. Pengujian menunjukkan adanya kerentanan terhadap serangan *Cross-Site Request Forgery* (CSRF) dan *Cross-Site Scripting* (XSS) yang memungkinkan modifikasi data tanpa izin resmi. Selain itu, terdapat temuan *Broken Access Control* di mana beberapa modul laporan masih dapat diakses melalui URL langsung tanpa melalui proses login yang valid. Hal ini mengindikasikan perlunya penguatan pada skrip validasi sesi di setiap halaman utama sistem.

5. KESIMPULAN

Sistem POS Kasir Codekop v2.0 merupakan solusi manajemen inventaris dan penjualan yang efektif untuk operasional toko skala kecil karena fitur-fiturnya yang komprehensif, mulai dari input data hingga cetak nota. Namun, hasil pengujian menyimpulkan bahwa aplikasi ini masih memerlukan perbaikan signifikan pada aspek keamanan siber. Penggunaan di lingkungan produksi sangat disarankan untuk melakukan pembaharuan ke versi terbaru yang telah menambal celah CVE-2023-36345 hingga CVE-2023-36348 guna menjamin integritas data transaksi.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 4, No. 12, Desember 2025
ISSN 2828-2442 (media online)
Hal 944-953

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan dan kontribusi dalam proses penyusunan dan pengembangan sistem ini, khususnya kepada:

1. **Universitas Pamulang** atas dukungan fasilitas akademik dan lingkungan yang kondusif untuk penelitian.
2. **Bapak Chairul Anwar** selaku dosen pembimbing yang telah memberikan arahan strategis, bimbingan teknis, dan motivasi selama proses penelitian berlangsung.
3. Fauzan1892 selaku pengembang repositori sumber terbuka pos-kasir-php yang telah menyediakan basis kode untuk penelitian dan pembelajaran ini.

Para penyedia layanan dokumentasi keamanan yang telah memberikan referensi terkait kerentanan system sehingga pengujian black box ini dapat dilaukan secara mendalam.

REFERENCES

Aisyah, S., Anwar, C., Satmoko, N. D., & Nuryanto, U. W. (2023). Role of product quality and store atmosphere on purchase decision of clothing product Vintage Vibes. *JEMSI (Jurnal Ekonomi, Manajemen, dan Akuntansi*, *9*(1), 172–178.

Anwar, C. (2019). Perancangan sistem informasi Human Resources Development pada PT. Semacom Integrated. *International Journal of Education, Science, Technology, and Engineering (IJESTE)*, *2*(1), 19–38. https://doi.org/10.36079/lamintang.ijeste-0201.16

Anwar, C. (2022). *Application of academic information system with Extreme Programming method (Case study: Jakarta International Polytechnic)* [Laporan]. [Penerbit tidak disebutkan].

Anwar, C. (2024a). Prediction of academic achievement of Pamulang University students using artificial neural networks. [Jurnal tidak disebutkan].

Anwar, C. (2024b). Rekomendasi teknis untuk pengolahan data berbasis web. *Jurnal Informatika Utama*, *2*(1), 50–54. https://doi.org/10.55903/jitu.v2i1.166

Anwar, C., & Harits, A. (2025). Perancangan sistem kuisioner penilaian kapabilitas framework COBIT 2019. *Jurnal Informatika Utama*, *3*(1), 42–51.

Anwar, C., & Riyanto, J. (2019). Perancangan sistem informasi Human Resources Development pada PT. Semacom Integrated. *International Journal of Education, Science, Technology, and Engineering (IJESTE)*, *2*(1), 19–38. https://doi.org/10.36079/lamintang.ijeste-0201.16

Anwar, C., Handijono, A., & Harits, A. (2025a). Pemanfaatan penggunaan sosial media dengan bijak dalam teknologi informasi di era digital di SMK Media Informatika. *Attamkiim: Jurnal Pengabdian Masyarakat*, *2*(1), 58–64.

Anwar, C., Handijono, A., & Harits, A. (2025b). Pemanfaatan penggunaan sosial media dengan bijak dalam teknologi informasi di era digital di SMK Media Informatika. *Journal of Community Service Synergy*, *1*(1), 71–77.

Anwar, C., Jagat, L. S., Yanti, I., Anjarsari, E., & Sholihah, N. A. (2023). Pengembangan media pembelajaran berbasis teknologi untuk meningkatkan kemampuan anak. *Caruban: Jurnal Ilmiah Ilmu Pendidikan Dasar*, *6*(2), 154–163.

Anwar, C., Kom, S., Kom, M., Santiari, C. N. P. L., & Sitorus, Z. (2023). *Buku referensi sistem informasi berbasis kearifan lokal*. CV Pustaka Ilmiah.

Farizy, S., Trisnawan, A. B., Silalahi, L. M., Yuliadi, B., Anwar, C., Alamsyah, D., ... & Sitorus, B. B. (2025). *Buku ajar jaringan komputer: Dari teori dasar hingga jaringan nirkabel*. CV Rey Media Grafika.

Handayani, T., Silalahi, L. M., Nugroho, S. S. P., Anwar, C., Mursyidin, I. H., Sumantri, A., ... & Yulianti, B. (2025). *Pengantar sistem informasi: Konsep, teknologi, dan implementasi*. CV Pustaka Informatika.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 4, No. 12, Desember 2025
ISSN 2828-2442 (media online)
Hal 944-953

IEEE. (1990). *IEEE standard glossary of software engineering terminology (IEEE Std 610.12-1990)*. IEEE Computer Society.

Indra, S., Anwar, C., Kom, S., Asparizal, S., Kom, M., Nur, R. A., ... & Hafrida, L. (2025). *Komputer dan masyarakat*. CV Rey Media Grafika.

Black, R. (2020). *Black-Box Testing: Techniques for Functional Testing of Software and Systems*. Wiley.

Codekop. (2022). *Dokumentasi Fitur Inventaris dan Notifikasi Stok*. Official Documentation.

Fauzan1892. (2022). *Aplikasi POS Kasir Codekop v2.0 - PHP & MySQL*. GitHub Repository.

ISO/IEC/IEEE 29119-1:2022. *Software and systems engineering — Software testing*.

Mustaqbal, M. S., dkk. (2015). *Pengujian Aplikasi Menggunakan Black Box Testing Boundary Value Analysis*.

National Vulnerability Database (NVD). (2023). *Analysis of Vulnerabilities in POS-Kasir-PHP*. NIST.

OWASP Foundation. (2021). *OWASP Top 10:2021 The Next Generation of Application Security*.

Pressman, R. S. (2019). *Software Engineering: A Practitioner's Approach*. McGraw-Hill.

Sommerville, I. (2021). *Software Engineering (10th ed.)*. Pearson.