P-ISSN : 2580-4316
E-ISSN : 2654-8054
DOI: https://doi.org/10.37817/ikraith-informatika.v9i3

Penerapan Pentesting pada EasyCart untuk Menghadapi Ancaman Keamanan Siber

[1]Mochamad Fahrul Reza, [2]Imam sutanto, S.kom , M.kom
[1,2]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul, DKI Jakarta

E-mail: [1]fahrulreza693@student.esaunggul.ac.id, [2]imam.sutanto@esaunggul.ac.id

ABSTRAK

Perkembangan e-commerce di era digital telah meningkatkan risiko keamanan siber, menjadikan aplikasi e-commerce target utama serangan karena menyimpan data sensitif pengguna. Penelitian ini bertujuan melakukan evaluasi keamanan sistematis pada EasyCart, sebuah aplikasi e-commerce berbasis Angular, Node.js, Express, dan SQLite. Evaluasi dilakukan melalui metode penetration testing berdasarkan standar Penetration Testing Execution Standard (PTES) yang mencakup tujuh tahapan utama, dengan analisis kerentanan mengacu pada OWASP Top 10. Hasil pengujian menunjukkan bahwa EasyCart memiliki beberapa kerentanan kritis, seperti injeksi SQL, cross-site scripting (XSS), dan broken access control. Penelitian ini juga menyajikan hasil perbandingan keamanan sebelum dan sesudah mitigasi diterapkan untuk menilai efektivitas perbaikan. Pendekatan ini terbukti efektif dalam mengidentifikasi kerentanan dan diharapkan dapat berkontribusi pada pengembangan sistem e-commerce yang lebih aman dan andal.

Kata kunci : ***keamanan siber, penetration testing, e-commerce, OWASP Top 10, PTES.***

ABSTRACT

The development of e-commerce in the digital era has increased cybersecurity risks, making e-commerce applications a prime target for attacks because they store sensitive user data. This study aims to conduct a systematic security evaluation of EasyCart, an e-commerce application based on Angular, Node.js, Express, and SQLite. The evaluation was conducted using the penetration testing method based on the Penetration Testing Execution Standard (PTES), which covers seven main stages, with vulnerability analysis referring to the OWASP Top 10. The test results showed that EasyCart had several critical vulnerabilities, such as SQL injection, cross-site scripting (XSS), and broken access control. This study also presents the results of a security comparison before and after mitigation was applied to assess the effectiveness of the improvements. This approach has proven effective in identifying vulnerabilities and is expected to contribute to the development of a more secure and reliable e-commerce system.

Keyword : ***Cybersecurity, penetration testing, e-commerce, OWASP Top 10, PTES.***

DOI: https://doi.org/10.37817/ikraith-informatika.v9i3
P-ISSN : 2580-4316
E-ISSN : 2654-8054

1. PENDAHULUAN

Perkembangan pesat teknologi informasi telah menjadikan e-commerce sebagai pilar utama ekonomi digital, memfasilitasi transaksi tanpa batas geografis. Di Indonesia, jumlah pengguna internet pada tahun 2024 mencapai 221,5 juta jiwa, dengan tingkat penetrasi 79,5%. Pertumbuhan ini mendorong adopsi e-commerce secara masif, namun diiringi dengan peningkatan ancaman keamanan siber yang signifikan. Platform e-commerce menjadi target utama serangan karena mengelola data sensitif pengguna dalam volume besar (Asosiasi Penyelenggara Jasa Internet Indonesia, 2024).

Ancaman ini bukanlah risiko teoretis, melainkan telah terbukti memberikan dampak kerugian masif di Indonesia. Sebagai contoh, pada tahun 2020, Tokopedia mengalami insiden kebocoran data yang berdampak pada lebih dari 91 juta akun penggunanya. Kasus serupa juga pernah dihadapi oleh Bukalapak, di mana jutaan data pengguna mereka bocor dan diperjualbelikan. Insiden-insiden ini menunjukkan bahwa kegagalan dalam mengidentifikasi dan memitigasi kerentanan secara proaktif dapat berakibat fatal (Indonesia, 2020).

Meskipun platform besar menjadi sorotan, aplikasi e-commerce skala kecil hingga menengah, serta aplikasi prototipe yang dikembangkan untuk tujuan akademis, seringkali dibangun tanpa audit keamanan yang memadai. Permasalahan utama inilah yang melatarbelakangi penelitian ini, yaitu belum adanya evaluasi keamanan sistematis pada aplikasi prototipe EasyCart. Oleh karena itu, penelitian ini bertujuan untuk menerapkan metode.

penetration testing berbasis Penetration Testing Execution Standard (PTES) dengan acuan kerentanan OWASP Top 10 guna mengidentifikasi celah keamanan, menganalisis risikonya, dan memberikan rekomendasi perbaikan yang konkret.

2. LANDASAN TEORI

2.1 Keamanan Informasi

Keamanan siber merupakan serangkaian praktik dan teknologi yang dirancang untuk melindungi sistem komputer, jaringan, dan data dari serangan, kerusakan, atau akses tidak sah. Dalam konteks e-commerce, keamanan siber menjadi krusial karena platform ini mengelola data sensitif dalam volume besar, seperti informasi pribadi pelanggan dan detail transaksi finansial, yang menjadikannya target utama bagi pelaku kejahatan siber (Silalahi, 2022).$

2.2*Penetration Testing*

Penetration testing, atau uji penetrasi, adalah sebuah metode evaluasi keamanan siber di mana seorang penguji mensimulasikan serangan secara etis terhadap sebuah sistem untuk menemukan dan mengeksploitasi kerentanan keamanan. Tujuannya adalah untuk mengidentifikasi celah keamanan dari sudut pandang penyerang sebelum celah tersebut ditemukan oleh pihak yang tidak bertanggung jawab. Penelitian ini secara spesifik menggunakan pendekatan

black-box testing, di mana pengujian dilakukan tanpa pengetahuan atau akses terhadap kode sumber internal aplikasi, meniru skenario serangan dari peretas eksternal (Patty et al., 2024).

2.3Kerangka Kerja Pengujian: PTES dan OWASP Top 10

Untuk memastikan proses pengujian berjalan sistematis dan relevan, penelitian ini mengombinasikan dua standar industri utama:

1. Penetration Testing Execution Standard (PTES): Standar ini berfungsi sebagai kerangka kerja yang memandu seluruh alur pengujian secara metodologis(PTES, 2014).

P-ISSN : 2580-4316
E-ISSN : 2654-8054
DOI: https://doi.org/10.37817/ikraith-informatika.v9i3

PTES mendefinisikan tujuh tahapan utama yang harus dilalui, yaitu :

- Pre-engagement,
- Intelligence Gathering,
- Threat Modeling,
- Vulnerability Analysis,
- Exploitation,
- Post-Exploitation, dan
- Reporting.

2. Open Web Application Security Project (OWASP) Top 10

OWASP Top 10 adalah sebuah dokumen standar yang berisi daftar peringkat sepuluh risiko keamanan aplikasi web yang paling kritis dan umum terjadi. Daftar ini diperbarui secara berkala berdasarkan data dari para ahli keamanan global dan berfungsi sebagai acuan (checklist) dalam penelitian ini untuk mengidentifikasi dan mengklasifikasikan jenis kerentanan yang ditemukan.

Dalam penelitian ini, PTES digunakan sebagai panduan proses dari awal hingga akhir, sementara OWASP Top 10 digunakan sebagai acuan konten pada tahap Vulnerability Analysis dan Exploitation. Kombinasi keduanya memastikan bahwa pengujian keamanan yang dilakukan tidak hanya terstruktur, tetapi juga fokus pada ancaman-ancaman yang paling relevan di dunia nyata saat ini.

3. METODOLOGI

Penelitian ini menerapkan metode penetration testing dengan pendekatan black-box. Dalam pendekatan ini, penguji memposisikan diri sebagai penyerang eksternal yang tidak memiliki pengetahuan atau akses terhadap kode sumber maupun arsitektur internal sistem. Desain penelitian dirancang dalam dua siklus utama: uji coba pertama untuk identifikasi kerentanan awal (baseline test), dan uji coba kedua pasca-penerapan mitigasi untuk memvalidasi efektivitas perbaikan yang direkomendasikan

3.1Planning (Perencanaan)

Objek yang diuji adalah EasyCart, sebuah aplikasi prototipe e-commerce fungsional yang dibangun sebagai model penelitian. Aplikasi ini dikembangkan dengan tumpukan teknologi modern yang umum digunakan, meliputi :

- Frontend: Angular
- Backend: Node.js dengan framework Express.js
- Database: SQLite
- Autentikasi: Menggunakan mekanisme JSON Web Token (JWT) untuk manajemen sesi dan kontrol akses

3.2 Kerangka Kerja dan Standar Pengujian

Proses pengujian secara sistematis mengadopsi dua standar industri utama:

1. Penetration Testing Execution Standard (PTES)
   kerangka kerja ini digunakan sebagai panduan alur metodologi yang terdiri dari tujuh tahapan, yaitu Pre-engagement, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, dan Reporting.

2. Open Web Application Security Project (OWASP) Top 10 2021
   Standar ini digunakan sebagai acuan untuk mengidentifikasi, mengklasifikasikan, dan menguji jenis-jenis kerentanan keamanan yang paling kritis dan umum terjadi pada aplikasi web..

3.2Prosedur Penelitian

Penelitian dilaksanakan melalui langkah-langkah sistematis sebagai berikut:

1. Tahap Intellegence Gathering
   Mengumpulkan informasi awal mengenai target easycart.id menggunakan alat bantu seperti Nmap untuk memindai port dan layanan yang berjalan, serta Wappalyzer untuk mengidentifikasi teknologi yang digunakan.

DOI: https://doi.org/10.37817/ikraith-informatika.v9i3
P-ISSN : 2580-4316
E-ISSN : 2654-8054

2. Tahap Vulnerability Analysis
   Melakukan pemindaian kerentanan secara otomatis menggunakan OWASP ZAP untuk mendapatkan gambaran awal celah keamanan. Analisis mendalam dilanjutkan secara manual menggunakan Burp Suite untuk mencegat dan memanipulasi request HTTP.

3. Tahap Exploitation
   Melakukan eksploitasi terhadap kerentanan yang teridentifikasi untuk memvalidasi dampaknya. Serangan spesifik seperti SQL Injection diuji menggunakan SQLMap , sementara serangan brute force diuji menggunakan Burp Suite Intruder. Semua temuan didokumentasikan dengan bukti berupa screenshot.

4. Tahap Reporting dan Mitigasi
   Seluruh temuan kerentanan beserta tingkat risikonya disusun dalam laporan. Berdasarkan laporan ini, dirancang rekomendasi mitigasi teknis untuk setiap celah keamanan.

5. Tahap Validasi (Uji Coba Kedua)
   Setelah rekomendasi mitigasi disimulasikan, pengujian ulang dilakukan dengan skenario dan payload serangan yang sama untuk memverifikasi apakah kerentanan berhasil ditutup dan keamanan sistem telah meningkat.

4. HASIL DAN PEMBAHASAN

4.1Ringkasan Temuan Awal

Hasil pengujian tahap pertama berhasil mengidentifikasi total 12 temuan kerentanan pada aplikasi EasyCart. Berdasarkan analisis risiko, temuan tersebut diklasifikasikan menjadi 5 kerentanan berisiko tinggi (high), 5 berisiko sedang (medium), dan 2 berisiko rendah (low). Kerentanan dengan dampak paling signifikan terkonsentrasi pada kategori *Broken Access Control*, *Injection*, dan *Identification & Authentication Failures*, yang berpotensi menyebabkan pengambilalihan akun hingga manipulasi data.

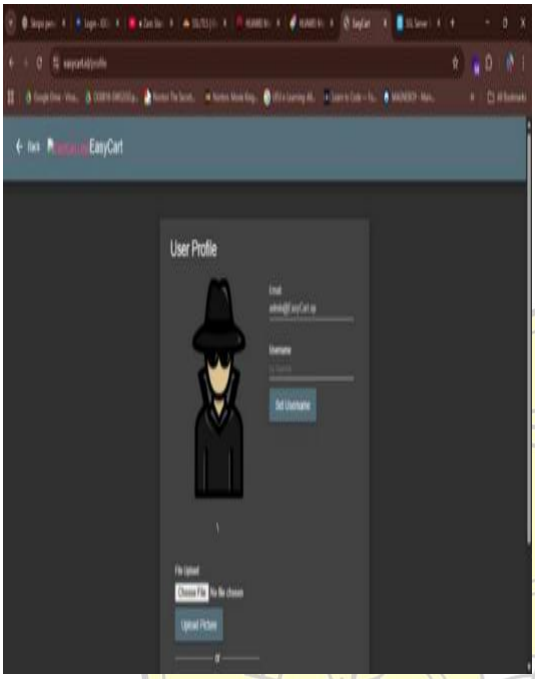
4.2 Analisis Kerentanan

Tabel 1.1 Analisis Temuan Kerentanan

Kategori OWASP Top 10	Deskripsi Kerentanan	Level Risiko
A01: Broken Access Control	Registrasi akun admin tanpa otorisasi.	Tinggi
A03: Injection	SQL Injection pada form login (Login Bypass).	Tinggi
A04: Insecure Design	Penggantian password tanpa verifikasi password lama.	Tinggi
A07: Identification & Authentication Failures	Tidak ada proteksi rate limiting (rentan Brute Force).	Tinggi
A05: Security Misconfiguration	Access log dapat diakses publik.	Sedang
A08: Software and Data Integrity Failures	Pemuatan script eksternal tanpa validasi integritas.	Sedang

P-ISSN : 2580-4316
E-ISSN : 2654-8054
DOI: https://doi.org/10.37817/ikraith-informatika.v9i3

- Bukti Eksploitasi Kerentanan SQL Injection pada Halaman Login



Gambar 4.1 *User Profil*

Serangan dilakukan pada form login aplikasi dengan menyuntikkan payload OR '1'='1'-- pada kolom input. Gambar ini menunjukkan hasil akhir eksploitasi, di mana payload tersebut berhasil melewati mekanisme autentikasi sistem dan memberikan akses tidak sah. Penyerang berhasil masuk dan melihat halaman profil pengguna dengan hak akses tertinggi (administrator), memvalidasi temuan kerentanan A03:Injection dengan level risiko Tinggi.

- Broken access control

Menunjukkan keberhasilan registrasi akun baru dengan hak akses admin. Ini juga sangat kritis.

- Stored XSS

Gambar 4.2 Request

Menunjukkan eksekusi script berbahaya (pop-up alert) di halaman yang seharusnya terlindungi. Ini adalah contoh klasik serangan pada aplikasi web.

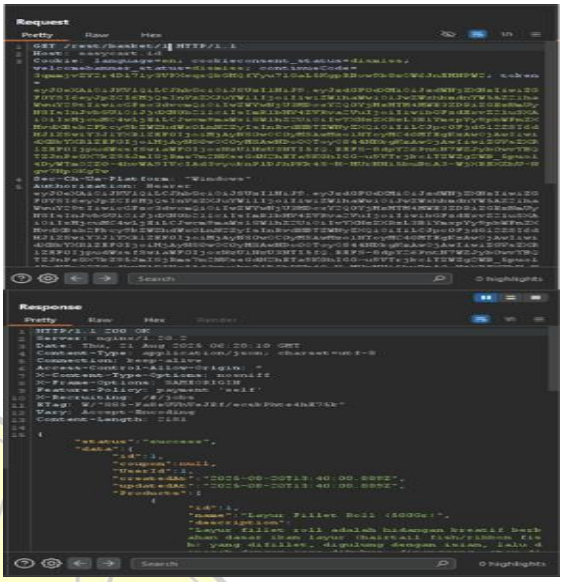
DOI: https://doi.org/10.37817/ikraith-informatika.v9i3
P-ISSN : 2580-4316
E-ISSN : 2654-8054

- IDOR

Gambar 4.3 Administrasion

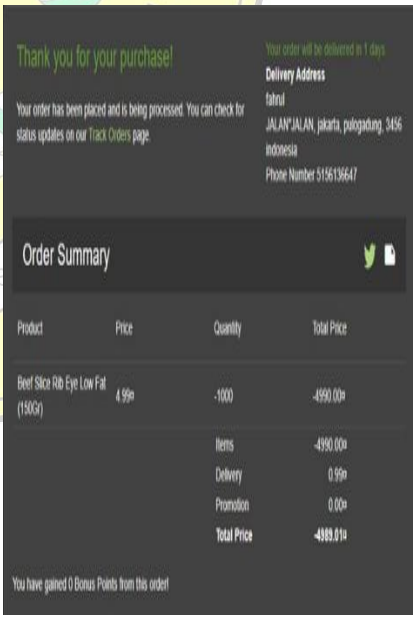
Menunjukkan kebocoran data pesanan pelanggan lain melalui manipulasi ID. Ini menyoroti risiko privasi.

- NoSQL Injection



Gambar 4.4 Sql Injection

Menunjukkan manipulasi logika bisnis (kuantitas dan harga produk). Ini sangat menarik karena dampaknya langsung ke transaksi.



Gambar 4.5 Track Order

P-ISSN : 2580-4316
E-ISSN : 2654-8054
DOI: https://doi.org/10.37817/ikraith-informatika.v9i3

4.3 Validasi Mitigasi

Setelah temuan awal diidentifikasi, serangkaian rekomendasi mitigasi—seperti penerapan parameterized query, penguatan validasi input, dan perbaikan konfigurasi server—disimulasikan dan sistem diuji ulang untuk memvalidasi efektivitasnya. Hasil pengujian kedua menunjukkan keberhasilan signifikan dalam menutup celah keamanan paling kritis.

Serangan SQL Injection pada form login berhasil diblokir sepenuhnya, di mana payload berbahaya tidak lagi dieksekusi oleh sistem. Serangan NoSQL Injection untuk memanipulasi data produk juga berhasil digagalkan setelah validasi input diterapkan. Selain itu, perbaikan pada konfigurasi server berhasil menyembunyikan access log yang sebelumnya terekspos dan menerapkan header keamanan yang direkomendasikan.

Meskipun demikian, pengujian validasi juga menemukan bahwa beberapa kerentanan masih tetap ada. Serangan Cross-Site Scripting (XSS) , serta beberapa celah pada Broken Authentication dan Broken Access Control masih dapat dieksploitasi. Temuan ini mengindikasikan bahwa meskipun perbaikan pada level kode sangat efektif untuk ancaman spesifik, beberapa kerentanan memerlukan perbaikan logika aplikasi yang lebih mendalam atau penerapan lapisan pertahanan tambahan.

4.4 Pembahasan

Berdasarkan penelitian yang dilakukan pada aplikasi EasyCart menggunakan metode Penetration Testing Execution Standard (PTES) dengan acuan OWASP Top 10 (2021), diperoleh beberapa kesimpulan sebagai berikut:

1. Pengujian Keamanan Aplikasi

Penelitian ini berhasil melakukan pengujian keamanan terhadap aplikasi EasyCart, sehingga memberikan gambaran menyeluruh mengenai tingkat kerentanannya. Dengan demikian, masalah pertama mengenai belum adanya pengujian keamanan dapat terjawab.

2. Jenis Kerentanan yang Ditemukan

Hasil uji menunjukkan terdapat 12 temuan kerentanan dalam aplikasi, dengan rincian 5 risiko tinggi, 5 risiko sedang, dan 2 risiko rendah. Kerentanan yang teridentifikasi meliputi SQL Injection, NoSQL Injection, Cross-Site Scripting (XSS), Broken Authentication, Broken Access Control, Insecure Design, Security Misconfiguration, Cryptographic Failures, Security Logging & Monitoring Failures, Software and Data Integrity Failures, serta Information Disclosure. Dengan demikian, masalah kedua terkait jenis kerentanan dapat teridentifikasi secara jelas, memberikan wawasan yang penting untuk langkah mitigasi dan perbaikan selanjutnya. Pengetahuan ini krusial untuk meningkatkan keamanan aplikasi dan melindungi data pengguna dari potensi ancaman.

3. Mitigasi yang Diterapkan

Rekomendasi mitigasi yang diberikan mencakup beberapa langkah penting, antara lain perbaikan kode aplikasi melalui validasi input, penggunaan parameterized query, dan output encoding untuk mencegah serangan injeksi. Selain itu, penguatan autentikasi diperlukan untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem. Konfigurasi server juga harus ditingkatkan dengan menambahkan security headers dan proteksi log guna memperkuat pertahanan. Penambahan Web Application Firewall (WAF) menjadi langkah tambahan yang efektif dalam melindungi aplikasi dari berbagai ancaman. Rekomendasi ini terbukti relevan dan sesuai dengan temuan kerentanan yang ada, sehingga secara efektif menjawab masalah ketiga dalam penelitian ini. Implementasi langkah-langkah mitigasi ini diharapkan dapat mengurangi risiko dan meningkatkan keamanan aplikasi secara keseluruhan.

DOI: https://doi.org/10.37817/ikraith-informatika.v9i3
P-ISSN : 2580-4316
E-ISSN : 2654-8054

4. Efektivitas Mitigasi

Setelah mitigasi diterapkan, dilakukan pengujian kedua yang menunjukkan bahwa kerentanan kritis berhasil ditutup. Risiko keseluruhan berkurang dari kategori tinggi-kritis menjadi rendah-sedang, meskipun masih terdapat kelemahan minor berupa information disclosure. Temuan ini membuktikan bahwa langkah mitigasi yang dilakukan efektif dalam meningkatkan keamanan aplikasi EasyCart, sehingga menjawab masalah keempat yang diidentifikasi dalam penelitian ini.

Secara keseluruhan, penelitian ini menyimpulkan bahwa penerapan metode penetration testing berbasis Penetration Testing Execution Standard (PTES) dengan acuan OWASP Top 10 sangat efektif dalam mengidentifikasi, mengevaluasi, dan meminimalisasi risiko keamanan pada aplikasi e-commerce. Metode ini tidak hanya membantu dalam menemukan kerentanan yang ada, tetapi juga memberikan panduan yang jelas untuk mitigasi yang tepat.

Hasil penelitian ini diharapkan dapat menjadi referensi berharga bagi pengembang dan profesional keamanan siber dalam membangun aplikasi yang lebih aman dan andal di masa depan. Selain itu, penelitian ini juga menekankan pentingnya melakukan pengujian keamanan secara berkala dan menerapkan praktik terbaik dalam pengembangan perangkat lunak. Dengan demikian, organisasi dapat lebih siap menghadapi ancaman siber yang terus berkembang dan melindungi data serta privasi pengguna dengan lebih baik. Melalui pendekatan proaktif ini, keamanan aplikasi dapat ditingkatkan, sehingga menciptakan ekosistem digital yang lebih aman.

4.4 Saran

Berdasarkan hasil penelitian yang telah dilakukan pada aplikasi e-commerce EasyCart, penulis menyadari bahwa masih terdapat keterbatasan dan ruang untuk pengembangan lebih lanjut. Oleh karena itu, beberapa saran yang dapat diberikan baik untuk pengembang aplikasi, peneliti selanjutnya, maupun praktisi keamanan informasi adalah sebagai berikut:

1. Pengujian Keamanan Rutin:
Pentesting, atau pengujian penetrasi, perlu dilakukan secara berkala, bukan hanya sekali pada tahap pengembangan, karena setiap pembaruan sistem dapat memperkenalkan kerentanan baru yang dapat dieksploitasi oleh penyerang. Lanskap ancaman dunia maya terus berkembang, sehingga pengujian rutin membantu organisasi untuk tetap satu langkah di depan, menyesuaikan strategi pertahanan, dan memastikan kepatuhan terhadap regulasi keamanan. Selain itu, pentesting berkala meningkatkan kesadaran keamanan di dalam tim, mengoptimalkan pengeluaran untuk perbaikan, dan mempersiapkan organisasi untuk merespons insiden dengan lebih efektif. Dengan demikian, pentesting merupakan komponen penting dalam menjaga integritas dan kepercayaan terhadap sistem informasi.

2. Penerapan Kontrol Keamanan Tambahan:
EasyCart menekankan pentingnya penggunaan Web Application Firewall (WAF), Intrusion Detection System (IDS), dan rate limiting sebagai langkah strategis untuk memperkuat lapisan keamanan aplikasi. WAF berfungsi untuk memfilter dan memantau lalu lintas HTTP, melindungi aplikasi dari serangan umum seperti SQL injection dan cross-site scripting. Sementara itu, IDS membantu mendeteksi aktivitas mencurigakan dan potensi ancaman dalam jaringan, memberikan peringatan dini untuk mencegah pelanggaran keamanan. Rate limiting, di sisi lain, mengatur jumlah permintaan yang dapat dilakukan pengguna dalam jangka waktu tertentu, mencegah serangan DDoS dan memastikan ketersediaan layanan.

P-ISSN : 2580-4316
E-ISSN : 2654-8054
DOI: https://doi.org/10.37817/ikraith-informatika.v9i3

Dengan menggabungkan ketiga solusi ini, EasyCart dapat menciptakan pertahanan yang lebih komprehensif dan efektif terhadap berbagai ancaman siber.

3. Pengembangan EasyCart:
EasyCart sebagai media penelitian memiliki potensi besar untuk dikembangkan lebih lanjut. Penambahan modul transaksi pembayaran nyata dapat memberikan pengalaman yang lebih realistis, memungkinkan pengguna untuk memahami proses pembayaran dan keamanan yang terkait. Integrasi API pihak ketiga, seperti layanan pengiriman dan sistem manajemen inventaris, akan menambah kompleksitas dan fungsionalitas aplikasi, menciptakan ekosistem yang lebih lengkap. Selain itu, pengembangan fitur keranjang belanja yang lebih kompleks, seperti rekomendasi produk berbasis kecerdasan buatan dan opsi penyimpanan barang, dapat meningkatkan pengalaman pengguna. Dengan pengembangan ini, EasyCart dapat berfungsi sebagai studi kasus yang lebih representatif terhadap aplikasi e-commerce modern, memberikan wawasan yang lebih mendalam bagi peneliti dan pengembang dalam memahami tantangan dan solusi dalam industri e-commerce saat ini.

4. Pengembangan aplikasi disarankan
Mengintegrasikan keamanan sejak tahap perancangan, atau yang dikenal sebagai Security by Design, adalah pendekatan yang sangat penting dalam pengembangan aplikasi. Dengan menerapkan prinsip-prinsip keamanan dari awal, potensi kerentanan dapat diidentifikasi dan diatasi sebelum aplikasi memasuki tahap implementasi dan produksi. Ini mencakup analisis risiko, penerapan kontrol keamanan, dan penggunaan praktik pengkodean yang aman. Dengan cara ini, organisasi tidak hanya mengurangi risiko pelanggaran data, tetapi juga menghemat waktu dan biaya yang mungkin timbul akibat perbaikan keamanan yang dilakukan setelah aplikasi diluncurkan. Pendekatan ini memastikan bahwa keamanan menjadi bagian integral dari siklus hidup pengembanga

5. KESIMPULAN

Penelitian ini berhasil melakukan pengujian keamanan terhadap aplikasi EasyCart, memberikan gambaran menyeluruh mengenai tingkat kerentanannya dan menjawab masalah pertama terkait minimnya pengujian sebelumnya. Hasil uji menunjukkan adanya 12 temuan kerentanan, yang terdiri dari 5 risiko tinggi, 5 risiko sedang, dan 2 risiko rendah. Jenis-jenis kerentanan yang ditemukan meliputi SQL Injection, NoSQL Injection, Cross-Site Scripting (XSS), Broken Authentication, Broken Access Control, Insecure Design, Security Misconfiguration, Cryptographic Failures, Security Logging & Monitoring Failures, Software and Data Integrity Failures, serta Information Disclosure. Temuan ini secara jelas menjawab masalah kedua mengenai jenis kerentanan yang ada.

Rekomendasi mitigasi yang diberikan mencakup perbaikan kode aplikasi melalui validasi input, penggunaan parameterized query, dan output encoding, serta penguatan autentikasi dan konfigurasi server dengan menambahkan security headers dan proteksi log. Selain itu, penambahan Web Application Firewall (WAF) juga direkomendasikan. Rekomendasi ini terbukti relevan dan sesuai dengan temuan kerentanan, sehingga berhasil menjawab masalah ketiga.

Setelah penerapan mitigasi, dilakukan pengujian kedua yang menunjukkan bahwa kerentanan kritis berhasil ditutup. Risiko keseluruhan berkurang dari kategori tinggi-kritis menjadi rendah-sedang, meskipun masih terdapat kelemahan minor berupa information disclosure. Hal ini menunjukkan bahwa meskipun langkah mitigasi telah diambil, tetap diperlukan pemantauan dan perbaikan berkelanjutan untuk memastikan keamanan aplikasi secara menyeluruh. Penelitian ini menekankan pentingnya pengujian keamanan yang berkelanjutan dan

penerapan best practices dalam pengembangan aplikasi untuk meminimalisir risiko dan meningkatkan ketahanan terhadap ancaman siber.

DAFTAR PUSTAKA

Asosiasi Penyelenggara Jasa Internet Indonesia. (2024). *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Indonesia, C. (2020). *Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual*. Indonesia, CNN. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

Patty, J. S., Education, N. S., & Indonesia, U. P. (2024). *PENETRATION TESTING OF A COMPUTERIZED PSYCHOLOGICAL ASSESSMENT WEBSITE USING SEVEN ATTACK VECTORS FOR CORPORATION WEBSITE SECURITY*. *5*(3), 831–842.

PTES. (2014). *High Level Organization of the Standard*. PTES, Penetration Testing Execution Standard. http://www.pentest-standard.org/index.php/Main_Page

Silalahi, F. D. (2022). Keamanan Cyber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1–285. http://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/367