Informatics for Educators And Professionals : Journal of Informatics
Vol. 10, No. 1, Juni 2025, 25 - 33
E-ISSN: 2548-3412
Terakreditasi **SINTA Peringkat 5**
Surat Keputusan Direktur Jenderal Pendidikan Tinggi, Riset, dan Teknologi, Nomor: 230/E/KPT/2022
masa berlaku mulai Volume 5 Nomor 1 Tahun 2020 sampai Volume 9 Nomor 2 Tahun 2024

Analisis Keamanan Aplikasi Berbasis Web Menggunakan Metode Penetration Testing (Studi kasus: E-Commerce As-Sakinah Mart)

Muhammad Yuwan Safri Nacikit[1], Miftahur Rahman[2*], Ari Eko Wardoyo[3]

[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jember
e-mail:[1]yuwansfr.braincore@gmail.com, [2]miftahurrahman@unmuhjember.ac.id,
[3]arieko@unmuhjember.ac.id

*Korespondensi e-mail: miftahurrahman@unmuhjember.ac.id

Diterima: 7 Maret 2025; Review: 10 Maret 2025; Disetujui: 22 April 2025

Cara sitasi: Nacikit MYS, Rahman M, Wardoyo AE. 2025. Analisis Keamanan Aplikasi Berbasis Web Menggunakan Metode Penetration Testing (Studi kasus: E-Commerce As-Sakinah Mart). Informatics for Educators and Professionals : Journal of Informatics. Vol.10 (1): 25-33.

Abstrak: Keamanan aplikasi berbasis *web* merupakan aspek krusial dalam memastikan integritas dan kerahasiaan data, terutama pada platform *e-commerce* yang rentan terhadap serangan siber. Penelitian ini bertujuan untuk menganalisis tingkat keamanan aplikasi web *E-Commerce* As-Sakinah Mart menggunakan metode penetration testing. Metode ini melibatkan simulasi serangan yang mungkin dilakukan oleh pihak tidak bertanggung jawab untuk mengidentifikasi kerentanan dalam sistem. Studi ini meliputi pengujian terhadap berbagai aspek, termasuk autentikasi pengguna, manajemen sesi, enkripsi data, serta perlindungan terhadap serangan *SQL Injection* dan *Cross-Site Scripting* (XSS). Hasil penelitian ini menunjukkan bahwa Assakinahmart.com telah memenuhi standar keamanan yang tinggi dan aman dari ancaman yang termasuk dalam OWASP Top 10-2021. ditemukan adanya kerentanan pada logika bisnis (*business logic vulnerability*) yang memungkinkan penyerang memanipulasi harga barang di dalam keranjang belanja sesuai keinginannya. Kerentanan ini dapat dimanfaatkan untuk mendapatkan produk dengan harga yang jauh lebih murah atau bahkan gratis, sehingga berpotensi merugikan pihak penyedia layanan. Sebagai rekomendasi, pengembang disarankan untuk menerapkan validasi harga di sisi server, melakukan verifikasi silang terhadap data transaksi sebelum diproses, serta menerapkan logika bisnis yang konsisten dan tidak dapat dimanipulasi melalui sisi klien. Selain itu, penting juga untuk melakukan audit keamanan secara berkala guna memastikan bahwa celah serupa tidak muncul kembali di masa mendatang. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi nyata dalam meningkatkan kesadaran serta tindakan preventif terhadap potensi ancaman keamanan pada aplikasi web, khususnya yang berkaitan dengan kelemahan pada logika bisnis.

Kata kunci: Keamanan *Web*, Penetration Testing, *E-commerce*, Kerentanan Aplikasi, As-Sakinah Mart.

Abstract: *Web application security is a crucial aspect in ensuring data integrity and confidentiality, especially on e-commerce platforms that are vulnerable to cyberattacks. This study aims to analyze the security level of the E-Commerce As-Sakinah Mart web application using penetration testing methods. This method involves simulating attacks that could be carried out by malicious actors to identify vulnerabilities within the system. The study includes testing various aspects such as user authentication, session management, data encryption, as well as protection against SQL Injection and Cross-Site Scripting (XSS) attacks. The results of this research show that Assakinahmart.com complies with high security standards and is protected*

from threats listed in the OWASP Top 10-2021. However, a business logic vulnerability was discovered that allows attackers to manipulate product prices in the shopping cart according to their preference. This vulnerability can be exploited to obtain products at significantly lower prices or even for free, potentially causing financial losses to the service provider. As a recommendation, developers are advised to implement server-side price validation, perform cross-verification of transaction data before processing, and ensure consistent business logic that cannot be manipulated from the client side. In addition, it is also important to conduct regular security audits to ensure that similar vulnerabilities do not reappear in the future. Thus, this study is expected to make a real contribution to raising awareness and promoting preventive actions against potential security threats on web applications, particularly those related to business logic flaws.

***Keywords**: Web Security, Penetration Testing, E-commerce, Application Vulnerabilities, As-Sakinah Mart.*

1. Pendahuluan

Era digitalisasi yang kita alami saat ini menghadirkan perubahan transformasional yang mencakup segala aspek kehidupan, terutama di dunia bisnis. Inovasi teknologi tidak hanya menjadi pendorong perkembangan, tetapi juga menjadi hal utama yang mampu mempercepat setiap proses, meningkatkan efisiensi operasional, dan memperbesar peluang baru yang belum pernah terjadi sebelumnya. Dalam paradigma bisnis modern, kehadiran teknologi menjadi kunci utama untuk menjawab tuntutan zaman [1]. Perkembangan teknologi saat ini tidak luput dari peran internet [2]. Internet adalah komunikasi jaringan global yang menghubungkan seluruh komputer di dunia meskipun berbeda sistem operasi dan mesin [3][4]. Internet merupakan suatu sarana sebagai sumber dari segala informasi online yang dapat diakses secara global [5]. Digital marketing adalah strategi pemasaran yang memanfaatkan kemajuan teknologi digital (internet) untuk memasarkan produk dan jasa secara online [6][7]. Salah satu teknik populernya adalah e-commerce, model penjualan produk dan jasa secara online melalui website perusahaan, email, atau media social [8].

Di era transformasi digital yang pesat, aplikasi berbasis website telah menjadi tulang punggung berbagai aktivitas, mulai dari bisnis, pemerintahan, hingga layanan publik. Namun, pertumbuhan aplikasi berbasis website juga diiringi dengan peningkatan risiko keamanan. Serangan siber seperti injeksi SQL, cross-site scripting (XSS), dan serangan brute force menjadi ancaman serius yang dapat mengakibatkan kerugian finansial, kebocoran data sensitif, dan kerusakan reputasi. Salah satu metode yang efektif untuk mengidentifikasi dan mengevaluasi celah keamanan dalam aplikasi berbasis website adalah penetration testing (pentest). Penetration testing melibatkan simulasi serangan dunia nyata oleh profesional keamanan yang terlatih untuk mengungkap kerentanan yang mungkin terlewatkan dalam proses pengembangan atau pengujian biasa. Dengan mengidentifikasi kerentanan yang ada dan memberikan rekomendasi perbaikan, penelitian ini diharapkan dapat berkontribusi dalam meningkatkan keamanan aplikasi berbasis website, melindungi data pengguna, dan menjaga kepercayaan terhadap layanan digital.

Pada penelitian [9] berjudul "Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux," hasil pengujian penetrasi pada website Pemerintah Kabupaten Kediri menemukan beberapa port terbuka yang memiliki akses 200. Setelah dilakukan serangan untuk masuk ke dalam direktori environment, ditemukan adanya Exposure of Sensitive Information (DBCredentials) yang dapat diekspos kepada pihak yang tidak berwenang. Hal ini memungkinkan terungkapnya informasi sensitif berupa username dan password yang dapat digunakan untuk mengakses halaman control panel (cp panel) admin. Temuan ini menegaskan pentingnya penerapan pengujian penetrasi secara rutin untuk mengidentifikasi potensi celah keamanan yang dapat dimanfaatkan oleh pihak yang berniat jahat. Oleh karena itu, penelitian ini berkontribusi dalam upaya meningkatkan ketahanan keamanan aplikasi berbasis website, baik di sektor pemerintahan maupun sektor lainnya, guna melindungi data pengguna dan menjaga integritas sistem.

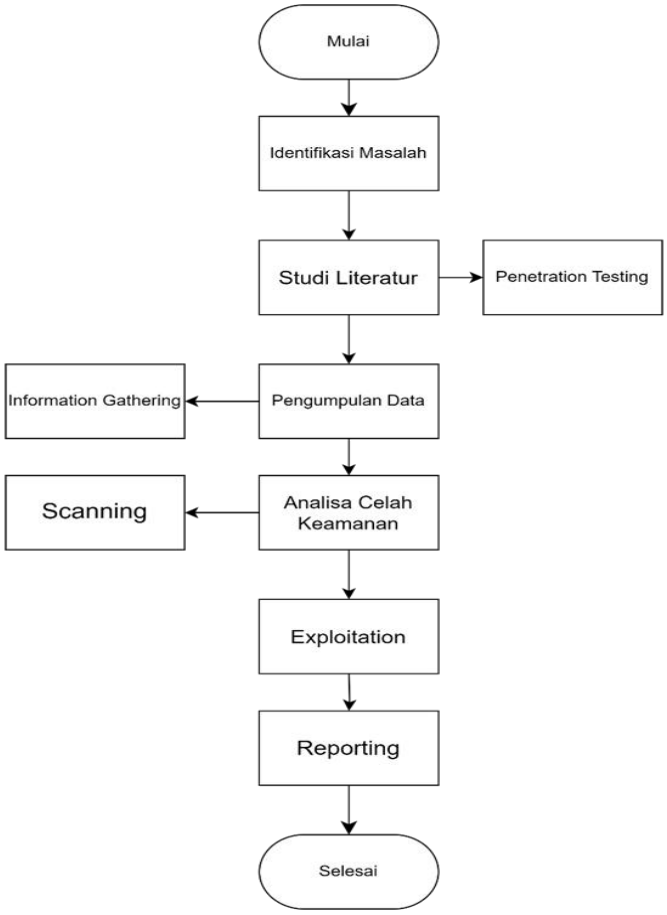
Keamanan aplikasi web, khususnya pada platform e-commerce, merupakan aspek yang sangat vital mengingat tingginya risiko serangan siber yang dapat mengakibatkan kerugian besar, baik secara finansial maupun reputasi. Serangan terhadap aplikasi e-commerce

seperti manipulasi transaksi, pencurian data pelanggan, dan eksploitasi celah logika bisnis (*business logic flaws*) telah menjadi ancaman nyata yang terus berkembang. Menurut laporan dari [OWASP, 2021], salah satu celah paling berbahaya dalam aplikasi web adalah kerentanan yang berkaitan dengan logika bisnis dan otorisasi yang lemah, yang sering kali tidak terdeteksi oleh pengujian konvensional.

Tujuan dari penelitian ini adalah untuk menganalisis dan mengidentifikasi kerentanan keamanan pada aplikasi web e-commerce As-Sakinah Mart menggunakan metode *penetration testing*, serta memberikan rekomendasi perbaikan berdasarkan temuan yang diperoleh. Penelitian ini diharapkan dapat berkontribusi dalam meningkatkan pemahaman dan kesadaran akan pentingnya pengujian keamanan secara rutin, serta memberikan masukan bagi pengembang dalam membangun aplikasi e-commerce yang lebih aman.

2. Metode Penelitian

Metode penelitian adalah serangkaian prosedur atau teknik yang digunakan oleh peneliti untuk mengumpulkan, menganalisis, dan menginterpretasikan data guna menjawab pertanyaan penelitian atau menguji hipotesis. Metode ini mencakup segala langkah yang diperlukan dalam proses penelitian, mulai dari perumusan masalah, pengumpulan data, analisis data, hingga pelaporan hasil penelitian. Penetration testing, atau uji penetrasi, adalah suatu proses pengujian keamanan yang melibatkan simulasi serangan terhadap sistem komputer, jaringan, atau aplikasi untuk mengidentifikasi kerentanan yang dapat dieksploitasi oleh pihak tidak berwenang. Tujuannya adalah untuk menemukan dan memperbaiki kelemahan sebelum dapat dimanfaatkan oleh penyerang yang sebenarnya.



Sumber: Hasil Penelitian (2024)

Gambar 1. Flowchart Penelitian

2.1 *Penetration Testing* (Pentesting)

Metode penetration testing adalah metode yang digunakan untuk mengevaluasi keamanan sistem dan jaringan computer [10][11]. Tujuannya adalah untuk mengidentifikasi kerentanan (celah keamanan) yang dapat dieksploitasi oleh penyerang sebelum mereka melakukannya di dunia nyata, sehingga kerentanan tersebut dapat diperbaiki sebelum menyebabkan kerusakan.

2.2 Pengumpulan Data (*Information Gathering*)

Pada tahap pengumpulan informasi, dilakukan pemetaan jaringan untuk mengenali host yang aktif, mengidentifikasi port yang terbuka, serta mengumpulkan data lebih lanjut mengenai sistem atau jaringan yang sedang diuji, seperti versi perangkat lunak yang digunakan, daftar pengguna, dan pengaturan sistem yang relevan [12]. Proses pengumpulan informasi ini terdiri dari dua tahapan utama, yaitu Information Gathering dan Footprinting. Information Gathering bertujuan untuk mengumpulkan data penting, seperti alamat IP, spesifikasi server, dan informasi lainnya yang akan digunakan dalam eksploitasi, dengan memanfaatkan berbagai alat seperti M theHarvester, Google dorking, Shodan, dan Recon-ng. Sementara itu, Footprinting, yang merupakan bagian dari Information Gathering, berfokus pada pencarian spesifikasi server secara rinci untuk mendapatkan gambaran lebih jelas mengenai sistem yang diuji.

2.3 Analisa Celah Keamanan

Analisis kerentanan akan dilakukan dengan vulnerability scanning, yaitu proses pemeriksaan data, karakteristik, dan struktur jaringan yang sudah diketahui untuk mengidentifikasi potensi celah keamanan. Proses ini menggunakan framework khusus yang dirancang untuk menemukan kerentanan pada jaringan komputer. Framework yang digunakan pada penelitian ini yaitu OWASP Testing Guide. Dalam upaya melakukan vurnerability scanning penelitian ini menggunakan OWASP ZAP untuk mendeteksi information disclosure. ZAP juga memiliki fitur untuk melakukan pengujian manual dan eksploitasi kerentanan [13].

2.4 Exploitasi

Sebagai bagian dari upaya untuk mengidentifikasi dan memperbaiki kerentanan keamanan pada sebuah sistem, kami menyajikan pengujian penetrasi (penetration testing) pada website testphp.vulnweb.com. Dalam tahap ini, peneliti melakukan serangan pada website berdasarkan hasil analisis kerentanan yang menunjukkan adanya celah cross site scripting. Serangan dilakukan menggunakan X-Spear, sebuah aplikasi scanner otomatis yang sangat berguna bagi pemula yang ingin belajar tentang cross site scripting dan keamanan web. Dengan menggunakan X-Spear, Anda dapat mengidentifikasi kerentanan cross site scripting pada situs web atau aplikasi web Anda sendiri dan mengambil langkah-langkah untuk memperbaikinya [14].

2.5 *Reporting*

Setelah ancaman atau serangan terhadap keamanan situs web teridentifikasi, langkah selanjutnya adalah menyusun laporan analisis yang komprehensif. Laporan ini sebaiknya mencakup detail ancaman atau serangan yang ditemukan, serta rekomendasi penanganan yang tepat untuk meningkatkan keamanan situs web tersebut. Rekomendasi ini dapat berupa tindakan teknis, seperti memperbarui perangkat lunak, menerapkan patch keamanan, atau mengkonfigurasi ulang pengaturan keamanan. Selain itu, rekomendasi juga dapat mencakup langkah-langkah non-teknis, seperti pelatihan kesadaran keamanan bagi pengguna atau pengembangan kebijakan keamanan yang lebih ketat [15].

Tabel 1. Temuan Pada Sistem Informasi Akademik

Report	**Hasil**
Jenis *Bug*	*Exposure of Sensitive Information (DB Credentials) to Unauthorized Actor*
Severity	Major
Level CVSS Base Score	5.5 (Medium)
URL Vulnerability	https://sia.unmuhjember.ac.id/log/injectLog.log
Impact	Memungkinkan *attacker* bisa mendapatkan data *sensitive* seperti *user, password,* kode enskripsi

3. Hasil dan Pembahasan

Hasil dari proses penetration testing yang telah dilakukan terhadap aplikasi *e-commerce* milik As-Sakinah *Mart* mencakup temuan kerentanan yang berhasil diidentifikasi pada setiap tahap.

3.1 Pengumpulan Data (*Information Gathering*)

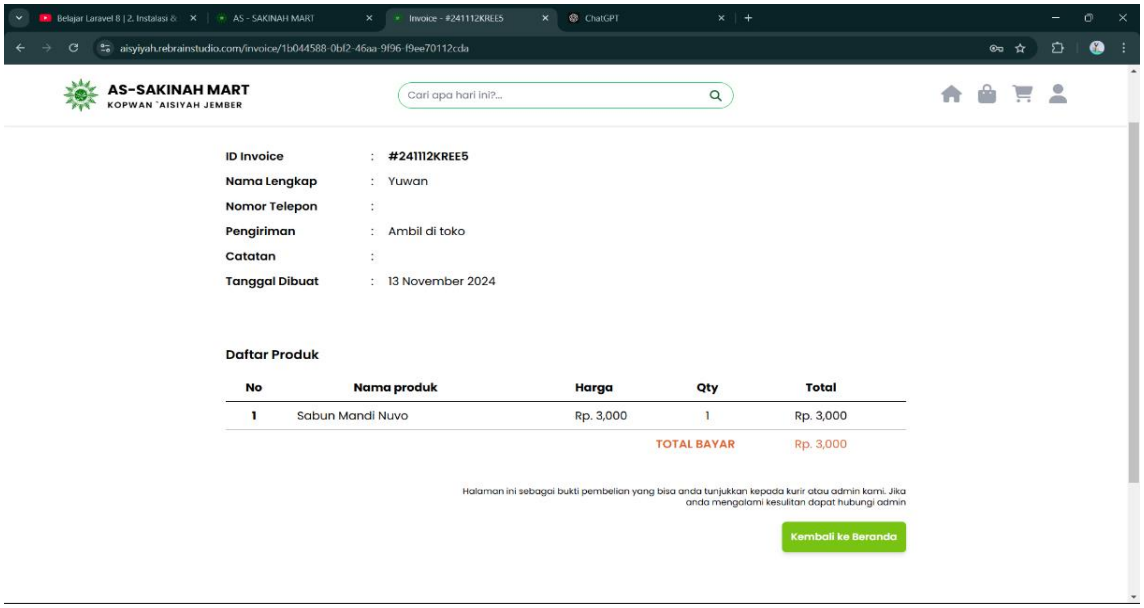
Pengumpulan informasi mengenai aplikasi *e-commerce* As-Sakinah *Mart* dikumpulkan melalui berbagai teknik seperti. Seperti menggunakan Ping memberikan informasi dasar tentang target untuk melihat ip yang nantinya akan digunakan pada tahap selanjutnya dan Nmap yang melakukan pemindaian port pada alamat ip target. Ini akan mengidentfikasi port terbuka dan layanan yang berjalan pada alamat ip tersebut, yang dapat memberikan petunjuk tentang potensi kerentanan. Akan tetapi tidak ada sebuah celah atau potensi kerentanan pada setiap *por*t yang diketahui. Pemindaian dengan *Nmap* dan *Ping* tidak menunjukkan kerentanan pada port atau layanan. Alamat IP dan infrastruktur server teridentifikasi dengan baik.

3.2 Analisa Celah Keamanan (*Scanning*)

Analisa celah keamanan dilakukan menggunakan *tools scanning* otomastis yang bertujuan untuk mengidentifikasi potensi kerentanan pada aplikasi *e-commerce* As-Sakinah *Mart.* Setelah dilakukan scanning otomastis. Pada scanning otomatis menggunakan *Gobuster* yang merupakan *tools* perintah yang dirancang untuk melakukan serangan *brute force* direktori dan file pada *server web*. Selain menggunakan *gobuster* pengujian ini juga menggunakan SQLMap untuk memindai situs web: Assakinahmart.com guna mengidentifikasi potensi kerentanan *SQL injection* yang mungkin ada. Hasil *scanning* kerentanan *sql injection* menggunakan tool sqlmap maupun manual dengan menggunakan *script* ('OR'1'='1) tidak ada kerentanan yang ditemukan. Setelah dilakukan *scanning* celah kerentaan juga dilakuakan scanning terhadap ip server aisyiyah.rebrainstudio.com dengan *tools* Nmap. Sehingga pada percobaan ditemukan CVE-2011-3192. CVE-2011-3192 adalah kerentanan yang terkait dengan cara *Apache HTTP Server* menangani permintaan *HTTP Range*. Kerentanan ini memungkinkan penyerang untuk menyebabkan serangan *Denial of Service (DoS)* dengan permintaan *HTTP Range* yang dibuat dengan buruk. *Tools* seperti *Gobuster* dan *SQLMap* tidak menemukan kerentanan *SQL Injection* atau direktori sensitif. Namun, pemindaian *Nmap* mengungkap kerentanan **CVE-2011-3192** (DoS pada *Apache HTTP Server*).

3.3 *Exploitation*

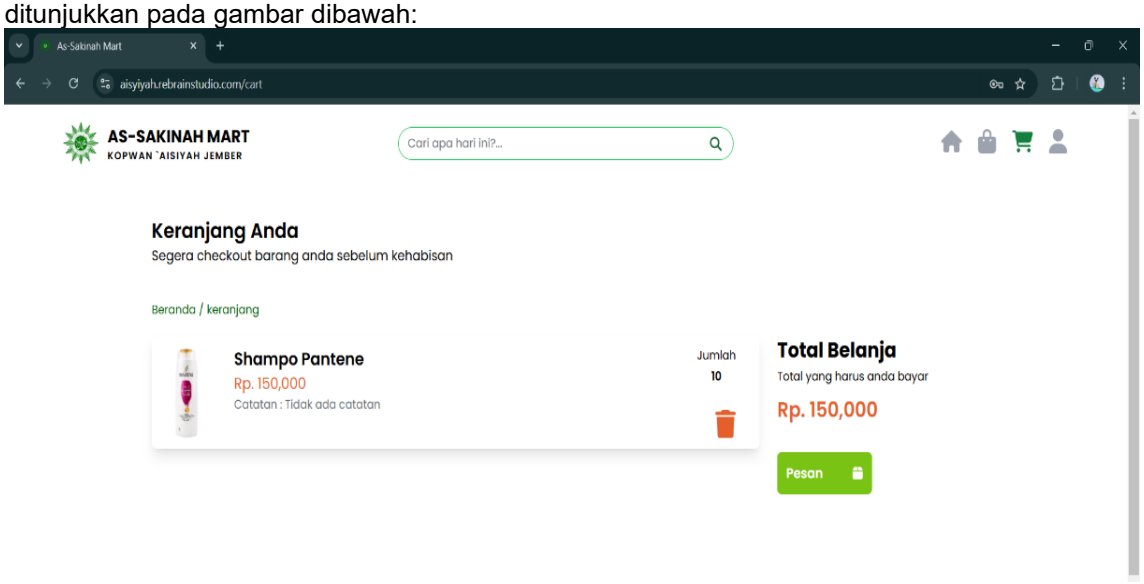
Cekout 1 (satu) buah produk dan masuk kedalam halam order seperti pada gambar dibawah:



Sumber: Hasil Penelitian (2024)

Gambar 2. Order

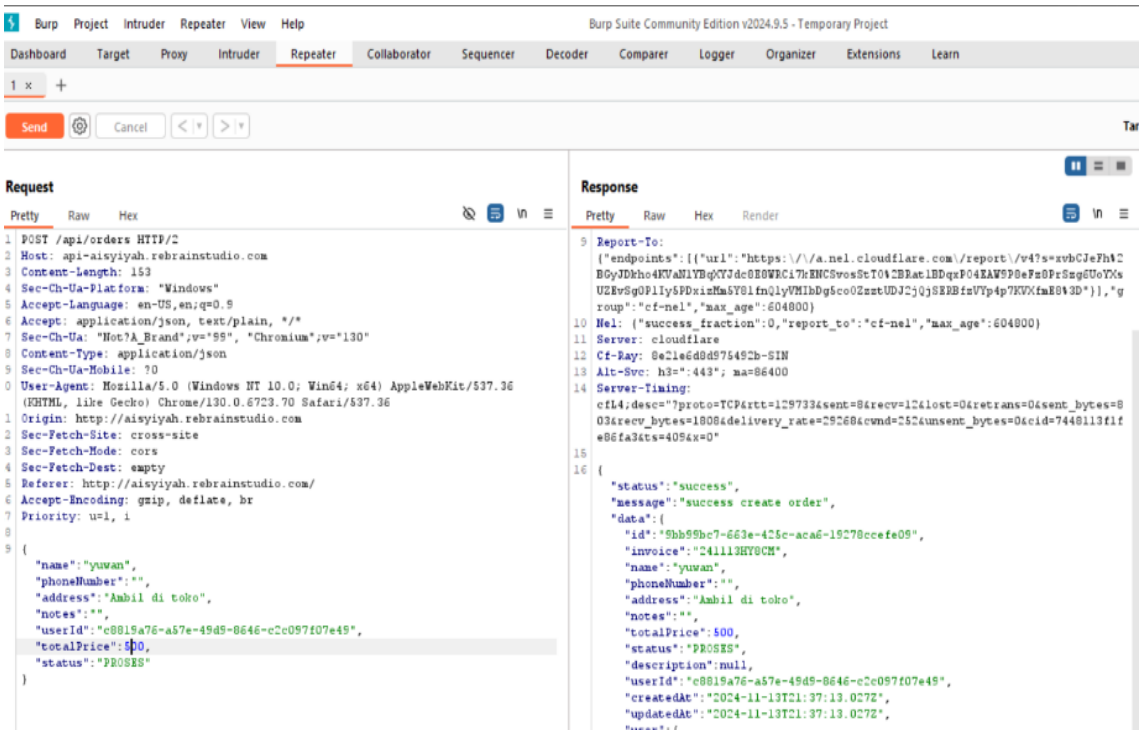
Kemudian cekout 1 barang lagi dengan jumlah yang lebih banyak seperti yang ditunjukkan pada gambar dibawah:



Sumber: Hasil Penelitian (2024)

Gambar 3. *Cart* Produk

Setelah melakukan seperti gambar diatas buka tools burpsuit untuk melakukan eksploitasi dengan mencari method post/api/order pada pembelian sebelumnya. Selanjutnya setelah menemukan method post /api/order send request pada menu repeater untuk memanipulasi harga sesuai yang peneliti inginkan, halaman repeater bisa dilihat pada gambar di bawah ini:

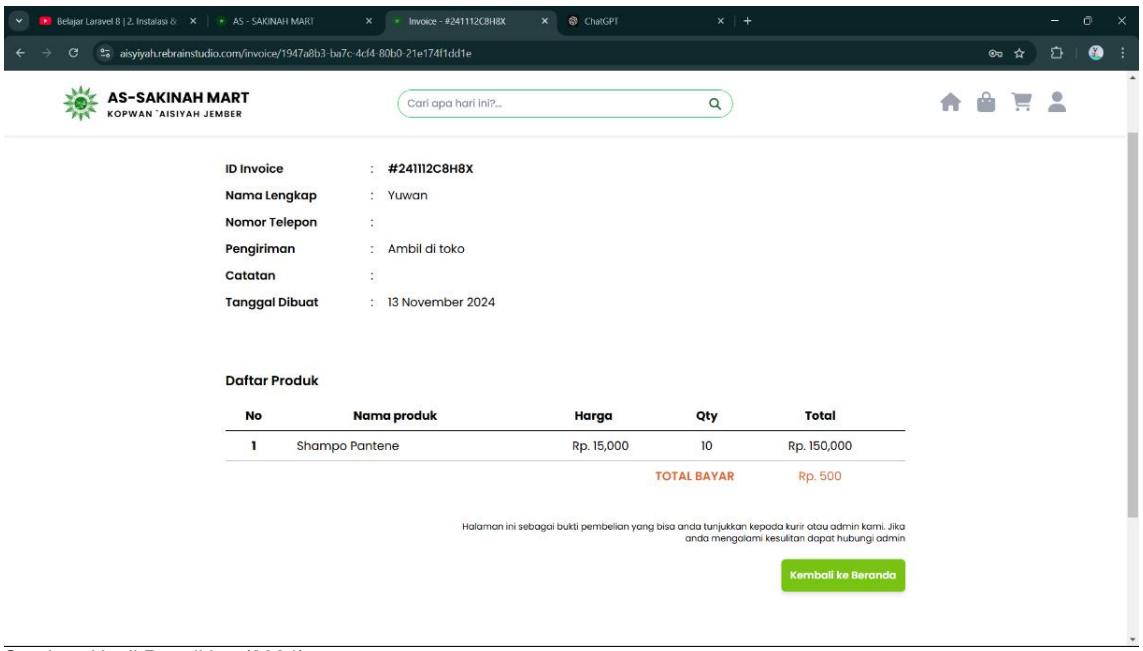


Sumber: Hasil Penelitian (2024)

Gambar 4. Halaman *Repeater*

Proses di atas menunjukan bagaimana exploitasi dilakukan, dengen mengirimkan request harga yang peneliti lakukan, response juga menunjukan status success yang artinya

harga telah dimanipulasi. Setelah melakukan eksploitasi seperti gambar diatas kembali ke menu utama dan liat hasil pada menu riwayat transaksi dan hasil bisa dilihat pada gambar disini:



Sumber: Hasil Penelitian (2024)

Gambar 5. Hasil eksploitasi dengan *tools burpsuite*

Gambar diatas menunjukan bahwa total bayar dan total harga berbeda yang artinya pembeli harus membayar sesuai dengan total bayar, exploitasi pada aplikasi ini sukses attacker atau hacker bisa melakukan manipulasi total bayar.

3.4 Report

Berdasarkan hasil penelitian yang telah dilakukan terbukti bahwa aplikasi *e-commerce* As-Sakinah Mart terindentifikasi kerentanan atau *bug business logic vulnerability,* dimana bug ini dapat mengakibatkan kerugian finansial yang signifikan bagi e-commerce. Jika tidak ditangani, penyerang dapat memanfaatkan kerentanan ini untuk membeli barang dengan harga negatif atau bahkan mendapatkan pengembalian uang yang tidak seharusnya.

Tabel 2. Report CWE-840

Report	**Hasil**
Jenis Bug	CWE-840 *Business Logic Vulnerability*. Kerentanan ini memungkinkan pengguna untuk memanipulasi harga sebelum menyelesaikan transaksi. Serangan ini mengeksploitasi kelemahan dalam alur bisnis aplikasi, bukan kelemahan teknis pada enkripsi atau autentikasi.
Severity	Major
Level CVSS Base Score	7.7 (High)
Skema Eksploitasi	-User menambahkan produk ke dalam keranjang. -Saat ke halaman checkout, user mengintersep request (menggunakan tools burpsuite). -Pada parameter harga di paload json atau http request harga di manipulasi. -Permintaan di forward ke server, dan sistem memproses checkout dengan harga yang telah dimanipulasi.
Ekspetasi vs Realitas	-Ekspetasi: Pengolahan harga seharusnya berada di server bukan pada front-end. -Realita: Pengolahan harga dilakukan di front-end sehingga dapat dimanipulasi ketika mengirim ke server.
Analisis Teknis	-Akar Masalah: Sistem hanya mengandalkan harga yang dikirimkan dari client-side, bukan dari backend atau database. Ini menimbulkan risiko trusting user input. -Penyebab Utama: a. Tidak ada validasi harga di backend. b. Tidak ada verifikasi data pada saat checkout. c. Sistem tidak memverifikasi ulang harga dengan data di server.
Mitigasi	-Pastikan harga produk diambil dan divalidasi langsung dari database backend, bukan dari

Report	Hasil
	input pengguna. -Enkripsi atau hash data sensitif (seperti harga) saat dikirim dari client ke server. -Gunakan token atau checksum untuk memvalidasi apakah data checkout telah dimanipulasi. -Implementasi log transaksi dan deteksi anomali harga untuk mendeteksi perubahan yang mencurigakan. -Pastikan transaksi memiliki session validation dan rate limiting untuk mencegah serangan otomatis.
Proof of Concept / Poc	Screenshot atau rekaman vidio yang menunjukan bagaimana kerentanan ini bisa dieksploitasi dan dampaknya.
Rekomendasi Tambahan	-Lakukan pentest secara berkala untuk memastikan kerentanan ini tidak muncul kembali. -Implementasi program Bug Bounty untuk mendeteksi kerentanan lebih awal. -Pelatihan keamanan bagi pengembang untuk meningkatkan pemahaman terkait business logic vulnerabilities.

Temuan penelitian ini memiliki implikasi signifikan bagi keamanan dan operasional As-Sakinah Mart:

a). Implikasi Teknis
Business Logic Flaw: Kerentanan ini menunjukkan ketergantungan sistem pada validasi *client-side*, yang mudah dimanipulasi. Hal ini mengancam integritas transaksi dan berpotensi menyebabkan kerugian finansial besar. CVE-2011-3192: Meski tidak langsung dieksploitasi, kerentanan ini membuka risiko *Denial of Service* yang dapat mengganggu ketersediaan layanan.

b). Implikasi Bisnis
Reputasi: Eksploitasi harga dapat merusak kepercayaan pelanggan dan mitra.
Kepatuhan: Kegagalan memenuhi standar keamanan seperti OWASP Top 10 dapat berdampak pada legalitas bisnis.

c). Rekomendasi
Validasi Server-Side: Harga produk harus divalidasi di *backend* sebelum diproses.
Enkripsi Data: Gunakan *hashing* atau token untuk melindungi data transaksi.
Audit Berkala: Pentesting rutin diperlukan untuk mendeteksi celah baru.

4. Kesimpulan

Tingkat keamanan aplikasi e-commerce bervariasi tergantung pada seberapa baik sistem tersebut dilindungi oleh protokol keamanan yang mutakhir dan seberapa cepat pengembang memperbarui sistem mereka untuk menanggulangi serangan siber terbaru. Penetration testing mampu mengidentifikasi berbagai kerentanan dalam aplikasi e-commerce, termasuk kelemahan dalam autentikasi, otorisasi, serta eksposur data sensitif. Tes ini juga sering kali mengungkap celah yang belum disadari dalam arsitektur aplikasi, seperti injeksi SQL, XSS (Cross-Site Scripting), dan kerentanan terkait konfigurasi server. Metode penetration testing terbukti efektif dalam mengungkap kelemahan keamanan pada aplikasi e-commerce, terutama dalam menemukan dan mengevaluasi risiko dari potensi ancaman sebelum dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Hasil penelitian ini menunjukkan bahwa website Assakinahmart.com telah memenuhi standar keamanan yang tinggi dan aman dari ancaman yang termasuk dalam OWASP Top 10-2021. Hal ini memberikan kepercayaan yang lebih besar kepada pengguna dan pemilik website bahwa data dan transaksi mereka dilindungi dengan baik. Penetration testing yang dilakukan membuktikan bahwa metode ini efektif dalam mengungkap potensi kerentanan dan memberikan rekomendasi perbaikan, sehingga mendukung peningkatan keamanan aplikasi. Oleh karena itu, penelitian ini memberikan kontribusi nyata dalam penerapan penetration testing untuk menjaga keamanan sistem informasi e-commerce. Meski demikian, penting untuk terus melakukan pemantauan dan pembaruan keamanan secara berkala untuk menjaga tingkat keamanan yang telah dicapai, mengingat ancaman siber terus berkembang seiring waktu.

Referensi

[1] T. A. Berutu, D. L. R. Sigalingging, G. K. V. Simanjuntak, and F. Siburian, “Pengaruh Teknologi Digital terhadap Perkembangan Bisnis Modern,” *Neptunus J. Ilmu Komput. Dan Teknol. Inf.*, vol. 2, no. 3, pp. 358–370, 2024, doi: 10.61132/neptunus.v2i3.258.

[2] M. Rahman, M. Dasuki, and H. Oktavianto, “Implementasi Manajemen Bandwidth Simple Queue Sebagai Optimalisasi Layanan Jaringan Internet Warga Menggunakan Metode NDLC,” J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 27–35, 2024, doi:

10.37859/coscitech.v5i1.6899
[3] M. A. S. iriansyah Prayitno, M. Rahman, and D. L. Pater, “Implementasi Manajemen Bandwidth Hierarchical Token Bucket (HTB) Menggunakan Metode Network Development Life Cycle (NDLC),” vol. 5, no. 2, pp. 120–128, 2024, doi: doi.org/10.37148/bios.v5i2.131.
[4] M. Rahman *et al.*, “Optimalisasi Jangkauan Sinyal Wireless Fidelity Menggunakan Mi WiFi Range Extender Pro,” *J. Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 164–171, 2023, doi: 10.37859/coscitech.v4i1.4630.
[5] M. Rahman, “Implementasi Web Content Filtering Pada Jaringan RT/RW Net Menggunakan Pi-Hole DNS Server,” *Gener. J.*, vol. 7, no. 1, pp. 50–60, 2023, doi: 10.29407/gj.v7i1.19818.
[6] M. Rahman, A. M. Zakiyyah, M. Dasuki, R. Umilasari, and G. Abdurrahman, “Pemberdayaan Pelaku Industri Rumah Tangga (IRT) Melalui Inovasi Pembuatan Korean Strawberry Milk Dan Pemasaran Produksi Berbasis Digital Marketing,” *Communnity Dev. J.*, vol. 5, no. 2, pp. 3407–3413, 2024, doi: 10.31004/cdj.v5i2.26826.
[7] R. Umilasari, Nurhalimah, and M. Rahman, “Increased Production and Marketing of Crackers Through Process Improvements in SR Crackers Home Industries in Wonosari,” *KONTRIBUSIA*, vol. 2, no. 2, p. 42, Sep. 2019, doi: 10.30587/kontribusia.v2i2.1009.
[8] A. M. Zakiyyah, R. Umilasari, and G. Abudurrahman, “Pendampingan Internet Marketing Di UMKM Mickline Jember,” Abdi Indones., vol. 1, no. 1, pp. 46–60, 2021.
[9] Firda, S. Putri, Y. B. Utomo, and H. Kurniadi, “Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux,” Pros. SEMNAS INOTEK (Seminar Nas. Inov. Teknol., vol. 7, no. 1, pp. 52–59, 2023.
[10] M. F. Asnawi and M. A. Nugroho, “Pengujian Keamanan Jaringan Menggunakan Metode Penetrasi Tes Pada Jaringan Smk Muhammadiyah 1 Wonosobo,” Device, vol. 12, no. 2, pp. 110–118, 2022, doi: 10.32699/device.v12i2.3687.
[11] D. E. Faishol, T. A. Cahyanto, M. Rahman, S. T. Informatika, F. Teknik, and U. M. Jember, “Analisis Dan Evaluasi Protokol Keamanan Jaringan Nirkabel Wi-Fi Protected Access 3 dengan Metode Penetration Testing,” vol. 9, no. 1, pp. 420–432, 2024, doi: 10.30645/jurasik.v9i1.749.
[12] A. Okario and H. Suputra, “Analisis Celah Keamanan Jaringan WPA dan WPA2 Dengan Menggunakan Metode Penetration Testing,” Jnatia, vol. 1, no. 4, pp. 1125–1130, 2023.
[13] M. Nur Fikri, B. Parga Zen, R. Adhitama, and E. Ahmad Firdaus, “Analisis Keamanan Sistem Informasi Website SMA Negeri 1 Sokaraja Menggunakan Metode Penetration Testing Execution Standard (PTES),” J. Inform., vol. 2, no. 2, pp. 19–27, 2023, doi: 10.57094/ji.v2i2.1046.
[14] R. N. Dasmen, T. L. Widodo, and M. Tio, “PENGUJIAN PENETRASI PADA WEBSITE ELEARNING2 . BINADARMA . AC . ID DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD),” vol. 11, no. 1, pp. 91–95, 2023, doi: 10.35508/jicon.v11i1.9809.
[15] Y. Mulyanto, M. T. A. Zaen, Y. Yuliadi, and S. Sihab, “Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest),” J. Inf. Syst. Res., vol. 4, no. 1, pp. 202–209, 2022, doi: 10.47065/josh.v4i1.2335.