E-ISSN 3047-1192.

Subse

BHATARA Multidisciplinary

https://subset.id/index.php/BHATARA

BMJ

# Valuasi Keamanan Informasi Pada Website Bakpia Tamansari Dan Semakar Adventure Shop Menggunakan Pendekatan Penetration Testing Dan Vulnerability Assessment

## *Information Security Valuation on the Bakpia Tamansari Website and Semakar Adventure Shop Using Penetration Testing and Vulnerability Assessment Approaches*

**Abel Kusuma[1,a)], Joko Dwi Santoso[2,b)], Hastari [3,c)], Ahlihi Masruro[4,d)], Sudarmanto[5,a)],**

[1,2)] Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta
[3,4)] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta
[5)] Program Studi Rekayasa Perangkat Lunak, Fakultas Teknologi Informasi, Universitas Teknologi Digital Indonesia
[a,b,c,d)]Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281

[e)]Jl. Raya Janti (Majapahit) No. 143, Karang Jambe, Banguntapan, Kabupaten Bantul, Daerah Istimewa Yogyakarta 55198

[*]Corresponding Author: Abel Kusuma, abelkusuma@students.amikom.ac.id
Received: 22 Juli 2026; Accepted: 31 Juli 2026

KEYWORDS

**Kata kunci:**
Uji keamanan web
Kerentanan aplikasi e-commerce
Penetration testing
OWASP
SQL injection

***Keywords:***
*Web security test*
*E-commerce app vulnerabilities*
*Penetration testing*
*OWASP*
*SQL injection*

ABSTRAK

**Abstrak.** Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan informasi pada dua platform e-commerce lokal, yaitu Bakpia Tamansari dan Semakar Adventure Shop, melalui pendekatan pengujian penetrasi (penetration testing) dan pemindaian kerentanan (vulnerability assessment). Metode yang digunakan adalah studi kasus dengan menerapkan seperangkat alat keamanan seperti Metasploit, Nmap, Nikto, SQLMap, dan OWASP ZAP untuk mengidentifikasi celah keamanan pada aspek jaringan, server, aplikasi web, dan basis data. Hasil penelitian menunjukkan bahwa kedua website memiliki kerentanan serupa dalam konfigurasi keamanan, terutama pada ketiadaan header keamanan penting (X-Frame-Options, X-Content-Type-Options), port layanan yang terbuka tanpa proteksi memadai, serta potensi serangan Cross-Site Request Forgery (CSRF). Bakpia Tamansari menunjukkan postur keamanan yang sedikit lebih baik dengan tidak adanya kebocoran file sensitif, sementara Semakar Adventure Shop teridentifikasi memiliki file konfigurasi (composer.lock) yang dapat diakses publik. Berdasarkan temuan tersebut, penelitian ini memberikan rekomendasi perbaikan berupa penerapan autentikasi multifaktor, penambahan header keamanan, penutupan port tidak diperlukan, serta peningkatan sistem pemantauan dan respons insiden. Implikasi penelitian ini diharapkan dapat menjadi acuan bagi pengelola platform e-commerce lokal dalam meningkatkan kesiapan keamanan informasi sesuai standar industri.

***Abstract.*** *This study aims to evaluate the level of information security on two local e-commerce platforms, namely Bakpia Tamansari and Semakar Adventure Shop, through penetration testing and vulnerability assessment. The method used is a case study by applying a set of security tools such as Metasploit, Nmap, Nikto, SQLMap, and OWASP ZAP to identify security vulnerabilities in aspects of the network, server, web application, and database. The results show that both websites have similar vulnerabilities in security configurations, especially in the absence of critical security headers (X-Frame-Options, X-Content-Type-Options), open service ports without adequate protection, and potential for Cross-Site Request*

*Forgery (CSRF) attacks. Bakpia Tamansari showed a slightly better security posture with no leakage of sensitive files, while Semakar Adventure Shop was identified as having a publicly accessible configuration file (composer.lock). Based on these findings, this study provides recommendations for improvement in the form of implementing multi-factor authentication, adding security headers, closing ports is not required, and improving incident monitoring and response systems. The implications of this research are expected to be a reference for local e-commerce platform managers in improving information security readiness according to industry standards.*

## 1. Pendahuluan

Perkembangan teknologi digital yang pesat telah membawa dampak signifikan terhadap transformasi bisnis, terutama di sektor e-commerce. Platform e-commerce tidak hanya berfungsi sebagai sarana transaksi, tetapi juga menjadi tempat penyimpanan data sensitif pengguna seperti informasi pribadi, riwayat pembelian, dan detail keuangan (Lazăr, 2023). Keamanan data tersebut menjadi sangat krusial mengingat maraknya ancaman siber seperti kebocoran data, pencurian identitas, dan serangan ransomware yang dapat merugikan baik pengguna maupun perusahaan. Oleh karena itu, implementasi sistem keamanan informasi yang robust menjadi kebutuhan mendasar bagi setiap platform digital. Penelitian ini berfokus pada evaluasi keamanan dua platform e-commerce lokal di Indonesia, yaitu Bakpia Tamansari dan Semakar Adventure Shop, untuk mengidentifikasi kerentanan yang ada dan memberikan rekomendasi perbaikan. Latar belakang penelitian ini dilatarbelakangi oleh semakin tingginya frekuensi serangan siber yang menargetkan platform e-commerce, terutama yang masih dalam tahap pengembangan atau berskala kecil. Studi oleh Wicaksono dkk. (2020) menunjukkan bahwa aplikasi berbasis web sering kali memiliki celah keamanan seperti *Broken Access Control, Cross-Site Scripting* (XSS), dan SQL Injection yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Kerentanan semacam itu berpotensi menyebabkan akses tidak sah ke data pengguna, manipulasi transaksi, hingga gangguan operasional. Bakpia Tamansari dan Semakar Adventure Shop dipilih sebagai objek penelitian karena mewakili usaha e-commerce lokal yang sedang berkembang dan memiliki kebutuhan mendesak untuk memperkuat sistem keamanannya. Evaluasi mendalam terhadap kedua platform ini diharapkan dapat memberikan gambaran nyata tentang tantangan keamanan yang dihadapi oleh bisnis e-commerce skala menengah di Indonesia. Rumusan masalah dalam penelitian ini adalah untuk mengidentifikasi kerentanan keamanan apa saja yang terdapat pada website Bakpia Tamansari dan Semakar Adventure Shop.

Pertanyaan penelitian difokuskan pada bagaimana tingkat kerentanan kedua platform terhadap serangan umum seperti *SQL Injection, Cross-Site Request Forgery* (CSRF), dan kebocoran informasi melalui konfigurasi server yang tidak aman (Alanda dkk., 2021). Selain itu, penelitian ini juga bertujuan untuk mengevaluasi efektivitas kontrol teknis keamanan yang telah diimplementasikan, seperti penggunaan *firewall,* enkripsi data, dan mekanisme autentikasi. Dengan menjawab pertanyaan-pertanyaan tersebut, diharapkan dapat dirumuskan rekomendasi yang tepat dan terukur untuk meningkatkan postur keamanan kedua website. Identifikasi celah keamanan secara komprehensif menjadi langkah awal yang kritis dalam membangun sistem e-commerce yang resilien terhadap ancaman siber.

Tujuan utama dari penelitian ini adalah untuk melakukan evaluasi keamanan informasi secara mendalam pada platform Bakpia Tamansari dan Semakar Adventure Shop dengan menggunakan berbagai alat *penetration testing* seperti *Metasploit, Nmap, Nikto, SQLMap, dan OWASP ZAP*. Penilaian dilakukan dengan memindai port terbuka, menganalisis konfigurasi server, menguji kerentanan terhadap injeksi, serta mengevaluasi header keamanan dan proteksi terhadap serangan berbasis web (Lachkov dkk., 2022). Hasil evaluasi ini kemudian akan dibandingkan dengan standar keamanan informasi yang diakui, seperti kontrol teknis dalam ISO 27001:2022, khususnya pada klausul yang berkaitan dengan teknologi. Selain itu, penelitian ini bertujuan untuk menyusun rekomendasi perbaikan yang spesifik dan dapat diimplementasikan oleh pengelola kedua platform. Diharapkan, rekomendasi tersebut dapat membantu meningkatkan kemampuan deteksi dan respons terhadap ancaman siber di masa depan.

## 2. Metode Penelitian

### *2.1. Konsep Bisnis Syariah dan Fikih Muamalah*

Bab ini menjelaskan kerangka metodologis yang digunakan dalam penelitian evaluasi keamanan informasi pada website Bakpia Tamansari dan Semakar Adventure Shop. Untuk mencapai tujuan penelitian, pendekatan studi kasus diterapkan dengan memanfaatkan metode pengujian penetrasi (penetration testing) dan pemindaian kerentanan (vulnerability assessment) secara sistematis. Metode ini dipilih karena kemampuannya dalam mengidentifikasi kelemahan teknis secara langsung dalam lingkungan yang menyerupai serangan nyata, sehingga hasil yang diperoleh bersifat empiris dan dapat ditindaklanjuti (Lachkov, Tawalbeh, & Bhatt, 2022). Penelitian ini menggunakan seperangkat alat (tools) keamanan yang telah teruji dan umum digunakan dalam praktik ethical hacking, seperti Metasploit, Nmap, Nikto, SQLMap, dan OWASP ZAP. Alur penelitian dirancang secara bertahap, mulai dari persiapan dan perizinan, identifikasi standar keamanan, eksekusi

pengujian, analisis temuan, hingga penyusunan rekomendasi. Dengan menerapkan metodologi yang terstruktur dan dapat direplikasi, diharapkan penelitian ini tidak hanya memberikan gambaran mendalam tentang kondisi keamanan kedua objek studi, tetapi juga berkontribusi pada pengembangan pendekatan pengujian keamanan berbasis standar untuk platform e-commerce lokal di Indonesia.

### *2.2. Alur Penelitian*

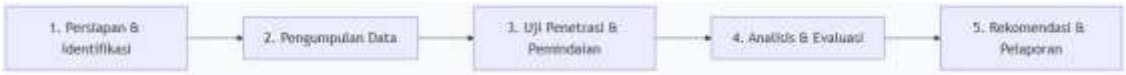
Alur penelitian dirancang secara sistematis dan terstruktur untuk memastikan setiap tahap pengujian dapat dilakukan secara metodologis, terukur, dan dapat dipertanggungjawabkan. Tahapan penelitian meliputi persiapan, identifikasi objek, pengumpulan data melalui pengujian teknis, analisis hasil, dan penyusunan rekomendasi seperti yang ditunjukkan pada Gambar 2.1. Proses pengujian mengacu pada kerangka ethical hacking dan standar pengujian keamanan aplikasi web yang umum digunakan dalam penelitian keamanan siber (OWASP, 2021).

### *2.3. Teknik Pengumpulan Data*

Pengumpulan data dilakukan melalui tiga teknik utama: wawancara semi-terstruktur dengan pengelola teknis kedua website, observasi langsung terhadap infrastruktur dan konfigurasi sistem, serta analisis dokumen seperti SOP (Standard Operating Procedure) dan surat izin pengujian. Data primer diperoleh melalui serangkaian pengujian teknis menggunakan alat-alat keamanan yang telah disebutkan, sedangkan data sekunder didapat dari studi literatur dan dokumentasi kebijakan keamanan yang relevan.

### *2.4. Instrumen dan Alat Penelitian*

Penelitian ini menggunakan seperangkat alat (tools) penetrasi yang berjalan pada sistem operasi Kali Linux sebagai platform pengujian. Alat-alat yang digunakan meliputi: Metasploit untuk pemindaian port dan eksploitasi kerentanan, Nmap untuk pemetaan jaringan dan deteksi layanan, Nikto untuk analisis keamanan server web, SQLMap untuk pengujian injeksi SQL, serta OWASP ZAP (Zed Attack Proxy) untuk pemindaian keamanan aplikasi web secara dinamis. Penggunaan alat-alat ini didasarkan pada efektivitasnya dalam mendeteksi berbagai jenis kerentanan yang umum ditemukan pada aplikasi web (Zimmerman, 2020).




**Gambar 1**. Alur Penelitian

### *2.5. Prosedur Analisis Data*

Data yang diperoleh dari hasil pemindaian dianalisis secara kualitatif dengan mengelompokkan temuan berdasarkan tingkat risiko (tinggi, sedang, rendah) dan kategori kerentanan (misalnya: konfigurasi, autentikasi, injeksi). Analisis dilakukan dengan membandingkan hasil pengujian dengan standar keamanan seperti OWASP Top 10 dan CIS Critical Security Controls. Hasil analisis kemudian diverifikasi melalui triangulasi metode dengan membandingkan temuan dari berbagai alat uji untuk memastikan keakuratan dan reliabilitas data.

### *2.6. Etika Penelitian*

Seluruh pengujian dilakukan setelah memperoleh izin tertulis dari pemilik masing-masing website. Penelitian dilaksanakan dalam ruang lingkup yang disepakati dan tidak mengganggu operasional layanan. Prinsip ethical hacking diterapkan dengan ketat, di mana tidak ada eksploitasi yang merusak, pengubahan data, atau akses di luar batas yang telah disetujui. Semua temuan kerentanan dilaporkan secara rahasia kepada pihak terkait sebagai bagian dari tanggung jawab penelitian.

### *2.7. Socioemotional Wealth (SEW) dan Stewardship Theory pada Perusahaan Keluarga*

Perusahaan keluarga merupakan salah satu bentuk organisasi bisnis yang memiliki karakteristik unik karena kepemilikan, pengelolaan, dan pengambilan keputusan sering kali berada dalam lingkup keluarga yang sama. Berbeda dengan perusahaan non-keluarga yang umumnya berorientasi pada maksimalisasi keuntungan finansial, perusahaan keluarga juga mempertimbangkan tujuan non-ekonomi yang berkaitan dengan keberlangsungan keluarga, nilai-nilai, reputasi, serta warisan antargenerasi (Nawaz, 2017). Dalam konteks ini, Socioemotional Wealth (SEW) dan Stewardship Theory menjadi dua landasan teori yang banyak digunakan untuk menjelaskan perilaku dan keputusan strategis perusahaan keluarga(Yudaruddin et al., 2023). Socioemotional Wealth (SEW) diperkenalkan oleh para peneliti sebagai konsep yang menggambarkan nilai-nilai nonfinansial yang ingin dipertahankan oleh keluarga pemilik perusahaan. SEW menekankan bahwa keluarga tidak hanya mengejar keuntungan ekonomi, tetapi juga berupaya menjaga identitas keluarga, mempertahankan kendali atas perusahaan, memperkuat hubungan sosial dengan para pemangku kepentingan, serta memastikan keberlanjutan

bisnis bagi generasi berikutnya. Dengan demikian, keputusan bisnis sering kali dipengaruhi oleh keinginan untuk melindungi kekayaan emosional tersebut, bahkan apabila keputusan tersebut mengurangi keuntungan jangka pendek (Yudaruddin et al., 2023).

## 3. Hasil dan Pembahasan

Bab ini menyajikan temuan empiris dari serangkaian pengujian keamanan yang dilakukan terhadap website Bakpia Tamansari dan Semakar Adventure Shop. Hasil evaluasi didasarkan pada pemindaian teknis menggunakan alat-alat penetrasi seperti Metasploit, Nmap, Nikto, SQLMap, dan OWASP ZAP, yang dirancang untuk mengidentifikasi kerentanan dalam aspek konfigurasi jaringan, keamanan aplikasi web, serta perlindungan data. Temuan yang diperoleh akan dibahas secara komparatif antara kedua platform untuk menggambarkan tingkat kesiapan keamanan masing-masing, dengan mengacu pada standar praktik keamanan informasi yang diakui seperti OWASP Top 10 dan prinsip pengendalian teknis ISO 27001. Pembahasan lebih lanjut akan mengaitkan setiap kerentanan yang teridentifikasi dengan potensi risiko eksploitasi, dampak terhadap pengguna, serta rekomendasi perbaikan yang bersifat teknis dan prosedural. Melalui analisis ini, diharapkan dapat diperoleh gambaran menyeluruh mengenai postur keamanan kedua website sekaligus memberikan landasan bagi pengembangan strategi peningkatan keamanan yang lebih efektif dan berkelanjutan.

### *3.1. Gambaran Umum Hasil Pengujian*

Pengujian keamanan terhadap website Bakpia Tamansari dan Semakar Adventure Shop dilakukan dengan menggunakan lima alat penetrasi utama selama periode Januari 2025. Hasil pemindaian menunjukkan bahwa kedua platform memiliki profil keamanan yang berbeda, dengan kerentanan umum yang ditemukan terutama pada konfigurasi server, header keamanan, dan pengelolaan akses jaringan. Meskipun tidak ditemukan kerentanan kritis seperti SQL injection atau remote code execution, beberapa kelemahan konfigurasi menimbulkan risiko menengah yang dapat dieksploitasi dalam serangan lebih lanjut. Temuan ini relevan dengan penelitian sebelumnya yang menunjukkan bahwa aplikasi web e-commerce lokal sering kali rentan terhadap kesalahan konfigurasi dan kurangnya implementasi mekanisme pertahanan berlapis (Wicaksono et al., 2020).

Proses pengujian diawali dengan pemindaian jaringan dan port menggunakan Metasploit dan Nmap untuk mengidentifikasi layanan yang terbuka, konfigurasi firewall, serta potensi pintu masuk yang tidak terlindungi. Hasil dari fase ini menjadi dasar untuk menentukan titik fokus pengujian lebih lanjut, terutama pada port yang berisiko tinggi seperti FTP (21) dan MySQL (3306). Selanjutnya, analisis server web dilakukan dengan Nikto untuk mengevaluasi konfigurasi keamanan server, dilanjutkan dengan OWASP ZAP yang berfungsi untuk memindai kerentanan aplikasi web secara dinamis, seperti CSRF, XSS, dan kebijakan keamanan konten. Fase terakhir adalah pengujian injeksi SQL menggunakan SQLMap terhadap parameter input yang rentan, yang divalidasi secara manual untuk memastikan akurasi temuan. Hasil dari ketiga fase tersebut kemudian dikonsolidasikan, dianalisis berdasarkan tingkat keparahan, dan dijadikan dasar untuk menyusun rekomendasi perbaikan yang terstruktur. Skema ini menegaskan bahwa keamanan informasi harus dievaluasi secara holistik, mulai dari infrastruktur hingga lapisan aplikasi. Pendekatan bertahap tidak hanya memastikan tidak ada celah yang terlewat, tetapi juga memungkinkan peneliti untuk memahami hubungan antarkerentanan yang dapat dieksploitasi secara beruntun (chained attack). Dengan demikian, rekomendasi yang dihasilkan tidak hanya bersifat teknis, tetapi juga strategis dalam membangun postur keamanan yang berlapis dan tangguh terhadap ancaman siber yang terus berkembang.

### *3.2. Analisis Hasil Pemindaian Port dan Layanan*

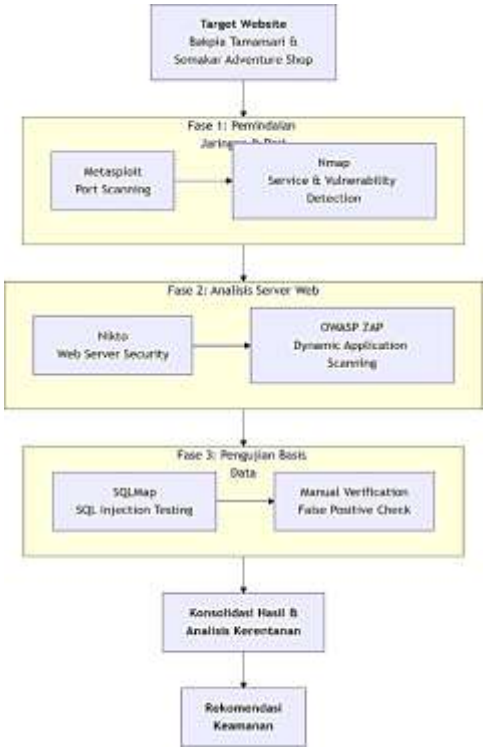
Pemindaian dengan Metasploit dan Nmap mengungkapkan bahwa kedua website memiliki port yang serupa dalam keadaan terbuka, yaitu port 21 (FTP), 80 (HTTP), 443 (HTTPS), dan 3306 (MySQL). Adanya port FTP dan MySQL yang terbuka tanpa proteksi tambahan meningkatkan risiko serangan brute force dan akses tidak sah ke data sensitif. Sementara itu, pemindaian Nmap juga mendeteksi potensi kerentanan CSRF (Cross-Site Request Forgery) pada formulir login dan pendaftaran di kedua situs. Hasil ini sejalan dengan temuan Alanda et al. (2021) yang menyatakan bahwa aplikasi web yang tidak mengimplementasikan token anti-CSRF rentan terhadap manipulasi permintaan oleh pihak ketiga.

### *3.3. Evaluasi Keamanan Aplikasi Web*

Penggunaan Nikto dan OWASP ZAP mengidentifikasi beberapa kelemahan konfigurasi keamanan yang signifikan, terutama terkait tidak adanya atau tidak lengkapnya header keamanan seperti X-Frame-Options, X-Content-Type-Options, dan Strict-Transport-Security. Selain itu, OWASP ZAP melaporkan penggunaan wildcard directive dalam kebijakan CSP (Content Security Policy) yang terlalu longgar, sehingga memungkinkan pemuatan sumber daya dari domain eksternal yang berpotensi berbahaya. Temuan ini menunjukkan kurangnya kesadaran terhadap prinsip security by design pada tahap pengembangan dan deployment website.

### *3.4. Perbandingan Kondisi Keamanan Kedua Website*

Berdasarkan hasil pengujian, dapat dilihat bahwa meskipun kedua website memiliki pola kerentanan yang mirip, terdapat perbedaan signifikan dalam hal eksposur informasi sensitif. Website Semakar Adventure Shop terbukti memiliki file konfigurasi (composer.lock) yang dapat diakses publik, sehingga meningkatkan risiko disclosure informasi. Sementara itu, Bakpia Tamansari menunjukkan perlindungan yang sedikit lebih baik terhadap akses file sensitif, meskipun tetap memiliki celah pada aspek autentikasi dan konfigurasi header.




**Gambar 2**. Skema Pengujian

**Table 1**.
Perbandingan Hasil Pemindaian Keamanan

| Aspek Evaluasi | Bakpia Tamansari | Semakar Adventure Shop |
|---|---|---|
| Port Terbuka (Metasploit) | 21 (FTP), 80 (HTTP), 443 (HTTPS), 3306 (MySQL) | 21 (FTP), 80 (HTTP), 443 (HTTPS), 3306 (MySQL) |
| Kerentanan CSRF (Nmap) | Terdeteksi pada formulir login/registrasi | Terdeteksi pada formulir login/registrasi dan halaman produk |
| Header Keamanan (Nikto) | Tidak ada X-Frame-Options, X-Content-Type-Options | Tidak ada X-Frame-Options, X-Content-Type-Options, HSTS |
| File Sensitif Terbuka (ZAP) | Tidak ditemukan | composer.lock dapat diakses publik |
| SQL Injection (SQLMap) | Tidak rentan | Tidak rentan |
| Risiko Rata-rata | Menengah-Sedang | Menengah-Tinggi |

### *3.5. Pembahasan dan Implikasi Temuan*

Temuan penelitian ini mengonfirmasi bahwa platform e-commerce skala kecil hingga menengah di Indonesia masih menghadapi tantangan serius dalam menerapkan praktik keamanan informasi yang komprehensif. Tidak adanya mekanisme autentikasi multifaktor (MFA) pada layanan SSH dan FTP, serta lemahnya konfigurasi header keamanan, menunjukkan bahwa aspek keamanan sering kali diabaikan karena keterbatasan sumber daya atau kurangnya pemahaman teknis (Lachkov et al., 2022). Kerentanan CSRF yang ditemukan pada kedua website juga mengindikasikan bahwa pengembangan fungsionalitas bisnis sering kali

diutamakan tanpa diimbangi dengan penerapan kontrol keamanan yang memadai. Secara lebih luas, temuan ini menyoroti perlunya pendekatan keamanan yang proaktif dan berkelanjutan, termasuk pelatihan kesadaran keamanan bagi pengembang dan administrator sistem, serta integrasi pengujian keamanan dalam siklus pengembangan perangkat lunak.

## 4. Kesimpulan

Berdasarkan hasil evaluasi keamanan yang dilakukan terhadap website Bakpia Tamansari dan Semakar Adventure Shop, dapat disimpulkan bahwa kedua platform e-commerce tersebut memiliki tingkat kesiapan keamanan informasi yang belum optimal, meskipun tidak ditemukan kerentanan kritis seperti SQL injection atau remote code execution. Secara umum, kerentanan yang teridentifikasi lebih banyak bersifat konfigurasi, seperti tidak adanya header keamanan yang penting (X-Frame-Options, X-Content-Type-Options, HSTS), port layanan yang terbuka tanpa proteksi tambahan (FTP, MySQL), serta potensi serangan Cross-Site Request Forgery (CSRF) pada formulir. Dari sisi perbandingan, Bakpia Tamansari menunjukkan postur keamanan yang sedikit lebih baik dibandingkan Semakar Adventure Shop, terutama dalam hal perlindungan informasi sensitif. Situs Semakar Adventure Shop terbukti mengungkap file konfigurasi (composer.lock) yang dapat diakses publik, sehingga meningkatkan risiko informasi disclosure. Namun, kedua website sama-sama memerlukan peningkatan signifikan dalam penerapan kontrol teknis, prosedur pemantauan, dan mekanisme respons insiden untuk mencapai tingkat keamanan yang sesuai dengan standar industri dan melindungi data pengguna dari ancaman siber yang semakin kompleks.

## Daftar Pustaka

Alanda, A., Satria, D., Ardhana, M. I., Dahlan, A. A., & Mooduto, H. A. (2021). Web application penetration testing using SQL injection attack. JOIV: International Journal on Informatics Visualization, 5(2), 182–187. https://doi.org/10.30630/joiv.5.2.574

Budarsa, N., Indrawan, G., & Gunadi, A. (2022). Analisis risiko keamanan informasi menggunakan metode OCTAVE Allegro dan Analytical Hierarchy Process pada data center pemerintah Kabupaten Buleleng. Jurnal Ilmu Komputer Indonesia (JIK), 7(1), 1–10.

Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). Sage Publications.

Jazuli, A., Salamah, I., & Soim, S. (2024). Deteksi tingkat kerentanan keamanan website dengan metode manual pentest dan tools Xspear. Edumatic: Jurnal Pendidikan Informatika, 8(2), 418–427. https://doi.org/10.29408/edumatic.v8i2.27109

Lachkov, P., Tawalbeh, L., & Bhatt, S. (2022). Vulnerability assessment for applications security through penetration simulation and testing. Journal of Web Engineering, 21(7), 2187–2208. https://doi.org/10.13052/jwe1540-9589.2178

Lazăra, A.-P. (2023). Security testing for e-commerce applications. Journal of Information Systems & Operations Management, 17(1), 45–56.

OWASP Foundation. (2021). OWASP testing guide v4.2. https://owasp.org/www-project-web-security-testing-guide/

Panjaitan, B., Abdurrahman, L., & Mulyana, R. (2022). Menggunakan kontrol annex: Studi kasus data center pemerintah daerah. Jurnal Teknologi dan Sistem Informasi, 10(1), 33–45.

Wicaksono, B., Kusumaningsih, R. Y. R., & Iswahyudi, C. (2020). Pengujian celah keamanan aplikasi berbasis web menggunakan teknik penetration testing dan DAST (Dynamic Application Security Testing). Jurnal Informatika, 8(1), 1–12. http://bagusw.win

Zimmerman, J. (2020). Penetration testing: A hands-on introduction to hacking. No Starch Press.