ANALISIS PERBANDINGAN KEAMANAN APLIKASI *WEB* PADA *PLATFORM E-COMMERCE* STUDI KASUS: SHOPEE, TIKTOK *SHOP* DAN FACEBOOK *MARKETPLACE* MENGGUNAKAN *DYNAMIC APPLICATION SECURITY TESTING* (DAST)

Dina Lestari Lubis, Fidyatun Nisa*, Athiyatul Ulya
Sistem Informasi, Universitas Malikussaleh
Bukit Indah, Blang Pulo, Kec. Muara Satu, Kota Lhokseumawe, Aceh, Indonesia
Fidyatun.nisa@unimal.ac.id

ABSTRAK

Perkembangan pesat *platform e-commerce* telah meningkatkan kebutuhan akan sistem keamanan aplikasi web yang andal untuk melindungi data pengguna dan integritas transaksi. Keamanan aplikasi web menjadi prioritas utama dalam layanan *e-commerce* yang memproses data sensitif dan transaksi pengguna. Kerentanan pada aplikasi web dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mencuri informasi, mengubah data, atau mengganggu layanan. Penelitian ini bertujuan untuk menganalisis dan membandingkan tingkat keamanan tiga *platform e-commerce* terkemuka seperti Shopee, TikTok *Shop*, dan Facebook Marketplace dengan menerapkan pendekatan *Dynamic Application Security Testing* (DAST). Pengujian dilakukan menggunakan alat Wapiti yang berfungsi untuk mengidentifikasi kerentanan keamanan dari sisi *runtime* aplikasi, tanpa perlu mengakses kode sumber. Hasil pengujian menunjukkan bahwa Shopee memiliki tingkat kerentanan yang lebih tinggi dibandingkan TikTok *Shop* dan Facebook *Marketplace*, baik dari segi jumlah kerentanan maupun tingkat keparahan risikonya. TikTok *Shop* dan Facebook *Marketplace* menunjukkan keamanan yang relatif lebih baik dengan temuan kerentanan yang lebih sedikit dan risiko yang lebih rendah. Penelitian ini menegaskan pentingnya pengujian keamanan secara berkala menggunakan pendekatan DAST sebagai langkah preventif dalam menghadapi ancaman siber yang terus berkembang, khususnya pada sektor *e-commerce* yang sangat bergantung pada kepercayaan pengguna.

Kata kunci: *Website, E-Commerce, DAST, Wapiti, Security Testing*

1. PENDAHULUAN

E-commerce atau perdagangan elektronik adalah gabungan dari teknologi, aplikasi, dan kegiatan bisnis yang memungkinkan perusahaan maupun individu sebagai konsumen untuk melakukan transaksi secara digital. Transaksi ini meliputi jual beli barang serta pertukaran informasi yang dilakukan melalui internet, televisi interaktif, situs web (WWW), atau berbagai jaringan komputer lainnya[1].

Platform seperti Shopee, Tiktok *Shop* dan Facebook *Marketplace* menjadi target utama bagi penjahat *cyber*, karena menangani *volume* transaksi begitu besar. Oleh karena itu, penting untuk memiliki sistem keamanan yang kuat dan terus diperbarui untuk menghadapi ancaman-ancaman ini [2].

Metode *Dynamic Application Security Testing* (DAST) merupakan salah satu pendekatan yang dapat digunakan untuk menganalisis celah keamanan pada aplikasi web. Penelitian terdahulu mengenai penerapan *Dynamic Application Security Testing (DAST)* pada aplikasi berbasis Android menunjukkan bahwa metode DAST mampu mengidentifikasi celah keamanan (*vulnerability*) yang tidak terdeteksi oleh SAST. DAST dapat secara otomatis melakukan pengujian terhadap setiap *activity* dalam aplikasi, yang dibuktikan dengan ditemukannya kerentanan pada *activity Insecure Data Storage*, termasuk celah keamanan seperti XSS dan *Database Breach*. Dengan Studi Kasus: *Website* Shopee, Tiktok *Shop* dan Facebook *Marketplace*, penelitian ini diharapkan dapat memanfaatkan hasil temuan studi sebelumnya untuk melakukan analisis lebih mendalam dan spesifik terhadap celah keamanan di Shopee, Tiktok *Shop* dan Facebook *Marketplace*. Peneliti berharap ketiga *platform* tersebut *c*ukup aman terhadap ancaman *cyber*, mengingat fitur transaksi dan data pribadi pengguna yang merupakan isu kritis dalam konteks keamanan *cyber* saat ini [3].

2. TINJAUAN PUSTAKA

2.1. Shopee

Shopee adalah platform *e-commerce* paling populer di Indonesia karena strategi pemasaran yang berhasil, seperti peluncuran *ShopeePay*, pengembangan fitur permainan interaktif baru, toko resmi dari berbagai merek terkenal, layanan gratis ongkir, program *Flash Sale*, Festival Belanja Bulanan, dan komitmen untuk memastikan kualitas situs web dan kepuasan pelanggan. Melalui proses pembayaran yang mudah dan efisien serta sistem logistik yang terintegrasi, Shopee memudahkan pembeli. Shopee juga membuat jual beli lebih mudah. *Platform* Shopee dapat diakses melalui *smartphone*, *desktop*, dan laptop.

2.2. Tiktok *Shop*

TikTok adalah sebuah *platform* media sosial yang berfokus pada video pendek kreatif berbasis

musik, yang diluncurkan oleh perusahaan asal Tiongkok, *ByteDance*, pada tanggal 20 September 2016. TikTok *Shop* bertujuan untuk mendorong minat belanja konsumen dan memperkuat posisinya di pasar digital [4].

2.3. Facebook *Marketplace*

Facebook *Marketplace* resmi diperkenalkan pada 14 Mei 2007. Dengan akses yang mudah, Facebook memfasilitasi masyarakat untuk berkomunikasi dan berinteraksi secara virtual, tanpa harus bertatap muka secara langsung [5]. Dalam konteks ini, komunikasi pemasaran berperan sebagai proses interaksi antara pembeli dan penjual yang bertujuan untuk membantu pengambilan keputusan dalam pemasaran, sekaligus memastikan terjadinya pertukaran yang saling menguntungkan. Proses ini mencakup pertukaran informasi secara dua arah antara semua pihak yang terlibat dalam aktivitas pemasaran [6].

2.4. Website

Website merupakan sebuah aplikasi yang memuat berbagai jenis dokumen multimedia seperti teks, gambar, audio, animasi, dan video, yang diakses melalui protokol HTTP (*Hyper Text Transfer Protocol*).

2.5. Keamanan Informasi

Ada tiga konsep utama, yang dikenal sebagai triad CIA, yang harus dipahami oleh siapa pun yang melindungi sistem informasi: kerahasiaan, integritas, dan ketersediaan [7].

Oleh karena itu, sangat penting bagi kita untuk melindungi komputer atau laptop dengan sistem keamanan dan proteksi yang memadai [8].

2.6. *Cyber Attack*

Cyber Attack (Serangan siber) merupakan aksi di dunia maya yang dapat bersifat ofensif maupun defensif dan berpotensi menimbulkan kerusakan terhadap target yang disasar. Terdapat berbagai jenis serangan siber yang dapat mengancam sebuah situs web, antara lain: SQL *Injection*, *Cross-Site Scripting* (XSS), Selain itu, masih banyak jenis serangan siber lainnya yang dapat membahayakan sistem [9].

2.7. *Dynamic Application Security Testing* (DAST)

DAST (*Dynamic Application Security Testing*) adalah metode pengujian keamanan yang dilakukan melalui antarmuka aplikasi yang terbuka. Teknik ini bertujuan untuk mendeteksi kerentanan pada aplikasi web saat aplikasi sedang dijalankan. DAST sangat efektif untuk mendeteksi kerentanan eksternal, namun kelemahannya terletak pada ketergantungan terhadap keahlian pakar keamanan dalam proses implementasinya, sehingga tingkat efektivitasnya sulit diukur secara konsisten [10].

2.8. Wapiti

Wapiti merupakan perangkat lunak gratis untuk pengujian keamanan web yang berfungsi mendeteksi kerentanan pada aplikasi berbasis web. Program ini menggunakan pendekatan *Black Box*, yaitu dengan tidak memeriksa kode sumber aplikasi, melainkan memindai halaman-halaman web untuk mengidentifikasi skrip dan formulir yang dapat digunakan sebagai titik injeksi data. Alat ini menghasilkan hasil dalam file HTML [11].

a. Kelebihan wapiti:
   - Wapiti mendukung metode serangan menggunakan permintaan HTTP GET dan POST.
   - Memberikan notifikasi ketika terjadi kejanggalan, seperti kesalahan 500 atau waktu tunggu (*timeout*).
   - Pengguna dapat dengan cepat dan mudah mengaktifkan atau menonaktifkan modul-modul serangan.
   - Pemindaian dapat dilakukan bersamaan dengan pelaksanaan serangan secara langsung.
b. Kelemahan Wapiti:
   - Memakan waktu yang lama ketika *scanning*

3. METODE PENELITIAN

3.1. Metode Pengumpulan Data

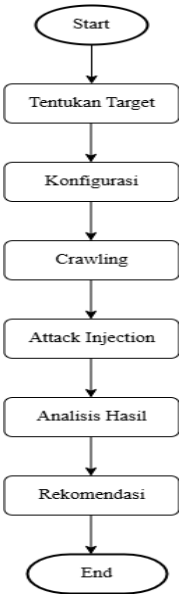
Metode pengumpulan data pada penelitian ini menggunakan metode kualitatif (studi kasus) pada tiga *website E-commerce* yaitu Shopee, Tiktok *shop* dan Facebook *Marketplace*. Metode ini digunakan peneliti dalam mengumpulkan informasi selama penelitian dan pengujian. Metode – metode pengumpulan data sebagai berikut:

a. Studi Literatur
   Peneliti mencari dan menggabungkan teori dari referensi seperti: *E-Book*, Jurnal, Skripsi, yang membahas keamanan aplikasi web, teknik *Dynamic Application Security Testing* (DAST), ancaman celah keamanan dan penelitian terdahulu yang relevan dengan topik keamanan aplikasi web.
b. Observasi
   Metode observasi melibatkan pengamatan langsung terhadap sistem. Mengamati fitur, layanan yang ada pada *website* shopee, tiktok *shop* dan facebook *marketplace*. Setelah itu menyiapkan lingkungan pengujian, melakukan pengujian dengan memindai *website* menggunakan DAST *tools* untuk mendeteksi potensi kerentanan. *Tools* yang akan digunakan adalah wapiti
c. Studi Dokumentasi
   E-commerce memiliki proses yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem, informasi, dan data penting. mengidentifikasi dan melaporkan ancaman keamanan siber. Masing-masing *e-commerce* telah menetapkan kebijakan keamanan dan privasi yang dirancang untuk melindungi data pengguna dan transaksi *online*. Namun, kemampuan implementasi kebijakan tersebut perlu diuji secara

teknis melalui metode *Dynamic Application Security Testing* (DAST) untuk mengidentifikasi potensi celah keamanan pada sisi aplikasi web.

3.2. Skema Pengujian Sistem

Berikut langkah-langkah atau tahapan dalam melakukan pengujian terhadapat penelitian.



Gambar 1. Skema alur pengujan

Langkah-langkah atau alur yang dilakukan pada penelitian ini meliputi:

a. *Start*/Mulai: merupakan tahapan/proses paling awal membuat penelitian
b. Tentukan target: Menentukan URL atau domain dari aplikasi web yang akan diuji keamanannya. Dalam penelitian ini, targetnya yaitu platform Shopee, TikTok *Shop* dan Facebook *Marketplace*.
c. Konfiguasi: Menentukan metode akses, mengatur fotmat hasil, dll
d. *Crawling*: Wapiti akan melakukan proses *crawling* (penelusuran halaman) untuk mengidentifikasititik-titik rentan (*endpoints/form*).
e. *Attack Injection: Tools* akan mengirimkan berbagai *payload* injeksi otomatis (seperti XSS, SQLi, *Command Injection*) ke parameter yang ditemukan saat *crawling*
f. Analisis Hasil: Analisis hasil kerentanan yang terdeteksi berdasarkan jenis kerentanan dan tingkat risiko (tinggi, sedang, rendah).
g. Rekomendasi: Memberikan saran perbaikan berdasarkan hasil analisis keamanan pada *platform* shopee, tiktok *shop* dan facebook *marketplace*
h. *End*/Selesai: Akhiri proses pengujian dan dokumentasikan hasilnya

4. HASIL DAN PEMBAHASAN

Adapun hasil pengujian dari *platform* Shopee, Tiktok *Shop* dan Facebook *Marketplace* tersebut sebagai berikut:

4.1. Shopee

Berdasarkan hasil pemindaian menggunakan Wapiti terhadap situs Shopee (http://shopee.co.id/) dengan metode *Dynamic Application Security Testing* (DAST), ditemukan beberapa kerentanan keamanan seperti gambar dibawah:

Wapiti vulnerability report

Target: http://shopee.co.id/

Date of the scan: Tue, 29 Apr 2025 13:19:46 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	4
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	4
HttpOnly Flag cookie	1
Open Redirect	0
Secure Flag cookie	1
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

Content Security Policy Configuration

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of
Cross Site Scripting (XSS) and data injection attacks.

Vulnerability found in /

Description HTTP Request cURL command line

Gambar 1. Hasil pengujian *platform* shopee

1. *Content security policy* (CSP) *Configuration*
   Kekurangan dalam konfigurasi CSP di Shopee adalah:
   a. *default-src* tidak dikonfigurasi
   b. *script-src* tidak dikonfigurasi
   c. *object-src* tidak dikonfigurasi
   d. *base-uri* tidak dikonfigurasi
2. HTTP *Secure Headers*
   Shopee tidak menetapkan header berikut:
   b. *X-Frame-Options*
   c. *X-XSS-Protection*
   d. *X-Content-Type-Options*
   e. *Strict-Transport-Security*
3. *Httponly Flag Cookie*
   Cookie LOCALE tidak memiliki atribut *HttpOnly*, Ini berarti bisa diakses via *JavaScript*, yang berisiko jika XSS berhasil disisipkan seperti *Cookie* bisa dicuri lewat skrip berbahaya dan potensi pencurian sesi atau pengambilalihan akun.

4. *Secure Flag Cookie*
   Secure Flag adalah atribut pada *cookie* yang memastikan *cookie* hanya dikirim melalui koneksi HTTPS, bukan HTTP. Tanpa *Secure*, *cookie* bisa bocor melalui koneksi tidak aman
   Solusi: Prioritaskan perbaikan CSP dan keamanan *cookie*, serta implementasi lengkap *HTTP Secure Headers*. Lakukan audit keamanan yang lebih mendalam.

4.2. Tiktok *Shop*

Berdasarkan hasil pemindaian menggunakan Wapiti terhadap situs Tiktok *Shop* (http://shop-id.tokopedia.com) dengan metode *Dynamic Application Security Testing* (DAST), ditemukan beberapa kerentanan keamanan seperti gambar dibawah:

Wapiti vulnerability report

Target: http://shop-id.tokopedia.com/

Date of the scan: Thu, 08 May 2025 10:17:59 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	2
HttpOnly Flag cookie	1
Open Redirect	0

Gambar 2. Hasil pengujian *platform* tiktok *shop*

1. *Content security policy* (CSP) *Configuration*
   Pada hasil pengujian ini Tiktok *Shop* tidak mengatur/ mengkonfigurasi *header Content-Security-Policy* dalam HTTP *response*-nya. Ini membuat aplikasi web rentan terhadap serangan seperti *Cross-Site Scripting* (XSS) dan data *injection*.
2. HTTP *Secure Headers*
   Adapun kerentanan yang ditemukan dalam pengujian TikTok *shop*:
   a. X-XSS-*Protection is not set*
   b. X-*Content-Type-Options is not set*
3. HttpOnly Flag Cookie
   HttpOnly adalah atribut keamanan pada *cookie* yang mencegah akses *cookie* tersebut melalui *JavaScript* dari sisi klien (*browser*). Solusi: Fokus pada perbaikan CSP dan implementasi *flag HttpOnly* pada *cookie ttwid*. Pastikan konfigurasi *HTTP Headers* yang tepat.

4.3. Facebook *Marketplace*

Berdasarkan hasil pemindaian menggunakan Wapiti terhadap situs Fecebook *Marketplace* (http://facebook.com/marketplace) dengan metode *Dynamic Application Security Testing* (DAST), ditemukan beberapa kelemahan keamanan seperti gambar dibawah:

Wapiti vulnerability report

Target: https://facebook.com/whitehat

Date of the scan: Tue, 29 Apr 2025 14:04:07 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	3
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

Content Security Policy Configuration

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including

Gambar 3. Hasil pengujian *platform* facebook *marketplace*

1. *Content Security Policy* (CSP) *Configuration*
   Tanpa CSP, skrip *eksternal* dari situs pihak ketiga (yang berbahaya) bisa dijalankan di *browser* pengguna. Ini merupakan kerentanan konfigurasi yang serius karena membiarkan *browser* pengguna menerima konten dari sumber tak terpercaya.
2. *HTTP Secure Headers*
   Berdasarkan hasil scan, ada tiga *HTTP header* penting yang tidak dikonfigurasi, yaitu:
   a. *X-Frame-Options is not set*
   b. X-*XSS-Protection is not set*
   c. *X-Content-Type-Options is not set*
   Solusi: Perbaiki konfigurasi CSP dan pastikan implementasi yang benar dari semua *HTTP Secure Headers* yang relevan.

4.4. Tingkat Risiko Keamanan

Dalam pengujian dengan metode DAST (*Dynamic Application Security Testing*) dengan *tools* wapiti dengan bantuan *command* tambahan dalam format JSON, hasil scan akan menunjukkan kerentanan yang ditemukan. Analisis tingkat risiko

keamanan pada penelitian ini bertujuan untuk menganalisis tingkat risiko keamanan dari kerentanan yang terdeteksi pada *platform* Shopee, Tiktok *Shop* dan Facebook *Marketplace*. Adapun analisis tingkat risiko keamanan dapat dilihat seperti tabel dibawah:

Tabel 1. Analisis tingkat risiko keamanan

Platform	**Jumlah Kerentanan**	**Kerentanan Utama**	**Tingkat Risiko**
Shopee	10	*Content Security Policy Configuration (4), HTTP Secure Headers (4), HttpOnly Flag Cookie (1), Secure Flag Cookie (1)*	*Low (Level* 1) Risiko kecil, dengan kemungkinan kecil terjadinya serangan dan dampak yang terbatas. Meliputi kebocoran informasi, kesalahan konfigurasi, dan kurangnya beberapa langkah keamanan
Tiktok *Shop*	4	*Content Security Policy Configuration (1), HTTP Secure Headers (2), HttpOnly Flag Cookie (1)*	*Low (Level* 1) Risiko kecil, dengan kemungkinan kecil terjadinya serangan dan dampak yang terbatas. Meliputi kebocoran informasi, kesalahan konfigurasi, dan kurangnya beberapa langkah keamanan
Facebook *Marketplace*	4	*Content Security Policy Configuration (1), HTTP Secure Headers (3),*	*Low (Level* 1) Risiko kecil, dengan kemungkinan kecil terjadinya serangan dan dampak yang terbatas. Meliputi kebocoran informasi, kesalahan konfigurasi, dan kurangnya beberapa langkah keamanan

Berdasarkan Tabel 1, analisis tingkat risiko menunjukkan kerentanan utama pada *platform* shopee, tiktok *shop* dan facebook *marketplace* yang terdeteksi hampir sama, hanya berbeda jumlah kerentanannya. Berdasarkan jumlah kerentanan, dapat mempengaruhi tingkat risiko keamanan. Berikut tingkat risiko keamanan pada:

1. Shopee
   Berdasarkan hasil pengujian keamanan Pada *platform* Shopee menggunakan *tools* wapiti dengan bantuan *command* tambahan dalam format JSON, diketahui bahwa semua kerentanan yang teridentifikasi berada pada Level 1, yang dikategorikan sebagai tingkat risiko rendah (*low*). Walaupun kerentanannya berada pada tingkat rendah, hal ini tidak boleh diabaikan sepenuhnya. Shopee tetap perlu melakukan langkah-langkah perbaikan sebagai bagian dari penerapan prinsip "*defense in depth*" atau pertahanan berlapis.
2. Tiktok *shop*
   Berdasarkan hasil pengujian keamanan terhadap *platform* TikTok *Shop* dengan menggunakan tools wapiti dan tambahan *command* JSON, ditemukan bahwa seluruh kerentanan yang teridentifikasi berada pada Level 1, yang berarti termasuk dalam kategori risiko rendah (*low*). Meskipun tingkat risiko kerentanannya tergolong rendah, tetap penting bagi pengelola sistem untuk menindaklanjuti temuan ini dengan langkah perbaikan yang sesuai. Dengan menerapkan perbaikan terhadap celah-celah kecil tersebut, TikTok *Shop* akan semakin memperkuat sistem keamanannya dan mengurangi kemungkinan kerentanan berkembang menjadi masalah yang lebih serius di kemudian hari.
3. Facebook *Marketplace*
   Berdasarkan hasil pengujian keamanan terhadap *platform* Facebook *Marketplace* dengan menggunanakan wapiti yang dilengkapi dengan tambahan *command* JSON, diketahui bahwa seluruh kerentanan yang terdeteksi dikategorikan dalam Level 1, yang berarti berada pada tingkat risiko rendah. Dengan melakukan perbaikan secara proaktif terhadap kerentanan *minor* yang ada, Facebook *Marketplace* dapat memastikan bahwa sistem tetap terlindungi dari potensi penyalahgunaan serta mempertahankan kepercayaan pengguna terhadap layanan yang mereka gunakan.

4.5. Analisis Perbandingan Keamanan Masing-Masing *Platform*

Setelah dilakukan pengujian keamanan menggunakan metode *Dynamic Application Security Testing* (DAST) dengan bantuan *tools* Wapiti, sejumlah kerentanan berhasil diidentifikasi pada masing-masing *platform e-commerce*, yaitu Shopee, TikTok *Shop*, dan Facebook *Marketplace*. Dengan mengetahui jenis-jenis kerentanan beserta level risikonya, kita dapat melakukan analisis komparatif terhadap tingkat keamanan dari ketiga *platform e-commerce* tersebut. Perbandingan ini memberikan wawasan mengenai bagaimana setiap *platform* menangani aspek keamanan web aplikasinya. Hasil perbandingan tersebut disajikan dalam Tabel 2, yang memperlihatkan perbedaan serta kesamaan dalam aspek kerentanan dan risiko keamanan pada Shopee, TikTok *Shop*, dan Facebook *Marketplace*.

Tabel 2. Analisis perbandingan keamanan

Shopee	**Tiktok *Shop***	**Facebook *Marketplace***
Kurang optimal pada Keamanan CSP & HTTP *Headers* (banyak kerentanan terdeteksi). *Cookie Security* juga Kurang optimal (isu *HttpOnly* & *Secure flag*).	Keamanan CSP & HTTP *Headers* Lebih baik dari Shopee, mirip Facebook *Marketplace* (jumlah kerentanan). *Cookie Security* menunjukkan Ada isu *HttpOnly* pada *cookie* tertentu.	Keamanan CSP & HTTP *Headers* Lebih baik dari Shopee (lebih sedikit kerentanan). *Cookie Security* Tampak baik (tidak ada kerentanan terdeteksi). Aspek lain tidak diketahui.
Potensi risiko XSS lebih tinggi karena masalah CSP dan *HttpOnly cookie*. Ancaman lain (*Malware*, DDoS, *Social Engineering*) tidak terdeteksi	Risiko XSS mirip shopee karena isu CSP dan *HttpOnly cookie*. Ancaman lain tidak terdeteksi	Risiko XSS lebih rendah tetapi tetap ada karena isu CSP. Ancaman lain tidak terdetesi
Tingkat keamanan rendah. Banyaknya kerentanan pada kebijakan keamanan dasar dan konfigurasi yang tidak aman menjadikannya *platform* yang memerlukan peningkatan signifikan diberbagai aspek teknis. Berdasarkan hasil pengujian dengan Wapiti.	Tingkat keamanan sedang. Meskipun lebih baik dari Shopee, masih ada beberapa kerentanan penting yang perlu ditangani, khususnya dalam manajemen *cookie* yang aman dan penguatan *header*.	Tingkat keamanan tinggi. Posturnya menunjukkan perhatian terhadap perlindungan sesi dan penggunaan kebijakan yang tepat, menjadikannya *platform* dengan keamanan paling kuat di antara ketiganya.

Berdasarkan hasil pengujian dan analisis perbandingan keamanan pada Tabel 2 di atas, pada *platform* Shopee, Tiktok *Shop*, dan Facebook *Marketplace* menunjukkan bahwa:

a. Facebook *Marketplace* memiliki sistem keamanan paling aman, diikuti oleh
b. TikTok *Shop* yang berada di posisi menengah, sementara
c. Shopee menunjukkan keamanan paling lemah dan memerlukan pembenahan serius terutama dalam penerapan CSP, *header* dan kebijakan *cookie*.

4.6. Kinerja Metode *Dynamic Application Security Testing* (DAST)

Kinerja DAST terhadap kerentanan yang terdeteksi sebagai berikut:

Alat DAST menganalisis *Header* HTTP yang dikirim oleh server. Ketidakadaan atau konfigurasi yang salah dari *header* – *header* ini akan langsung terdeteksi dalam respon HTTP. DAST juga efektif dalam mengevaluasi atribut *cookie* yang ditetapkan oleh server dalam *header set cookie*. Ketidakadaan *flag HttpOnly dan Secure* akan mudah teridentifikasi. Secara keseluruhan, metode dast kemungkinan berkontribusi signifikan dalam mengidentifikasi dan mengevaluasi celah keamanan terkait konfigurasi keamanan dasar (CSP, HTTP *Headers*, *Cookie Security*) pada ketiga *platform* tersebut, seperti yang terlihat pada hasil pengujian wapiti. Kemampuannya untuk menganalisis *respons* http secara dinamis sangat cocok untuk mendeteksi masalah – masalah ini.

4.7. Rekomendasi Perbaikan

Berdasarkan hasil pengujian keamanan menggunakan alat DAST seperti Wapiti, ditemukan sejumlah kerentanan yang berpotensi membahayakan integritas, kerahasiaan, dan ketersediaan sistem yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan serangan terhadap aplikasi web. Oleh karena itu, untuk meningkatkan keamanan pada *platform* shopee, tiktok *shop* dan facebook *marketplace* diperlukan langkah-langkah perbaikan yang tepat guna memitigasi risiko yang ditimbulkan. Adapun rekomendasi perbaikan untuk masing-masing jenis kerentanan adalah sebagai berikut:

1. Shopee:
   a. *Tambahkan konfigurasi Content Security Policy* (CSP) *Header* untuk mencegah serangan injeksi skrip
   b. Sertakan *HttpOnly* ke dalam HTTP *Header Response*, sehingga *cookie* tidak dapat diakses melalui skrip klien
   c. Terapkan *Header Strict-Transport-Security* untuk memastikan semua komunikasi menggunakan HTTPS
2. Tiktok Shop:
   a. *Tambahkan konfigurasi Content Security Policy* (CSP) *Header* untuk mencegah serangan injeksi skrip
   b. Tambahkan *Header X-Content-Type-Options* digunakan guna mencegah serangan MIME *Sniffing*
   c. Mengatur *header X-XSS-Protection* menjadi X-XSS-*Protection*: 1; *mode=block*
   d. pastikan bahwa *flag Http Only* disetel untuk semua *cookie*
3. Facebook *Marketplace:*
   a. *Tambahkan konfigurasi Content Security Policy* (CSP) *Header* untuk mencegah serangan injeksi skrip.
   b. Tambahkan *Header X-Content Type Options* digunakan guna mencegah serangan MIME *Sniffing*
   c. Gunakan *X-XSS-Protection*: 1; *mode=block* untuk melindungi *website* dari serangan XXS
   d. Menggunakan *Content-Security-Policy:frame-ancestors 'none'*; yang dapat mencegah domain apapun membuat *framing*

5. KESIMPULAN DAN SARAN

Hasil pengujian keamanan menggunakan metode *Dynamic Application Security Testing* (DAST) dengan *tools* Wapiti pada *platform e-commerce* seperti Shopee, TikTok *Shop*, dan Facebook *Marketplace* mengungkapkan adanya kerentanan yang signifikan pada lapisan konfigurasi keamanan dasar aplikasi web. Kerentanan yang terdeteksi pada shopee: *Content Security Policy Configuration (4), HTTP Secure Headers (4), HttpOnly Flag Cookie (1), Secure Flag Cookie (1)***.** Adapun pada Tiktok *Shop: Content Security Policy Configuration (1), HTTP Secure Headers (2), HttpOnly Flag Cookie (1)* dan pada Facebook *Marketplace: Content Security Policy Configuration (1), HTTP Secure Headers (3)***.** Berdasarkan hasil pengujian, Facebook *Marketplace* memiliki sistem keamanan paling aman, diikuti oleh TikTok *Shop* yang berada di posisi menengah, sementara Shopee menunjukkan keamanan paling lemah dan memerlukan pembenahan serius terutama dalam penerapan CSP, *header* dan kebijakan *cookie*. Lakukan langkah- langkah rekomendasi perbaikan untuk meningkatkan keamanan pada *platform* shopee, tiktok *shop* dan facebook *marketplace.*

DAFTAR PUSTAKA

[1] N. Yuni Pratiwi *Et Al.*, "Membantu Umkm Dalam Memasarkan Produk Di Marketplace Shopee Dan Tokopedia Author 1)," Vol. 2, No. 2, Pp. 135–142, 2021.

[2] D. M. Asviara, E. Jerliana, F. I. Aditya, A. R. Pratama, and R. T. Nugroho, "Analisis Efektivitas Sistem Manajemen Keamanan Di Perusahaan Shopee Dalam Meningkatkan Proteksi Data," vol. 2, no. 7, pp. 735–741, 2024.

[3] B. Wicaksono, R. Yuliana Rachmawati Kusumaningsih, C. Iswahyudi, J. Informatika, and I. Akprind, "Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik Penetration Testing Dan Dast (Dynamic Application Security Testing)," vol. 8, no. 1, 2020, [Online]. Available: http://bagusw.win.

[4] S. D. Yanti, S. Astuti, and C. Safitri, "Pengaruh Pengalaman Belanja Online Dan Kepercyaan Terhadap Minat Beli Ulang Di Tiktok Shop (Studi Kasus Mahasiswa Fkip Uhamka 2018)," *Jurnal EMT KITA*, vol. 7, no. 1, pp. 47–61, Jan. 2023, doi: 10.35870/emt.v7i1.728.

[5] U. Adab and D. Dakwah, "Analisis Komunikasi Primer Pada Fitur Marketplace Di Media Sosial Facebook Skripsi Diajukan Untuk Memenuhi Syarat-Syarat Guna Memperoleh gelar (S.Sos)," 2024.

[6] A. Amir, A. Gani, M. Sufri, and M. H. Syahnur, "Strategi Komunikasi Pemasaran Bisnis dan Online dalam Meningkatkan Penjualan Pada Jejaring Media Sosial, Facebook Marketplace," *Center of Economic Student Journal*, vol. 6, no. 3, pp. 2621–8186, 2023, doi: 10.56750/csej.v6i3.622.

[7] "Keamanan Siber (Cyber Security) - Google Books." Accessed: May 16, 2025. [Online]. Available: https://www.google.co.id/books/edition/Keamanan_Siber_Cyber_Security/k3lSEQAAQBAJ?hl=id&gbpv=0

[8] "Jaringan dan Komunikasi Data - Fidyatun Nisa, Yonky Pernando, Ertie Nur Hartiwati, Faramita Dwitama, Gubtha Mahendra Putra - Google Books." Accessed: Dec. 07, 2024. [Online]. Available: https://books.google.co.id/books?hl=en&lr=&id=7f4xEQAAQBAJ&oi=fnd&pg=PP1&dq=info:zVeytxNCSv0J:scholar.google.com&ots=HyTkZGWLNX&sig=NGdTeOm0su7WJaVGKLliYrg5Bf8&redir_esc=y#v=onepage&q&f=false

[9] S. Andriyani, M. Fajar Sidiq, and B. Parga Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar," 2023.

[10] A. Elanda and R. Lintang Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada Stmik Rosma Dengan Menggunakan Owasp Top 10," 2021

[11]J. Shahid, M. K. Hameed, I. T. Javed, K. N. Qureshi, M. Ali, and N. Crespi, "A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions," *Applied Sciences (Switzerland)*, vol. 12, no. 8, Apr. 2022, doi: 10.3390/app12084077