JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i3.9900

ANALISIS KERENTANAN INSECURE DIRECT OBJECT REFERENCE PADA PENYEDIA LAYANAN SOCIAL MEDIA MARKETING BERBASIS WEBSITE

Ilham Arif Farabi[1], Purwantoro[2], Susilawati Sobur[3]

[1,2,3]Universitas Singaperbangsa Karawang; Jl. HS. Ronggo Waluyo, Puseurjaya, Telukjambe Timur, Karawang; 0267641177

Keywords:
Insecure Direct Object Reference; IDOR; Broken Access Control; Parameter Tampering; Web Application Security.

Corespondent Email:
ilhamfarabi33@gmail.com

Abstrak. Penelitian ini membahas analisis kerentanan *Insecure Direct Object Reference (IDOR)* pada *platform* penyedia layanan *Social Media Marketing (SMM)* berbasis *website*. Permasalahan utama yang dikaji adalah potensi kelemahan kontrol akses pada endpoint *API* atau *URL* yang menggunakan parameter objek secara langsung. Penelitian menggunakan metode *Action Research* dengan tahapan *diagnosing*, *action planning*, *action taking*, *evaluating*, dan *learning*. Pengujian dilakukan melalui *pendekatan black-box testing* dengan teknik *parameter tampering* menggunakan dua akun uji dan bantuan *tools* Reqable untuk melakukan *packet interception*. Hasil penelitian menunjukkan bahwa sebagian besar fitur tidak memiliki indikasi kerentanan *IDOR*, namun ditemukan celah pada fitur *Ticket Support*, khususnya *endpoint* /pages/ticket_open?id=. Ketika parameter *ID* tiket dimodifikasi, sistem menampilkan pesan kesalahan tetapi masih membocorkan sebagian isi percakapan tiket. Kerentanan bersifat *read-only IDOR* karena pengguna tidak dapat mengirim atau mengubah pesan tiket milik pengguna lain. Perbaikan dilakukan dengan menambahkan mekanisme *redirect* dan *exit* pada kondisi akses tidak sah sehingga eksekusi program berhenti sepenuhnya. Setelah perbaikan diterapkan, respons server berubah dari 200 OK menjadi 302 *Redirect*, menunjukkan bahwa kontrol akses telah berjalan lebih efektif.

Abstract. *This study discusses the analysis of Insecure Direct Object Reference (IDOR) vulnerabilities in a website-based Social Media Marketing (SMM) service provider platform. The main problem is the potential weakness of access control on API endpoints and URLs that use direct object parameters. The Action Research method was applied with stages of diagnosing, action planning, action taking, evaluating, and learning. Testing was conducted using a black-box testing approach with parameter tampering techniques, involving two test accounts and Reqable tool for packet interception. Results show that most features did not indicate IDOR vulnerabilities. However, a vulnerability was found in the Ticket Support feature, particularly on the /pages/ticket_open?id= endpoint. When the ticket ID parameter was modified, the system displayed an error message but still leaked part of the ticket conversation. The identified vulnerability was categorized as read-only IDOR because the user could not send or modify messages in another user's ticket. The mitigation was implemented by adding a redirect mechanism followed by an exit function when unauthorized access was detected. After the fix, the server response changed from 200 OK to 302 Redirect, indicating that the access control mechanism had become more effective.*

1. PENDAHULUAN

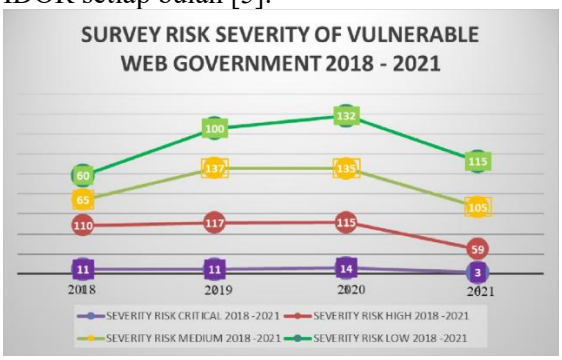
Layanan Social Media Marketing (SMM) kini menjadi salah satu strategi utama dalam menjangkau audiens secara luas di era digital, khususnya di Indonesia yang mengalami lonjakan signifikan dalam penggunaan media sosial. Laporan DataReportal Digital 2025: Indonesia mencatat 143 juta identitas pengguna media sosial aktif, setara 50,2% dari total populasi 285 juta jiwa pada Januari 2025 [1].

Gambar 1. Pengguna Media Sosia di Indonesia

Berbagai studi menunjukkan bahwa media sosial berperan aktif dalam pembentukan persepsi dan keputusan pembelian konsumen. Media sosial diposisikan sebagai sumber informasi yang efektif dan kredibel bagi konsumen sebelum melakukan pembelian, serta berdampak nyata pada keputusan pembelian [2]. Faktor jejaring sosial, pengaruh sosial, dan konten pada media sosial menunjukkan keterkaitan yang positif dengan perilaku pembelian konsumen.

Di sisi lain, percepatan adopsi layanan digital tidak selalu diikuti dengan prioritas keamanan aplikasi. Salah satu isu paling dominan pada aplikasi web modern adalah Broken Access Control. Laporan OWASP Top 10 menyebutkan bahwa 94% aplikasi web yang diuji rentan terhadap Broken Access Control, termasuk kerentanan Insecure Direct Object Reference (IDOR), yang menempati urutan pertama dalam kategori risiko keamanan [3].

IDOR merupakan bentuk kelemahan otorisasi yang terjadi ketika aplikasi secara langsung mengekspos referensi objek terhadap sumber daya internal, seperti file atau catatan dalam database [4]. Praktik ini memungkinkan pengguna memodifikasi parameter pada URL sehingga dapat memperoleh akses ke informasi milik pengguna lain tanpa otorisasi yang semestinya. HackerOne mencatat bahwa IDOR merupakan salah satu kerentanan yang paling sering ditemukan dengan lebih dari 200 laporan IDOR setiap bulan [5].



Gambar 2. Survey BSSN terhadap 70 web pemerintah

Di tingkat nasional, survei BSSN terhadap 70 website pemerintah pada periode 2018–2021 mencatat 1.289 kerentanan dengan tren peningkatan yang signifikan dari tahun ke tahun [6]. Platform SMM yang menjadi objek penelitian ini (SMM-XYZ) memiliki riwayat insiden celah keamanan yang menyebabkan kerugian finansial hingga Rp1.148.572, akibat selisih harga pada 70 pesanan antara Harga Order dengan Harga Server.

Platform SMM umumnya menangani informasi penting berupa data akun pengguna, riwayat pesanan, detail transaksi, serta integrasi dengan layanan pihak ketiga melalui API. Apabila kerentanan IDOR terjadi pada sistem semacam ini, dampak yang ditimbulkan tidak hanya berupa kebocoran data pribadi, tetapi juga berpotensi menyebabkan manipulasi transaksi, penyalahgunaan layanan, hingga kerugian finansial.

Berbagai penelitian sebelumnya telah mengkaji IDOR pada aplikasi pendidikan dan LMS, namun belum menyentuh konteks layanan komersial digital seperti platform SMM yang memiliki karakteristik teknis berbeda [7][8]. Penelitian ini bertujuan mengidentifikasi dan menganalisis kerentanan IDOR pada platform SMM-XYZ menggunakan metode black-box testing dengan pendekatan Action Research, sekaligus memberikan penanganan langsung berupa perbaikan kode

2. TINJAUAN PUSTAKA

2.1 Keamanan Aplikasi Web

Keamanan aplikasi web merupakan aspek krusial dalam pengembangan sistem berbasis web. Keamanan aplikasi web merupakan

komponen utama dari setiap bisnis yang berbasis web [9]. Setiap aplikasi website harus selalu menjaga keamanannya agar proses bisnis dapat berjalan aman dari ancaman yang dapat disalahgunakan

2.2 Insecure Direct Object Reference

IDOR merupakan bentuk spesifik dari kerentanan Broken Access Control yang memungkinkan pengguna mengakses objek tertentu dalam suatu sistem hanya dengan memodifikasi parameter pada URL atau permintaan API, tanpa melalui proses otorisasi yang memadai [10]. IDOR merupakan kerentanan keamanan yang terjadi ketika aplikasi mengizinkan pengguna mengakses suatu objek secara langsung tanpa memeriksa atau memvalidasi input yang dimasukkan oleh pengguna tersebut [11].

2.3 Penetration Testing

Penetration testing merupakan metode pengujian keamanan dengan cara mensimulasikan serangan siber untuk mengidentifikasi dan mengeksploitasi kerentanan yang ada [13]. Pendekatan black-box testing dilakukan tanpa akses ke kode sumber aplikasi, merepresentasikan sudut pandang penyerang murni yang mengandalkan teknik manipulasi input dan output [14].

2.4 Parameter Tampering

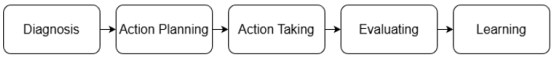
Parameter tampering dilakukan dengan memanipulasi parameter yang dikirim antara klien dan server untuk mengubah data aplikasi, seperti kredensial pengguna, izin akses, harga produk, atau kuantitas [15]. Dalam kaitannya dengan penelitian ini, parameter tampering menjadi dasar teknis yang menjelaskan bagaimana kerentanan IDOR dapat dieksploitasi dengan memodifikasi parameter yang merujuk langsung ke objek internal seperti id, order_id, atau ticket_id.

2.5 Action Research

Action Research adalah pendekatan penelitian yang menggabungkan tindakan langsung di lapangan dengan proses evaluasi. Action Research menekankan pentingnya kolaborasi antara teori dan praktik, di mana peneliti dapat bekerja sama untuk menyelesaikan permasalahan nyata yang dihadapi di lapangan [16]. Metode ini memiliki lima tahapan: Diagnosing, Action Planning, Action Taking, Evaluating, dan Learning.

3. METODE PENELITIAN

3.1 Metodologi Action Research



Gambar 3. Tahapan Action Research

Penelitian ini menggunakan pendekatan Action Research yang terdiri dari lima tahapan utama, yaitu: (1) Diagnosing, (2) Action Planning, (3) Action Taking, (4) Evaluating, dan (5) Learning. Pemilihan metode ini didasarkan pada fleksibilitasnya untuk terlibat secara langsung dan berkelanjutan dalam setiap tahapan, mulai dari identifikasi permasalahan keamanan hingga penerapan tindakan perbaikan.

3.2 Objek Penelitian

Objek penelitian ini adalah kerentanan IDOR pada platform SMM-XYZ, sebuah layanan Social Media Marketing berbasis web yang beroperasi di Indonesia. Platform ini menyediakan layanan peningkatan interaksi (likes, followers, views) di berbagai media sosial (Instagram, TikTok, Facebook, dll.). Fokus utama adalah pada parameter URL dari platform SMM-XYZ yang mungkin rentan terhadap celah keamanan IDOR.

3.3 Tahapan Penelitian

Tahap Diagnosing bertujuan mengidentifikasi kondisi awal platform SMM-XYZ terkait potensi IDOR melalui pemetaan endpoint API dan parameter URL yang mengandung potensi objek langsung. Tahap Action Planning menyusun rencana pengujian penetrasi terhadap parameter yang teridentifikasi, menentukan skenario uji coba, alat bantu (Reqable), dan batasan pengujian. Tahap Action Taking mengimplementasikan skenario pengujian yang dipilih. Tahap Evaluating membandingkan perilaku sistem terhadap permintaan sah dan yang dimodifikasi. Tahap Learning menyimpulkan hasil dan menerapkan perbaikan pada kode sumber.

3.4 Skenario Pengujian

Berdasarkan panduan OWASP WSTG [12], dua skenario pengujian dirancang dan diterapkan:

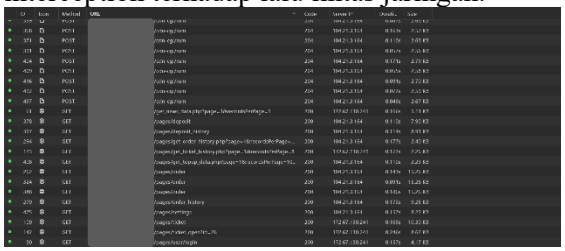
1. Skenario Uji 1 – Akses Objek Tanpa Autentikasi: Pengujian dilakukan dengan mengakses endpoint detail tiket (/pages/ticket_open?id=26) setelah pengguna melakukan logout dari sistem.
2. Skenario Uji 2 – Prediksi ID / ID Enumeration: Pengujian dilakukan dengan memodifikasi nilai parameter id secara bertahap (dari id=26 milik akun pertama menjadi id=27 milik akun kedua) untuk mengakses tiket yang bukan milik pengguna.

Seluruh pengujian dilakukan menggunakan dua akun uji dengan pendekatan non-destructive (tidak merusak sistem yang sedang berjalan).

4. HASIL DAN PEMBAHASAN

4.1 Diagnosing: Identifikasi Endpoint

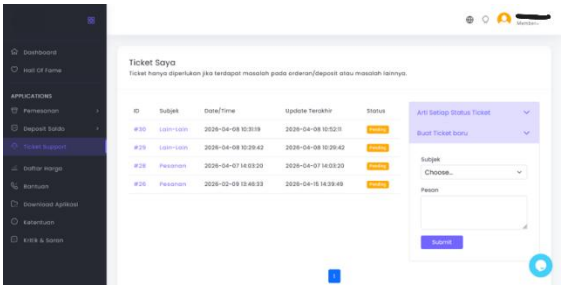
Observasi langsung dilakukan terhadap seluruh fitur website SMM-XYZ menggunakan tools Reqable untuk melakukan packet interception terhadap lalu lintas jaringan.



Gambar 4. Packet Interception menggunakan Reqable

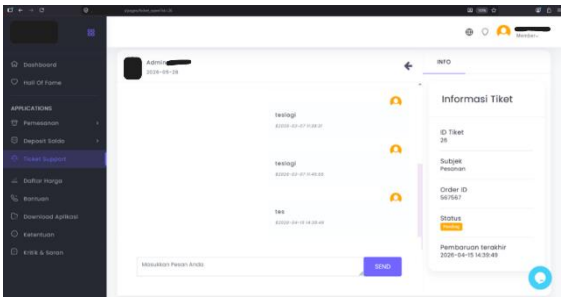
Fokus utama observasi diarahkan pada fitur yang melibatkan pertukaran data transaksional: (1) Pemesanan layanan, (2) Pengisian saldo, (3) Pengelolaan Ticket Support, (4) Ubah password, (5) Order History, dan (6) Deposit History.

Hasil observasi menunjukkan bahwa sebagian besar fitur menggunakan metode POST dengan parameter pada body request tanpa referensi objek langsung pada URL, sehingga tidak mengindikasikan potensi IDOR. Namun, ditemukan satu pengecualian pada fitur Pengelolaan Ticket Support, khususnya halaman detail percakapan tiket.



Gambar 5. Halaman Ticket Support

Akses ke detail tiket dilakukan melalui endpoint /pages/ticket_open dengan menyertakan parameter id pada query URL, seperti id=30. Hal ini menunjukkan bahwa akses terhadap data tiket bergantung pada nilai parameter id yang dapat berpotensi dimanipulasi. Kondisi ini mengindikasikan adanya potensi kerentanan IDOR apabila tidak disertai dengan validasi otorisasi yang memadai.



Gambar 6. Halaman Obrolan Tiket dengan endpoint /pages/ticket_open?id=

4.2 Action Planning: Rencana Pengujian

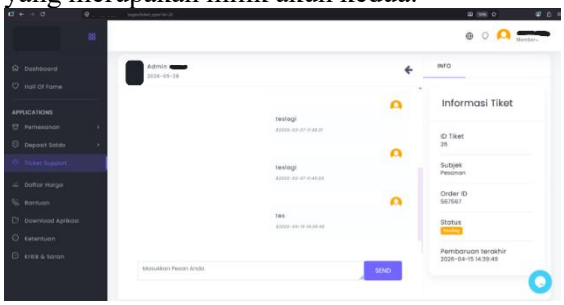
Berdasarkan hasil diagnosing, fokus pengujian diarahkan pada endpoint /pages/ticket_open?id= yang menggunakan parameter id sebagai referensi objek langsung. Teknik parameter tampering dipilih karena sesuai dengan karakteristik kerentanan IDOR. Pengujian akan dilakukan menggunakan dua akun uji (akun pertama dan akun kedua) untuk melakukan pengujian dengan lingkungan yang aman.

4.3 Action Taking: Pelaksanaan Pengujian

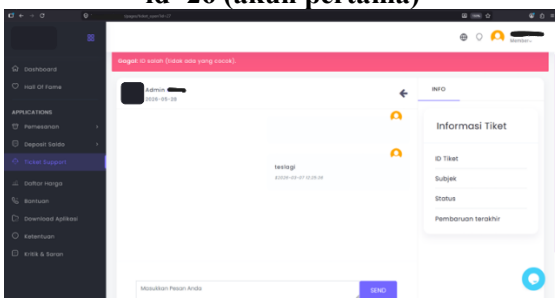
Pada Skenario Uji 1 (Akses Tanpa Autentikasi), setelah mendapatkan URL endpoint tiket (/pages/ticket_open?id=26), pengguna melakukan logout dari sistem dan mengakses endpoint tersebut secara langsung tanpa sesi autentikasi. Request yang dikirim mengalami redirect ke beberapa halaman hingga berakhir di /pages/landing.html. Dengan demikian, akses langsung ke endpoint tanpa

autentikasi tidak menampilkan data tiket, sehingga tidak ditemukan celah IDOR pada skenario ini.

Pada Skenario Uji 2 (Prediksi ID / ID Enumeration), pengujian dimulai dari ID tiket yang valid milik akun pertama (id=26), kemudian dilakukan modifikasi menjadi id=27 yang merupakan milik akun kedua.



Gambar 7. Halaman Detail Tiket dengan id=26 (akun pertama)



Gambar 8. Halaman Detail Tiket dengan id=27 (akun kedua)

Ketika parameter URL dimodifikasi dari id=26 menjadi id=27, sistem menampilkan pesan error "Gagal: ID salah (tidak ada yang cocok)". Namun, meskipun terdapat pesan error tersebut, sebagian isi percakapan tiket (misalnya pesan "teslagi") tetap terlihat di halaman. Panel informasi tiket di sisi kanan tidak menampilkan detail (kosong), mengindikasikan inkonsistensi dalam penanganan akses data.

Dilakukan pula percobaan pengiriman pesan ke tiket yang bukan milik pengguna. Hasilnya menunjukkan sistem tidak memproses pengiriman pesan, sehingga pesan tidak berhasil dikirim. Hal ini menandakan bahwa meskipun terdapat kelemahan pada sisi kontrol akses baca (read access), sistem masih memiliki pembatasan pada sisi aksi perubahan data (write access). Dengan kata lain, kerentanan yang ditemukan bersifat read-only IDOR.

4.4 Evaluating: Evaluasi Hasil Pengujian

Hasil evaluasi menunjukkan bahwa endpoint detail tiket pada website SMM-XYZ terbukti rentan terhadap IDOR berbasis parameter tampering yang bersifat read-only.

Skenario Pengujian	Kondisi Pengujian	Hasil yang Diharapkan	Hasil Aktual	Status Kerentanan
Akses objek tanpa autentikasi	Pengguna mengakses detail tiket setelah logout / tanpa sesi login aktif	Sistem menolak akses dan menampilkan respons tidak terotorisasi (401/403 atau halaman login)	Data tiket tidak ditampilkan, sistem melakukan redirect ke halaman lain	Tidak ditemukan celah IDOR tanpa autentikasi
Prediksi ID / ID Enumeration	User A mencoba membuka tiket milik User B dengan mengubah nilai parameter id	Sistem menolak akses sepenuhnya dan tidak menampilkan data tiket apa pun	Sistem menampilkan pesan error, tetapi sebagian isi percakapan tiket milik pengguna lain tetap terlihat	Ditemukan celah IDOR pada akses baca data

Tabel 1. Hasil Pengujian Kerentanan

Walaupun sistem telah mencoba memberikan pesan kesalahan dan membatasi aksi perubahan data, kontrol akses yang diterapkan belum efektif karena masih memungkinkan terjadinya kebocoran sebagian data milik pengguna lain.

Analisis kode sumber menunjukkan bahwa penanganan akses tidak sah hanya sebatas menampilkan pesan kesalahan tanpa menghentikan keseluruhan proses eksekusi program. Akibatnya, kode selanjutnya tetap dijalankan dan merender sebagian data tiket, sehingga informasi sensitif tetap terlihat. Blok kode yang bermasalah Adalah:

```
} else {
    $msg_type = "error";
    $msg_content = "<b>Gagal:</b> ID
    salah...";
}
```

Temuan ini memperlihatkan bahwa validasi autentikasi saja tidak cukup; aplikasi juga harus menerapkan pemeriksaan otorisasi berbasis kepemilikan objek pada setiap request yang mengandung parameter identifikasi, disertai penghentian eksekusi program secara eksplisit.

4.5 Learning: Perbaikan dan Mitigasi

Analisis kode sumber menunjukkan bahwa penanganan akses tidak sah hanya sebatas menampilkan pesan kesalahan tanpa menghentikan keseluruhan proses eksekusi program. Akibatnya, kode selanjutnya tetap dijalankan dan merender sebagian data tiket, sehingga informasi sensitif tetap terlihat. Blok kode yang bermasalah Adalah:

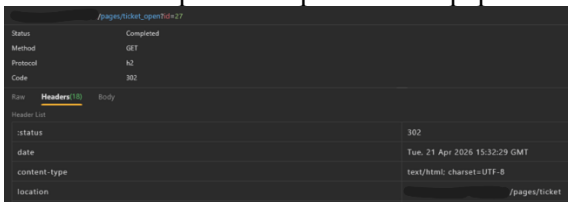
Sebagai langkah perbaikan, dilakukan perubahan mekanisme penghentian proses pada kondisi ketika validasi kepemilikan objek tidak terpenuhi. Blok penanganan error yang semula hanya menampilkan pesan kesalahan diganti dengan perintah redirect ke halaman tiket utama disertai fungsi exit untuk menghentikan seluruh alur eksekusi program:

```
} else {
    header("Location:".$cfg_baseurl."pages/
    ticket");
    exit;
}
```

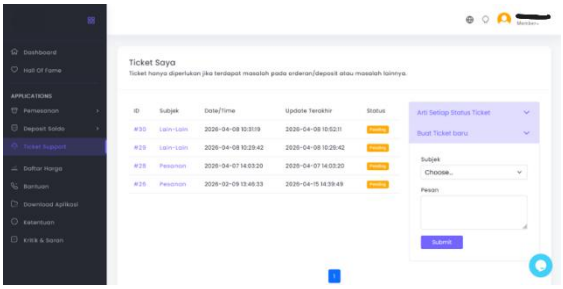
Pengujian ulang pasca-perbaikan menunjukkan perbedaan yang signifikan. Sebelum perbaikan, server merespons dengan status 200 OK dan menampilkan isi tiket milik pengguna lain.

Gambar 9. Response Code Sebelum Diperbaiki (HTTP 200 OK)

Setelah perbaikan diterapkan, server memberikan respons 302 Found dan secara otomatis mengalihkan pengguna ke halaman utama tiket tanpa menampilkan data apapun.



Gambar 10. Response Code Setelah diperbaiki (HTTP 302 Redirect)



Gambar 11. Halaman setelah Redirect ID Tiket yang Tidak Sesuai

Perbedaan status kode HTTP antara 200 OK dan 302 Redirect menjadi indikator penting keberhasilan mitigasi. Perubahan ini menandakan bahwa mekanisme validasi dan kontrol akses telah berjalan dengan efektif. Dengan kombinasi redirect dan exit, sistem kini memastikan tidak ada lagi kebocoran data akibat eksekusi lanjutan ketika terjadi akses tidak sah.

Dari pembelajaran ini, dapat disimpulkan bahwa keamanan aplikasi tidak hanya bergantung pada validasi input, tetapi juga pada bagaimana sistem mengelola alur eksekusi dan respons terhadap permintaan yang tidak sah. Perbaikan sederhana berupa penambahan exit setelah header redirect terbukti efektif menutup celah IDOR secara langsung pada sistem yang diteliti, tanpa memerlukan perubahan arsitektur yang kompleks.

5. KESIMPULAN

a. Kerentanan IDOR berhasil diidentifikasi dan diuji menggunakan pendekatan Action Research melalui black-box testing dengan metode parameter tampering pada endpoint /pages/ticket_open?id=. Hasil pengujian menunjukkan bahwa sistem rentan terhadap read-only IDOR. Ketika parameter id dimodifikasi dari milik Akun Pertama (id=26) menjadi milik Akun Kedua (id=27), sistem menampilkan pesan kesalahan, tetapi tetap membocorkan sebagian isi percakapan tiket milik pengguna lain. Hal ini disebabkan oleh validasi kepemilikan objek yang belum diimplementasikan secara menyeluruh karena kode hanya menampilkan pesan gagal tanpa menghentikan eksekusi program.
b. Langkah penanganan telah berhasil diterapkan dan diverifikasi secara langsung pada kode sumber aplikasi. Perbaikan

dilakukan dengan mengganti blok penanganan kesalahan yang sebelumnya hanya menampilkan pesan, menjadi perintah header("Location: ...") diikuti dengan exit. Pengujian ulang pasca-perbaikan menunjukkan perubahan respons server dari 200 OK menjadi 302 Redirect, menandakan bahwa kontrol akses telah berfungsi secara efektif dan celah IDOR berhasil ditutup.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Purwantoro, M.Kom. dan Ibu Susilawati Sobur, M.Si. selaku pembimbing yang telah memberikan bimbingan dan arahan selama penelitian ini berlangsung. Terima kasih pula kepada pihak SMM-XYZ yang telah memberikan izin penelitian dan akses untuk melaksanakan pengujian keamanan pada platform mereka.

DAFTAR PUSTAKA

[1] S. Kemp, "Digital 2025: Indonesia," DataReportal – Global Digital Insights, Feb. 2025. [Online]. Available: https://datareportal.com/reports/digital-2025-indonesia

[2] A. Shrestha, A. Karki, M. Bhushan, S. Joshi, and S. Gurung, "Effects of Social Media Marketing on Consumer Buying Behavior," New Perspective: Journal of Business and Economics, vol. 6, no. 1, pp. 74–82, 2023.

[3] "A01 Broken Access Control – OWASP Top 10:2021," OWASP Foundation, 2021. [Online]. Available: https://owasp.org/Top10/A01_2021-Broken_Access_Control/

[4] S. E. Prasetyo, Haeruddin, and Tiara, "Evaluasi Kerentanan Insecure Direct Object Reference pada Aplikasi Pendaftaran Sidang Universitas XYZ," Journal of Applied Computer Science and Technology, vol. 5, no. 2, pp. 165–171, 2024.

[5] "The Rise of IDOR," HackerOne, Apr. 2021. [Online]. Available: https://www.hackerone.com/blog/rise-idor

[6] D. Suyitno, E. H. Ramadhani, and S. Suryantoro, "Survey analysis of vulnerability on the Indonesian government websites," 2024. doi: 10.1063/5.0187156

[7] S. E. Prasetyo, N. Hasanah, and G. Wijaya, "Pengujian Keamanan Learning Management System TutorLMS Terhadap Kerentanan Insecure Design dan Broken Access Control," Telcomatics, vol. 7, no. 2, 2022.

[8] D. Putra et al., "Detection and Prevention of Insecure Direct Object References (IDOR) in Website-Based Applications," 2023.

[9] M. Aydos, Ç. Aldan, E. Coşkun, and A. Soydan, "Security testing of web applications: A systematic mapping of the literature," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 9, pp. 6775–6792, 2022.

[10] S. E. Prasetyo, Haeruddin, and Tiara, "Evaluasi Kerentanan Insecure Direct Object Reference pada Aplikasi Pendaftaran Sidang Universitas XYZ," JACOST, vol. 5, no. 2, pp. 165–171, 2024.

[11] E. Amissah and F. Bentil, "Exposing Insecure Direct Object Reference (IDOR) Vulnerabilities in Academic Publication Platforms: A Case Study," International Journal of Engineering Research, vol. 13, no. 08, 2024.

[12] "WSTG - Latest," OWASP Foundation. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/04-Testing_for_Insecure_Direct_Object_References

[13] N. T. Cong, L. H. Toan, and T. Minh, "An overview of static and dynamic analysis in application security testing," Journal of Military Science and Technology, vol. 99, pp. 1–11, 2024.

[14] S. C. Mulyo Rachmanto et al., "Pengujian Aplikasi Sapawarga (Jabar Super Apps) Menggunakan Metode Black Box Testing," JITET, vol. 12, no. 3, 2024.

[15] "Web Parameter Tampering," OWASP Foundation. [Online]. Available: https://owasp.org/www-community/attacks/Web_Parameter_Tampering

[16] S. Vrhovec, D. Fujs, L. Jelovčan, and A. Mihelič, "Evaluating Case Study and Action Research Reports: Real-world Research in Cybersecurity," JUCS, vol. 26, no. 7, pp. 827–853, 2020.

[17] M. Alhamed and M. M. H. Rahman, "A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions," Applied Sciences, vol. 13, no. 12, p. 6986, 2023.

[18] M. H. Alfarizi et al., "Detection and Analysis of Packet Sniffing Attacks Using Wireshark on Wifi Networks," JTOS, vol. 8, no. 2, pp. 1084–1090, 2025.