Memanfaatkan Kerentanan *Broken Access Control* Pada *Website* Orami Untuk Membatalkan Pesanan Dan Meniru Identitas Pengguna

Ahmad Ray Septa Firdaus[1], Apriade Voutama[2]
[1,2]Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang
e-mail: [1]ahmad.raysepta@gmail.com, [2]apriade.voutama@staff.unsika.ac.id

Abstrak

Orami adalah sebuah *website e-commerce* yang menyediakan produk-produk kebutuhan bayi, anak-anak, dan ibu hamil. Pada penelitian ini membahas sebuah kerentanan pada *website* Orami yang memungkinkan penyerang untuk membatalkan pesanan dari akun pengguna lain dan meniru identitas pengguna. Dampak yang mungkin terjadi dari eksploitasi kerentanan ini adalah hilangnya kepercayaan pengguna terhadap situs Orami, terutama jika kerentanan ini disalahgunakan secara luas. Selain itu, kerugian finansial dapat terjadi jika banyak pesanan dibatalkan secara tidak sah dan pengguna memilih untuk membeli dari situs lain yang dianggap lebih aman. Kerentanan ini berhasil dieksploitasi dengan mendapatkan kode order korban melalui fitur histori pesanan dan kemudian mengubah nilai parameter pada fitur pembatalan pemesanan di akun penyerang. Metode penelitian ini mencakup analisis kerentanan, evaluasi dampak kerentanan, identifikasi solusi, pelaporan kerentanan, dan implementasi solusi. Hasil penelitian menunjukkan bahwa *website* Orami rentan terhadap serangan *Broken access control* dan telah dilakukan tindakan perbaikan oleh pengembang *website*.

Kata Kunci: *Website*, *Penetration Testing*, *Broken access control*, Burp Suite

Exploiting The Broken Access Control Vulnerability In The Orami Application For Order Cancellation And User Impersonation

Abstract

Orami is an e-commerce website that provides products for babies, children, and pregnant women. This research discusses a vulnerability in the Orami website that allows an attacker to cancel orders from another user's account and impersonate their identity. The potential impact of exploiting this vulnerability could lead to a loss of user trust in the Orami site, especially if it is widely abused. Additionally, financial losses could occur if many orders are canceled fraudulently and users choose to purchase from other sites deemed more secure. The vulnerability was exploited by obtaining the victim's order code through the order history feature and then modifying the parameter value in the cancellation order feature on the attacker's account. This research methods includes vulnerability analysis, impact evaluation, solution identification, vulnerability reporting, and solution implementation. The results of the study show that the Orami website is vulnerable to Broken access control attacks and the website developers has fixed the vulnerability.

Keywords: *Website, Penetration Testing, Broken access control, Burp Suite*

1. Pendahuluan

Pada perkembangan zaman seperti saat ini dunia digital semakin berperan penting dalam kehidupan manusia. Setiap tahunnya pasti terdapat berbagai inovasi terbaru terhadap perkembangan teknologi. Teknologi informasi dapat membantu suatu organisasi dalam menemukan strategi bisnis baru dan dapat membantu organisasi seperti perusahaan, sekolah, dan pemerintahan [1]. Pada saat ini juga Teknologi informasi dan komputasi berkembang sangat pesat, baik di tingkat perangkat keras maupun perangkat lunak. Perkembangan teknologi informasi disambut hangat oleh berbagai bidang kehidupan sosial, seperti bisnis, kehidupan sosial, termasuk pendidikan. Contohnya adalah pembuatan *website* dan internet [2].

Website merupakan bagian dari sistem komputerisasi yang memiliki berbagai fitur yang dirancang untuk memenuhi kebutuhan dalam memasukkan data tertentu dengan tujuan untuk menyederhanakan, mempercepat, dan merekam data secara akurat [3]. Keberadaan teknologi berbasis *website* mempermudah pengguna dalam mengakses sistem karena dapat diakses dari mana saja dan pada perangkat apa pun [4].

Website telah menjadi salah satu media utama untuk menyajikan informasi dan layanan, baik bagi individu maupun perusahaan. Akan tetapi, *website* juga rentan terhadap serangan dan ancaman keamanan cyber, yang dapat mengakibatkan kerusakan pada data dan informasi, serta merugikan pengguna *website*. Oleh karena itu, diperlukan pengujian keamanan pada *website* secara berkala. Pengujian keamanan pada *website* penting untuk dilakukan untuk memeriksa kesalahan-kesalahan yang ada pada program agar tidak bedampak pada kerugian yang timbul dari kesalahan tersebut [5].

Salah satu masalah keamanan yang sering ditemukan adalah *Broken access control*. Kerentanan ini memungkinkan penyerang melakukan akses yang tidak sah terhadap fungsionalitas dan data, seperti meretas akun pengguna lain, mengakses file sensitif, melakukan modifikasi data pengguna lain, memodifikasi hak akses, dan sebagainya [6]. Salah satu contoh dari kerentanan ini dapat ditemukan pada *website* Orami, sebuah platform *e-commerce* di Indonesia.

Penulis menemukan celah keamanan pada *website* Orami yang memungkinkan penyerang untuk membatalkan pesanan dari semua akun pengguna, dan memberikan alasan pembatalan palsu kepada korban yang telah dibatalkan. Penyerang dapat memanfaatkan celah ini untuk memanipulasi sistem dan merugikan pengguna lain. Tujuan dari jurnal ini adalah untuk meningkatkan kesadaran tentang pentingnya keamanan informasi dan untuk memperbaiki kerentanan keamanan pada *website* Orami. Selain itu, diharapkan jurnal ini juga dapat menjadi acuan bagi institusi lain dalam melakukan pengujian keamanan pada *website* mereka.

2. Metode Penelitian

Metode penelitian yang dapat dilakukan untuk mengevaluasi kerentanan pada *website* tersebut adalah sebagai berikut:

a. Analisis kerentanan
   Menganalisis kerentanan yang ditemukan dengan lebih mendalam. Penulis melakukan analisis pada kerentanan situs web, menggunakan alat pengujian keamanan seperti Burp Suite, serta melakukan uji coba dengan menggunakan teknik serangan *Broken access control* [7].
b. Evaluasi dampak kerentanan
   Setelah menganalisis kerentanan, penulis perlu mengevaluasi dampak yang mungkin terjadi akibat kerentanan tersebut. Dalam kasus ini, dampaknya adalah penyerang dapat membatalkan pesanan dari semua pengguna situs web dan mengirimkan pesan palsu ke korban.
c. Identifikasi solusi
   Berdasarkan hasil analisis dan evaluasi dampak, penulis perlu mengidentifikasi solusi untuk mengatasi kerentanan. Solusi ini dapat berupa saran perbaikan kepada developer situs web tersebut.

d. Melaporkan Kerentanan
Setelah sampai tahap identifikasi solusi, tahap selanjutnya yaitu membuat laporan tentang penemuan celah keamanan. Tahap ini bertujuan untuk melaporkan hasil dari pengujian keamanan yang telah dilakukan, yaitu mengidentifikasi jenis kerentanan apa yang ditemukan pada *website* [8]. Buatlah langkah-langkah mendapatkan kerentanan tersebut secara detail dan mudah dipahami oleh developer *website*-nya.

e. Implementasi solusi (fix bug)
Setelah penulis melaporkan kerentanan, developer *website* perlu mengimplementasikan saran perbaikan tersebut pada situs web yang terdampak. Hal ini dapat dilakukan dengan bekerja sama dengan pemilik situs web atau dengan menghubungi penyedia layanan situs web.

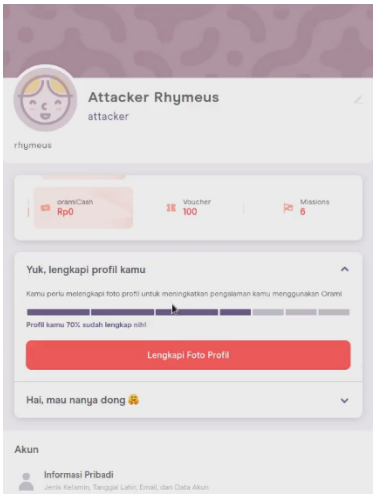
Dalam melakukan penelitian terhadap kerentanan pada *website*, perlu diperhatikan pula aspek-etika penelitian [9]. Penulis telah melaporkan temuan kerentanan ini terhadap pemilik *website* dan memberikan rekomendasi terkait cara mengatasi kerentanan tersebut. Kerentanan ini juga telah diperbaiki oleh pemilik *website*. Oleh karena itu, penulis menggunakan metode penelitian sampai pada poin Implementasi Solusi.

3. Hasil Dan Pembahasan

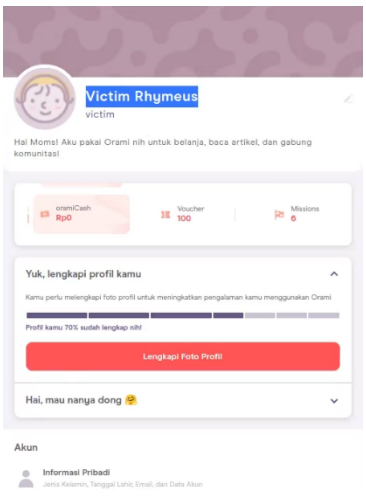
Proses yang dilakukan untuk menemukan celah keamanan pada *website* meliputi analisis kerentanan, evaluasi dampak kerentanan, identifikasi solusi, melaporkan Kerentanan dan implementasi solusi. Pada proses eksploitasi kerentanan menggunakan *tools* Burp Suite dalam menemukan celah keamanan pada *website* Orami.

Analisis kerentanan

Pertama-tama, penyerang melakukan pendaftaran dua akun pada *website* target. Satu akun dibuat sebagai akun penyerang, sedangkan yang lainnya sebagai akun korban.

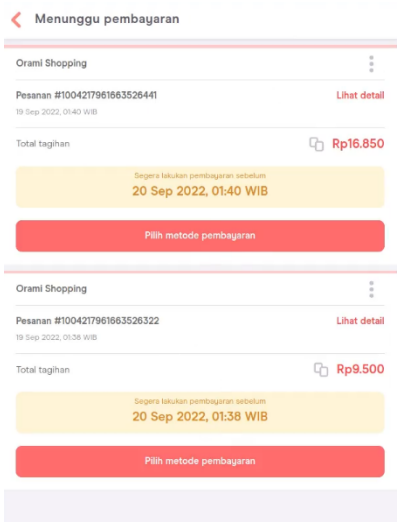


Gambar 1 Akun penyerang

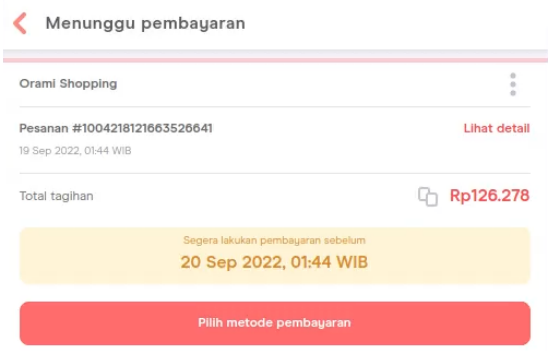


Gambar 2 Akun korban

Setelah memiliki kedua akun tersebut, penyerang melanjutkan dengan melakukan proses *checkout* pada masing-masing akun. Pada akun penyerang, proses *checkout* ini melibatkan pemesanan dua barang secara bersamaan. Tujuan dari langkah ini adalah untuk mendapatkan parameter yang rentan terhadap eksploitasi.

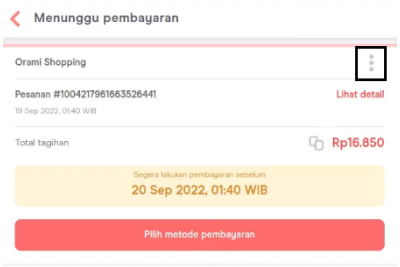


Gambar 3 *Checkout* pada akun penyerang



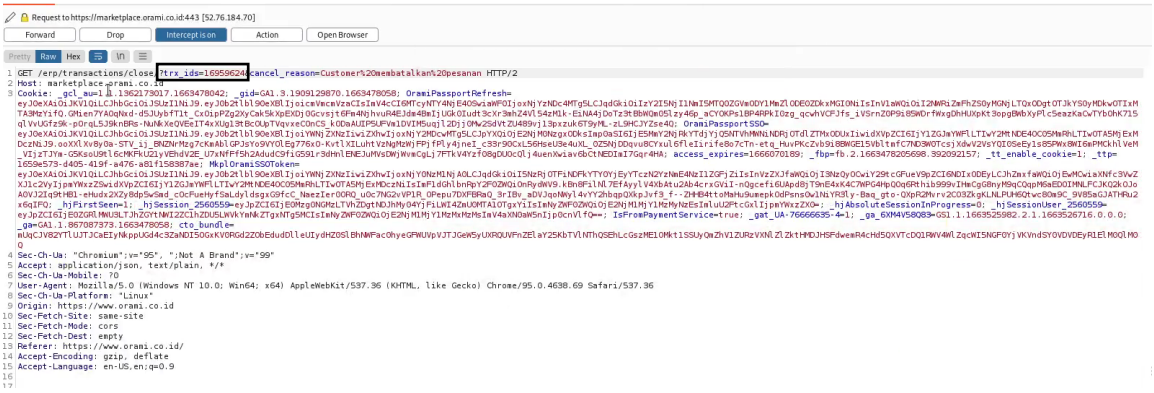
Gambar 4 *Checkout* pada akun korban

Kemudian, dalam kasus ini saya telah membuat akun korban, sehingga saya dapat mengakses akun tersebut untuk mendapatkan kode pesanan yang terdapat di dalamnya. Untuk melakukannya, saya membuka fitur histori pesanan pada akun korban, tangkap permintaan (*request*) menggunakan perangkat lunak "burp suite" dan mengklik tanda titik tiga yang terletak di pojok kanan atas. Setelah itu, klik pesanan dibatalkan, dan melalui analisis permintaan (*request*) yang ada, saya dapat melihat bahwa terdapat parameter bernama "trx_ids" yaitu kode pesanan korban.



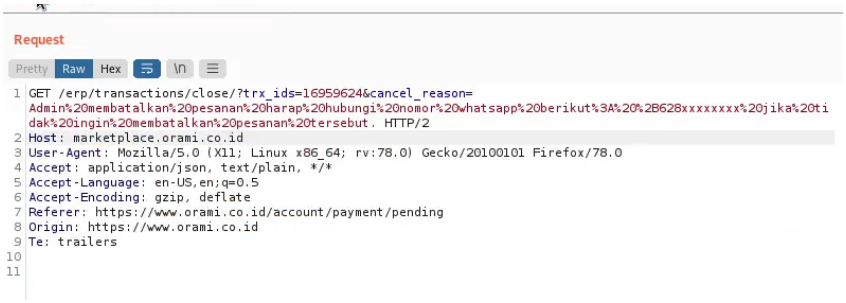
Gambar 5 Opsi Batalkan Pesanan

Gambar 6 Tombol batalkan Pesanan



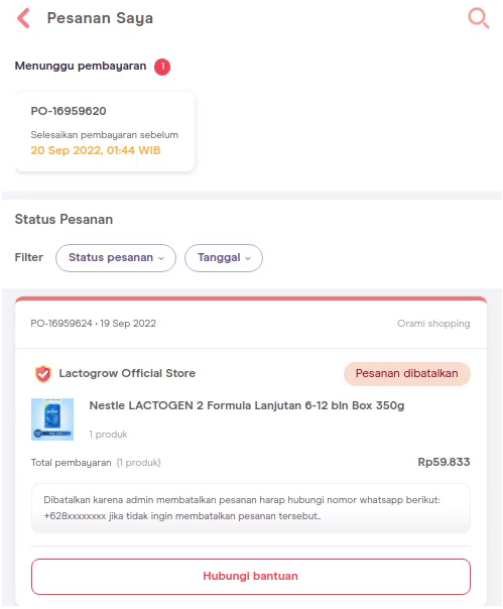
Gambar 7 Kode pesanan pada akun korban

Langkah selanjutnya, penyerang melakukan langkah yang serupa dengan apa yang dilakukan pada akun korban yaitu membatalkan pesanan hingga memperoleh kode pesanan dengan menggunakan perangkat lunak "burp suite". Kemudian, mengganti parameter "trx_ids" atau kode pesanan yang dimiliki oleh korban. Penyerang juga menghapus bagian *cookie* pada perangkat "burp suite" dan mengisi parameter "cancel_reason" dengan pesan atau alasan pembatalan palsu yang mengaku sebagai admin yang membatalkan pesanan.



Gambar 8 Eksploitasi kerentanan pada sisi penyerang

Dengan melakukan serangkaian langkah ini, korban akan mengalami dampak dari eksploitasi kerentanan ini yang disebut sebagai *Broken access control* atau lebih spesifiknya *Insecure Direct Object Reference* (IDOR). Kerentanan ini memungkinkan penyerang untuk memanipulasi objek-objek atau sumber daya yang seharusnya tidak dapat diakses olehnya. Sebagai contoh dalam kasus ini, penyerang dapat menghapus pesanan korban yang seharusnya memiliki tingkat kerahasiaan atau keamanan. Dampak selanjutnya yaitu mengakibatkan korban mendapatkan manipulasi pesan atau alasan pembatalan palsu yang dapat merugikan mereka. Detail antarmuka korban yang mengalami dampak kerentanan ini dapat dilihat dalam Gambar 9.



Gambar 9 Antarmuka korban yang terkena dampak serangan

Evaluasi dampak kerentanan

Kerentanan yang ditemukan pada *website* Orami memiliki dampak yang cukup serius. Penyerang dapat memanfaatkan kerentanan ini untuk membatalkan pesanan dari semua user/akun yang terdaftar pada *website* tersebut, serta mengirimkan pesan kepada korban dengan alasan yang dipalsukan. Penyerang juga dapat mengaku sebagai admin yang membatalkan pesanan, dengan mencantumkan nomor telepon penyerang sebagai nomor admin.

Dampak yang mungkin terjadi dari eksploitasi kerentanan ini adalah hilangnya kepercayaan pengguna terhadap situs tersebut, terutama jika kerentanan tersebut disalahgunakan secara luas. Selain itu, kerugian finansial dapat terjadi jika banyak pesanan dibatalkan secara tidak sah dan pengguna memilih untuk membeli dari situs lain yang dianggap lebih aman [10].

Identifikasi solusi

Dalam fitur pembatalan pesanan, diperlukan mekanisme otorisasi yang lebih kuat karena kemungkinan hak akses pengguna dapat diubah menjadi hak akses admin hanya dengan menghapus *header cookie* pada burp suite. Ini penting untuk memastikan bahwa hanya pengguna yang memiliki hak akses yang sesuai yang dapat menggunakan fitur tersebut.

Untuk mencegah penyalahgunaan, disarankan untuk memisahkan hak akses antara pengguna, pengguna lain dan admin. Pengguna hanya boleh memiliki hak untuk membatalkan pesanan yang mereka buat sendiri, sedangkan admin harus memiliki hak untuk membatalkan pesanan pengguna lain.

Saran perbaikan selanjutnya yaitu hanya admin yang dapat memberikan alasan pembatalan, oleh karena itu parameter pada cancel_reason harus diperbaiki sehingga hanya admin yang dapat memberikan alasan pembatalan kepada pengguna biasa.

Melaporkan Kerentanan

Pada tanggal 19 September 2022, Melalui Layanan Orami Care Center saya melaporkan adanya sebuah kerentanan pada *website* Orami yang memungkinkan penyerang untuk membatalkan pesanan dari semua user/akun, serta dapat memanipulasi alasan pembatalan pesanan tersebut. Kemudian pada tanggal 26 September 2022, tim Orami memberikan kabar lebih lanjut kepada pelapor bahwa bug tersebut akan diperbaiki dan akan memberikan apresiasi berupa hadiah sebesar 1.000.000 IDR. Proses ini disebut sebagai tahap triage untuk menentukan kejelasan dari laporan kerentanan yang dilaporkan. Pada tanggal 10 Oktober 2022, tim Orami telah berhasil memperbaiki kerentanan tersebut dan memberikan hadiah apresiasi kepada saya sebagai tanda terima kasih atas kontribusinya dalam membantu meningkatkan keamanan *website* mereka. Menurut saya, Orami menunjukkan tanggapannya yang cepat dalam menangani laporan kerentanan yang dilaporkan oleh saya. Tindakan yang diambil mencakup tahap triage, fix, dan rewards sebagai bentuk apresiasi kepada pelapor.

Implementasi solusi (fix bug)

Solusi yang diimplementasikan adalah dengan memperbaiki mekanisme otorisasi pada fitur pembatalan pesanan dan memisahkan hak akses antara pengguna, pengguna lain dan admin. Selain itu, parameter pada cancel_reason juga perlu diperbaiki sehingga hanya admin yang dapat memberikan alasan pembatalan kepada pengguna biasa. Setelah dilakukan triage, bug tersebut dianggap layak dan telah diperbaiki oleh tim developer pada tanggal 10 Oktober 2022.

Hasil pengujian

Hasil pengujian menunjukkan bahwa kerentanan tersebut telah teratasi dan tidak dapat lagi dimanfaatkan oleh penyerang untuk membatalkan pesanan dari akun lain serta memberikan alasan palsu. Oleh karena itu, dapat disimpulkan bahwa *website* Orami telah aman dari kerentanan *Broken access control* pada endpoint trx_ids dan cancel reason setelah diperbaiki oleh pihak Orami

4. Kesimpulan

Dalam pengujian terhadap *website* Orami, dilakukan analisis kerentanan dengan menggunakan *tools* Burp Suite untuk mengidentifikasi kerentanan pada *website*. Ditemukan kerentanan dengan tingkat risiko tinggi yaitu *broken access control*, yang memungkinkan penyerang untuk membatalkan pesanan dari semua akun, dan memungkinkan penyerang untuk memberikan alasan palsu untuk pembatalan tersebut [11].

Berdasarkan hasil dari pengujian terdapat kesimpulan yaitu bahwa kerentanan keamanan pada *website* Orami dapat memiliki dampak serius terhadap kepercayaan pengguna dan kerugian finansial. Karena itu, diperlukan langkah-langkah yang efektif untuk mengatasi atau mencegah penyalahgunaan dan meningkatkan otorisasi pada fitur pembatalan pesanan. Solusi yang disarankan adalah memisahkan hak akses antara pengguna, pengguna lain, dan admin, serta memperbaiki parameter pada cancel_reason agar hanya admin yang dapat memberikan alasan pembatalan. Penerapan solusi tersebut dapat membantu meningkatkan keamanan *website* Orami dan mencegah kejadian serupa di masa depan. Untuk penelitian selanjutnya, disarankan untuk melibatkan uji penetrasi yang lebih mendalam serta mempertimbangkan aspek keamanan secara menyeluruh dalam pengembangan *website* guna mencegah kerentanan semacam ini terjadi kembali.

5. Daftar Pustaka

[1] B. Prabaningrum, A. Voutama, and N. Heryana, "BERBASIS *WEBSITE* DALAM PENGELOLAAN LABA RUGI (STUDI KASUS : CV GEGER HANJUANG)," vol. 7, no. 1, pp. 671–680, 2023.

[2] A. Voutama and E. Novalia, "Perancangan Aplikasi M-Magazine Berbasis Android Sebagai Sarana Mading Sekolah Menengah Atas," *J. Tekno Kompak*, vol. 15, no. 1, p. 104, 2021, doi: 10.33365/jtk.v15i1.920.

[3] A. V. E. R. Ramadhan, K. Prihandani, "Penerapan Metode Agile Pada Development Aplikasi Pengelolaan Data Magang Berbasis Web Menggunakan Framework Laravel," *J. Ilm. Wahana Pendidik.*, vol. 9, no. April, pp. 144–154, 2023.

[4] C. Oktavia, A. Voutama, and B. A. Dermawan, "Sistem Pakar Diagnosis Hama Dan Penyakit Tanaman Stroberi Dengan Metode Certainty Factor Berbasis Web," *J. Ilm. Wahana Pendidik.*, vol. 8, no. 15, pp. 117–127, 2022, [Online]. Available: https://doi.org/10.5281/zenodo.7040696

[5] E. Novalia and A. Voutama, "Black Box Testing dengan Teknik Equivalence Partitions Pada Aplikasi Android M-Magazine Mading Sekolah," *Syntax J. Inform.*, vol. 11, no. 01, pp. 23–35, 2022, doi: 10.35706/syji.v11i01.6413.

[6] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis *Website* Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 6, no. 2, p. 185, 2021, doi: 10.24114/cess.v6i2.24777.

[7] Divyaniyadav, D. Gupta, D. Singh, D. Kumar, and U. Sharma, "Vulnerabilities and security of web applications," *2018 4th Int. Conf. Comput. Commun. Autom. ICCCA 2018*, pp. 1–5, 2018, doi: 10.1109/CCAA.2018.8777558.

[8] A. W. Wardhana and H. B. Seta, "Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada *Website* Universitas XYZ," *Inform. J. Ilmu Komput.*, vol. 17, no. 3, p. 226, 2021, doi: 10.52958/iftk.v17i3.3653.

[9] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada *Website* Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *Jurnal Algoritma*, vol. 18, no. 1. pp. 77–86, 2021. doi: 10.33364/algoritma/v.18-1.827.

[10] M. Agreindra Helmiawan, E. Firmansyah, I. Fadil, Y. Sofivan, F. Mahardika, and A. Guntara, "Analysis

of Web Security Using Open Web Application Security Project 10," *2020 8th Int. Conf. Cyber IT Serv. Manag. CITSM 2020*, 2020, doi: 10.1109/CITSM50537.2020.9268856.

[11] M. Rafi Ramdani, N. Heryana, and A. Susilo Yuda Irawan, "Penetration Testing pada *Website* Universitas Singaperbangsa Karawang Menggunakan Open Web Application Security Project (OWASP)," *J. Pendidik. dan Konseling*, vol. 4, no. 4, pp. 5522–5529, 2022.