Faktor Exacta

Vol. 18, No. 2, June 2025, pp. 201~207
eISSN: 2502-339X, pISSN: 1979-276X, DOI: https://doi.org/10.30998/faktorexacta.v18i2.27979

Broken Acces Control pada Website: System Literature Review

Sri Anita
Fakultas Bisnis dan Teknologi, Universitas Pertiwi, Indonesia

Article Info

Article history:

Received Feb 10, 2025
Revised Sept 09, 2025
Accepted Sept 15, 2025

Keywords:

Broken Access Control,
Types of website attacks,
Defacement,
Broken access control attack detection technology

ABSTRACT

Websites are essential tools for organizations, enabling them to showcase their reputation, products, and services to the public 24/7. However, high visibility also makes them prime targets for cyberattacks. A critical vulnerability known as Broken Access Control is a frequent cause of website defacement, leading to significant financial loss and reputational damage. This paper analyzes the causes of this vulnerability and proposes an AI-driven prevention model. The methodology combines a Systematic Literature Review of existing AI security research with the development of a new preventative technology. The proposed AI system demonstrated excellent performance, successfully detecting and blocking 100% of 10 simulated attacks. Protecting web assets is crucial. A failure to do so can compromise personal data, disrupt operations, and cause severe financial and reputational harm with lasting consequences.

Corresponding Author:

Sri Anita,
Faculty of Business and Technology,
Universitas Pertiwi,
Email: sri.anita@pertiwi.ac.id

1. PENDAHULUAN

Era digital telah menyebabkan banyaknya serangan keamanan informasi yang sebagian besar ditujukan pada *website-website* baik sektor pemerintahan dan sektor komersil (swasta) di Indonesia. Seperti wabah penyakit yang menyebar hanya dengan hitungan detik dapat menyerang puluhan bahkan ratusan website[1]. Hal uniknya target *website* yang disusupi tidak hanya sektor pemerintahan namun sektor komersil. Tentunya jika sudah disusupi oleh serangan maka akan sangat merugikan pemilik website dan tentu juga merugikan entitas yang mengakses website tersebut karena *website* sudah berubah informasinya. Dalam artikel ini ada dua pembahasan utama yaitu apa saja yang menjadi faktor utama website menjadi target serangan-serangandan hal apa saja yang perlu dilakukan sebagai langkah antisipasi terhadap serangan *website* .

Defacement adalah bentuk umum serangan terhadap situs *website*. Dalam serangan ini, konten situs yang sah digantikan seluruhnya atau sebagian oleh penyerang sehingga menyertakan konten yang memalukan bagi pemilik situs [2][3], misalnya gambar yang mengganggu, pesan politik, bentuk tanda tangan penyerang, dan sebagainya. Adapun jenis serangan yang biasa menyerang *website-website* adalah merubah menjadi situs judi *online*, situs pornografi, dan penyalahgunaan isi informasi dalam website tersebut. Hal lain yang akan disampaikan adalah faktor yang menyebabkan *website* tersebut bisa disusupi oleh serangan [4], [5]. Karena selama ini penyusup menggunakan mesin untuk melakukan pencarian yang dimana *website-website* tersebut secara teknis tidak dipelihara dan tidak pernah dilakukan pembaharuan keamanan informasi dasar.

Broken Acces Control adalah salah satu kerentanan serangan didalam aplikasi *website* yang sering terjadi dan menimbulkan kerugian dan risiko yang besar [6][7], hal yang seharusnya dapat diantisipasi dan penting untuk diketahui oleh entitas yang memiliki aplikasi *website*. Diharapkan dengan artikel ini dapat memberikan pedoman untuk memahami apa saja yang perlu dilakukan jika memiliki situs *website* supaya aman dari serangan-serangan seperti *defacement* dan yang lainnya. Dalam artikel ini pembahasan akan disajikan dari pengalaman pribadi yang sudah dilakukan dan hasil dari *system literature review* dari artikel baik nasional dan internasional.

2. LITERATURE REVIEW

A.*Vertical Acces Control*

Salah satu masalah kerentanan dalam aplikasi *website* yang sering di identifikasi, kerentanan menimbulkan risiko yang siginifikan. Contoh untuk menggambarkannya adalah ketika hak akses rendah (user biasa) dapat mengakses atau melakukan tindakan yang hanya tersedia pengguna dengan hak akses lebih tinggi (*administrator*/super admin)[5].

B.*Horizontal Acces Control*

Jenis kerentanan keamanan yang terjadi ketika pengguna atau penyerang dengan tingkat hak istimewa atau akses tertentu memperoleh akses tidak sah ke sumber daya atau fungsi yang ditujukan untuk pengguna lain dengan hak istimewa atau tingkat akses yang sama. Artinya saat pengguna atau penyerang dapat bergerak secara lateral melalui sistem dan mengakses data atau fungsi yang tidak boleh mereka akses[4].

C.*Broken Access Control*

Menjadi salah satu kerentanan berdasarkan **OWASP10** [6]. Kontrol akses merupakan aturan kebijakan akses otoritas dalam penggunaan teknologi informasi (aplikasi) dengan batasan-batasan yang dibuat sesuai dengan akses sehingga pengguna tidak dapat bertindak di luar izin yang sudah diberikan akses otoritas dalam teknologi informasi (aplikasi)[5]. Kegagalan *control* akses biasanya menyebabkan pengungkapan informasi yang tidak sah, modifikasi, atau penghancuran semua data atau pelaksanaan fungsi bisnis di luar batas pengguna.

3. METODOLOGI PENELITIAN

Systematic literature review adalah pendekatan dalam penelitian yang dilakukan dengan mencari referensi berdasarkan landasan teori yang relevan dengan masalah yang ditemukan. Dimana sumber-sumber referensi bisa dicari dari buku, artikel, dan karya ilmiah laporan penelitian ataupun *website online* yang membahas keilmuwan tertentu di internet.

Tahapan penelitian

Tahapan penelitian yang digambarkan pada gambar 1, merupakan ilustrasi pencarian sumber peneliti untuk mencari artikel dan laporan ilmiah. Dengan menggunakan *keyword* "*OWASP top 10*" dan "*Information Technology Security*" pada beberapa jurnal seperti *sciendirect*, *google schoolar*, dan pencarian *google search engine*. Kemudian setelah mendapatkan artikel yang sesuai dengan *study case*, artikel tersebut di *download* untuk di terjemahkan dan dikumpulkan informasi terkait *study case* yang sedang di teliti. Tahap terakhir setelah membaca artikel yaitu tahap pemilihan paper dan artikel yang terpilih yang berkaitan dengan *study case*.

Gambar 1. Tahapan Penelitian

4. HASIL DAN PEMBAHASAN

4.1. Hasil Pencarian *System Literature Review*

Tabel 1. Pencarian *System Literature Review*

Jenis Ancaman Aplikasi Website	Referensi
Broken Access Control	[1], [2], [7],[8],[3], [5], [9]
Vertical Acces Control	[7],[10], [11]
Horizontal Acces Control	[6],[10], [11],
Pencegahan Broken Acces Control	[1], [6], [8], [12], [13], [14], [15], [16]–[19]
Teknologi Mencegah Broken Acces Control	[1], [7], [8],[20], [21]

4.2. *Broken Acces Control*

Berikut dijelaskan mengenail faktor penyebab kerentanan pada aplikasi *website* karena *broken acces control* dan hal yang perlu dilakukan untuk antisipasi kerentanan *broken acces control* [1], [7], [8], [12].

1. **Penyebab Kerentanan**

   Hal yang biasa terjadi adalah sebagai berikut:

- Pelanggaran terhadap prinsip hak istimewa akses otoritas sebagai contoh *operator input*, modifikasi laporan dan menghapus laporan, di mana akses hanya boleh diberikan untuk kemampuan, peran, atau pengguna tertentu, namun tersedia untuk siapa saja yang bukan hanya operator.

- Melewati pemeriksaan kontrol akses dengan memodifikasi URL (pengrusakan parameter atau penelusuran paksa), status aplikasi internal, atau halaman HTML, atau dengan menggunakan alat serangan yang memodifikasi permintaan API.
- Mengizinkan, melihat atau mengedit akun orang lain, dengan memberikan pengenal uniknya seperti ID *Card*, *Finger Print*, dll.(referensi objek langsung tidak aman)
- Mengakses API dengan kontrol akses yang hilang untuk *POST*, *PUT* dan *DELETE*.
- Meningkatan hak akses otoritas menjadi istimewa. Bertindak sebagai pengguna tanpa login atau bertindak sebagai admin saat login sebagai pengguna.
- Manipulasi metadata, seperti memutar ulang atau merusak token kontrol akses *JSON Web Token* (JWT), atau cookie atau bidang tersembunyi yang dimanipulasi untuk meningkatkan hak istimewa atau menyalahgunakan pembatalan JWT.
- Kesalahan konfigurasi CORS (akses *website* A ternyata dapat dilakukan melalui akses *website* B) memungkinkan akses API dari sumber yang tidak sah/tidak tepercaya.
- Memaksa penjelajahan ke halaman yang diautentikasi sebagai pengguna yang tidak diautentikasi atau ke halaman yang memiliki hak istimewa sebagai pengguna standar.

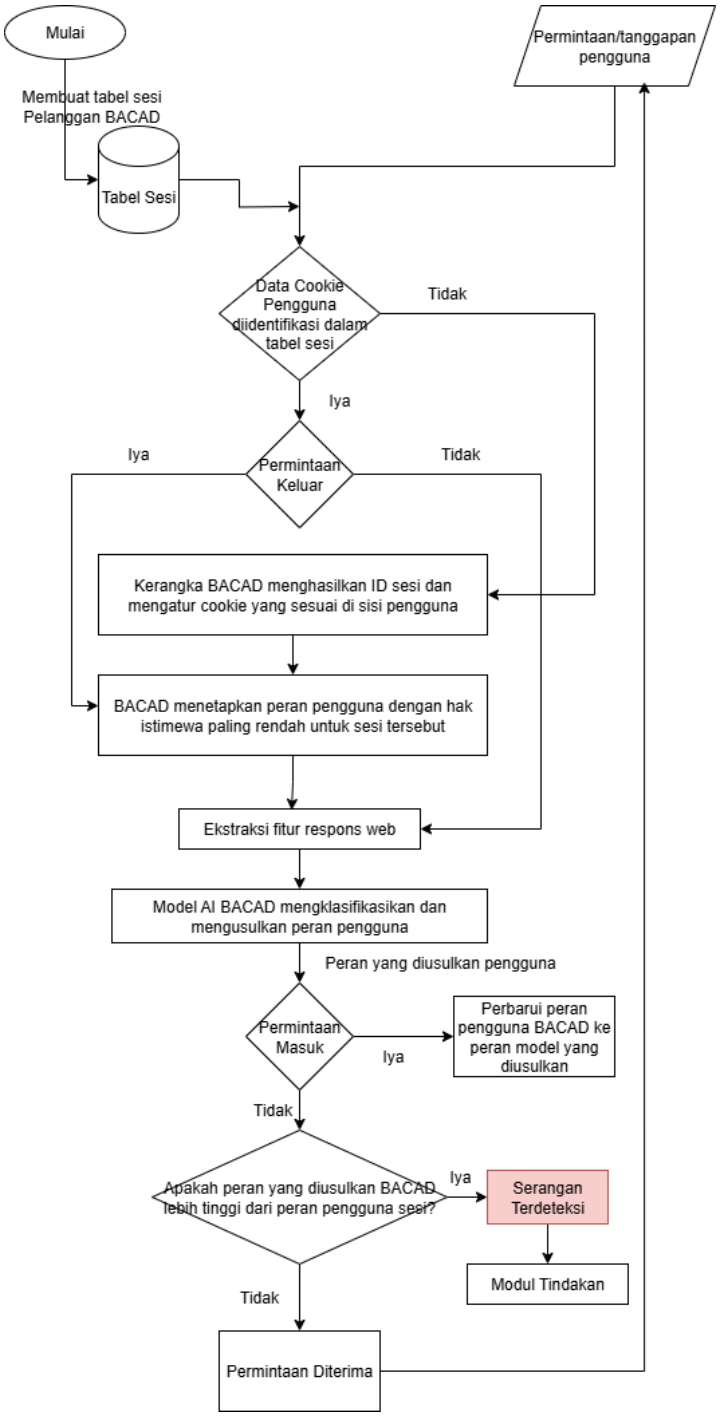
2. Cara Mencegah

- Kontrol akses hanya efektif dalam kode sisi *server* tepercaya atau API tanpa *server*, di mana penyerang tidak dapat mengubah pemeriksaan kontrol akses atau metadata. Kecuali untuk sumber daya publik, tolak secara *default*.
- Menerapkan mekanisme kontrol akses satu kali dan menggunakannya kembali di seluruh aplikasi, termasuk meminimalkan penggunaan *Cross-Origin Resource Sharing* (CORS).
- Kontrol akses model harus menegakkan kepemilikan rekaman, bukan menerima bahwa pengguna dapat membuat, membaca, memperbarui, atau menghapus rekaman apa pun.
- Persyaratan batas bisnis aplikasi yang unik harus diterapkan oleh model domain.
- Nonaktifkan daftar direktori *server website* dan pastikan metadata *file* (mis., .git) dan *file* cadangan tidak ada dalam *root web*.
- Catat kegagalan kontrol akses, beri tahu admin bila perlu (misalnya, kegagalan berulang).
- Batasi tingkat akses API dan pengontrol untuk meminimalkan bahaya dari alat serangan otomatis.
- Pengidentifikasi sesi stateful harus dibatalkan di *server* setelah *logout*. Token JWT tanpa kewarganegaraan sebaiknya berumur pendek sehingga peluang bagi penyerang dapat diminimalkan. Untuk JWT yang berumur lebih lama, sangat disarankan untuk mengikuti standar *OAuth* untuk mencabut akses.
- Pengembang dan staf QA harus menyertakan unit kontrol akses fungsional dan pengujian integrasi.

4.3. Mesin Deteksi *Broken Acces Control*

Berdasarkan penelusuran mengenai teknologi yang sudah dilakukan pada penelitian sebelumnya terdapat beberapa usulan teknologi mesin otomatis pendeteksi kerentanan pada *broken acces control*, hasil penelusurannya sebagai berikut:

1. BACAD: *AI Based Framework for detecting vertical broken acces control*
   Dalam pembuatan mesin AI untuk deteksi jenis serangan *vertical broken access control* [7]dengan desain sebagai berikut pada gambar 2:



Gambar 2. *Flowchart* BACAD Desain

Penjelasan singkat mengenai kerangka gambar 2 sebagai berikut:
kerangka kerja yang memanfaatkan teknik AI canggih untuk mentralisir eksploitasi dan serangan jenis *vertical broken acces control* secara *real time* menggunakan dinamikan dan teknik praktis. Proses deteksi terdiri dari dua langkah. Langkah pertama adalah membuat klasifikasi peran pengguna menggunakan model kecerdasan buatan (AI) tingkat lanjut yang dibuat dalam fase pembelajaran (Data latih dan data test). Tahap pembelajaran meliputi konfigurasi awal BACAD dan pembuatan lalu lintas peran pengguna aplikasi yang digunakan untuk pelatihan model AI. Model AI pada BACAD menganalisis permintaan dan respons web menggunakan ekstraksi fitur yang kuat dan mengatur *hyperparameter* dinamis untuk memastikan performa optimal di beragam skenario. Langkah kedua adalah langkah pengambilan keputusan, yang menentukan apakah pasangan permintaan-respons yang masuk bersifat jinak atau

merupakan serangan dengan memvalidasinya vs kumpulan informasi sesi BACAD. Evaluasi terhadap spektrum dunia nyata dan aplikasi *website* demonstrasi menyoroti efisiensi luar biasa dalam mendeteksi eksploitasi VBAC, memberikan kekuatan perlindungan aplikasi terhadap serangkaian serangan VBAC yang berbeda. Selain itu menunjukan bahwa BACAD mengatasi permasalahan VBAC dengan menghadirkan solusi yang aplikasi, dinamis, fleksibel, dan teknologi mandiri untuk mengatasi risiko kerentanan VBAC. Dengan demikian BACAD memberikan kontribusi yang signifikan terhadap upaya berkelanjutan yang bertujuan untuk meningkatkan keamanan aplikasi website.

2. Hasil Kinerja Mesin AI Detektor Kerentanan

Hasil deteksi menunjukkan efektivitas BACAD dalam mengidentifikasi serangan *Vertical Broken Acces Control* (VBAC) di berbagai aplikasi *website* target. Semua serangan yang dilakukan berhasil dideteksi di semua kasus, menghasilkan nol negatif palsu. Ini merupakan pencapaian penting karena menunjukkan bahwa sistem ini sangat andal dalam mengidentifikasi upaya akses tidak sah itu mengeksploitasi kerentanan kontrol akses vertikal. Kekokohan deteksi mekanismenya belum diuji melalui 10 serangan bervariasi per kerentanan BACAD secara konsisten menghasilkan hasil yang akurat, apapun serangannya urutan atau identitas pengguna yang diasumsikan selama pengujian [7]. Temuan ini menekankan kemampuan BACAD untuk beradaptasi dengan berbagai skenario dan konfigurasi serangan di dunia nyata, sehingga menunjukkan keandalannya dan keserbagunaan dalam lingkungan aplikasi yang berbeda. Selain itu, tidak adanya negatif palsu meningkatkan kepercayaan terhadap kerangka kerja, karena ini menunjukkan bahwa tidak ada skenario serangan VBAC yang lolos tanpa terdeteksi. Akibatnya, BACAD membuktikan dirinya sebagai alat deteksi yang andal, memastikan bahwa tindakan dan fungsi sensitif tetap terlindungi akses tidak sah. Sedangkan hasil menunjukkan bahwa model AI efektif dalam mendeteksi pengguna peran, masih ada kemungkinan kecil untuk salah mengidentifikasi peran pengguna. Keberhasilan ini dapat dikaitkan dengan integrasi model AI dengan BACAD kerangka logika tingkat lanjut, yang memungkinkan serangan efisien dan efektif deteksi. Kombinasi ini memungkinkan deteksi yang lebih kuat dan akurat mekanisme, memanfaatkan kemampuan model AI untuk memahami dan belajar peran pengguna yang berbeda dalam konteks yang disediakan oleh logika kerangka kerja untuk mengidentifikasi upaya akses tidak sah secara efektif. Evaluasi waktu respons menunjukkan bahwa penerapan BACAD meningkat waktu respons, terutama karena komponen *Mitmproxy* yang digunakan untuk intersepsi lalu lintas. Meskipun penundaan ini minimal dan dapat diterima, lakukan optimasi *Mitmproxy* atau *framework pipeline* dapat mengurangi *overhead* lebih lanjut. Itu modul deteksi itu sendiri menambahkan sedikit penundaan tambahan, menunjukkan ruang untuk perbaikan tanpa mengorbankan kinerja keamanan. Hasil penelitian ini tidak dapat dibandingkan secara langsung dengan pendekatan lain karena metode tersebut tidak memanfaatkan AI dan malah mengandalkannya teknik kerajinan tangan dengan banyak aturan adat, banyak di antaranya sangat spesifik untuk domainnya masing-masing. Selain itu, ini metode alternatif sangat bergantung pada teknologi tertentu dan kerangka pembangunan. Apalagi surat kabar yang bersangkutan sering menghilangkan banyak detail penting yang diperlukan untuk implementasi ulang, seperti langkah algoritmik yang tepat, kumpulan data, prosedur pra-pemrosesan data, dan pengaturan parameter yang mempersulit upaya reproduksi apa pun melakukan perbandingan langsung.

Pada percobaan aplikasi BACAD dirancang untuk membuat deteksi adanya serangan akses dalam bentuk *Vertical Broken Acces Control*. BACAD membuat tabel yang berisi akun (ID sesi) dan mengatur cookie yang sesuai dengan sisi pengguna berdasarkan klasifikasi peran pengguna menggunakan model kecerdasan buatan (AI), sebelumnya sudah didaftarkan. Dalam simulasi BACAD ini akan menetapkan peran setiap pengguna yang jumlahnya disesuaikan dengan pengguna asli. Selain menetapkan pengguna juga disertai dengan hak akses istimewa berdasarkan hierarki akses istimewa mulai paling rendah hingga akses istimewa tertinggi disetiap sesinya. Setiap akun dan hak akses akan diekstrasi dan disertai responnya. Model AI BACAD mengklasifikasikan dan mengusulkan peran pengguna, kemudian peran yang diusulkan oleh pengguna saat permintaan masuk jika bernilai sesuai dengan daftar tabel sesi maka akan memperbaharui peran pengguna di model BACAD, jika tidak maka model akan memeriksa apakah peran sudah sesuai dengan sesi pengguna jika iya maka hal itu serangan dan terdeteksi sebagai serangan. Tujuannya ada mensimulasikan teknik model AI pada BACAD untuk mendeteksi serangan Broken Acces. Dalam proses simulasi dilakukan 10 kali percobaan dengan menggunakan permintaan masuk login dengan dataset yang sudah disesuikan dengan kemungkinan2 identitas dari setiap akun. Batasan dalam percobaan ini hanya dilakukan dengan spesifikasi serangan jenis broken acces control dan tidak berlaku pada jenis serangan lain. Hal yang menjadi objek adalah akun yang sudah didaftarkan dengan spesifikasi model BACAD.

Analisis dan penilaian mendalam terpisah dilakukan untuk mengevaluasi efektivitas dan kinerja model AI, yang merupakan komponen inti kerangka kerja BACAD. Presisi, Recall, Skor F1, dan Akurasi merupakan

metrik kinerja yang diakui secara luas dalam domain AI. Oleh karena itu, metrik-metrik ini digunakan untuk menilai kinerja model secara komprehensif. Akurasi mengukur ketepatan keseluruhan model dengan menghitung rasio instans yang diprediksi dengan benar terhadap total instans. Presisi, didefinisikan sebagai rasio prediksi positif sejati terhadap total prediksi positif. Recall, didefinisikan sebagai rasio prediksi positif sejati terhadap semua positif aktual yang menilai kemampuan model untuk mengidentifikasi instans positif. Terakhir, Skor F1, rata-rata harmonis dari presisi dan recall, menyediakan metrik tunggal yang menyeimbangkan kedua hal tersebut, sehingga sangat berguna untuk dataset yang tidak seimbang.

4.4. Deteksi Manual

Selain menggunakan mesin untuk mencari dan deteksi dini terhadap kerentanan pada *broken acces control* ada langkah lain yang dapat dilakukan, yaitu diarahkan untuk mencari *log* aktivitas yang berupa jurnal kehidupan dari *website* tersebut melalui akses dari sisi *server website*. Tentunya dengan cara ini, dipastikan yang melakukan adalah professional yang sudah mengerti dengan baik seluk beluk terkait *website* dan sudah memahami dasar-dasar keilmuwan kerentanan.

5. PENUTUP

Broken Access Control merupakan salah satu kerentanan paling signifikan yang tercantum dalam daftar OWASP Top 10, mencerminkan tingginya frekuensi dan dampak serangan yang terjadi secara global, termasuk pada situs-situs di Indonesia. Kerentanan ini tidak hanya berpotensi menimbulkan kerugian finansial, tetapi juga dapat menyebabkan pelanggaran data pribadi, penurunan reputasi organisasi, serta konsekuensi hukum dan gangguan operasional yang serius. Oleh karena itu, pemilik dan pengelola website perlu meningkatkan kewaspadaan terhadap pengelolaan hak akses pengguna, serta menerapkan langkah-langkah proteksi yang sistematis dan berkelanjutan. Artikel ini diharapkan dapat memberikan pemahaman awal yang komprehensif mengenai pentingnya kontrol akses yang aman, sekaligus mendorong kesadaran kolektif untuk memperkuat sistem keamanan informasi. Ke depan, penelitian lanjutan yang mengarah pada pengembangan framework deteksi dini terhadap broken access control dan kerentanan sejenis sangat diperlukan, guna mendukung terciptanya ekosistem digital yang lebih aman dan tangguh di Indonesia.

DAFTAR PUSTAKA

[1] J. Mupokosera, “Financial Services Information Security Culture: The Effect of Technology, People and Environment,” *Proc. 2023 2nd Zimbabwe Conf. Inf. Commun. Technol. ZCICT 2023*, 2023, doi: 10.1109/ZCICT59466.2023.10552881.

[2] J. B. Ullrich and J. Lam, “Defacing websites via SQL injection,” *Netw. Secur.*, vol. 2008, no. 1, pp. 9–10, Jan. 2008, doi: 10.1016/S1353-4858(08)70007-2.

[3] G. Davanzo, E. Medvet, and A. Bartoli, “Anomaly detection techniques for a web defacement monitoring service,” *Expert Syst. Appl.*, vol. 38, no. 10, pp. 12521–12530, Sep. 2011, doi: 10.1016/J.ESWA.2011.04.038.

[4] M. Ghorbanzadeh and H. R. Shahriari, “ANOVUL: Detection of logic vulnerabilities in annotated programs via data and control flow analysis,” *IET Inf. Secur.*, vol. 14, no. 3, pp. 352–364, May 2020, doi: 10.1049/IET-IFS.2018.5615.

[5] L. Zhong, “A Survey of Prevent and Detect Access Control Vulnerabilities,” Apr. 2023, Accessed: Sep. 14, 2025. [Online]. Available: http://arxiv.org/abs/2304.10600

[6] “Biz Serve IT Blog | Insights on Cybersecurity.” https://www.bizserveit.com/blogs/horizontal-privilege-escalation-broken-access-control (accessed Jan. 12, 2025).

[7] A. Anas, A. A. Alhelbawy, S. El Gamal, and B. Youssef, “BACAD: AI-based framework for detecting vertical broken access control attacks,” *Egypt. Informatics J.*, vol. 28, p. 100571, Dec. 2024, doi: 10.1016/J.EIJ.2024.100571.

[8] F. Younas, A. Raza, N. Thalji, L. Abualigah, R. A. Zitar, and H. Jia, “An efficient artificial intelligence approach for early detection of cross-site scripting attacks,” *Decis. Anal. J.*, vol. 11, p. 100466, Jun. 2024, doi: 10.1016/J.DAJOUR.2024.100466.

[9] Q. Wang, J. Sun, C. Wang, S. Zhang, S. Xuanyuan, and B. Zheng, “Access Control Vulnerabilities Detection for Web Application Components,” *Proc. - 2020 IEEE 6th Intl Conf. Big Data Secur. Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conf. High Perform. Smart Comput. HPSC 2020 2020 IEEE Intl Conf. Intell. Data Secur. IDS 2020*, pp. 24–28, May 2020, doi: 10.1109/BIGDATASECURITY-HPSC-IDS49724.2020.00016.

[10] C. Hou, J. Shi, M. Cui, and Q. Yang, “Attack versus Attack: Toward Adversarial Example Defend Website Fingerprinting Attack,” *Proc. - 2021 IEEE 20th Int. Conf. Trust. Secur. Priv. Comput.*

Commun. Trust. 2021, pp. 766–773, 2021, doi: 10.1109/TRUSTCOM53373.2021.00111.

[11] D. Arnaldy and A. R. Perdana, "Implementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack," *Proc. - 2019 2nd Int. Conf. Comput. Informatics Eng. Artif. Intell. Roles Ind. Revolut. 4.0, IC2IE 2019*, pp. 188–192, Sep. 2019, doi: 10.1109/IC2IE47452.2019.8940872.

[12] "A01 Broken Access Control - OWASP Top 10:2021." https://owasp.org/Top10/A01_2021-Broken_Access_Control/ (accessed Jan. 11, 2025).

[13] L. Qi, H. Huang, F. Li, R. Malekian, and R. Wang, "A novel shilling attack detection model based on particle filter and gravitation," *China Commun.*, vol. 16, no. 10, pp. 112–132, Oct. 2019, doi: 10.23919/JCC.2019.10.008.

[14] S. Chen, D. Ou, C. Jiang, J. Shen, L. Yan, and S. Guo, "Power Attack and Detection Technology in Data Centers: A Survey," *Proc. 2020 IEEE Int. Conf. Commun. Comput. Cybersecurity, Informatics, CCCI 2020*, Nov. 2020, doi: 10.1109/CCCI49893.2020.9256459.

[15] S. Anita, S. Aditya Mahadany, and W. Lelisa Army, "Cryptographic Failures pada Website: System Literature Review," *Pros. Disem. Nas. Has. Penelit. dan Pengabdi. Kpd. Masy.*, vol. 2, no. 1, Aug. 2025, doi: 10.30998/DINAMIKA.V2I1.8392.

[16] J. Shi, R. Li, and W. Hou, "A Mechanism to Resolve the Unauthorized Access Vulnerability Caused by Permission Delegation in Blockchain-Based Access Control," *IEEE Access*, vol. 8, pp. 156027–156042, 2020, doi: 10.1109/ACCESS.2020.3018783.

[17] B. Zhang, J. Li, J. Ren, and G. Huang, "Efficiency and Effectiveness of Web Application Vulnerability Detection Approaches: A Review," *ACM Comput. Surv.*, vol. 54, no. 9, Oct. 2021, doi: 10.1145/3474553.

[18] B. O. Kose, V. Coskun, and A. Coskun, "An Innovative Risk Score Based Corporate Access Control Management System," *ISAS 2023 - 7th Int. Symp. Innov. Approaches Smart Technol. Proc.*, 2023, doi: 10.1109/ISAS60782.2023.10391575.

[19] F. A. W. Dharmasatya and Y. Asnar, "Detection of Broken Access Control Vulnerability Using Graph Representation," *Proc. 2024 IEEE Int. Conf. Data Softw. Eng. Data-Driven Innov. Transform. Ind. Soc. ICoDSE 2024*, pp. 84–89, 2024, doi: 10.1109/ICODSE63307.2024.10829892.

[20] N. S. M. Farras, J. Loderick, H. A. Saputri, and A. C. Sari, "Exploring Penetration Testing: A Comparative Analysis of Brute Force Directory Tools in Vulnerability Analysis Phase," *2024 2nd Int. Conf. Technol. Innov. Its Appl.*, pp. 1–6, Sep. 2024, doi: 10.1109/ICTIIA61827.2024.10761451.

[21] M. Souppaya, K. Scarfone, and D. Dodson, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities", doi: 10.6028/NIST.SP.800-218.