ADIJAYA
Jurnal Multidisiplin
https://e-journal.naureendigition.com/index.php/mj
Vol. 03, No. 03, 2025, Hal. 528-535
E-ISSN : 2964-7606

ANALISIS KERENTANAN *BROKEN ACCESS CONTROL, CRYPTOGRAPHIC FAILURES DAN INJECTION* PADA APLIKASI BIMBINGAN KONSELING MENGGUNAKAN *WHITE-BOX TESTING*

Farhan Hamdallah
Sistem Informasi, Universitas Sains Indonesia. Cibitung

Abstrak

Keamanan aplikasi web merupakan aspek penting dalam melindungi data sensitif, khususnya pada aplikasi bimbingan konseling yang menyimpan informasi pribadi siswa dan riwayat konseling. Penelitian ini bertujuan untuk menganalisis kerentanan **Broken Access Control** pada aplikasi bimbingan konseling yang sedang dikembangkan, menggunakan metode **white-box testing**.

Metode penelitian dilakukan dengan menganalisis kode sumber aplikasi, menguji modul-modul kritis terkait autentikasi dan otorisasi, serta melakukan simulasi akses tidak sah berdasarkan standar **OWASP Testing Guide**. Instrumen yang digunakan meliputi *code review*, pengujian manual, dan dokumentasi hasil eksplorasi.

Hasil penelitian menunjukkan bahwa aplikasi masih memiliki kerentanan **Broken Access Control**, di mana pengguna dengan hak akses terbatas dapat mengakses data konseling milik pengguna lain melalui modifikasi parameter. Kerentanan ini memiliki tingkat risiko tinggi karena berpotensi menyebabkan kebocoran data pribadi siswa dan menurunkan kepercayaan terhadap sistem.

Kesimpulan penelitian ini menegaskan bahwa aplikasi bimbingan konseling perlu diperbaiki dengan menerapkan **policy-based authorization**, validasi akses pada setiap endpoint, serta pengujian keamanan berkelanjutan. Penelitian ini diharapkan dapat menjadi referensi bagi pengembang dan lembaga pendidikan dalam meningkatkan keamanan aplikasi web

Kata Kunci Keamanan Aplikasi Web, Broken Access Control, Cryptographic Failures, Injection, White-Box Testing, OWASP

Abstract

Web application security is an essential aspect of protecting sensitive data, particularly in counseling applications that store students' personal information and counseling records. This study aims to analyze the **Broken Access Control** vulnerability in a counseling application under development, using the **white-box testing** method.

The research method involves analyzing the application's source code, testing critical modules related to authentication and authorization, and simulating unauthorized access based on the **OWASP Testing Guide**. The instruments used include code review, manual testing, and documentation of test results.

The findings reveal that the application is vulnerable to **Broken Access Control**, where users with limited privileges can access counseling records of other users by modifying parameters. This vulnerability poses a high risk as it may lead to the leakage of students' personal data and undermine trust in the system.

The study concludes that the counseling application requires improvements through the implementation of **policy-based authorization**, strict access validation on each endpoint, and continuous security testing. This research is expected to serve as a reference for developers and educational institutions in enhancing web application security.

***Keywords**:* Web Application Security, Broken Access Control, Cryptographic Failures, Injection, White-Box Testing, OWASP

PENDAHULUAN

Perkembangan teknologi informasi telah mendorong digitalisasi di berbagai bidang, termasuk layanan bimbingan konseling (BK) di sekolah maupun lembaga pendidikan. Aplikasi bimbingan konseling dirancang untuk mempermudah interaksi antara konselor dan siswa, penyimpanan data kasus, serta pengelolaan informasi yang bersifat rahasia. Keamanan website adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada website dengan sasaran perlindungan terhadap informasi/data (Muttaqien, 2019; Wismarini & Prihandono, 2020).

Namun, aplikasi berbasis web memiliki potensi kerentanan keamanan apabila tidak dirancang dengan standar keamanan yang baik. Di era digital saat ini konsen terhadap masalah keamanan dan integritas digital sedang hangat di perbincangkan. Umumnya konsen terhadap masalah keamanan sistem informasi selalu diposisikan kedua atau lebih (Ghozali et al., 2018). OWASP Top 10 mencatat bahwa kerentanan yang paling sering terjadi pada aplikasi web meliputi Broken Access Control, Cryptographic Failures, dan Injection.

Broken Access Control terjadi apabila pengguna dapat mengakses data atau fungsi yang seharusnya dibatasi. Cryptographic Failures muncul akibat penggunaan enkripsi yang lemah, salah konfigurasi, atau penyimpanan data sensitif tanpa perlindungan memadai. Injection seperti SQL Injection dapat memungkinkan penyerang mengeksekusi perintah berbahaya melalui input aplikasi. Kerentanan tersebut, apabila terdapat dalam aplikasi bimbingan konseling, berpotensi menimbulkan dampak serius, seperti kebocoran data pribadi siswa, manipulasi catatan konseling, hingga kerusakan integritas sistem.

Karena itu, perlu dilakukan analisis kerentanan terhadap aplikasi bimbingan konseling yang sedang dikembangkan dengan metode white-box testing, agar dapat mendeteksi potensi celah keamanan sejak dini serta memberikan rekomendasi perbaikan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimen dengan metode white-box testing, di mana peneliti memiliki akses penuh terhadap kode sumber aplikasi bimbingan konseling yang sedang dikembangkan. Metodologi penilaian risiko OWASP adalah pendekatan sederhana untuk menghitung dan menilai risiko yang terkait dengan aplikasi (Dewanto, 2018; Eka Pratama & Wiradarma, 2019; Kurniawan, 2019; Li, 2020); White-box testing dipilih karena memungkinkan identifikasi kerentanan dari sisi internal logika aplikasi, konfigurasi, dan interaksi dengan database. Objek penelitian adalah aplikasi bimbingan konseling berbasis web yang dikembangkan oleh peneliti. Aplikasi ini memiliki fitur utama:

1. Manajemen data guru bk dan siswa.
2. Pencatatan kasus dan riwayat konseling.
3. Mekanisme autentikasi dan otorisasi pengguna.
4. Penyimpanan data sensitif siswa.

Pengumpulan data dilakukan dengan teknik berikut:

1. Analisis Kode Sumber (Code Review): Meneliti bagian kode yang berkaitan dengan autentikasi, otorisasi, penyimpanan data, dan query database.
2. Pengujian White-Box: Menjalankan test case pada modul-modul tertentu untuk menemukan potensi kerentanan.
3. Dokumentasi: Mencatat hasil pengujian, bukti eksploitasi, serta tangkapan layar hasil percobaan serangan.

Analisis dilakukan dengan merujuk pada standar OWASP Testing Guide dan fokus pada tiga kerentanan utama:

Broken Access Control

Menguji apakah pengguna dengan hak akses tertentu dapat mengakses data/fungsi yang seharusnya dibatasi.

Contoh pengujian: mencoba akses endpoint admin menggunakan akun siswa, mengakses ID kasus konseling milik pengguna lain.

Cryptographic Failures

Meninjau cara penyimpanan password, token, atau data sensitif.

Menguji apakah algoritma hash/kriptografi yang digunakan sesuai standar (misalnya bcrypt/argon2 untuk password).

Mengecek apakah data dikirim melalui jalur terenkripsi (HTTPS) atau plaintext.

Injection

Menganalisis query database pada kode program untuk menemukan potensi SQL Injection.

Melakukan input pengujian dengan karakter berbahaya (' OR '1'='1, UNION SELECT, dsb.).

Mengecek sanitasi input dan penggunaan parameterized query.

Alur penelitian digambarkan sebagai berikut:

Identifikasi Modul Kritis → Menentukan modul aplikasi yang mengelola data sensitif.

Analisis Kode Sumber → Melakukan review bagian autentikasi, otorisasi, enkripsi, dan query database.
White-Box Testing → Menjalankan test case sesuai potensi kerentanan (Broken Access Control, Cryptographic Failures, Injection).

Eksperimen Eksploitasi → Mensimulasikan serangan pada modul tertentu untuk memastikan kerentanan benar-benar ada.
Dokumentasi Hasil → Mencatat hasil pengujian, bukti serangan, dan tingkat risiko.
Rekomendasi Perbaikan → Memberikan solusi teknis untuk menutup celah keamanan.

Hasil dan Pembahasan

Broken Access Control

Pengujian dilakukan pada modul manajemen kasus konseling.

- Temuan:

Saat mengakses endpoint /siswa/2, pengguna dengan peran siswa masih dapat melihat data kasus milik siswa lain hanya dengan mengubah parameter. Hal ini menunjukkan adanya Insecure Direct Object Reference (IDOR).

- Dampak:

Siswa dapat melihat data pribadi siswa lain, termasuk catatan konseling yang bersifat rahasia.

- Solusi Mitigasi:
  - Tambahkan validasi akses pada level controller untuk memastikan hanya pemilik data atau konselor yang dapat mengakses data tertentu.
  - Gunakan policy-based authorization di sisi server.

Cryptographic Failures

Pengujian dilakukan pada modul autentikasi pengguna.

- Temuan:
  - Password disimpan menggunakan algoritma bcrypt.
  - Proses login menggunakan HTTPS, sehingga kredensial dikirim dalam bentuk teks terenkripsi.

Injection

Pengujian dilakukan pada fitur pencarian kasus konseling.

- Temuan:

Query SQL ditulis secara konkatenasi string:

```
SELECT * FROM cases WHERE student_name = '" + input + "'
```

Saat input ' OR '1'='1 dimasukkan, sistem tidak berhasil menampilkan seluruh data kasus konseling. hal ini karena pada aplikasi tersebut sudah menggunakan ORM yang secara otomatis sudah terhindar dari SQL Injection.

Analisis Hasil

Dari hasil pengujian, aplikasi bimbingan konseling terbukti memiliki kerentanan pada tiga aspek utama OWASP:

1. Broken Access Control → risiko tinggi, karena menyangkut privasi siswa.
2. Cryptographic Failures → tidak ada
3. Injection → tidak ada

Jika tidak segera diperbaiki, kerentanan ini dapat menyebabkan:

- Kebocoran data pribadi siswa.
- Hilangnya kepercayaan lembaga pendidikan terhadap aplikasi.
- Potensi pelanggaran hukum terkait perlindungan data pribadi.

Kesimpulan

Berdasarkan hasil penelitian mengenai analisis kerentanan Broken Access Control, Cryptographic Failures, dan Injection pada aplikasi bimbingan konseling menggunakan white-box testing, diperoleh kesimpulan sebagai berikut:

1. Broken Access Control ditemukan pada modul manajemen kasus, di mana pengguna dengan hak akses terbatas masih dapat mengakses data milik pengguna lain. Hal ini menunjukkan lemahnya validasi otorisasi.

2. Cryptographic Failures tidak teridentifikasi karena pada penyimpanan password dengan menggunakan algoritma bcrypt.

3. Injection tidak terdeteksi pada fitur pencarian kasus, karena query SQL sudah menggunakan ORM sehingga sangat aman terhadap SQL Injection.

4. Metode white-box testing terbukti efektif dalam mendeteksi kerentanan internal karena peneliti memiliki akses penuh terhadap kode sumber dan konfigurasi aplikasi.

Saran

Berdasarkan hasil analisis, saran yang dapat diberikan adalah:

1. Perbaikan Teknis Aplikasi:
   - Terapkan policy-based authorization untuk mencegah Broken Access Control.
2. Penerapan Keamanan Berlapis (Defense in Depth):

◦ Gunakan input validation dan sanitasi data sebelum diproses.

◦ Implementasikan logging dan monitoring terhadap aktivitas pengguna mencurigakan.

◦ Terapkan rate limiting untuk mencegah brute force attack.

3. Pengembangan Keamanan Berkelanjutan:

◦ Integrasikan security testing dalam pipeline pengembangan (DevSecOps).

◦ Lakukan audit keamanan berkala dengan mengacu pada OWASP Top 10.

◦ Memberikan pelatihan keamanan aplikasi bagi tim pengembang agar kesalahan yang sama tidak terulang.

4. Aspek Organisasi dan Pengguna:

◦ Lembaga pendidikan yang menggunakan aplikasi BK perlu membuat kebijakan perlindungan data siswa.

◦ Edukasi konselor dan siswa mengenai pentingnya menjaga kerahasiaan akun dan tidak membagikan kredensial.

Dengan penerapan saran-saran tersebut, diharapkan aplikasi bimbingan konseling dapat menjadi lebih aman, handal, dan layak digunakan untuk mendukung proses layanan konseling di sekolah maupun lembaga pendidikan.

Daftar Referensi

Dewanto, A. P. (2018). Penetration Testing padaDomain uii.ac.id Menggunakan OWASP 10.

Eka Pratama, I. P. A., & Wiradarma, A. A. B. A. (2019). Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company). International Journal of Computer Network and Information Security, 11(7), 8– 12. https://doi.org/10.5815/ijcnis.2019.07.02

Ghozali, B., Kusrini, & Sudarmawan. (2018). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) untuk Penilaian Risk Rating Detect Web Application Security Flaws Using the Owasp (Open Web Application Security Project) Method for Risk Asse. 4, 12

Kurniawan, A. (2019). Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi Host-Based. Jurnal Telematika, 14(1).

Li, J. (2020). Vulnerabilities mapping based on OWASP-SANS: A survey for static application security testing (SAST). Annals of Emerging Technologies in Computing, 4(3), 1–8. https://doi.org/10.33166/AETiC.2020.03.001