Terbit online pada laman web jurnal: **http://journal.isas.or.id/index.php/JACOST**

JOURNAL OF APPLIED COMPUTER SCIENCE AND TECHNOLOGY (JACOST)

Vol. 5 No. 2 (2024) 165 – 171 | ISSN: 2723-1453 (Media Online)

Evaluasi Kerentanan Insecure Direct Object Reference pada Aplikasi Pendaftaran Sidang Universitas XYZ

Stefanus Eko Prasetyo[1], Haeruddin[2], Tiara[3]
[123]Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam
[1]stefanus@uib.ac.id, [2]haeruddin@uib.ac.id, [3]2032028.tiara@uib.edu*

Abstract

This study aims to analyze and evaluate the vulnerability of Insecure Direct Object Reference (IDOR) in the thesis registration web application at XYZ University, as well as to provide improvement recommendations to enhance the security of students' personal data. The IDOR vulnerability allows unauthorized access to students' personal documents, which can jeopardize privacy and information security. Utilizing an action research methodology consisting of four stages: diagnosis, action taking, evaluation, and learning, this research identifies the URL patterns generated when students upload documents such as ID cards, family cards, birth certificates, diplomas, and photos. During the action-taking phase, the researcher conducts attacks using Burp Suite to test the vulnerability by modifying URL parameters based on the identified patterns. The testing results indicate that all documents can be accessed without proper authorization, with a status code of 200 indicating successful access. These findings underscore the necessity for stricter security improvement measures in the thesis registration application to protect students' personal data. The implications of this research highlight the importance of implementing tighter access controls and better input validation in higher education applications to prevent potential data leaks in the future. This study makes a significant contribution to enhancing information security within educational environments.

Keywords: *Higher Education Application Security; Personal Data Protection; Security Vulnerability; Action Research Methodology.*

Abstrak

Penelitian ini bertujuan untuk menganalisis dan mengevaluasi kerentanan Insecure Direct Object Reference (IDOR) dalam aplikasi web pendaftaran sidang di Universitas XYZ serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan data pribadi mahasiswa. Kerentanan IDOR memungkinkan akses tidak sah terhadap dokumen pribadi mahasiswa, yang dapat membahayakan privasi dan keamanan informasi. Menggunakan metodologi penelitian tindakan yang terdiri dari empat tahapan: diagnosis, pengambilan tindakan, evaluasi, dan pembelajaran, penelitian ini mengidentifikasi pola URL yang dihasilkan saat mahasiswa mengunggah dokumen seperti KTP, Kartu Keluarga, Akte Lahir, Ijazah, dan Pas Foto. Pada fase pengambilan tindakan, peneliti melakukan serangan menggunakan aplikasi Burp Suite untuk menguji kerentanan dengan memodifikasi parameter URL berdasarkan pola yang teridentifikasi. Hasil pengujian menunjukkan bahwa semua dokumen dapat diakses tanpa otorisasi yang sesuai, dengan kode status 200 yang menunjukkan keberhasilan akses. Temuan ini menekankan perlunya langkah-langkah perbaikan keamanan yang lebih ketat dalam aplikasi pendaftaran sidang untuk melindungi data pribadi mahasiswa. Implikasi dari penelitian ini menunjukkan pentingnya penerapan kontrol akses yang lebih ketat dan validasi input yang lebih baik dalam aplikasi pendidikan tinggi guna mencegah potensi kebocoran data di masa mendatang. Penelitian ini memberikan kontribusi signifikan terhadap peningkatan keamanan informasi dalam lingkungan pendidikan.

Kata kunci: Keamanan Aplikasi Pendidikan Tinggi; Perlindungan Data Pribadi; Kerentanan Keamanan; Metode Penelitian Tindakan.

1. Pendahuluan

Saat ini, dunia semakin terhubung berkat perkembangan teknologi informasi [1]. Perkembangan teknologi yang pesat memberikan dampak positif dan perubahan signifikan pada bidang pendidikan [2]. Dengan dukungan teknologi yang tersedia, setiap aktivitas pendidikan menjadi lebih mudah, cepat, dan murah, serta informasi yang melimpah dapat diakses dengan mudah kapan saja dan di mana saja sesuai kebutuhan [3]. Sebagai contoh, data diri pelajar kini disimpan oleh institusi pendidikan menggunakan aplikasi web. Aplikasi web yang menyimpan data penting tersebut tentunya harus dilengkapi dengan keamanan informasi yang baik. Perkembangan teknologi informasi telah mengubah cara institusi pendidikan menyimpan dan mengelola data pribadi mahasiswa. Namun, masih terdapat banyak tantangan dalam menjaga keamanan

informasi. Keamanan informasi diartikan sebagai perlindungan informasi dari berbagai ancaman yang dapat mempengaruhi aspek kerahasiaan, ketersediaan, dan integritas [4].

Namun, keamanan informasi pada aplikasi web di Indonesia masih belum memadai, sehingga menyebabkan meningkatnya masalah kebocoran data pribadi [5]. Hal ini terjadi karena manajemen data yang buruk dan kurangnya langkah pencegahan keamanan yang kuat pada aplikasi tersebut, menciptakan celah bagi pihak yang tidak bertanggung jawab untuk mencuri data pribadi. Keamanan data sangat penting, terutama mengingat potensi risiko yang tinggi [6]. Kasus kebocoran data pribadi dalam beberapa tahun terakhir menunjukkan betapa seriusnya masalah ini, dengan data pribadi yang dijual oleh pihak tidak bertanggung jawab untuk keuntungan maksimal. Kebocoran data dapat mengakibatkan pengungkapan informasi sensitif seperti nama lengkap, jenis kelamin, agama, kebangsaan, alamat, dan data pribadi lainnya [7], [8].

Sebagai contoh, sepanjang tahun 2022 hingga 2023, sejumlah kasus kebocoran data terjadi, termasuk kebocoran data pengguna SIM card oleh Bjorka yang mencakup Nomor Induk Kependudukan (NIK) dan nomor telepon provider dengan nilai diperkirakan mencapai Rp743,5 juta [9]. Kasus lain melibatkan pengungkapan 34 juta data paspor yang dijual seharga Rp150 juta [10], serta kebocoran data Dinas Kependudukan dan Pencatatan Sipil sebanyak 337 juta data [11], [12]. Dari kasus-kasus tersebut, jelas bahwa data pribadi merupakan aset berharga yang memiliki nilai tinggi. Penerapan perlindungan yang tepat terhadap data pribadi sangat penting dalam era teknologi informasi ini, terutama sejak pandemi COVID-19 [13]. Keamanan dan privasi menjadi isu utama bagi perusahaan yang mengadopsi komputasi awan untuk penyimpanan data [14].

Aplikasi website yang digunakan oleh perusahaan swasta maupun pemerintahan seringkali menjadi target utama serangan siber karena menyimpan data pribadi. Keberhasilan serangan tersebut dapat merugikan reputasi instansi terkait, menurunkan kredibilitas dan kepercayaan publik akibat kebocoran data pengguna. Kompleksitas aplikasi web juga meningkatkan peluang terjadinya serangan [15]. Untuk mencegah insiden serangan siber yang meningkat, pemerintah telah memasukkan UU Kejahatan Siber (Cyber Law) ke dalam UU ITE Nomor 11 Tahun 2008 dengan harapan dapat membantu mengatasi dan mengurangi kejahatan di dunia digital [16].

Universitas XYZ memiliki aplikasi website yang digunakan oleh mahasiswa untuk menyelesaikan administrasi pendaftaran sidang tugas akhir, yaitu Sistem Informasi Daftar Sidang. Aplikasi ini wajib digunakan oleh mahasiswa untuk mendaftar sidang tugas akhir dan meminta mereka mengunggah dokumen pribadi seperti KTP, Kartu Keluarga, Akte Lahir, Ijazah Sekolah, dan foto pribadi sebagai syarat pendaftaran.

Salah satu celah keamanan yang memungkinkan penyerang mendapatkan data pribadi adalah melalui Broken Access Control. Berdasarkan pemeringkatan celah keamanan website oleh Open Web Application Security Project (OWASP) pada tahun 2021 dan 2023, Broken Access Control menempati posisi pertama. Kategori ini naik dari posisi kelima pada tahun 2017 ke urutan teratas pada tahun 2021 dan tetap di posisi tersebut pada laporan 2023. Broken Access Control terjadi ketika akses yang benar hanya diberikan kepada peran tertentu tetapi dapat diakses oleh semua orang [17]. Kerentanan ini bisa disebabkan oleh berbagai faktor seperti kesalahan konfigurasi, Insecure Direct Object References (IDOR), atau manajemen sesi yang tidak aman. IDOR adalah kerentanan yang disebabkan oleh lemahnya otorisasi dalam sistem. Kerentanan ini terjadi ketika aplikasi mengekspos referensi langsung ke sumber daya seperti file atau catatan dalam database. Situasi ini memungkinkan pengguna untuk memodifikasi URL dan mendapatkan akses ke informasi pengguna lain [18].

Penelitian terkait Insecure Direct Object Reference (IDOR) telah dilakukan sebelumnya [19], berfokus pada identifikasi dan mitigasi kerentanan IDOR menggunakan metode Bug Bounty. Penelitian tersebut menekankan pentingnya penerapan kontrol akses yang tepat dan langkah-langkah keamanan untuk mencegah serangan IDOR. Penelitian lain [20] menggunakan metode penetration testing untuk menguji kerentanan IDOR pada URL aplikasi web tertentu. Meskipun telah ada penelitian tentang IDOR, masih terdapat kesenjangan dalam penerapan kontrol akses yang efektif di aplikasi pendidikan tinggi. Sebagian besar penelitian sebelumnya lebih banyak berfokus pada pengujian kerentanan tanpa memberikan solusi konkret untuk meningkatkan keamanan aplikasi. Ini menunjukkan perlunya penelitian lebih lanjut yang tidak hanya mengidentifikasi kerentanan tetapi juga menawarkan rekomendasi perbaikan yang dapat diterapkan secara praktis.

Penelitian terkait kerentanan aplikasi web dengan menggunakan model OWASP versi 4 untuk menganalisis kerentanan aplikasi web dengan kombinasi alat keamanan [21]. Penelitian ini menemukan berbagai kerentanan seperti belum diterapkannya HTTPS dan kerentanan terhadap serangan XSS serta SQL injection. Penulis juga memberikan saran untuk pengembangan lebih lanjut, termasuk penambahan status level untuk masing-masing tahapan dan diskusi mengenai potensi celah keamanan [21].

Penelitian lainnya tentang kerentanan pada aplikasi web dalam konteks pengelolaan tugas akhir Program Penelitian Pendidikan XYZ dari Universitas Pendidikan Ganesha sebagai studi kasus [22]. Penelitian ini

DOI : https://doi.org/10.52158/jacost.v5i2.873

bertujuan mendeteksi dan mengevaluasi kerentanan menggunakan teknik penilaian dan pengujian penetrasi berdasarkan OWASP Top 10 2017. Metodologi eksperimen ini menggunakan Burp Suite untuk pemindaian otomatis dan manual serta wawancara untuk menilai kerentanan [22]. Penelitian [23] berfokus pada analisis keamanan website Dinas Tenaga Kerja dan Transmigrasi sebagai saluran interaksi antara masyarakat dan pemerintah. Hasil penelitian menunjukkan adanya beberapa kerentanan seperti pesan kesalahan dan *cookie* sesi tanpa tanda HttpOnly.

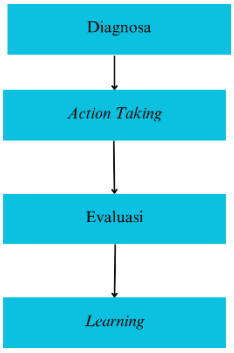
Penelitian lainnya mengidentifikasi masalah keamanan pada sistem manajemen pembelajaran (LMS) menggunakan metode *action research* dan memberikan rekomendasi untuk meningkatkan keamanan sistem [17]. Penelitian lainnya berfokus pada pengujian penetration testing menggunakan metode IDOR, menunjukkan bahwa IDOR dapat dieksploitasi jika akses langsung diberikan ke objek berdasarkan input pengguna tanpa perlindungan memadai [24]. Hal ini sejalan dengan [25] mengenai IDOR sebagai masalah serius dalam keamanan aplikasi.

Penelitian ini bertujuan untuk menganalisis dan mengevaluasi kerentanan IDOR dalam aplikasi website pendaftaran sidang di Universitas XYZ, serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan data pribadi mahasiswa. Dengan menggunakan metode penelitian tindakan yang terdiri dari diagnosis, pengambilan tindakan, evaluasi, dan pembelajaran, penelitian ini diharapkan dapat memberikan pemahaman yang lebih baik mengenai pola URL yang dihasilkan saat mahasiswa mengunggah dokumen penting. Dengan demikian, hasil penelitian ini tidak hanya berkontribusi pada pengetahuan akademis, tetapi juga memberikan solusi praktis untuk meningkatkan keamanan informasi dalam lingkungan pendidikan.

2. Metode Penelitian

Penelitian ini menggunakan metode penelitian tindakan untuk menganalisis kerentanan Insecure Direct Object Reference (IDOR) pada aplikasi website pendaftaran sidang di Universitas XYZ. Metode ini dipilih karena memungkinkan peneliti terlibat langsung dalam proses penelitian dan memberikan solusi praktis terhadap masalah yang dihadapi. Metode penelitian tindakan terdiri dari empat tahapan yang dapat dilihat pada Gambar 1, yaitu diagnosis, pengambilan tindakan, evaluasi, dan pembelajaran.

Tahap pertama adalah diagnosis. Pada tahap ini, peneliti mengidentifikasi sumber daya yang diunggah ke aplikasi web pendaftaran sidang di Universitas XYZ. Peneliti melakukan pengumpulan data dengan cara mengunggah dokumen yang diwajibkan, seperti KTP, Kartu Keluarga, Akte Lahir, Ijazah, dan Pas Foto. Proses ini bertujuan untuk memahami pola URL yang dihasilkan oleh sistem ketika dokumen diunggah.



Gambar 1. Metode Action Research

Setelah mendapatkan informasi mengenai pola URL tahap berikutnya adalah pengambilan tindakan, peneliti melakukan serangan dengan menggunakan aplikasi Burp Suite. Aplikasi ini digunakan untuk mencoba mengakses dokumen pribadi mahasiswa dengan memodifikasi parameter URL berdasarkan pola yang telah diidentifikasi. Tahap ini bertujuan untuk menguji kerentanan IDOR dan mengumpulkan bukti akses tidak sah terhadap data pribadi mahasiswa.

Tahap selanjutnya adalah evaluasi. Pada tahap evaluasi, peneliti menganalisis hasil dari pengambilan tindakan. Hasil pengujian diolah untuk menentukan apakah dokumen pribadi mahasiswa dapat diakses tanpa otorisasi yang sesuai. Evaluasi ini juga mencakup identifikasi potensi risiko dan kelemahan dalam implementasi kontrol akses aplikasi.

Tahap terakhir adalah pembelajaran, di mana peneliti mereview semua hasil dari tahapan sebelumnya. Penelitian ini menghasilkan rekomendasi perbaikan yang dapat diterapkan untuk meningkatkan keamanan aplikasi web pendaftaran sidang serta melindungi data pribadi mahasiswa.

Dengan menggunakan metode action research ini, diharapkan penelitian dapat memberikan kontribusi nyata dalam meningkatkan keamanan aplikasi pendidikan tinggi dan melindungi data pribadi mahasiswa dari potensi kebocoran.

3. Hasil dan Pembahasan

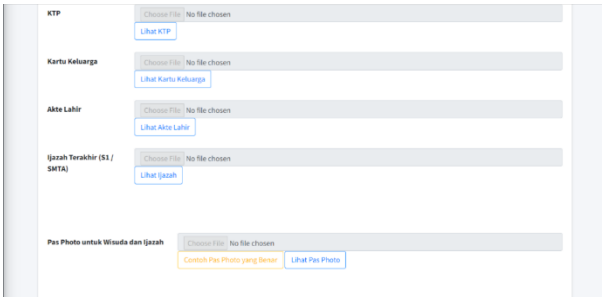
Pada tahapan diagnosis, peneliti mendapatkan informasi target melalui uji coba langsung mengunggah file yang diwajibkan oleh aplikasi daftar sidang universitas XYZ. Pengumpulan informasi dilakukan dengan metode white hat, dimana peneliti diberikan akun mahasiswa untuk melakukan uji coba. Dari Gambar 2. setiap mahasiswa yang akan melakukan pendaftaran sidang wajib mengunggah file dokumen KTP, Kartu Keluarga, Akte lahir, Ijazah Terakhir, dan Pas Photo untuk ijazah. Keseluruhan dokumen yang diupload menghasilkan alamat URL yang terlihat polanya pada Tabel 1. setiap dokumen tersimpan pada direktori assets yang memiliki

DOI : https://doi.org/10.52158/jacost.v5i2.873

subdirektori ktp, aktelahir, kk, ijazah, dan pasphoto. Dari URL yang didapatkan juga menunjukkan referensi objek dokumen memiliki pola Nomor Induk Mahasiswa (NIM) sebagai penamaan file (xxxxxx adalah NIM yang sudah disamarkan) dengan akhiran _KTP.pdf, _AL.pdf, _KK.pdf, _IJ.pdf, dan _PP.jpg.

Tabel 1. Daftar URL Diagnosa Unggahan File

Dokumen	Url Target Pengujian
KTP	daftarsidang.xyz.ac.id/assets/ktp/xxxxxxx_KTP.pdf
Akte Lahir	daftarsidang.xyz.ac.id/assets/aktelahir//xxxxxxx_AL.pdf
Kartu Keluarga	daftarsidang.xyz.ac.id/assets/kk/xxxxxxx_KK.pdf
Ijazah	daftarsidang.xyz.ac.id/assets/ijazah/xxxxxxx_IJ.pdf
Pas Photo	daftarsidang.xyz.ac.id/assets/pasphoto/xxxxxxx_PP.jpg



Gambar 2. Halaman Upload Dokumen

Pada tahap pengambilan tindakan, dengan pola dokumen yang sudah didapatkan pada tahapan sebelumnya, dilakukan serangan menggunakan bantuan aplikasi burp suite, target serangan pada tahapan aksi ini dapat dilihat pada Tabel 2. yaitu untuk mendapatkan objek berupa data dokumen pribadi yang sudah pernah diunggah oleh mahasiswa pada aplikasi daftar sidang. Peneliti menggunakan burp suite untuk melakukan permintaan terus menerus dengan menggunakan referensi NIM (xxxxxxx) menjadi parameter angka yang ditambahkan satu angka setiap permintaan kepada aplikasi dengan pola URL pada Tabel 1.

Tabel 2. Daftar Target Pengujian Kerentanan

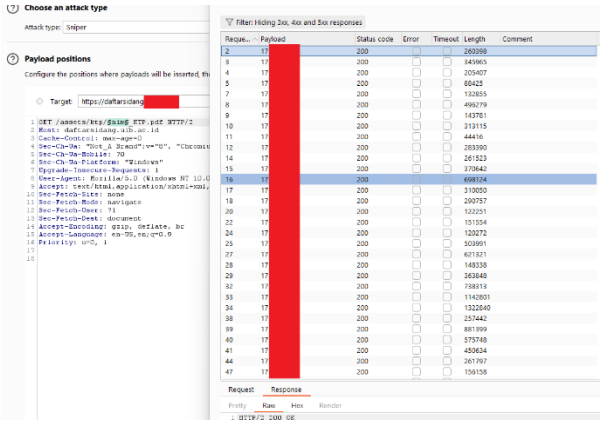
No	Target Pengujian
1	Mendapatkan Kartu Tanda Penduduk
2	Mendapatkan Akta Kelahiran
3	Mendapatkan Kartu Keluarga
4	Mendapatkan Ijazah Terakhir
5	Mendapatkan Pas Foto Ijazah

Dari Tabel 3, terlihat bahwa semua dokumen yang diuji dapat diakses dengan mengganti parameter NIM pada URL. Status kode 200 menunjukkan bahwa file tersebut dapat diunduh tanpa perlu autentikasi yang sah.

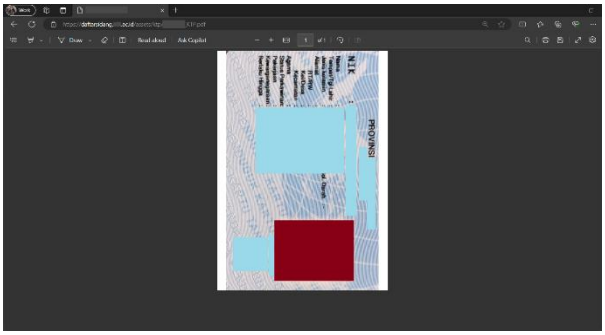
Dapat dilihat pada Gambar 3. serangan IDOR untuk mendapatkan objek KTP menggunakan burp suite melakukan permintaan terus menerus pada URL KTP dengan mengganti referensi NIM mengurutkan pola angka ada yang menghasilkan status code 200, yang artinya file KTP dengan NIM tersebut ada dan bisa diunduh. Untuk membuktikannya peneliti mengakses salah satu URL yang memberikan hasil status code 200, dapat dilihat pada Gambar 4. objek KTP yang berisi data pribadi dapat diakses langsung tanpa harus login kedalam sistem.

Tabel 3. Status Akses Serangan

Dokumen	Url Target Pengujian	Status Akses
KTP	daftarsidang.xyz.ac.id/assets/ktp/xxxxxxx_KTP.pdf	Dapat diakses (200)
Akte Lahir	daftarsidang.xyz.ac.id/assets/aktelahir//xxxxxxx_AL.pdf	Dapat diakses (200)
Kartu Keluarga	daftarsidang.xyz.ac.id/assets/kk/xxxxxxx_KK.pdf	Dapat diakses (200)
Ijazah	daftarsidang.xyz.ac.id/assets/ijazah/xxxxxxx_IJ.pdf	Dapat diakses (200)
Pas Photo	daftarsidang.xyz.ac.id/assets/pasphoto/xxxxxxx_PP.jpg	Dapat diakses (200)



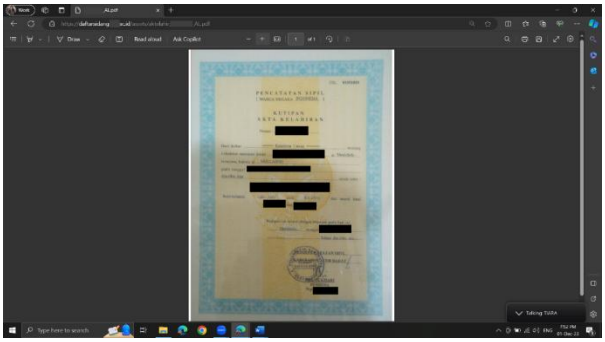
Gambar 3. Serangan IDOR pada objek KTP Menggunakan Burp Suite



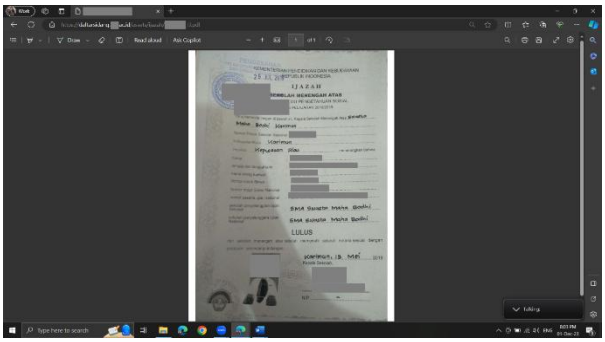
Gambar 4. File KTP Yang Ada Pada Aplikasi Daftar Sidang

Dengan pola yang serupa pada objek dokumen akte lahir dan ijazah terakhir, dengan mengganti referensi parameter URL pada bagian NIM yang sudah disesuaikan berdasarkan NIM mahasiswa yang didapatkan melalui uji coba burp suite sebelumnya dapat dilihat pada Gambar 5 dan Gambar 6 dimana objek dokumen akte lahir dan ijazah terakhir mahasiswa dapat diakses dan diunduh. Dengan pola yang sederhana hanya mengganti referensi NIM dapat mengakses data pribadi objek dokumen akte lahir dan ijazah terakhir mahasiswa.

DOI : https://doi.org/10.52158/jacost.v5i2.873

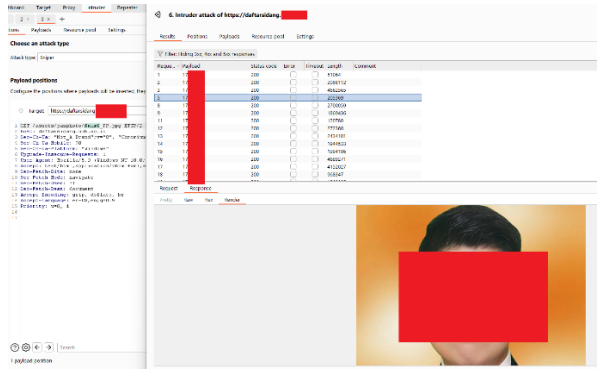


Gambar 5. File Akte Lahir Yang Ada Pada Aplikasi Daftar Sidang

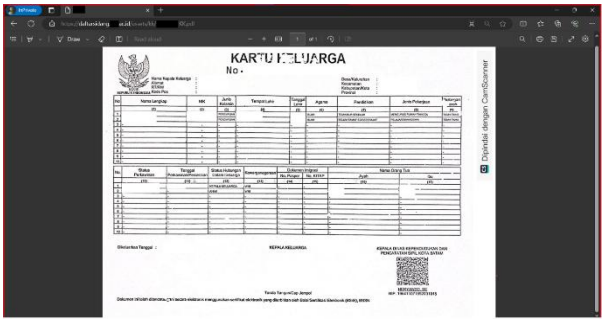


Gambar 6. File Ijazah Terakhir Yang Ada Pada Aplikasi Daftar Sidang

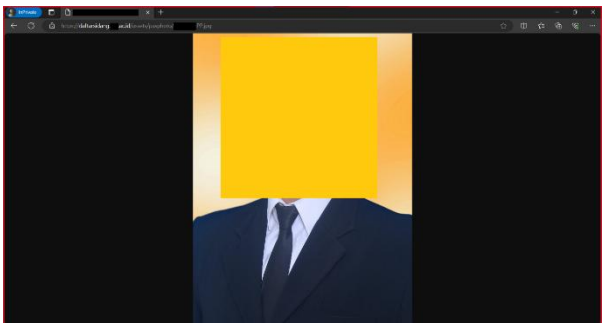
Dengan teknik IDOR yang sama, peneliti melakukan serangan pada objek kartu keluarga dan pas photo menggunakan burp suite, hasil yang didapatkan serupa seperti serangan sebelumnya dimana terdapat respon status code 200 yang menandakan bahwa objek tersebut ada seperti pada Gambar 7. yang menunjukkan tampilan dari objek pas photo mahasiswa. Untuk lebih jelasnya dari NIM yang memberikan respon status code 200, di ujicoba menggunakan browser untuk mengakses langsung objek file kartu keluarga dan pas foto dengan pola Tabel 1. dapat dilihat pada Gambar 8 dan Gambar 9 dimana objek kartu keluarga dan pas foto dapat langsung diakses melalui browser.



Gambar 7. Serangan IDOR pada objek Pas Foto Menggunakan Burp Suite



Gambar 8. File Kartu Keluarga Yang Ada Pada Aplikasi Daftar Sidang



Gambar 9. File Pas Photo Yang Ada Pada Aplikasi Daftar Sidang

Pada tahapan evaluasi, dari hasil pengujian pada aplikasi website daftar sidang Universitas XYZ, terdapat kerentanan IDOR pada objek data pribadi mahasiswa yaitu Kartu Tanda Penduduk, Ijazah Terakhir, Kartu Keluarga, Akte Kelahiran, serta Pas Photo yang diupload kedalam sistem. Objek ini dapat diakses dengan mengetahui pola referensi pada setiap objek.

Hasil penelitian ini menunjukkan bahwa aplikasi website pendaftaran sidang di Universitas XYZ rentan terhadap kerentanan Insecure Direct Object Reference (IDOR). Temuan ini sejalan dengan penelitian sebelumnya yang dilakukan oleh Listartha et al. (2019), yang juga menemukan bahwa banyak aplikasi pendidikan tinggi menghadapi tantangan serupa dalam penerapan kontrol akses yang efektif. Misalnya, dalam studi tersebut, peneliti menunjukkan bahwa meskipun beberapa aplikasi memiliki langkah-langkah keamanan seperti autentikasi, mereka masih dapat dieksploitasi karena kebijakan kontrol akses yang lemah.

Penelitian ini menegaskan pentingnya penerapan kontrol akses yang lebih ketat dan validasi input yang lebih baik untuk mencegah akses tidak sah ke data pribadi mahasiswa. Kerentanan IDOR yang ditemukan memungkinkan penyerang untuk mengakses dokumen pribadi dengan hanya mengetahui pola URL, menunjukkan bahwa keamanan informasi di aplikasi ini belum memadai.

Namun, ada beberapa keterbatasan dalam penelitian ini. Pertama, penelitian dilakukan dengan menggunakan akun mahasiswa yang diberikan untuk pengujian. Hal ini mungkin tidak mencerminkan seluruh potensi serangan yang dapat dilakukan oleh penyerang dengan akses yang

DOI : https://doi.org/10.52158/jacost.v5i2.873

lebih luas. Kedua, penelitian ini terfokus pada satu aplikasi di Universitas XYZ, sehingga hasilnya mungkin tidak sepenuhnya representatif untuk aplikasi lain di institusi pendidikan tinggi di Indonesia. Oleh karena itu, penelitian lebih lanjut diperlukan untuk mengeksplorasi kerentanan di aplikasi pendidikan lainnya serta untuk menguji efektivitas langkah-langkah mitigasi yang diterapkan.

Implikasi dari hasil penelitian ini sangat signifikan. Institusi pendidikan tinggi perlu menyadari pentingnya keamanan data pribadi mahasiswa dan harus mengambil tindakan proaktif untuk memperkuat kebijakan kontrol akses dan meningkatkan sistem keamanan mereka. Upaya ini tidak hanya akan melindungi data mahasiswa tetapi juga akan meningkatkan kepercayaan masyarakat terhadap institusi pendidikan. Selain itu, penelitian ini juga dapat menjadi acuan bagi pengembang aplikasi pendidikan tinggi dalam merancang sistem yang lebih aman dan tahan terhadap serangan siber.

4. Kesimpulan

Berdasarkan hasil penelitian dan analisis yang telah dilakukan terhadap aplikasi website daftar sidang Universitas XYZ, dapat disimpulkan bahwa terdapat kerentanan IDOR yang signifikan. Kerentanan ini memungkinkan akses tidak sah terhadap data pribadi mahasiswa, seperti objek KTP, Kartu Keluarga, Akte Lahir, Ijazah, dan foto pribadi, yang semestinya dilindungi dengan ketat oleh universitas. Pengujian yang dilakukan pada penelitian ini menunjukkan bahwa dengan mengetahui pola referensi NIM pada URL, penyerang dapat dengan mudah mengakses dan mendownload dokumen-dokumen yang bersifat pribadi dan sensitif tanpa perlu memiliki otorisasi yang sesuai. Keberadaan kerentanan ini mengindikasikan bahwa masih terdapat kelemahan dalam implementasi kontrol keamanan aplikasi web yang perlu segera dilakukan untuk melindungi kebocoran data pribadi mahasiswa.

Pembelajaran yang didapatkan dari penelitian ini adalah pentingnya penerapan akses kontrol yang lebih ketat dan verifikasi otorisasi yang lebih cermat, terutama dalam manajemen sesi dan konfigurasi aplikasi. Diperlukan pula penguatan pada kontrol keamanan untuk mencegah manipulasi URL yang dapat membuka celah bagi serangan IDOR. Penggunaan teknik enkapsulasi objek, *Role Based Access Control* (RBAC) dan validasi di server-side dapat diterapkan sebagai langkah yang diterapkan untuk mengurangi risiko eksploitasi kerentanan IDOR. Selain itu, diharapkan adanya peningkatan kesadaran dan kompetensi pengembang dalam menerapkan praktik keamanan aplikasi web agar dapat mengurangi kemungkinan munculnya celah keamanan serupa di masa depan, sehingga, institusi pendidikan tinggi dapat melindungi data pribadi mahasiswa dan meningkatkan kepercayaan masyarakat terhadap keamanan aplikasi mereka

Daftar Rujukan

[1] A. Adisel, "Manajemen Sistem Informasi Pembelajaran," *Journal of Administration and Educational Management (Alignment)*, vol. 2, no. 2, 2019, doi: 10.31539/alignment.v2i2.900.

[2] R. S. Perdana, "Audit Keamanan Sistem Informasi Akademik Menggunakan Framework NIST Sp 800-26 (Studi Kasus : Universitas Sangga Buana YPKP Bandung)," *Infotronik : Jurnal Teknologi Informasi dan Elektronika*, vol. 3, no. 1, 2018, doi: 10.32897/infotronik.2018.3.1.83.

[3] I. N. 'Abidah, M. A. Hamdani, dan Y. Amrozi, "Implementasi Sistem Basis Data Cloud Computing pada Sektor Pendidikan," *KELUWIH: Jurnal Sains dan Teknologi*, vol. 1, no. 2, 2020, doi: 10.24123/saintek.v1i2.2868.

[4] S. Nurul, S. Anggrainy, dan S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim)," *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)*, vol. 3, no. 5, 2022, doi: 10.31933/jemsi.v3i5.

[5] I. I. Nugroho, R. Pratiwi, dan S. R. Az Zahro, "Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia," *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, vol. 1, no. 2, 2021, doi: 10.15294/ipmhi.v1i2.53698.

[6] H. Haeruddin, G. Wijaya, dan H. Khatimah, "Sistem Keamanan Work From Anywhere Menggunakan VPN Generasi Lanjut," *JITU : Journal Informatic Technology And Communication*, vol. 7, no. 2, hlm. 102–113, Nov 2023, doi: 10.36596/jitu.v7i2.1086.

[7] D. D. Firmansyah Putri dan M. H. Fahrozi, "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)," *Borneo Law Review*, vol. 5, no. 1, 2021, doi: 10.35334/bolrev.v5i1.2014.

[8] H. S. Disemadi, N. Z. Silviani, dan D. Jaya,, "Literasi Masyarakat Pesisir terhadap Perlindungan Data Pribadi dalam Transaksi Financial Technology," *Jurnal Abdimasa,* vol. 5, no. 2, 2022.

[9] Z. Hardiansyah, "1,3 Miliar Data SIM Card Diduga Bocor, Begini Respons 3 Opsel dan Kominfo," Kompas Cyber Media. Diakses: 22 Desember 2023. [Daring]. Tersedia pada: https://tekno.kompas.com/read/2022/09/02/10200017/1-3-miliar-data-sim-card-diduga-bocor-begini-respons-3-opsel-dan-kominfo?page=all

[10] N. P. Bestari, "Ulah Hacker Bjorka, 34 Juta Data Paspor Warga RI Dijual Murah," CNBC Indonesia. Diakses: 22 Desember 2023. [Daring]. Tersedia pada: https://www.cnbcindonesia.com/tech/20230705163052-37-451615/ulah-hacker-bjorka-34-juta-data-paspor-warga-ri-dijual-murah

[11] G. D. Prasasti, "Dugaan 337 Juta Data Dukcapil Kemendagri Bocor, Ini Penjelasan Pakar Keamanan Siber," Liputan6. Diakses: 22 Desember 2023. [Daring]. Tersedia pada: https://www.liputan6.com/tekno/read/5346009/dugaan-337-juta-data-dukcapil-kemendagri-bocor-ini-penjelasan-pakar-keamanan-siber?page=2

[12] "Deretan Kasus Kebocoran Data Pribadi di Indonesia Sepanjang 2022-2023," METROTVNEWS.COM. Diakses: 3 Desember 2023. [Daring]. Tersedia pada: https://www.metrotvnews.com/play/NA0CXWqa-deretan-kasus-kebocoran-data-pribadi-di-indonesia-sepanjang-2022-2023

[13] N. Nurhidayati, S. Sugiyah, dan K. Yuliantari, "Pengaturan Perlindungan Data Pribadi Dalam Penggunaan Aplikasi Pedulilindungi," *Widya Cipta: Jurnal Sekretari dan Manajemen*, vol. 5, no. 1, 2021, doi: 10.31294/widyacipta.v5i1.9447.

[14] G. Wijaya dan N. Surantha, "Multi-layered Security Design and Evaluation for Cloud-based Web Application: Case Study of Human Resource Management System," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 5, hlm. 674–679, 2020, doi: 10.25046/aj050583.

[15] H. A. Noman dan O. M. F. Abu-Sharkh, "Code Injection Attacks in Wireless-Based Internet of Things (IoT): A Comprehensive

Review and Practical Implementations," *Sensors*, vol. 23, no. 13. 2023. doi: 10.3390/s23136067.

[16] Mohd. Y. DM, Addermi, dan J. Lim, "Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia," *Jurnal Pendidikan dan Konseling*, vol. 4, 2022, doi: https://doi.org/10.31004/jpdk.v4i5.7977.

[17] S. E. Prasetyo, N. Hasanah, dan G. Wijaya, "Pengujian Keamanan Learning Management System TutorLMS Terhadap Kerentanan Insecure Design dan Broken Access Control," *Telcomatics*, vol. 7, no. 2, 2022, doi: 10.37253/telcomatics.v7i2.7357.

[18] R. A. Putra, I. A. Kautsar, H. Hindarto, dan S. Sumarno, "Detection and Prevention of Insecure Direct Object References (IDOR) in Website-Based Applications," *Procedia of Engineering and Life Science*, vol. 4, 2023, doi: 10.21070/pels.v4i0.1435.

[19] S. Singh dan M. Dandotiya, "An Efficient Approach for Mitigating Insecure Direct Object Reference (IDOR) Bug Bounty Method," *Int J Res Appl Sci Eng Technol*, vol. 11, no. 6, 2023, doi: 10.22214/ijraset.2023.53953.

[20] I. P. A. E. Pratama dan A. M. Rhusuli, "Penetration Testing on Web Application Using Insecure Direct Object References (IDOR) Method," dalam *9th International Conference on ICT for Smart Society: Recover Together, Recover Stronger and Smarter Smartization, Governance and Collaboration, ICISS 2022 - Proceeding*, 2022. doi: 10.1109/ICISS55894.2022.9915074.

[21] M. Yunus, "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework OWASP Versi 4," *Jurnal Ilmiah Informatika Komputer*, vol. 24, no. 1, 2019, doi: 10.35760/ik.2019.v24i1.1988.

[22] E. Listartha, G. Arna, J. Saskara, D. Gede, dan S. Santyadiputra, "Pengujian Kerentanan Dan Penetrasi Keamanan Pada Aplikasi Web Manajemen Skripsi Prodi Xyz," *ScientiCO : Computer Science and Informatics Journal*, vol. 4, no. 2, 2021.

[23] D. Aryanti, Nurholis, dan J. Nashar Utamajaya, "Analisis Kerentanan Keamanan Website Menggunakan Metode Owasp (Open Web Application Security Project) Pada Dinas Tenaga Kerja," *Jurnal Syntax Fusion*, vol. 1, no. 03, 2021, doi: 10.54543/fusion.v1i03.53.

[24] I. P. A. E. Pratamadan dan A. M. Rhusuli, "Penetration Testing on Web Application Using Insecure Direct Object References (IDOR) Method" *International Conference on ICT For Smart Society*, 2022.

[25] S. Yulianto, R. R. Abdullah dan B. Soewito, "Comprehensive Analysis and Remediation of Insecure Direct Object References (IDOR) Vulnerabilities in Android APIs," 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), Bogor, Indonesia, 2023, pp. 23-28, doi: 10.1109/ICoCICs58778.2023.10276919.