Pasinformatik, Volume 5, Issue 1, January 2026
E-ISSN : 2986-5360

Analisis Keamanan Website Universitas Pasundan Menggunakan Metode *Penetration Testing* Berbasis Kerangka Kerja PTES

Yulius Yogi Yuwono*, Doddy Ferdiansyah, Miftahul Fadli Muttaqin*****

Jurusan Teknik Informatika, Fakultas Teknik, Universitas Pasundan
Jln. Dr. Setiabudhi no. 193 Bandung, Jawa Barat
*yulius.203040125@mail.unpas.ac.id, **doddy@unpas.ac.id, ***fadli@unpas.ac.id

Abstrak: Website universitas memiliki peran penting dalam mendukung layanan akademik dan administratif bagi mahasiswa, dosen, dan staf, serta menjadi pusat pengelolaan data institusi. Seiring meningkatnya pemanfaatan tekno*log*i informasi, risiko ancaman keamanan siber terhadap website universitas juga semakin tinggi. Salah satu tantangan utama dalam menjaga keamanan sistem adalah mengidentifikasi dan mencegah kerentanan yang berpotensi dieksploitasi oleh pihak tidak berwenang. Website Universitas Pasundan (www.unpas.ac.id) memiliki potensi terpapar berbagai serangan siber, khususnya *Local File Inclusion* (LFI), *Insecure Direct Object References* (IDOR), dan *Broken Access Control*, yang dapat mengakibatkan kebocoran informasi, modifikasi data, serta gangguan layanan. Penelitian ini bertujuan untuk menganalisis tingkat keamanan website Universitas Pasundan menggunakan teknik *penetration testing* berbasis kerangka kerja *Penetration Testing Execution Standard* (PTES). Metode PTES diterapkan secara sistematis melalui tahapan *information gathering*, *threat modeling*, *vulnerability analysis*, *exploitation*, *post-exploitation*, dan *reporting* untuk mengidentifikasi serta mengevaluasi kerentanan yang ada. Hasil penelitian menunjukkan bahwa beberapa parameter sistem terindikasi rentan terhadap serangan LFI, IDOR, dan *Broken Access Control*. Temuan tersebut mengindikasikan adanya potensi risiko terhadap kerahasiaan, integritas, dan ketersediaan data. Berdasarkan hasil pengujian, penelitian ini memberikan rekomendasi teknis untuk meningkatkan keamanan website, meliputi penerapan kontrol akses yang lebih ketat, peningkatan validasi *input*, serta perbaikan konfigurasi sistem guna meminimalkan risiko eksploitasi kerentanan di masa mendatang.

Kata Kunci: Keamanan Website*, Penetration Testing, Local File Inclusion* (LFI), *Insecure Direct Object References* (IDOR), *Broken Access Control,*

I. PENDAHULUAN

Website telah menjadi pusat interaksi utama bagi universitas di era digital ini, menghubungkan mahasiswa, dosen, staf, dan publik. Website universitas tidak hanya menyajikan informasi akademik, tetapi juga menyimpan data sensitif seperti data pribadi, rekam jejak akademik, dan hasil penelitian. Melindungi data-data tersebut dari ancaman siber yang terus berkembang menjadi krusial, sehingga keamanan siber website universitas perlu mendapat perhatian serius. Seperti yang diungkapkan oleh OWASP (2023), "Aplikasi web modern sering kali menangani data sensitif, seperti informasi pribadi, detail kartu kredit, dan rahasia bisnis. Kerentanan dalam aplikasi web dapat mengekspos data ini kepada penyerang yang tidak sah, yang mengakibatkan kerusakan finansial, kerusakan reputasi, dan masalah hukum." (OWASP, 2023).

PTES menyediakan kerangka kerja umum untuk melakukan *penetration testing* dengan cara yang konsisten dan terstruktur. Ini membantu memastikan bahwa semua area penting dari aplikasi atau sistem diuji secara menyeluruh." (PTES, 2020). Maka sudah selayaknya keamanan jaringan harus lebih diperhatikan untuk melindungi sistem dari ancaman serangan yang semakin canggih dan beragam, terlebih lagi ketika jaringan lokal sudah terhubung ke internet maka ancaman keamanan jaringan akan semakin meningkat. Misalnya ddos *attack* dan sebagainya, juga serangan *hacker*, *virus*, *trojan* yang semuanya merupakan ancaman yang tidak bisa di abaikan (Hasibuan & Elhanafi, 2022).

Keamanan Sistem Informasi adalah bagaimana kita dapat mencegah penipuan cheating atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Menurut Nurul, S. A. (Nurul et al., 2022). *Penetraton Testing* adalah serangkaian metode dan prosedur yang dilakukan dengan tujuan untuk menguji atau melindungi keamanan suatu organisasi. *Penetration Testing* membantu untuk menemukan kerentanan yang ada dalam suatu organisasi dan memeriksa apakah penyerang akan dapat mengeksploitasi hingga mendapatkan akses yang tidak sah (Hidayatulloh & Saptadiaji, 2021). PTES dimulai pada awal tahun 2009 dan berawal dari pertemuan antara anggota pendiri disaat membicarakan tentang kepentingan atau kelemahan dalam *penetration testing* yang ada sekarang (Standard, T, P., 2018). Fase PTES didesain untuk menjelaskan sebuah *Penetration Testing* dan memastika *client* bahwa sebuah usaha *level* standarisasi akan diperluas pada *Penetration Testing* oleh semua orang yang melakukan tipe assestment ini.

Seiring meningkatnya ketergantungan terhadap sistem berbasis web, risiko serangan siber terhadap aplikasi web juga semakin tinggi. Kerentanan pada website dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk memperoleh akses tidak sah, mencuri informasi sensitif, memodifikasi data, hingga mengganggu ketersediaan layanan. Berdasarkan laporan OWASP Top 10, kerentanan aplikasi web yang sering ditemukan antara lain *Local File Inclusion* (LFI), *Insecure Direct Object References* (IDOR), dan *Broken Access Control*. Ketiga jenis kerentanan tersebut berpotensi menimbulkan dampak serius terhadap aspek kerahasiaan, integritas, dan ketersediaan sistem informasi.

Website Universitas Pasundan sebagai salah satu sarana utama layanan digital akademik memiliki potensi risiko keamanan yang perlu dianalisis secara menyeluruh. Kompleksitas sistem, banyaknya subdomain, serta interaksi pengguna yang beragam meningkatkan kemungkinan munculnya celah keamanan. Oleh karena itu, diperlukan suatu pendekatan pengujian keamanan yang sistematis dan terstandar untuk mengidentifikasi serta mengevaluasi kerentanan yang ada pada website universitas. Tujuan dari penelitian ini adalah menganalisis tingkat risiko keamanan website Universitas Pasundan berdasarkan temuan kerentanan LFI, IDOR, dan *Broken Access Control* serta mengevaluasi dampak potensial yang ditimbulkan. Selain itu, penelitian ini juga bertujuan untuk memberikan rekomendasi teknis sebagai upaya mitigasi guna meningkatkan postur keamanan website. Hasil penelitian diharapkan dapat menjadi bahan evaluasi bagi pengelola sistem informasi universitas serta menjadi referensi bagi penelitian selanjutnya di bidang keamanan aplikasi web dan infrastruktur jaringan.

II. KERANGKA DASAR PENELITIAN

A. Penetration Testing pada Aplikasi Web

Penetration testing (uji penetrasi) merupakan metode evaluasi keamanan yang mensimulasikan aktivitas penyerang secara terkendali untuk mengidentifikasi, memverifikasi, dan menilai dampak kerentanan pada sistem. Dalam konteks aplikasi web, penetration testing dilakukan untuk menemukan celah pada permukaan serangan (attack surface) seperti autentikasi, otorisasi, validasi input, manajemen sesi, konfigurasi server, serta kontrol akses terhadap objek dan resource. Hasil uji penetrasi tidak hanya berupa daftar kelemahan, tetapi juga bukti teknis terverifikasi (proof of finding) yang menunjukkan bagaimana kerentanan dapat dieksploitasi dan apa konsekuensi risikonya terhadap kerahasiaan, integritas, serta ketersediaan layanan (CIA triad).

Pada penelitian ini, penetration testing diterapkan sebagai pendekatan terapan (applied security assessment) untuk menilai keamanan website institusi, yaitu Universitas Pasundan (domain: unpas.ac.id). Pengujian difokuskan pada kerentanan aplikasi web yang umum terjadi pada sistem informasi publik, khususnya pada aspek kontrol akses dan pengelolaan input/parameter yang berpotensi memunculkan akses tidak sah maupun kebocoran informasi.

B. Kerangka Penetration Testing Execution Standard (PTES)

Agar proses penetration testing berjalan sistematis dan dapat dipertanggungjawabkan, penelitian ini menggunakan Penetration Testing Execution Standard (PTES) sebagai kerangka dasar (baseline). PTES membagi proses pengujian ke dalam enam fase utama: (1) information gathering, (2) threat modeling, (3) vulnerability analysis, (4) exploitation, (5) post-exploitation, dan (6) reporting. Kerangka ini digunakan sebagai acuan konseptual penelitian dan membantu memastikan aktivitas uji tersusun dari pemetaan target hingga pelaporan rekomendasi mitigasi. Gambar 1 menyajikan Penetration Testing Life Cycle berbasis PTES yang digunakan sebagai rujukan tahap konseptual pada penelitian ini.

Gambar 1. Penetration Testing Life Cycle berbasis PTES

Penjelasan ringkas setiap fase PTES adalah sebagai berikut:

1. Information Gathering: mengumpulkan informasi terkait aset, endpoint, teknologi, serta karakteristik permukaan serangan (mis. struktur URL, parameter umum, modul layanan, dan indikasi teknologi).
2. Threat Modeling: menyusun skenario ancaman berdasarkan informasi awal, termasuk asumsi pelaku, tujuan, dan titik lemah potensial yang diprioritaskan untuk diuji.
3. Vulnerability Analysis: mengidentifikasi indikasi kerentanan melalui pengujian terarah (mis. manipulasi parameter, uji akses objek, dan uji validasi input), serta melakukan validasi awal untuk memisahkan false positive dari temuan nyata.
4. Exploitation: membuktikan kerentanan secara terkendali melalui langkah exploit yang tidak merusak sistem, dengan tujuan memperoleh bukti bahwa celah dapat dimanfaatkan.
5. Post-Exploitation: menilai dampak lanjutan dari exploit terhadap CIA triad, misalnya kemungkinan eskalasi akses, akses data sensitif, atau akses resource yang seharusnya tidak tersedia bagi pengguna tidak berwenang.
6. Reporting: mendokumentasikan temuan, bukti teknis, klasifikasi tingkat risiko (High/Medium/Low), serta rekomendasi mitigasi dan prioritas perbaikan.

Dalam penelitian ini, PTES berfungsi sebagai referensi dasar untuk membingkai alur pengujian. Implementasi operasional (langkah-langkah yang dilakukan, batasan ruang lingkup, dan output tiap tahap) dijelaskan pada bagian Metodologi Penelitian.

III. METODE PENELITIAN

Penelitian ini merupakan penelitian terapan dengan pendekatan evaluatif-teknis melalui penetration testing pada website Universitas Pasundan (https://www.unpas.ac.id). Kerangka kerja yang digunakan adalah PTES sebagai acuan proses (lihat Gambar 1 pada Bagian Kerangka Dasar Penelitian). Pengujian dibatasi pada tiga kategori kerentanan aplikasi web, yaitu Local File Inclusion (LFI), Insecure Direct Object References (IDOR), dan Broken Access Control (BAC).

Objek penelitian adalah aplikasi/layanan web pada domain unpas.ac.id yang dapat diakses secara publik. Ruang lingkup pengujian meliputi identifikasi endpoint dan parameter yang relevan, validasi indikasi kerentanan, serta pembuktian temuan secara terkendali. Penelitian ini tidak melakukan tindakan yang dapat mengganggu ketersediaan layanan (mis. DoS), tidak mengubah data produksi, dan tidak melakukan perusakan sistem.

Prosedur pengujian dilakukan melalui langkah operasional berikut:

1) Pemetaan target: menginventarisasi halaman/endpoint, pola URL dan parameter, serta indikasi teknologi yang digunakan.
2) Perumusan skenario uji: menentukan prioritas uji untuk LFI, IDOR, dan BAC berdasarkan endpoint yang ditemukan.
3) Uji dan validasi kerentanan:
   a. LFI: menguji parameter yang berpotensi memuat file/path dengan variasi input untuk melihat adanya indikasi akses file lokal.
   b. IDOR: menguji perubahan nilai referensi objek (mis. ID) untuk melihat apakah akses terhadap objek lain dapat terjadi tanpa otorisasi yang semestinya.
   c. BAC: menguji konsistensi kontrol akses terhadap fitur/endpoint yang seharusnya dibatasi berdasarkan peran (role) atau status autentikasi.
4) Pembuktian temuan (controlled exploitation): melakukan pembuktian minimal (minimum proof) untuk memastikan temuan valid, tanpa melampaui ruang lingkup dan tanpa menurunkan ketersediaan layanan.
5) Dokumentasi bukti: mencatat endpoint/parameter yang diuji, respons sistem (mis. status code, respons body yang relevan), serta bukti pendukung (screenshot/log) untuk setiap temuan.
6) Penyusunan rekomendasi: merumuskan mitigasi teknis yang spesifik untuk tiap temuan (mis. penguatan otorisasi server-side, validasi input, pembatasan akses berbasis role/ownership).

Setiap temuan diklasifikasikan ke tingkat risiko High/Medium/Low berdasarkan kombinasi kemudahan eksploitasi dan dampak terhadap kerahasiaan, integritas, dan ketersediaan (CIA triad). Klasifikasi ini digunakan untuk menentukan prioritas perbaikan dan menyusun rekomendasi mitigasi yang terarah.

Pengujian dilakukan secara bertanggung jawab dengan prinsip tidak merusak, tidak mengubah data produksi, dan tidak mengganggu layanan. Bukti yang dikumpulkan dibatasi pada kebutuhan verifikasi temuan dan tidak dipublikasikan secara rinci apabila dapat meningkatkan risiko penyalahgunaan.

IV. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil pelaksanaan pengujian keamanan pada website Universitas Pasundan menggunakan metodo*logi* *Penetration Testing* Execution Standard (PTES). Pengujian difokuskan pada tiga kategori kerentanan utama, yaitu *Local File Inclusion* (LFI),

Insecure Direct Object References (IDOR), dan *Broken Access Control* (BAC). Proses pengujian dilakukan secara sistematis sesuai tahapan PTES yang meliputi *information gathering*, threat modeling, vulnerability analysis, exploitation, post-exploitation, dan reporting.

Hasil pengujian menunjukkan bahwa website Universitas Pasundan memiliki beberapa celah keamanan dengan tingkat risiko yang bervariasi. Temuan kerentanan ini mengindikasikan adanya kelemahan pada mekanisme validasi *input*, pengelolaan hak akses, serta kontrol otorisasi pengguna. Kerentanan tersebut berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengakses data sensitif, memodifikasi informasi, atau mengganggu layanan sistem informasi akademik.

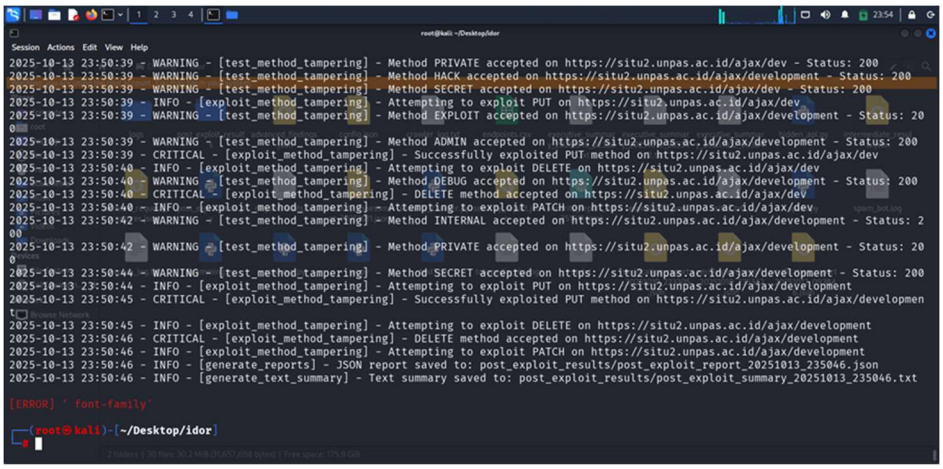
A. Hasil Pengujian Kerentanan *Local File Inclusion* (LFI)

Pengujian Local File Inclusion dilakukan dengan menganalisis parameter URL yang menerima *input* dari pengguna dan berpotensi memanggil *file* pada sisi *server*. Berdasarkan hasil *information gathering*, ditemukan beberapa *endpoint* yang menggunakan parameter dinamis untuk menampilkan konten tertentu. Parameter tersebut diuji dengan teknik *directory traversal* untuk mengidentifikasi kemungkinan akses terhadap *file* sistem. Hasil pengujian menunjukkan bahwa pada kondisi tertentu, aplikasi tidak melakukan validasi *input* secara ketat. Hal ini memungkinkan terjadinya percobaan pembacaan *file* internal *server*. Meskipun tidak semua payload berhasil dieksploitasi, respons sistem mengindikasikan adanya kelemahan pada mekanisme *input sanitization*. Temuan ini dikategorikan sebagai risiko *medium*, karena dalam skenario tertentu dapat berkembang menjadi risiko tinggi apabila dikombinasikan dengan kesalahan konfigurasi *server*.

Gambar 2. Hasil dari *Local File Inclusion*

B. Hasil Pengujian Kerentanan *Insecure Direct Object References* (IDOR)

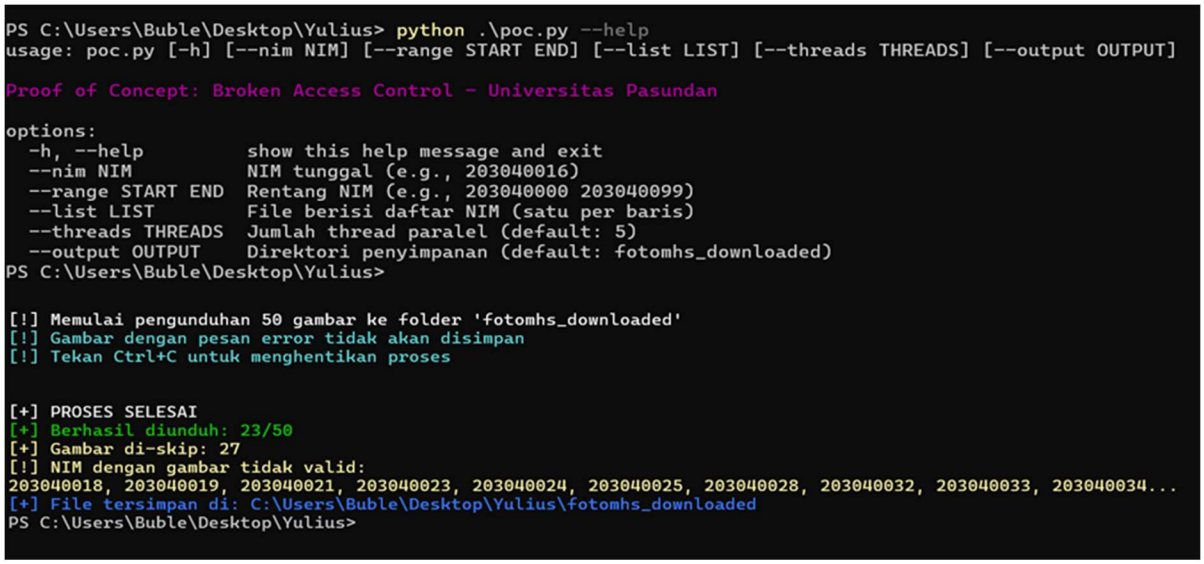
Pengujian IDOR difokuskan pada pengaksesan objek data melalui manipulasi parameter identitas, seperti ID pengguna atau ID dokumen. Berdasarkan hasil observasi, beberapa fitur aplikasi menggunakan parameter numerik secara langsung tanpa mekanisme verifikasi kepemilikan objek. Hasil pengujian menunjukkan bahwa dengan memodifikasi nilai parameter tertentu, pengguna dapat mengakses data yang seharusnya tidak memiliki hak akses. Kondisi ini mengindikasikan lemahnya kontrol otorisasi pada lapisan aplikasi. Kerentanan IDOR yang ditemukan memiliki tingkat risiko *high*, karena berpotensi menyebabkan kebocoran data pribadi dan informasi akademik.



Gambar 3. Hasil dari *Insecure Direct Object References*

C. Hasil Pengujian Kerentanan *Broken Access Control*

Pengujian *Broken Access Control* dilakukan dengan menguji pembatasan hak akses antara peran pengguna yang berbeda. Pengujian mencakup upaya mengakses fitur administratif menggunakan akun dengan hak akses terbatas. Hasil pengujian menunjukkan bahwa terdapat beberapa fungsi yang masih dapat diakses tanpa otorisasi yang sesuai. Kondisi ini menunjukkan bahwa penerapan kontrol akses belum sepenuhnya mengikuti prinsip least privilege. Kerentanan ini dikategorikan sebagai risiko *high*, karena memungkinkan eskalasi hak akses dan penyalahgunaan sistem.



Gambar 4. *Log* Terminal Eksekusi Skrip Eksfiltrasi Foto Mahasiswa

D. Pembahasan

Temuan kerentanan LFI, IDOR, dan *Broken Access Control* menunjukkan bahwa website Universitas Pasundan masih memiliki kelemahan pada aspek keamanan aplikasi web. Hasil ini sejalan dengan temuan OWASP Top 10 yang menyebutkan bahwa kontrol akses yang tidak memadai dan validasi *input* yang lemah merupakan penyebab utama kebocoran data pada aplikasi web modern (OWASP, 2023). Jika dibandingkan dengan penelitian sejenis dalam lima tahun terakhir, hasil penelitian ini memiliki kesamaan dalam pola kerentanan, khususnya pada IDOR dan *Broken Access Control*. Namun, kontribusi utama penelitian ini terletak pada penerapan metodo*log*i PTES secara menyeluruh pada lingkungan universitas, yang masih relatif jarang dilakukan pada penelitian sebelumnya.

1. Eksploitasi : Kerentanan ini teridentifikasi pada *endpoint* foto mahasiswa (https://situ2.unpas.ac.id/uploads/unpas/fotomhs/{NIM}.jpg). Penelitian ini membuktikan bahwa *endpoint* ini tidak memiliki validasi otorisasi berbasis sesi (session). Dengan memanipulasi parameter NIM pada URL, request HTTP GET berhasil mengakses data (foto) milik mahasiswa lain. Post-Eksploitasi: Untuk mendemonstrasikan dampak risiko tinggi, penulis mengembangkan custom script Python. Script ini berhasil melakukan eksfiltrasi data (unduhan foto) secara massal, membuktikan adanya kebocoran data pribadi dalam skala besar.
2. Eksploitas i: Kerentanan ini dieksploitasi menggunakan teknik Method Tampering pada hidden API *endpoint*s (misal: /ajax/development). Penulis membuktikan bahwa *endpoint* yang seharusnya bersifat read-only (hanya menerima GET) ternyata juga menerima request HTTP berbahaya (PUT dan DELETE) tanpa autentikasi yang valid. Post-Eksploitasi: Menggunakan custom script PostExploitationFramework, penulis berhasil mengirimkan payload PUT/DELETE yang diterima oleh *server* (HTTP 200 OK). Ini mengonfirmasi potensi modifikasi dan penghapusan data arbitrer oleh penyerang.
3. Eksploitasi : Kerentanan teridentifikasi pada *endpoint* OJS (journal.unpas.ac.id). Payload LFI yang dimanipulasi tidak mengembalikan *file* sistem, melainkan string Base64 yang mencurigakan, yang mengindikasikan information disclosure. Post-Eksploitasi: Penulis melakukan investigasi dengan decoding berlapis (Langkah 1: Base64 Decode, Langkah 2: URL Decode). Proses ini berhasil mengungkap data konfigurasi internal yang sensitif, termasuk data kontak (WhatsApp, SMS, dan email).

Selain itu, penelitian ini tidak hanya mengidentifikasi kerentanan, tetapi juga menyajikan simulasi eksploitasi yang menggambarkan dampak nyata terhadap sistem. Pendekatan ini memberikan nilai tambah dibandingkan penelitian terdahulu yang umumnya berhenti pada tahap pemindaian kerentanan. Hasil penelitian ini menegaskan pentingnya penerapan secure coding practices, access control enforcement, serta pengujian keamanan secara berkala. Dengan memperbaiki kerentanan yang ditemukan, universitas dapat meningkatkan kepercayaan pengguna dan melindungi data akademik dari ancaman siber yang semakin kompleks.

V. KESIMPULAN

Penelitian ini berhasil mengevaluasi tingkat keamanan website Universitas Pasundan dengan mengidentifikasi tiga kategori kerentanan kritis, yaitu *Local File Inclusion* (LFI), *Insecure Direct Object References* (IDOR), dan *Broken Access Control*. Berdasarkan pengujian menggunakan kerangka kerja PTES, ditemukan bahwa kerentanan IDOR dan *Broken Access Control* berada pada tingkat risiko *High* karena memungkinkan penyerang melakukan eksfiltrasi data pribadi (foto mahasiswa) secara massal melalui *custom script* serta manipulasi data melalui *endpoint* API yang tersembunyi. Sementara itu, kerentanan LFI dikategorikan pada risiko *medium* yang berpotensi mengungkap informasi konfigurasi internal *server*. Temuan ini mengonfirmasi adanya kelemahan signifikan pada mekanisme validasi *input* dan kontrol otorisasi berbasis sesi (*session*) pada aplikasi. Sebagai langkah mitigasi, universitas disarankan untuk segera menerapkan *secure coding practices*, memperketat kontrol akses dengan prinsip *least privilege*, serta melakukan pengujian keamanan secara periodik guna melindungi integritas dan kerahasiaan data akademik.

REFERENSI

[1] Hasibuan, M., & Elhanafi, A. M. (2022). *Penetration Testing* Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Black Box.
[2] Hidayatulloh, S., & Saptadiaji, D. (2021). *Penetration Testing* pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). 77–86.
[3] Jaringan, T., & Koprawi, M. (2020). InfoTekJar : Jurnal Nasional Informatika dan Dampak dan Pencegahan Serangan File Inclusion: Perspektif Developer. 2, 0–4.
[4] Judul, H., Industri, F. T., & Indonesia, U. I. (2020). PENGEMBANGAN APLIKASI USERNAME FINDER BERBASIS OSINT FRAMEWORK UNTUK.
[5] Khaldun, U. I. (2020). ANALISIS KEAMANAN APLIKASI WEB PRODI TEKNIK INFORMATIKA UIKA MENGGUNAKAN ACUNETIX WEB. 2, 110–120.
[6] Muhyidin, Y., Totohendarto, M. H., Undamayanti, E., & Salsabilla, C. N. (2015). Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking Comparison of Website Security Levels Using Nmap and Nikto with Ethical Hacking Methods. 1–10.
[7] Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM). 3(5), 564–573.
[8] Putra, R. A., & Kautsar, I. A. (2023). Procedia of Engineering and Life Science Vol. 4 June 2023 Detection and Prevention of *Insecure Direct Object References* (IDOR) in Website-Based Applications Deteksi dan Pencegahan *Insecure Direct Object References* (IDOR) Pada Aplikasi Berbasis Website. 4(June).
[9] Raharjo, S., & Iswahyudi, C. (2023). ANALISIS KEAMANAN JARINGAN MIKROTIK ISP INDONESIA MENGGUNAKAN SEARCH ENGINE SCADA SHODAN DENGAN METODE EXPLOIT WINBOX CRITICAL VULNERABILITY. 11(01), 17–23.
[10] Ramadhan, M. F. A., Ilmananda, A. S., Informasi, F. T., Malang, U. M., Candi, P., Malang, K., Timur, J., Acaman, A., & Testing, V. (2024). KAMPUS MENGGUNAKAN METODE OWASP ZAP. 8(4), 7985–7991.