Jurnal Informasi dan Teknologi

https://jidt.org/jidt

2023 Vol. 5 No. 2 Hal: 120-128 e-ISSN: 2714-9730

Evaluasi Keamanan Privilege Terintegerasi JSON Web Token pada Sistem Informasi Akademik

Irwan Darmawan[1✉], Muhammad Umar Mansyur[2], Khana Zulfana Imam[3], Moh. Syahdan[4]

[1,2,3,4] Fakultas Teknik Universitas Madura

darmawan@unira.ac.id

Abstrak

Penelitian Ini Menggunakan Metode Eksperimental Untuk Mengukur Pengaruh Pendaftaran Online Terhadap Kepuasan Pengguna. Terdapat Enam Tahapan Dalam Penelitian Ini, Yaitu Identifikasi Masalah, Tinjauan Pustaka, Penentuan Variabel, Pengumpulan Data, Analisis Data, Dan Kesimpulan. Identifikasi Masalah Difokuskan Pada Otorisasi Menggunakan JSON Web Token (JWT) Pada Sistem Informasi Akademik Terpadu. Studi Pustaka Dilakukan Untuk Memahami Teori Keamanan Privilege, JWT, Dan Sistem Informasi Manajemen Akademik Terpadu. Temuan Penelitian Menunjukkan Bahwa JWT Dapat Digunakan Untuk Otorisasi Pengguna Pada Sistem Informasi Akademik Terpadu. Penelitian Sebelumnya Juga Mengungkapkan Risiko Keamanan Pada Sistem Informasi Akademik Tanpa Enkripsi. Variabel Penelitian Meliputi Keamanan Otentikasi, Keamanan Privilege, JWT, Dan Sistem Informasi Manajemen Akademik Terpadu. Data Dikumpulkan Melalui Observasi, Wawancara Dengan Pembuat Sistem, Dan Uji Penetrasi. Analisis Data Dilakukan Untuk Mengidentifikasi Kelemahan Dalam Sistem Otorisasi Menggunakan JWT Dan Memberikan Rekomendasi Peningkatan Keamanan. Analisis Ini Mengevaluasi Keamanan Privilege Pada Sistem Informasi Akademik Terpadu Yang Menggunakan JWT. Dalam Tahap Kesimpulan, Temuan Dari Analisis Data Digunakan Untuk Menyimpulkan Hasil Penelitian Dan Memberikan Rekomendasi Pengembangan Penelitian Selanjutnya. Penelitian Ini Memberikan Pemahaman Lebih Lanjut Tentang Pengaruh Pendaftaran Online Dan Manfaat Penggunaan JWT Dalam Meningkatkan Keamanan Dan Kinerja Sistem Informasi Akademik Terpadu.

Kata Kunci: JWT, Privilege, Otorisasi, Sistem Informasi Akademik, Otentikasi.

1. Pendahuluan

Sistem Informasi Manajemen Akademik Terpadu memiliki peran yang sangat penting dalam menjalankan berbagai kegiatan administrasi dan manajemen di lingkungan Universitas. Dalam era digital dan kebutuhan akan keamanan yang semakin meningkat, menjaga keamanan otorisasi dalam system informasi menjadi suatu hal yang krusial[1]. Pasal 28G ayat (1) UUD 1945 menjelaskan bahwa setiap orang berhak atas perlindungan data pribadi[2]. Dari pasal tersebut dapat disimpulkan bahwa keamanan data yang dibocorkan dapat menjadi tindak pindana. Selaras dengan upaya dalam mewujudukan perlindungan data. Maka, diperlukan system informasi yang memang dirancang dengan tingkat keamanan yang tinggi[3]. Salah satu metode yang dapat digunakan dalam proses otentikasi dan mengamankan otorisasi adalah JSON Web Token (JWT)[4], [5]. Namun, penting untuk mengevaluasi keamanan dan efektivitas mekanisme otorisasi yang diimplementasikan menggunakan JWT. Evaluasi tersebut bertujuan untuk memastikan bahwa hak akses pengguna terlindungi secara efektif dan mencegah serangan serta penyalahgunaan yang berpotensi terjadi[6], [7].

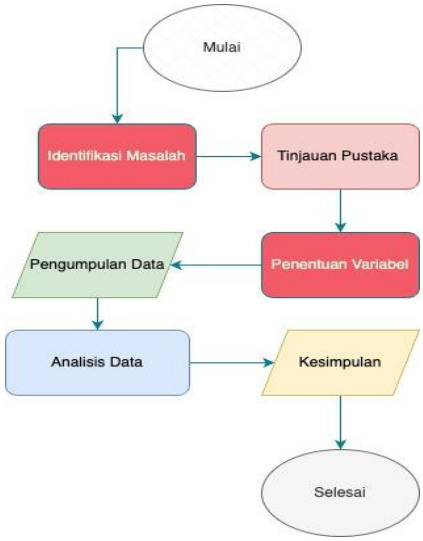
Dalam penelitian ini, peneliti akan melakukan analisis mendalam terhadap implementasi dan penggunaan JSON Web Token (JWT) dalam system informasi akademik. Tempat penelitian yang diambil adalah Universitas Madura. Mengingat, Universitas Madura mengimplementasikan JSON WEB Token dalam proses otorisasi dan otentikasinya. Adapun metode penelitian yang digunakan meliputi pengumpulan data, pengamatan langsung terhadap sistem, serta uji penetrasi terhadap keamanan otorisasi. Hasil evaluasi akan memberikan gambaran yang jelas mengenai keamanan otorisasi yang ada dalam SIMAT, serta identifikasi potensi kerentanan yang perlu diperhatikan. Melalui evaluasi ini, diharapkan akan diperoleh pemahaman yang lebih baik tentang keamanan privilege dan penerapan yang tepat dari JSON Web Token (JWT) dalam system informasi akademik khusunya system informasi akademik di universitas madura. Harapan dari hasil penelitian ini dapat memberikan wawasan yang berguna bagi pengembangan dan perbaikan sistem otorisasi dalam SIMAT. Selain itu, dengan pemahaman yang lebih baik tentang keamanan otorisasi khususnya di Universitas Madura dapat memastikan bahwa data dan hak akses pengguna terlindungi dengan baik, serta mencegah risiko kejahatan di dunia cyber yang dapat membahayakan integritas dan kerahasiaan sistem.

Diterima: 06-07-2023 | Revisi: 06-07-2023| Diterbitkan: 06-07-2023 | doi: 10.37034/jidt.v5i1.368

Penelitian ini diharapkan dapat memberikan kontribusi yang berarti dalam pengembangan keamanan otorisasi dalam sistem informasi manajemen akademik terpadu. Selain itu, hasil penelitian ini juga diharapkan dapat memberikan manfaat yang nyata bagi Universitas Madura dalam menjaga integritas dan keamanan data di lingkungan akademik.

2. Metode Penelitian

Metode penelitian yang akan digunakan adalah metode eksperimental. Metode eksperimental merupakan penelitian yang dilakukan dengan memberikan perlakuan guna membangkitkan reaksi dari apa yang diteliti untuk mengetahui akibatnya[8], [9]. Untuk lebih jelasnya mengenai alur atau tahapan yang dilakukan pada penelitian ini, lihat gambar 1. Objek tempat penelitian yang akan dilakukan adalah Universitas Madura.



Gambar 1 Tahapan Penelitian

Pada gambar 1 terdapat 6 tahapan dalam penelitian yang akan dilakukan. Tahapan pertama adalah identifikasi masalah, kemudian dilanjutkan dengan tahapan kedua yaitu tinjauan Pustaka. Tahapan ketiga adalah penentuan variable. Dari penentuan hasil penentuan variable tersebut tahapan yang akan ditempuh selanjutnya adalah analisis data. Kemudian tahapan terakhir adalah memberikan kesimpulan berdasarkan penelitian yang telah dilakukan.

2.1. Indentifikasi Masalah

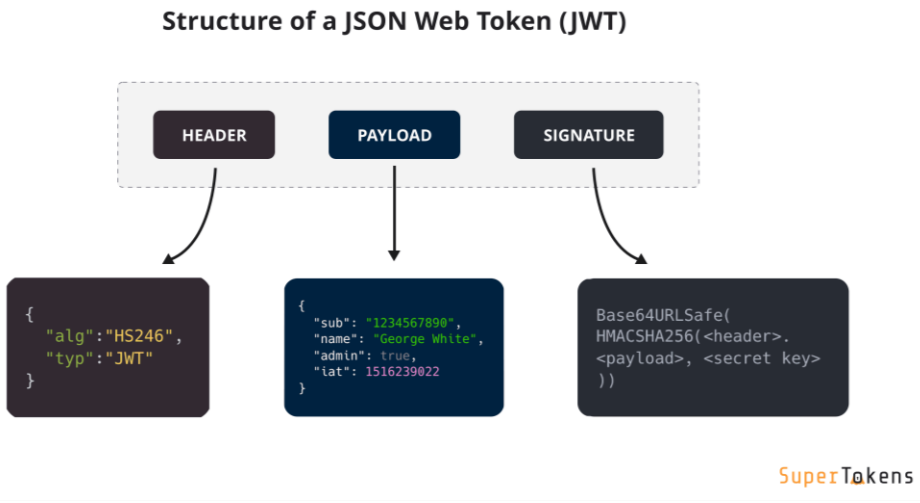
Tahap ini merupakan tahapan awal dimana peneliti melakukan identifikasi masalah terhadap permasalahan yang akan diteliti. Tahapan ini memiliki fungsi untuk membatasi lingkup penelitian agar tidak terlalu luas sehingga akan lebih mudah untuk dilakukan. Penelitian ini akan fokus pada masalah keamanan otorisasi dalam sistem informasi akademik terpadu yang menggunakan JSON Web Token (JWT). Adapun masalah yang akan diteliti meliputi kelemahan dalam mekanisme otorisasi, masa kadaluarsa token setelah logout, keamanan dalam penyimpanan token, dan kekurangan dalam implementasi audit logging. Dengan membatasi lingkup penelitian pada masalah-masalah tersebut, peneliti akan menganalisis dan mengevaluasi kelemahan yang ada serta memberikan rekomendasi untuk meningkatkan keamanan otorisasi dalam sistem informasi akademik terpadu menggunakan JSON Web Token (JWT).

2.2. Tinjauan Pustaka

Pada tahap ini, peneliti perlu melakukan studi pustaka untuk memahami dasar teori yang terkait dengan keamanan privilege, JSON Web Token (JWT), dan sistem informasi manajemen akademik terpadu. Selain itu, peneliti juga perlu mengumpulkan informasi mengenai penelitian terdahulu yang terkait dengan masalah yang akan diteliti.

2.2.1 JSON Web Token (JWT)

JWT merupakan sebuah token yang menyimpan informasi untuk proses otentikasi dan penukaran informasi [10], [11]. JWT umumnya digunakan dalam proses otorisasi karena token yang dihasilkan berisi informasi mengenai siapa yang mengakses system [12], [13]. Informasi yang terdapat pada token JWT dapat dilihat pada gambar 2.



Gambar 2 Jenis Informasi Token JWT

Sumber: SuperTokens.com

Pada gambar 2 terdapat 3 jenis informasi yang disimpan di dalam token. 3 jenis informasi tersebut adalah *header*, *payload* dan *signature*[14]. Pada header, terdapat informasi tentang jenis token dan penandatanganan algoritma yang digunakan[15], [16]. Kemudian di bagian payload terdapat beberapa data dari transaksi tersebut [17]. Sistem yang menggunakan JWT dapat menyimpan informasi tentang pengguna di bagian payload ini. Bagian terakhir dari JWT adalah signature. Di bagian signature ini terdapat secret key atau kunci rahasia yang digunakan sebagai proses enkripsi validasi dari header dan payload[18]

Pada sumber lain, terdapat penelitian tentang sistem informasi akademik yang melakukan proses otentikasi secara manual tanpa enkripsi dengan menggunakan JWT. Penelitian tersebut menunjukkan bahwa akun mahasiswa dapat termonitoring oleh data sesi HTTP POST. Penelitian tersebut juga mengungkapkan bahwa proses otentikasi secara manual tanpa adanya enkripsi saat di-post ke server memiliki risiko tinggi terhadap keamanan data[19].

2.3. Penentuan Variabel

Setelah tahap tinjauan pustaka telah selesai ditempuh maka, langkah selanjunya dalam penelitian ini adalah menentukan variabel-variabel yang akan diteliti. Adapun variabel yang akan diteliti dalam penelitian ini adalah keamanan otentikasi dan privilege pada sistem informasi manajemen akademik terpadu menggunakan JSON Web Token (JWT). Untuk lebih jelasnya tentang variabel yang ditentukan perhatikan tabel 1.

Tabel 1. Tabel Penentuan Variabel

Variabel	Keterangan	Tipe Variabel
Keamanan Otentikasi	Tingkat keamanan proses otentikasi pada sistem informasi manajemen akademik terpadu di Universitas Madura menggunakan JSON Web Token (JWT)	Dependen
Keamanan Privilege	Tingkat keamanan proses privilege pada sisten informasi manajemen akademik terpadu di Universitas Madura menggunakan JSON Web Token (JWT)	Dependen
JSON Web Token	Token yang digunakan untuk proses otentikasi dan privilege pada system informasi manajemen akademik terpadu	Independen
Sistem Informasi Manajemen Akademik Terpadu	Sistem yang digunakan untuk manajemen data akademik di Universitas Madura	Kontrol

2.4. Pengumpulan Data

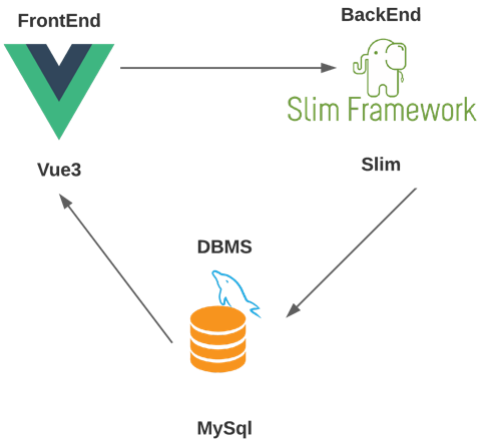
Pada tahap ini, peneliti melakukan pengumpulan data melalui beberapa tahapan. Tahapan tersebut antara lain dapat dilihat sebagaimana berikut:

2.4.1 Uji Penetrasi

Melakukan uji penetrasi terhadap sistem. Uji penetrasi dilakukan dengan menggunakan beberapa pendekatan seperti memodifikasi jenis informasi yang tersimpen di dalam token. Kemudian mengirim token hasil modifikasi ke system. Hasil uji penetrasi akan dicatat oleh peneliti dan akan dilakukan analisa terhadap data yang didapatkan. Uji Penetrasi melibatkan aplikasi HTTP Client. Mengingat kemudahan dalam menginject token modifikasi terhadap system.

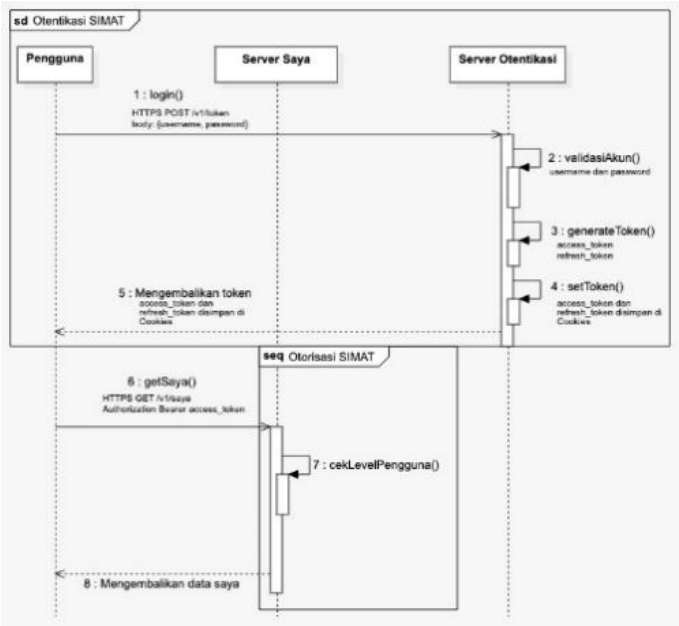
2.4.2 Inverview

Secara kesluruhan, Sistem Informasi Manajemen Akademik Terpadu di Universitas Madura menggunakan framework yang terdiri dari framework back end dan front end. Stack tersebut dapat dilihat pada gambar 3. Pada gambar 3. Terdapat 3 stack yang digunakan dalam membangun Sistem Informasi Manajemen Akademik Terpadu di Universitas Madura. Di sisi frontend framework yang digunakan adalah Vue3. Sedangkan di bagian backend, framework yang digunakan adalah Slim. Database management system yang digunakan adalah MySql.



Gambar 3 Arsitektur SIMAT UNIRA

Dari arsitektur pada gambar 3. Selanjutnya peneliti menginterview tim pengembang SIMAT dan menghasilkan *flow* dari proses otentikasi berbasis jwt. Alur dari proses otentikasi digambarkan dengan sequence diagram. Sequence diaram adalah suatu diagram yang menggambarkan interaksi antara objek dalam sebuah system dalam bentuk sequence atau urutan pesan yang dikirimkan diantara objek-objek[20]. Untuk lebih jelasnya perhatikan gambar 4.



Gambar 4 Sequence Diagram Otentikasi dan Otorisasi SIMAT

Pada gambar 4. Proses pertama yang dilakukan adalah login. Proses login mengirimkan body username dan password dalam bentuk Objek berupa JSON. Kemudian JSON tersebut dikirimkan ke endpoint /v1/token. Server akan melakukan proses validasi terhadap JSON yang dikirim. Jika JSON yang dikirim terverifikasi maka secara otomatis, token akan dibuat dan akan disimpan pada session storage yang ada pada browser pengguna.

Proses yang terjadi pada gambar 4. Melibatkan komunikasi antara sisi client dengan server. Dari sisi client, username dan password dikirimkan ke server. Sedangkan dari sisi server akan menerima username dan password yang dikirimkan oleh client. Karena proses penyimpanan token disimpan pada session storage pada browser maka proses penyimpanan token dilakukan di sisi client. Proses yang dilakukan tersebut adalah proses otententikasi.

Pada proses otorisasi, client akan menggunakan access_token yang telah disimpan pada session storage untuk melakukan request ke server dengan method GET pada endpoint /v1/saya. Selanjutnya, access_token akan disertakan di header dengan tipe otorisasi bearer. Kemudian server akan mendecode token access tersebut menggunakan secret key pada JWT untuk memastikan apakah token yang didecode tersebut valid atau tidak.
Jika acces_token yang didecode valid, maka server akan memberikan akses kepada client untuk mengakses endpoint /v1/saya. Namun jika access_token tidak valid atau sudah tidak berlaku, maka server akan memberikan response error kepada client. Proses otorisasi bertujuan untuk memastikan bahwa hanya pengguna yang memiliki hak akses yang sesuai yang dapat mengakses data pada endpoint tertentu.

2.5 Analisis Data

Pada tahap ini, data yang telah dikumpulkan akan dilakukan analisis data untuk mengevaluasi kemananan privilege pada sistem informasi akademik terpadu menggunakan JSON Web Token (JWT). Adapun tujuan dari analisis data adalah peneliti dapat mengidentifikasi masalah dan potensi risiko keamanan yang terkait dengan pengunaan JWT pada sistem, serta menghasilkan rekomendasi untuk meningkatkan keamanan dan kinerja dari sistem yang diteliti.

2.6. Kesimpulan

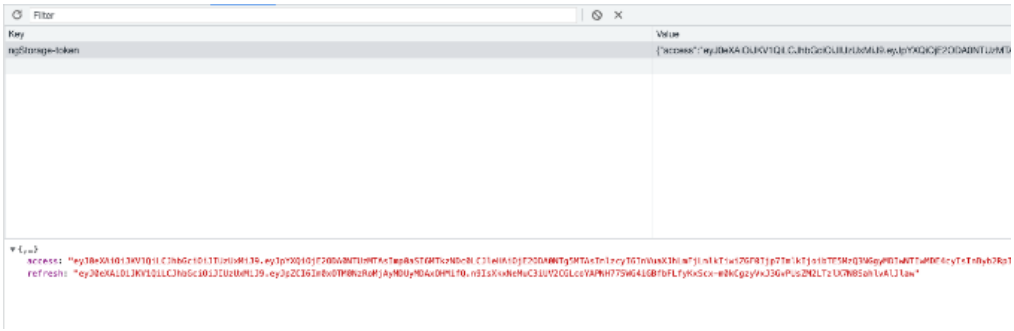
Tahap ini merupakan tahap terakhir dalam penelitian ini. Hasil dari analisis data yang dilakukan oleh peneliti dapat memberikan kesimpulan berupa fakta dari data yang didapatkan. Pada tahapan ini, peneliti akan menyimpulkan hasil dari apa yang telah diteliti serta akan memberikan rekomendasi atau saran terkait pengembangan penelitian selanjutnya.

3 Hasil dan Pembahasan

Adapun tujuan utama dari penelitian ini adalah untuk mengetahui dan mengevaluasi keamanan otorisasi yang terdapat pada system informasi manajemen akademik terpadu di universitas madura. Dari metode penelitian yang telah ditulis sebelumnya, terdapat tahap pengumpulan data. Dalam tahap pengumpulan data terdapat 3 langkah yang ditempuh yaitu, melakukan pengamatan dan wawancara dengan pembuat sistem. Melakukan uji penetrasi terhadap sistem kemudian membuat anilis dari data yang telah dikumpulkan.

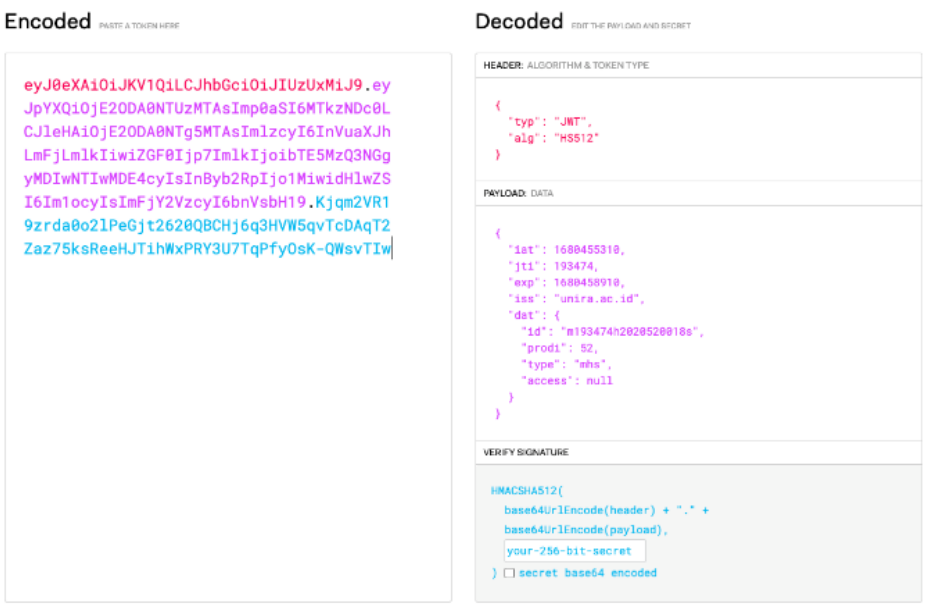
Pengujian pertama dilakukan dari sisi backend, pertama peneliti mengaktifkan aplikasi wireshark untuk memonitoring inputan username dan password. Monitoring dilakukan dengan cara menghubungkan 2 perangkat pada jaringan wifi yang sama. Kemudian, wireshark dihidupkan. Selang waktu 5 detik saat perangkat lain login menggunakan akun yang telah terdaftar. Wireshark tidak dapat mengcapture password dan username user yang dimasukkan pada device lain. Dimana device lain tersebut sudah terhubung dengan jaringan yang sama

Karena cara tersebut tidak berhasil, pengujian kedua, peneliti memantau session storage yang terdapat pada menu application dalam browser chrome. Setelah di amati, dalam menu session storage terdapat token_access, dan refresh. Session storage yang tersimpan pada browser dapat dilihat pada gambar 5.



Gambar 5 Token di Session Storage

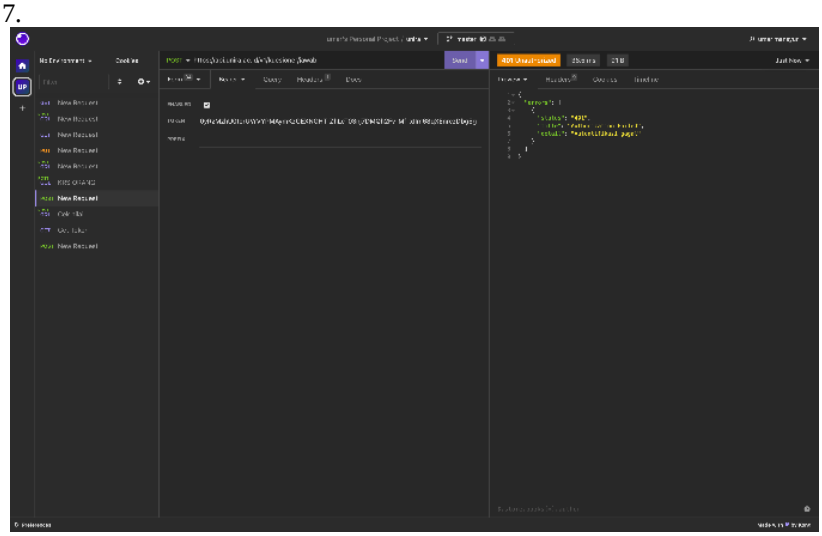
Karena token_access merupakan token yang menyimpan informasi maka selanjutnya, token tersebut di decode melalui website jwt.io. Untuk lebih jelasnya perhatikan gambar 6.



Gambar 6 Decode Token

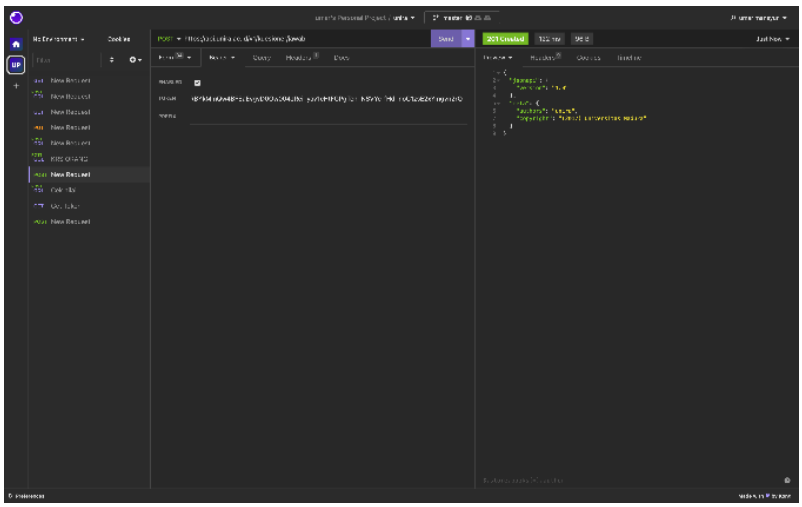
Pada gambar 6. Terdapat 3 jenis informasi yang telah disimpan. Kemudian peneliti mencoba mengubah type yang awalnya mhs menjadi admin dibagian payload. Header dan signature dibiarkan. Token hasil modifikasi kemudian dimasukkan ke token yang lama. Namun cara tersebut tetap tidak berhasil. Karena secret_key yang terdapat di JWT ikut berubah ketika ada perubahan di bagian payload. Perubahan tersebutlah yang dapat menyebabkan sistem dapat mengenali secret_key yang tidak sesuai dengan secret_key yang telah disimpan di sisi server.

Pengujian ketiga, peneliti menggunakan bantuan software http client insomnia. Peneliti menyimpan token lama yang telah di logout oleh user. Kemudian, token tersebut diletakkan pada header menggunakan otorisasi bearer. Perhatikan gambar 7.



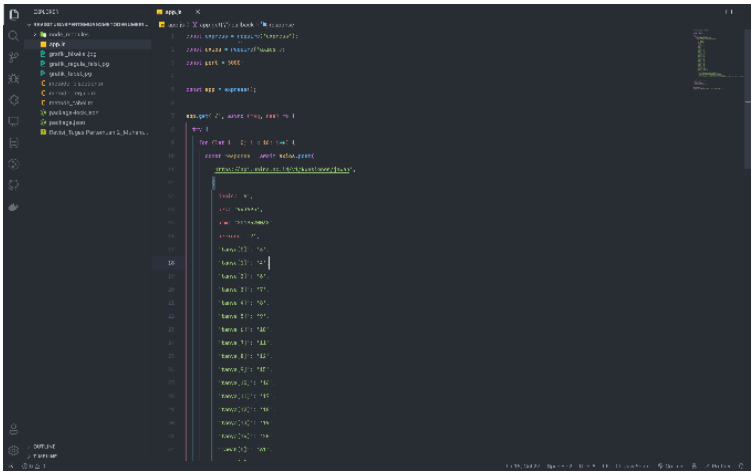
Gambar 7 Mengakses endpoint kuesioner

Pada gambar 7 token lama dimasukkan dan digunakan untuk mengakses endpoint kuesioner. Token tersebut dikenali sebagai token yang sudah kadaluarsa, sehingga sistem menunjukkan bahwa status permintaan 401. Kode tersebut memiliki arti unauthorized atau permintaah tidak sah. Kemudian, peneliti menggunakan token akses yang baru, dan mengakses endpoint tersebut. Sistem menunjukkan status berhasil dengan kode 201. Perhatikan gambar 8.



Gambar 8 Akses enpoint kuesioner dengan token baru

Peneliti membuat kode untuk mengakses endpoint kuesioner dan mengisi datanya sebanyak 100 kali. Kemudian peneliti memasukkan NIM yang berbeda dari informasi yang disimpan pada token. Kodenya dapat dilihat pada gambar 9.



Gambar 9 Post endpoint kuesioner 100 kali

Dari percobaan gambar 9. Sistem tetap merespon 201. Artinya tidak ada algoritma yang mencegah kuesioner yang dikirimkan. Dari percobaan gambar 9 juga, akun yang digunakan bukan berasal dari nim yang sama. Namun token yang digunakan adalah hasil generate dari token yang berbeda. Dan sistem tetap merespon 201. Dari hal tersebut dapat dipahami bahwa proses otorisasi tidak sepenuhnya digunakan dengan baik pada endpoint kuesioner. Hal tersebut bukan karena proses otorisasi jwt yang lemah karena pada gambar 6 token meyimpan id mahasiswa, dan id tersebut harusnya digunakan sebagai proses validasi terhadap token untuk proses input kuesioner.

Dari beberapa percobaan yang dilakukan, penggunaan jwt terhadap proses autentikasi dan otorisasi di Sistem Akademik Universitas Madura belum dimanfaatkan secara maksimal. Hal tersebut dikarenakan masih terdapat endpoint yang dapat menembus hak otorisasi user lain. Token lama yang telah di logout oleh pengguna tidak diblokir oleh sistem. Sehingga, pengguna lain yang masih memiliki token dapat mengakses data dari server SIMAT tanpa melalui proses otentikasi terlebih dahulu.

Untuk memaksimalkan penggunaan JWT dalam proses autentikasi dan otorisasi di Sistem Akademik Universitas Madura, ada beberapa langkah yang dapat diambil:

1. Pembaruan JWT: Pastikan bahwa token JWT yang digunakan memiliki mekanisme pembaruan yang tepat. Setelah seorang pengguna melakukan logout, sistem harus secara otomatis memblokir token yang telah digunakan tersebut agar tidak bisa digunakan lagi oleh pengguna lain.
2. Mekanisme Penyimpanan Token: Pastikan sistem menggunakan mekanisme penyimpanan token yang aman. Token harus disimpan secara terenkripsi dan dilindungi dari akses yang tidak sah. Disarankan untuk menggunakan penyimpanan token yang tahan terhadap serangan seperti database yang terenkripsi atau sistem manajemen token khusus.

3. Penghapusan Token yang Kadaluwarsa: Setiap token JWT harus memiliki waktu kadaluwarsa yang terdefinisi dengan baik. Setelah waktu kadaluwarsa, token harus dihapus secara otomatis dari sistem. Dengan demikian, bahaya penggunaan token yang telah kedaluwarsa dapat dihindari.
4. Audit Logging: Implementasikan audit logging untuk melacak aktivitas autentikasi dan otorisasi. Dengan melacak log ini, Anda dapat memantau penggunaan token dan mendeteksi aktivitas mencurigakan atau pelanggaran keamanan.
5. Uji Keamanan: Lakukan uji keamanan secara menyeluruh terhadap sistem autentikasi dan otorisasi, termasuk penggunaan JWT. Uji keamanan ini harus mencakup serangan umum seperti serangan injeksi, serangan pencurian token, dan serangan brute force.
6. Pembaruan dan Pemantauan Keamanan yang Terus-Menerus: Pastikan sistem tetap diperbarui dengan versi terbaru dari pustaka atau framework yang digunakan untuk mengelola autentikasi dan otorisasi. Selalu pantau kerentanan keamanan yang baru ditemukan dan lakukan langkah-langkah yang diperlukan untuk memperbaikinya.

Dengan mengimplementasikan langkah-langkah tersebut, keamanan hak akses otorisasi dapat ditingkatkan. sehingga akses dari pengguna yang terlarang dapat ditolak oleh system.

7. Kesimpulan

Dalam penelitian ini, ditemukan bahwa penggunaan JWT dalam autentikasi dan otorisasi di Sistem Akademik Universitas Madura belum maksimal. Terdapat kelemahan seperti adanya endpoint yang dapat mengakses hak otorisasi user lain dan token lama yang tidak diblokir setelah logout. Untuk meningkatkan keamanan, disarankan melakukan pembaruan JWT, menggunakan mekanisme penyimpanan token yang aman, menghapus token yang kadaluwarsa, menerapkan audit logging, melakukan uji keamanan menyeluruh, dan melakukan pembaruan dan pemantauan keamanan secara terus-menerus.

Ucapan Terimakasih

Terima kasih yang sebesar-besarnya kepada seluruh responden yang telah berpartisipasi dalam penelitian ini. Ucapan terima kasih juga kami haturkan kepada pihak Universitas Madura yang telah memberikan akses dan dukungan dalam pengumpulan data. Tidak lupa, kami mengucapkan terima kasih kepada rekan-rekan yang telah memberikan masukan dan bantuan dalam proses penelitian ini. Semua kontribusi dari pihak-pihak tersebut sangat berarti bagi kesuksesan penelitian ini.

Daftar Rujukan

[1] L. Saeed and G. Abdallah, “Security with JWT,” in *Pro Cloud Native Java EE Apps: DevOps with MicroProfile, Jakarta EE 10 APIs, and Kubernetes*, L. Saeed and G. Abdallah, Eds., Berkeley, CA: Apress, 2022, pp. 293–308. doi: 10.1007/978-1-4842-8900-6_11.

[2] U. dan Kebutuhan Pembaruan and W. Djafar, “Hukum Perlindungan Data Pribadi di Indonesia.” [Online]. Available: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

[3] G. A. Riyadi and Toto Tohir Suriaatmadja, “Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi,” *Bandung Conference Series: Law Studies*, vol. 3, no. 1, Jan. 2023, doi: 10.29313/bcsls.v3i1.4945.

[4] J. Teknika and M. Agarina, “Implementasi Scrum Agile Development Pada Sistem Informasi E-Mentor Di Kemahasiswaan IIB Darmajaya,” *Jurnal Teknika*, vol. x, No.x, pp. 1–5, 2021.

[5] R. Melyanti, M. Iqbal, and M. Muhardi, “Sistem Informasi Manajemen Penelitian dan Pengabdian Masyarakat di Bagian P3M (Studi Kasus: STMIK Hang Tuah Pekan Baru),” *Jurnal Ilmu Komputer*, vol. 9, no. 2, pp. 165–176, Oct. 2020, doi: 10.33060/jik/2020/vol9.iss2.186.

[6] C. Safitri, “JSON Web Token Leakage Avoidance using Token Split and Concatenate in RSA256,” *43 | Indonesian Journal of Computing, Engineering, and Design*, vol. 5, no. 1, p. 5, 2023, doi: 10.35608/ijoced.v5i1.325.

[7] K. Devika, R. Dhivya, and N. Sangeetha, “Json Web Token Used in MERN Stack for Makinge-Commerce Web-Application,” 2021. [Online]. Available: www.ijrpr.com

[8] A. Jaedun, “Metode Penelitian Eksperimen,” *Metodologi Penelitian Eksperimen*, pp. 0–12, 2011.

[9] D. N. Puspayani, “Upaya Peningkatan Hasil Belajar Biologi Materi Pokok Keunikan Hutan Hujan Tropis Melalui Penerapan Metode Eksperimen,” *Jurnal Pedagogi dan Pembelajaran*, vol. 2, no. 1, pp. 97–104, 2019.

[10] A. Umarjati and A. Wibowo, “Implementasi JWT pada Aplikasi Presensi dengan Validasi Fingerprint, Geotagging dan Device Checker,” *Jurnal RESTI (Rekayasa Sistem dan …*, 2020, [Online]. Available: http://www.jurnal.iaii.or.id/index.php/RESTI/article/view/2650

[11] P. Painem and H. Soetanto, "Sistem Presensi Pegawai Berbasis Web Service Menggunakan Metode Restfull Dengan Keamanan JWT Dan Algoritma Haversine," *Fountain of Informatics Journal*, 2020, [Online]. Available: https://ejournal.unida.gontor.ac.id/index.php/FIJ/article/view/4906

[12] V. Bertocci, *JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens*. ietf.org, 2021. [Online]. Available: https://www.ietf.org/proceedings/104/slides/slides-104-oauth-sessa-jwt-profile-for-access-token-00.pdf

[13] W. Niewolski, T. W. Nowak, M. Sepczuk, and Z. Kotulski, "Token-based authentication framework for 5g mec mobile networks," *Electronics (Switzerland)*, vol. 10, no. 14, 2021, doi: 10.3390/electronics10141724.

[14] J. Satrio Utama and A. Dwi Indriyanti, "Pengamanan Restful API Web Service Menggunakan Json Web Token (Studi Kasus: Aplikasi Siakadu Mobile Unesa)," *JEISBI*, vol. 04, p. 2023.

[15] E. Edy, F. Ferdiansyah, W. Pramusinto, and S. Waluyo, "Pengamanan Restful API menggunakan JWT untuk Aplikasi Sales Order," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 3, no. 2, pp. 106–112, 2019, doi: 10.29207/resti.v3i2.860.

[16] L. V Jánoky, P. Ekler, and J. Levendovszky, "Evaluating the Performance of a Novel JWT Revocation Strategy," *Acta Cybernetica*, vol. 25, no. 2, pp. 307–318, 2021, doi: 10.14232/ACTACYB.289455.

[17] I. S. Tsany and N. Qmariasih, "Rancang Bangun Aplikasi Event Management Untuk Manajemen Data Peserta KLiKS Dengan Secure Web API Berdasarkan OWASP API Top Ten 2019," 2022.

[18] L. Jánoky, J. Levendovszky, and P. Ekler, *A Novel JWT Revocation Algorithm*. real.mtak.hu, 2020. [Online]. Available: http://real.mtak.hu/113127/1/CSCS2020.pdf

[19] K. I. Satoto, "Analisis Keamanan Sistem Informasi Akademik Berbasis Web Di Fakultas Teknik Universitas Diponegoro," *Seminar Nasional Aplikasi Sains dan Teknologi ISSN:1979-911X*, no. 13 Desember, pp. 175–186, 2008.

[20] I. Kharisma Raharjana, "UATAN MODEL SEQUENCE DIAGRAM DENGAN REVERSE ENGINEERING APLIKASI BASIS DATA PADA SMARTPHONE UNTUK MENJAGA KONSISTENSI DESAIN PERANGKAT LUNAK," 2015.