ANALISIS KEAMANAN *WEBSITE* SISTEM INFORMASI TUGAS AKHIR (SITASI) MENGGUNAKAN METODE *PENETRATION TESTING*

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:

RENGGA RENALDI
12050313320

UIN SUSKA RIAU

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2025

LEMBAR PERSETUJUAN

ANALISIS KEAMANAN *WEBSITE* SISTEM INFORMASI TUGAS AKHIR (SITASI) MENGGUNAKAN METODE *PENETRATION TESTING*

TUGAS AKHIR

Oleh:

RENGGA RENALDI
12050313320

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 10 Juli 2024

Ketua Program Studi	Pembimbing
Eki Saputra, S.Kom., M.Kom.	**Mona Fronita, S.Kom., M.Kom.**
NIP. 198307162011011008	**NIP. 198403032023212027**

LEMBAR PENGESAHAN

ANALISIS KEAMANAN *WEBSITE* SISTEM INFORMASI TUGAS AKHIR (SITASI) MENGGUNAKAN METODE *PENETRATION TESTING*

TUGAS AKHIR

Oleh:

RENGGA RENALDI
12050313320

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 03 Juli 2025

Pekanbaru, 10 Juli 2024
Mengesahkan,

Dekan	Ketua Program Studi
Dr. Yuslenita Muda, S.Si., M.Sc.	**Eki Saputra, S.Kom., M.Kom.**
NIP. 197701032007102001	**NIP. 198307162011011008**

DEWAN PENGUJI:

Ketua : **Eki Saputra, S.Kom., M.Kom.**

Sekretaris : **Mona Fronita, S.Kom., M.Kom.**

Anggota 1 : **T. Khairil Ahsyar, S.Kom., M.Kom.**

Anggota 2 : **M. Jazman, S.Kom., M.Infosys.**

Lampiran Surat :
Nomor : Nomor 25/2021
Tanggal : 10 September 2021

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini :

Nama :Rengga Renaldi
NIM :12050313320
Tempat/ Tgl. Lahir : Tembilahan,21 Juni 2001
Fakultas/Pascasarjana :Sains dan Teknologi
Prodi :Sistem Informasi
Judul Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya* :

ANALISIS KEAMANAN WEBSITE SISTEM INFORMASI TUGAS AKHIR (SITASI) MENGGUNAKAN METODE PENETRATION TESTING

Menyatakan dengan sebenar-benarnya bahwa :

1. Penulisan Disertasi/Tesis/Skripsi/Karya Ilmiah lainnya* dengan judul sebagaimana tersebut di atas adalah hasil pemikiran dan penelitian saya sendiri.
2. Semua kutipan pada karya tulis saya ini sudah disebutkan sumbernya.
3. Oleh karena itu Disertasi/Tesis/Skripsi/Karya Ilmiah lainnya* saya ini, saya nyatakan bebas dari plagiat.
4. Apa bila dikemudian hari terbukti terdapat plagiat dalam penulisan Disertasi/Tesis/Skripsi/(Karya Ilmiah lainnya)* saya tersebut, maka saya bersedia menerima sanksi sesuai peraturan peraturan perundang-undangan.

Demikian Surat Pernyataan ini saya buat dengan penuh kesadaran dan tanpa paksaan dari pihak manapun juga.

Pekanbaru, 14 Juli 2025

Yang membuat pernyataan

METERAI TEMPEL 5AMX348596960

RENGGA RENALDI
12050313320

**pilih salah salah satu sesuai jenis karya tulis*

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin penulis dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman dan tanggal pinjam pada *form* peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Pekanbaru, 10 Juli 2024
Yang Membuat Pernyataan,

RENGGA RENALDI
NIM. 12050313320

LEMBAR PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Dengan menyebut nama Allah yang maha pengasih lagi maha penyayang

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Segala puji syukur kehadirat Allah *Subhanahu Wa Ta'ala* atas segala rahmat, nikmat dan karunia-Nya yang senantiasa mengiringi setiap langkah hidup saya hingga titik ini. *Shalawat* serta salam semoga senantiasa tercurah kepada Nabi Muhammad *Shallallahu 'Alaihi Wasallam*, sang pembawa cahaya kebenaran, beserta keluarga, sahabat dan seluruh pengikut beliau hingga akhir zaman. *Allahumma Sholli 'Ala Sayyidina Muhammad wa 'Ala Ali Sayyidina Muhammad.*

Dengan segala kerendahan hati, karya ini saya persembahkan untuk Ayahanda Rahmadi, dan Ibunda Rina Defriati tercinta yang selalu menjadi tempat pulang paling tenang dan menjadi sumber kekuatan dalam setiap perjuangan saya. Di balik setiap langkah yang saya ambil, ada do'a mereka yang diam-diam menguatkan. Pengorbanan, kasih sayang dan dukungan tanpa batas dari mereka adalah alasan utama saya mampu berdiri sejauh ini. Semoga Allah *Subhanahu Wa Ta'ala* selalu menjaga kesehatan Ayah, dan semoga surga terbaik Allah anugerahkan kepada Ibu, atas cinta dan perjuangannya yang tidak pernah terucap. Teruntuk sahabat dan teman-teman seperjuangan, terima kasih atas semangat, bantuan, tawa dan pelajaran hidup yang kalian berikan. Kalian adalah bagian dari kisah yang akan selalu saya kenang dan kepada semua pihak yang tidak dapat saya sebutkan yang telah memberikan do'a, dukungan, dan kontribusi dalam proses ini, saya ucapkan terima kasih yang sebesar-besarnya. Semoga Allah *Subhanahu Wa Ta'ala* memberikan Rahmat serta Hidayahnya agar kita hambanya dapat terus berdo'a kepada-nya, *Aamiin Ya Rabbal 'Alamiin*.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

KATA PENGANTAR

Alhamdulillahi Rabbil 'Alamin, bersyukur kehadirat Allah *Subhanahu Wa Ta'ala* atas segala rahmat dan karunia-Nya sehingga peneliti dapat menyelesaikan Tugas Akhir ini. Shalawat serta salam kita ucapkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Sholli'Ala Sayyidina Muhammad Wa'Ala Ali Sayyidina Muhammad*. Tugas Akhir ini dibuat sebagai salah satu syarat untuk mendapatkan gelar Sarjana Komputer di Program Studi Sistem Informasi Universitas Islam Negeri Sultan Syarif Kasim Riau.

Pada penulisan Tugas Akhir ini, terdapat beberapa pihak yang sudah berkontribusi dan mendukung peneliti baik berupa materi, moril, dan motivasi. Peneliti ingin mengucapkan banyak terima kasih kepada:

1. Ibu Prof. Dr. Hj. Leny Nofianti MS, SE., M.Si., AK., CA sebagai Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Ibu Dr. Yuslenita Muda, S.Si., M.Sc sebagai Dekan Fakultas Sains dan Teknologi.
3. Bapak Eki Saputra, S.Kom., M.Kom sebagai Ketua Program Studi Sistem Informasi serta sebagai Ketua Sidang yang telah berkenan membantu peneliti dalam perjalanan menyelesaikan Tugas Akhir.
4. Ibu Siti Monalisa, ST., M.Kom sebagai Sekretaris Program Studi Sistem Informasi serta sebagai Dosen Pembimbing Akademik yang telah berkenan untuk membimbing peneliti untuk menyelesaikan Tugas Akhir ini.
5. Bapak Tengku Khairil Ahsyar, S.Kom., M.Kom sebagai Kepala Laboratorium Program Studi Sistem Informasi serta sebagai Penguji I yang telah memberikan saran dan masukan kepada peneliti dalam penulisan Tugas Akhir ini.
6. Ibu Mona Fronita, S.Kom., M.Kom sebagai Dosen Pembimbing Tugas Akhir yang telah meluangkan waktu, tenaga, dan pikiran dalam membimbing peneliti hingga peneliti dapat menyelesaikan Laporan Tugas Akhir ini.
7. Bapak Muhammad Jazman, S.Kom., M.Infosys sebagai Penguji II yang telah memberikan saran dan masukan kepada peneliti dalam penulisan Tugas Akhir ini.
8. Para Dosen Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau yang telah memberikan ilmu yang bermanfaat serta memberikan motivasi dan arahan untuk menyelesaikan studi perkuliahan.
9. Kedua orang tua peneliti yaitu Ayahanda Rahmadi, dan Ibunda Rina Defriati

yang selalu memberikan kasih sayang dan menjadi motivasi terkuat peneliti untuk bertahan pada masa studi dan menyelesaikan pendidikan Strata 1 (S1).

10. Seluruh keluarga dan saudara, Terima kasih atas doa dan dukungannya.
11. Dania Amira yang telah membantu peneliti dalam penelitian ini dengan memberikan saran dan masukan.

Semoga segala doa dan dorongan yang telah diberikan selama ini menjadi amal kebajikan dan mendapat balasan setimpal dari Allah *Subhanahu Wa Ta'ala*. Peneliti menyadari bahwa penulisan Tugas Akhir ini masih banyak terdapat kekurangan dan jauh dari kata sempurna. Untuk itu, kritik dan saran yang membangun sangat diharapkan untuk kesempurnaan Tugas Akhir ini dengan menghubungi peneliti melalui *e-mail* di 12050313320@students.uin-suska.ac.id. Semoga laporan ini bermanfaat bagi kita semua, akhir kata peneliti ucapkan terima kasih.

Pekanbaru, 10 Juli 2024

Peneliti,

RENGGA RENALDI

NIM. 12050313320

p-ISSN : 2302-8149
e-ISSN : 2540-9719
Vol 14 No. 4, 2025

JURNAL SISTEM INFORMASI

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS ISLAM INDRAGIRI
TEMBILAHAN - RIAU

JURNAL SISTEMASI sistem informasi

p-ISSN : 2302 - 8149
e-ISSN : 2540 - 9719
Akreditasi Kemendikbudristek
No. 79/E/KPT/2023
Peringkat Sinta 3 (Tiga)
Vol 11 No 1 Tahun 2022 s/d Vol 15 No 2 Tahun 2026

Vol 14, No 5 (2025)

Sistemasi: Jurnal Sistem Informasi

DOI: https://doi.org/10.32520/stmsi.v14i5

Table of Contents

Articles

Sistemasi: Jurnal Sistem Informasi
Volume 14, Nomor 5, 2025: 2258-2265
ISSN:2302-8149
e-ISSN:2540-9719

Analisis Keamanan *Website* Sistem Informasi Tugas Akhir (SITASI) menggunakan Metode *Penetration Testing*

Security Analysis of the Final Project Information System (SITASI) Website using Penetration Testing Method

[1]Rengga Renaldi, [2]Mona Fronita*, [3]Tengku Khairil Ahsyar, [4]Muhammad Jazman
[1,2,3,4]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau
[1,2,3,4]Jl. HR. Soebrantas No. KM. RW. 15, Simpang Baru, Pekanbaru, Riau, Indonesia
*e-mail: renggagggg6@gmail.com

(***received*:** 10 June 2025, ***revised*:** 23 June 2025, ***accepted*:** 23 June 2025)

Abstrak

Website Sistem Informasi Tugas Akhir (SITASI) berperan penting dalam mendukung proses administrasi akademik di Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau. Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan website pasca *maintenance* menggunakan metode *penetration testing* dengan alat OWASP *Zed Attack Proxy* (ZAP). Hasil pengujian menemukan delapan kerentanan, terdiri dari dua dengan tingkat ancaman sedang (*medium*), empat rendah (*low*), dan dua bersifat informasional. Risiko sedang mencakup absennya token Anti-CSRF dan tidak diterapkannya *Content Security Policy* (CSP), yang dapat membuka peluang serangan seperti CSRF dan XSS. Risiko rendah meliputi pemuatan JavaScript dari domain pihak ketiga, pengungkapan informasi melalui *header X-Powered-By* dan Server, serta tidak diterapkannya *HTTP Strict Transport Security* (HSTS). Dua temuan informasional terkait dengan komentar mencurigakan dalam kode dan pengaturan *Cache-Control* yang tidak tepat. Perbaikan dilakukan berdasarkan praktik keamanan OWASP, termasuk penerapan token CSRF, konfigurasi header CSP dan HSTS, serta penghapusan informasi sensitif dari respons server. Evaluasi ulang menunjukkan bahwa seluruh risiko telah berhasil diminimalkan. Penelitian ini menegaskan bahwa pendekatan pengujian penetrasi dan mitigasi berbasis standar terbukti efektif dalam meningkatkan ketahanan keamanan aplikasi web, khususnya dalam lingkungan akademik.

Kata kunci: penetration testing, OWASP ZAP, keamanan website

Abstract

The Final Project Information System (SITASI) website plays a critical role in supporting academic administrative processes at the Faculty of Science and Technology, UIN Sultan Syarif Kasim Riau. This study aims to evaluate the website's security level following recent maintenance using penetration testing, conducted with the OWASP Zed Attack Proxy (ZAP) tool. The testing revealed eight vulnerabilities, including two classified as medium risk, four as low risk, and two informational. The medium-risk issues involved the absence of an Anti-CSRF token and the lack of a Content Security Policy (CSP), both of which could expose the system to attacks such as CSRF and XSS. The low-risk findings included loading JavaScript from third-party domains, information disclosure via X-Powered-By and Server headers, and the absence of HTTP Strict Transport Security (HSTS). The two informational findings involved suspicious comments in the code and improper Cache-Control settings. Remediation actions were implemented based on OWASP security best practices, including the integration of CSRF tokens, configuration of CSP and HSTS headers, and removal of sensitive information from server responses. A follow-up evaluation confirmed that all identified risks had been successfully mitigated. This study highlights that penetration testing combined with standard-based mitigation is effective in enhancing web application security resilience, particularly within academic environments.

Keywords: *penetration testing, OWASP ZAP, website security*

ISSN:2302-8149
e-ISSN:2540-9719

1 Pendahuluan

Keamanan informasi telah menjadi isu krusial seiring dengan meningkatnya penggunaan teknologi informasi dan komunikasi dalam berbagai sektor, termasuk dunia pendidikan tinggi. Website sebagai salah satu elemen penting dalam sistem informasi modern, kini tidak hanya berfungsi sebagai media penyampaian informasi, tetapi juga sebagai sarana penyimpanan dan pengelolaan data sensitif yang menyangkut identitas, proses akademik, dan administrasi [1]. Salah satu contoh implementasi sistem informasi di lingkungan akademik adalah Sistem Informasi Tugas Akhir (SITASI) milik Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau. SITASI berfungsi sebagai platform utama dalam pengelolaan seminar tugas akhir mahasiswa, penyimpanan dokumen, dan komunikasi akademik antara mahasiswa, dosen pembimbing, dan penguji.

Namun, perubahan teknologi yang cepat serta pembaruan sistem melalui kegiatan maintenance tidak menjamin keamanan situs secara otomatis tetap terjaga. Menurut Prahendratno, dkk, ancaman terhadap sistem digital cenderung meningkat seiring berkembangnya teknologi dan pola serangan [2]. Berdasarkan observasi awal, setelah dilakukan *maintenance* pada SITASI pada tahun 2023, belum terdapat pengujian keamanan lanjutan untuk mengevaluasi kemungkinan munculnya celah keamanan baru. Padahal, dalam konteks keamanan siber, perubahan sekecil apa pun dalam struktur atau konfigurasi sistem dapat berpotensi membuka vektor serangan baru. Hal ini menunjukkan adanya kebutuhan mendesak untuk melakukan evaluasi keamanan menyeluruh melalui pendekatan teknis yang valid. Pengujian penetrasi (*penetration testing*) merupakan salah satu metode yang umum digunakan untuk mengidentifikasi dan mengevaluasi kerentanan dalam sistem web, dengan mensimulasikan serangan seperti yang dilakukan oleh peretas sesungguhnya [3]. Salah satu *tools* yang efektif untuk melakukan pengujian ini adalah OWASP *Zed Attack Proxy* (ZAP), yaitu perangkat lunak *open-source* yang dirancang khusus untuk mendeteksi berbagai jenis kerentanan pada aplikasi berbasis web [4]. Penelitian terdahulu yang dilakukan oleh Sofyan, Sugiarto, dan Akbar, juga menunjukkan bahwa OWASP ZAP mampu mengidentifikasi celah keamanan pada sistem informasi akademik secara efisien dan sistematis [5].

Permasalahan utama dalam penelitian ini adalah bagaimana tingkat keamanan website SITASI setelah dilakukan *maintenance*. Untuk menjawab hal tersebut, dilakukan analisis kerentanan menggunakan metode *penetration testing* berbasis OWASP ZAP. Tujuan dari penelitian ini adalah untuk mengidentifikasi potensi kerentanan pada website SITASI, menganalisis tingkat keparahan setiap kerentanan, serta memberikan rekomendasi perbaikan berbasis standar keamanan OWASP. Penelitian ini diharapkan memberikan kontribusi dalam penguatan sistem keamanan informasi di lingkungan akademik dan menjadi referensi untuk pengelolaan sistem web yang aman dan andal.

2 Tinjauan Literatur

Penelitian mengenai keamanan aplikasi web semakin berkembang seiring meningkatnya jumlah serangan siber yang ditujukan pada sistem berbasis web. Berbagai studi telah dilakukan untuk mengidentifikasi kerentanan yang umum terjadi pada sistem informasi di lingkungan akademik. Rosaliah et al. [6], melakukan pengujian pada sistem informasi manajemen (SIM) menggunakan pendekatan OWASP Top Ten, dan menemukan bahwa serangan *Broken Authentication*, *Sensitive Data Exposure*, dan *Security Misconfiguration* merupakan kerentanan dominan. Meski demikian, penelitian tersebut tidak secara khusus meneliti situs akademik berbasis seminar atau tugas akhir mahasiswa. Ghozali et al. [7], menerapkan *risk rating* OWASP untuk menilai keamanan sistem informasi harga komoditas milik instansi pemerintah, dan menyimpulkan bahwa tingkat risiko tersebar pada kategori *low*, *medium*, dan *high*. Namun, fokusnya lebih pada sistem informasi publik, bukan sistem akademik internal.

Sementara itu, Sofyan et al. [5], menerapkan *penetration testing* menggunakan *tools Acunetix* pada website perguruan tinggi dan menemukan satu kerentanan tingkat tinggi, tiga medium, dan enam rendah. *Tools* yang digunakan berbeda dari OWASP ZAP yang lebih fleksibel untuk eksplorasi manual dan integrasi ke dalam CI/CD. Penelitian oleh Fachri et al. [8], yang menguji web server Sistem Informasi Akademik dengan metode uji penetrasi standar berhasil mengidentifikasi kerentanan level tinggi seperti *port* terbuka dan pengungkapan kredensial. Namun, mereka tidak melakukan analisis terhadap pengamanan aplikasi berbasis web yang bersifat dinamis dan kompleks seperti

ISSN:2302-8149
e-ISSN:2540-9719

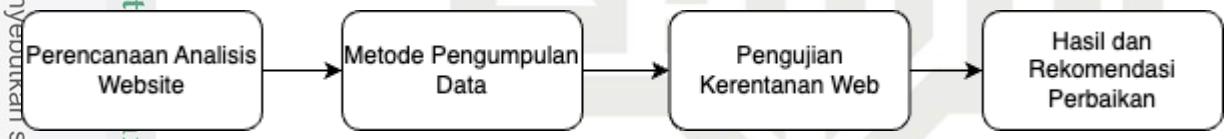
SITASI. Di sisi lain, Abdillah et al. [9], menggabungkan pendekatan *Dynamic Application Security Testing* (DAST) dengan teknik *penetration testing* untuk mendeteksi XSS, *Broken Access Control*, dan *SQL Injection*. Meski pendekatan mereka cukup komprehensif, objek penelitian tidak mengarah ke aplikasi akademik seperti sistem seminar atau tugas akhir.

Penelitian-penelitian tersebut menunjukkan bahwa berbagai metode pengujian telah digunakan untuk mengevaluasi keamanan situs web, namun sebagian besar masih berfokus pada sistem *non-akademik*, sistem *e-commerce*, atau hanya mengandalkan pengujian otomatis tanpa pendalaman struktural. Tidak ditemukan penelitian sebelumnya yang secara khusus mengevaluasi keamanan sistem SITASI pasca-*maintenance*, dengan pendekatan *penetration testing* berbasis OWASP ZAP secara menyeluruh. Padahal, setelah proses *maintenance*, konfigurasi sistem dan layanan web sangat mungkin berubah, dan tanpa pengujian ulang, potensi celah keamanan baru tidak dapat terdeteksi.

Website merupakan kumpulan halaman daring yang menyajikan informasi dan dapat bersifat statis maupun dinamis, diakses melalui peramban tanpa perlu instalasi tambahan, serta bergantung pada koneksi internet. Dalam konteks keamanan, website menjadi salah satu objek penting dalam penetration testing, yaitu metode pengujian keamanan dengan mensimulasikan serangan untuk mengidentifikasi kerentanan yang bisa dieksploitasi dan memberikan rekomendasi perbaikan. Salah satu standar yang umum digunakan dalam praktik ini adalah OWASP (Open Web Application Security Project), organisasi nirlaba yang menyediakan panduan keamanan aplikasi web, termasuk *OWASP Top Ten* yang menjadi referensi global dalam mitigasi risiko keamanan. Untuk mendukung proses pengujian, digunakan alat seperti OWASP ZAP, sebuah perangkat lunak open-source yang bertindak sebagai *man-in-the-middle proxy* untuk mendeteksi celah keamanan secara otomatis maupun manual. Semua upaya ini bertujuan untuk meningkatkan keamanan website, yaitu menjaga data dan infrastruktur dari akses ilegal, manipulasi, serta gangguan, yang merupakan bagian dari cakupan lebih luas dalam keamanan siber, yakni perlindungan menyeluruh terhadap sistem digital agar kerahasiaan, integritas, dan ketersediaannya tetap terjaga serta sesuai dengan regulasi yang berlaku.

3 Metode Penelitian

Penelitian ini bertujuan untuk menganalisis kerentanan pada situs web Sistem Informasi Tugas Akhir (SITASI) menggunakan metode *penetration testing* berbasis OWASP ZAP. Proses pengujian dilakukan melalui lima tahapan utama, perencanaan analisis situs web, pengumpulan data, pengujian kerentanan, interpretasi hasil, serta perumusan rekomendasi perbaikan. Alur kegiatan ini ditampilkan pada Gambar 1.



Gambar 1. Alur penelitian pengujian kerentanan website SITASI

a) Perencanaan Analisis Website

Tahap perencanaan analisis situs web dilakukan dengan mengidentifikasi domain target, struktur halaman, dan komponen utama yang akan diuji. Peneliti juga meninjau ulang pembaruan sistem yang dilakukan pada tahun 2023, termasuk perubahan antarmuka, penambahan fitur, serta pergeseran elemen navigasi yang dapat memengaruhi potensi kerentanan. Perencanaan ini juga mencakup penyesuaian konfigurasi alat uji agar dapat berjalan secara optimal terhadap lingkungan sistem SITASI, serta penentuan cakupan pengujian yang relevan dengan fungsionalitas utama situs.

b) Metode Pengumpulan Data

Pengumpulan data dilakukan melalui dua metode, yaitu observasi dan studi literatur. Observasi dilakukan sejak Januari 2024 untuk mengamati langsung kondisi dan perubahan situs SITASI pasca-*maintenance*. Selama periode tersebut, diamati adanya perubahan signifikan pada tampilan, fitur, dan struktur halaman. Studi literatur dilakukan dengan menelaah jurnal, buku, prosiding, tugas akhir, dan sumber digital yang relevan sebagai dasar penguatan teori dan metode.

ISSN:2302-8149
e-ISSN:2540-9719

c) Pengujian Kerentanan Web

Pengujian dilakukan terhadap website SITASI yang digunakan dalam proses administrasi seminar tugas akhir di lingkungan Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau. Aplikasi OWASP ZAP versi 2.11.1 digunakan sebagai alat utama untuk mendeteksi potensi kerentanan. Aplikasi ini diinstal pada sistem operasi Windows 11 dan dijalankan dengan konfigurasi standar. Target situs dimasukkan ke dalam ZAP, kemudian dilakukan pemindaian otomatis menggunakan metode spider tradisional untuk menelusuri serta menganalisis struktur halaman dan parameter rentan.

d) Hasil dan Rekomendasi Perbaikan

Setelah pemindaian selesai, OWASP ZAP menyajikan hasil berupa peringatan, tingkat risiko, dan detail teknis dari masing-masing kerentanan yang ditemukan. Informasi tersebut digunakan untuk merumuskan langkah-langkah perbaikan yang disesuaikan dengan jenis kerentanan, dengan tujuan meningkatkan keamanan sistem secara menyeluruh.

Bahan dan alat dalam penelitian menggunakan *software* dan *hardware* sebagai bahan literature penelitian, untuk spesifikasi *software* dan *hardware* dapat dilihat Tabel 1.

Tabel 1. Bahan dan alat penelitian

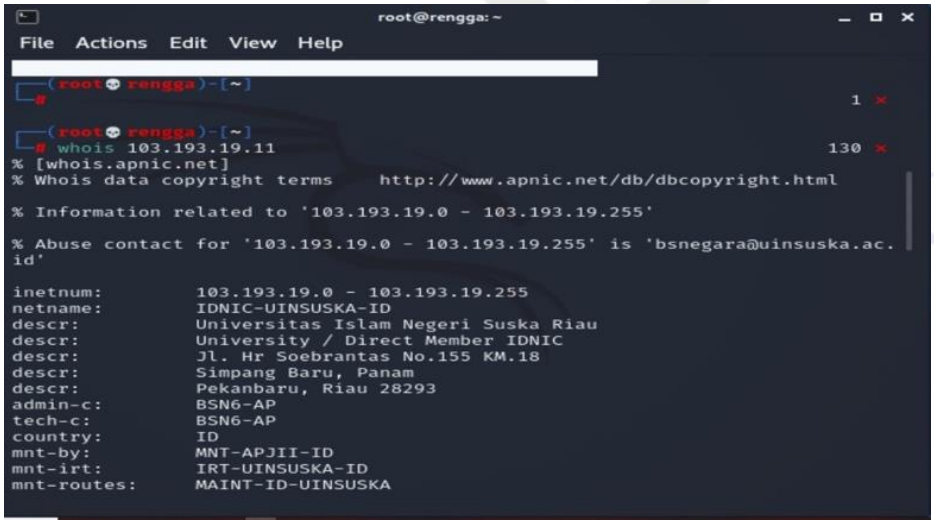
Hardware	Software
Lenovo thinkpad T470 Processor : intel (R) Celeron (R) CPU 3955U @ 2.00GHz RAM : 8 GB System type : 64-bit *Operating system*, x64-*based processor*	OWASP ZAP

4 Hasil dan Pembahasan

Penelitian ini menghasilkan temuan mengenai kondisi keamanan website Sistem Informasi Tugas Akhir (SITASI) setelah dilakukan pengujian menggunakan metode penetration testing. SITASI merupakan platform penting dalam pengelolaan seminar tugas akhir di lingkungan Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau. Dengan perannya yang kritis dalam memproses dan menyimpan data akademik, diperlukan evaluasi mendalam terhadap potensi celah keamanan sistem. Pengujian dilakukan menggunakan tiga perangkat utama, yaitu Whois, Zenmap, dan OWASP ZAP.

a) Implementasi *Tools* Whois

Hasil Whois (Gambar 2) menunjukkan bahwa domain SITASI berada dalam pengelolaan resmi UIN Sultan Syarif Kasim Riau, dengan alamat dan kontak teknis yang terdaftar. Informasi ini penting dalam konteks pelaporan dan koordinasi keamanan.

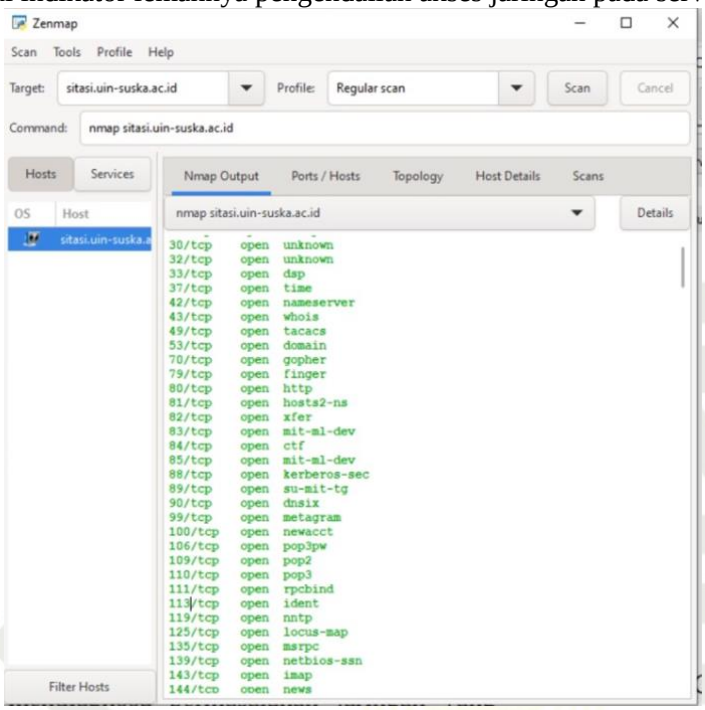


Gambar 2. Hasil implementasi *tools* whois

ISSN:2302-8149
e-ISSN:2540-9719

b) Implementasi *Tools* Zenmap

Melalui Zenmap (Gambar 3), ditemukan sejumlah *port* terbuka pada server target, termasuk *port* 80 (HTTP), 110 dan 143 (layanan email), serta *port-port* lama seperti 79 dan 113 yang dapat meningkatkan permukaan serangan. Absennya *port* 443 (HTTPS) juga menandakan bahwa komunikasi data belum dienkripsi dengan baik, sehingga berisiko terhadap serangan *man-in-the-middle*. Konfigurasi port yang terbuka tanpa pengamanan yang memadai menjadi indikator lemahnya pengendalian akses jaringan pada server.



Gambar 3. Hasil implementasi tools zenmap

c) Implementasi *Tools* OWASP ZAP

Berdasarkan hasil analisis keamanan menggunakan OWASP *Zed Attack Proxy* (ZAP), ditemukan delapan jenis kerentanan dengan tingkat ancaman yang bervariasi, dua termasuk kategori sedang (*medium*), empat rendah (*low*), dan dua bersifat informasional (*informational*).

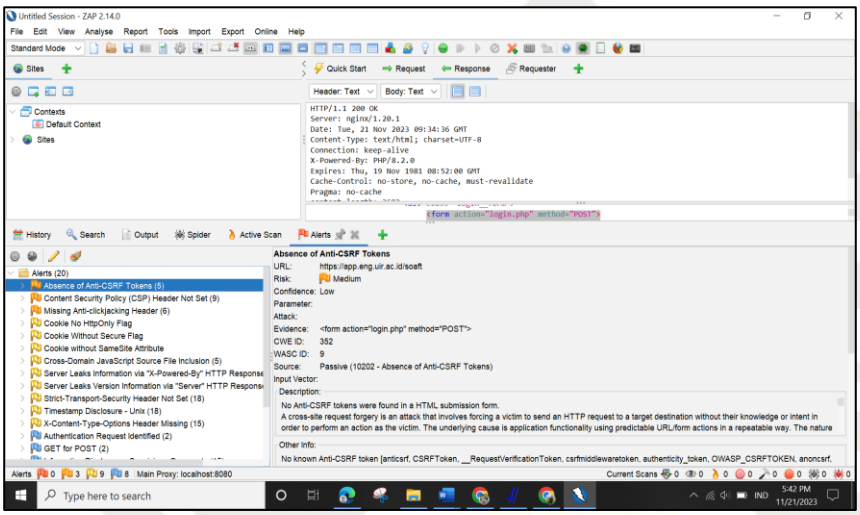
Kerentanan ini menunjukkan adanya celah keamanan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab untuk menyerang aplikasi web. Hasil implementasi *tools* OWASP ZAP dan solusi yang diberikan dapat dilihat pada Gambar 4 dan Tabel 2.

Tabel 2. Hasil implementasi *tools* OWASP ZAP

No	Jenis Ancaman	Tingkat Ancaman	Solusi Singkat dari OWASP ZAP
1	*Absence of Anti-CSRF Tokens*	*Medium*	Gunakan *token* anti-CSRF di setiap formulir menggunakan *library* seperti OWASP *CSRFGuard*.
2	*Content Security Policy (CSP) Not Implemented*	*Medium*	Tambahkan *header Content-Security-Policy* pada konfigurasi server dan aplikasi.
3	*Cross-Domain JavaScript Source Inclusion*	*Low*	Batasi pemuatan *file JavaScript* hanya dari domain yang terpercaya dan gunakan *whitelist*.
4	*Server Leaks via 'X-Powered-By' Header*	*Low*	Hapus atau sembunyikan *header X-Powered-By* dari konfigurasi server.

ISSN:2302-8149
e-ISSN:2540-9719

5	*Server Version Disclosure via 'Server' Header*	*Low*	Ubah atau sembunyikan informasi pada *header* server agar tidak menunjukkan versi perangkat.
6	*Absence of HTTP Strict Transport Security (HSTS)*	*Low*	Terapkan header *Strict-Transport-Security* untuk memaksa koneksi HTTPS.
7	*Information Disclosure via Suspicious Comments*	*Informational*	Hapus komentar kode yang mengandung informasi teknis atau internal yang sensitif.
8	*Re-examine Cache Control Directives*	*Informational*	Konfigurasi *header Cache-Control* untuk menghindari *caching* konten sensitif (*no-store*).



Gambar 4. Hasil implementasi tools OWASP ZAP

Hasil analisis menggunakan OWASP ZAP menemukan delapan kerentanan pada website SITASI, terdiri atas dua kerentanan sedang (*medium*), empat rendah (*low*), dan dua bersifat informasional. Temuan paling signifikan adalah tidak adanya token Anti-CSRF dan ketiadaan *Content Security Policy* (CSP), yang tergolong kerentanan sedang dan berpotensi memungkinkan serangan seperti CSRF dan XSS.

Kerentanan tingkat rendah mencakup pemuatan *JavaScript* dari domain pihak ketiga, kebocoran informasi melalui *header 'X-Powered-By'* dan *'Server'*, serta absennya implementasi *HTTP Strict Transport Security* (HSTS). Dua kerentanan informasional meliputi komentar mencurigakan dalam skrip dan pengaturan *Cache-Control* yang tidak optimal.

Meskipun tidak ditemukan kerentanan kritis, kelemahan konfigurasi dan arsitektur ini tetap berpotensi membahayakan keamanan sistem. Rekomendasi mitigasi mencakup penerapan CSRF token, konfigurasi CSP dan HSTS, penghapusan metadata dari header HTTP, serta penguatan validasi input dan pengelolaan sesi yang aman.

5 Kesimpulan

Penelitian ini mengevaluasi tingkat keamanan website Sistem Informasi Tugas Akhir Mahasiswa (SITASI) pasca-*maintenance* menggunakan metode *penetration testing* berbasis OWASP *Zed Attack Proxy* (ZAP). Pengujian mengacu pada standar OWASP Top 10 dan bertujuan mengidentifikasi serta menangani celah keamanan pada sistem. Hasil pengujian menemukan delapan kerentanan, dua dengan tingkat ancaman sedang (*medium*), empat rendah (*low*), dan dua bersifat informasional. Tidak ditemukan kerentanan kritis, namun celah yang ada tetap berpotensi mengganggu integritas, kerahasiaan, dan ketersediaan sistem. Jenis kerentanan meliputi absennya token Anti-CSRF, ketiadaan *Content Security Policy* (CSP), pemuatan *JavaScript* dari domain eksternal, kebocoran informasi

ISSN:2302-8149
e-ISSN:2540-9719

server melalui *header 'X-Powered-By'* dan *'Server'*, absennya *HTTP Strict Transport Security* (HSTS), komentar mencurigakan dalam kode, serta konfigurasi *Cache-Control* yang tidak optimal. Tindak lanjut dilakukan dengan menerapkan rekomendasi keamanan, seperti penambahan token CSRF, konfigurasi header CSP dan HSTS, penyembunyian informasi server, validasi sumber eksternal, serta pembersihan komentar skrip. Setelah implementasi, pengujian ulang menunjukkan bahwa seluruh risiko telah diminimalkan, tanpa ditemukan alert baru. Kesimpulannya, keamanan website SITASI meningkat secara signifikan setelah penerapan perbaikan. Penelitian ini membuktikan bahwa metode uji penetrasi disertai tindak lanjut berbasis *best practice* merupakan pendekatan efektif untuk meningkatkan keamanan sistem informasi akademik secara berkelanjutan.

Referensi

[1] Y. Mulyanto, E. Haryanti, dan J. Jumirah, "Analisis Keamanan *Website* SMAN 1 Sumbawa menggunakan Metode *Vulnerability Asesement*: Analisis Keamanan Website SMAN 1 Sumbawa menggunakan Metode *Vulnerability Asesement*," *Jurnal Informatika Teknologi dan Sains (Jinteks)*, Vol. 3, No. 3, hlm. 394–400, 2021.

[2] A. Prahendratno *dkk.*, Strategi Bisnis Digital: Optimalisasi & Otomtisasi Sebuah Bisnis menggunakaan Media Digital. PT. Sonpedia Publishing Indonesia, 2023.

[3] M. R. Ardiansyah *dkk.*, "Analisis Kerentanan Keamanan *Website* menggunakan Metode *PTES (Penetration Testing Execution And Standart)*," *Nuansa Informatika*, Vol. 18, No. 2, hlm. 145–153, 2024.

[4] A. F. Hasibuan dan D. Handoko, "Analisis Keretanan *Website* dengan Aplikasi Owasp Zap," *Jurnal Ilmu Komputer dan Sistem Informasi*, Vol. 2, No. 2, hlm. 257–270, 2023.

[5] H. Sofyan, M. Sugiarto, dan B. M. Akbar, "*Implementation of Penetration Testing on Websites to Improve Security of Information Assets* UPN 'Veteran' Yogyakarta," *Telematika: Jurnal Informatika dan Teknologi Informasi*, Vol. 20, No. 2, hlm. 153–162, 2023.

[6] Y. T. A. Rosaliah, J. Jayanta, dan B. Hananto, "Pengujian Celah Keamanan *Website* menggunakan Teknik *Penetration Testing* dan Metode OWASP TOP 10 pada Website SIM xxx," dalam *Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya*, 2021, hlm. 752–761.

[7] B. Ghozali, K. Kusrini, dan S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website menggunakan Metode *Owasp (Open Web Application Security Project)* untuk Penilaian *Risk Rating*," *Creative Information Technology Journal*, Vol. 4, No. 4, hlm. 264–275, 2019.

[8] F. Fachri, A. Fadlil, I. Riadi, A. Dahlan, Y. Jln Soepomo, dan I. Artikel, "Analisis Keamanan *Webserver* menggunakan *Penetration Test*," *J. Inform*, Vol. 8, No. 2, hlm. 183–190, 2021.

[9] E. Abdillah, R. Khoriyah, A. Abqariy, dan P. Susilo, "Pengembangan Keamanan *Website* menggunakan Teknik *Penetration Testing* dan *DAST (Dynamic Application Security Testing)*," *Media Jurnal Informatika*, Vol. 14, hlm. 112, Des 2022, doi: 10.35194/mji.v14i2.2546.

[10] J. N. Ginting, "Perancangan dan Pembuatan Sistem Informasi Penerimaan Mahasiswa Baru berbasis *Website*," *Jurnal Nasional Teknologi Komputer*, Vol. 2, No. 2, hlm. 51–59, 2022.

[11] W. Wiyanto, S. Fadhilah, dan A. Siswandi, "*E-Tourism* sebagai Media Wisata Kabupaten Bekasi berbasis *Website*," *Journal of Practical Computer Science*, Vol. 2, No. 1, hlm. 1–14, 2022, doi: 10.37366/jpcs.v2i1.1035.

[12] S. Hidayatulloh dan D. Saptadiaji, "*Penetration Testing* pada Website Universitas ARS menggunakan *Open Web Application Security Project (OWASP)*," *Jurnal Algoritma*, Vol. 18, No. 1, hlm. 77–86, 2021.

[13] D. F. Priambodo, A. D. Rifansyah, dan M. Hasbi, "*Penetration Testing Web* XYZ berdasarkan OWASP Risk Rating," *Teknika*, Vol. 12, No. 1, hlm. 33–46, 2023.

[14] G. Guntoro, L. Costaner, dan M. Musfawati, "Analisis Keamanan *Web Server Open Journal System* (OJS) menggunakan Metode ISSAF dan *OWASP* (Studi Kasus OJS Universitas Lancang Kuning)," *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, Vol. 5, No. 1, hlm. 45–55, 2020.

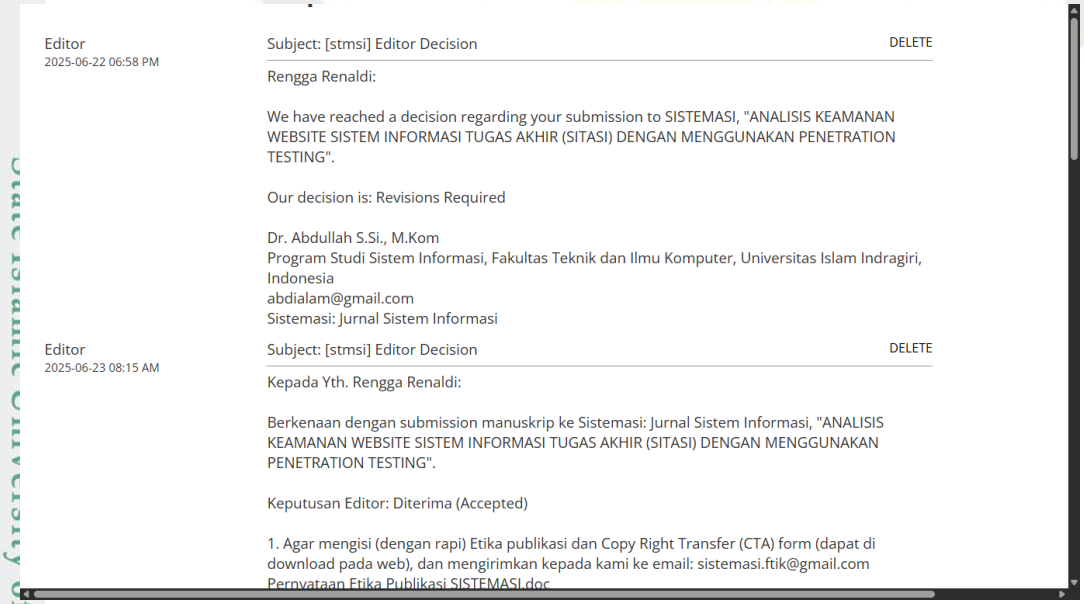
ISSN:2302-8149
e-ISSN:2540-9719

[15] P. Jarupunphol, S. Seatun, dan W. Buathong, "*Measuring Vulnerability Assessment Tools' Performance on the University Web Application*.," *Pertanika J Sci Technol*, Vol. 31, No. 6, 2023.
[16] Y. Yudiana, A. Elanda, dan R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi *E-Office* berbasis *Website* pada STMIK Rosma dengan menggunakan *OWASP* Top 10," *CESS (Journal of Computer Engineering, System and Science)*, Vol. 6, No. 2, hlm. 185–191, 2021.
[17] G. H. Editya dan S. Mulyati, "Aplikasi *Mobile One Time Password* nenggunakan *Algoritma MD5* dan *SHA1* untuk meningkatkan Keamanan *Website*," *SKANIKA: Sistem Komputer dan Teknik Informatika*, Vol. 1, No. 2, hlm. 618–623, 2018.
[18] J. T. Santoso, "Teknologi Keamanan *Siber (Cyber Security)*," *Penerbit Yayasan Prima Agus Teknik*, hlm. 1–173, 2023.

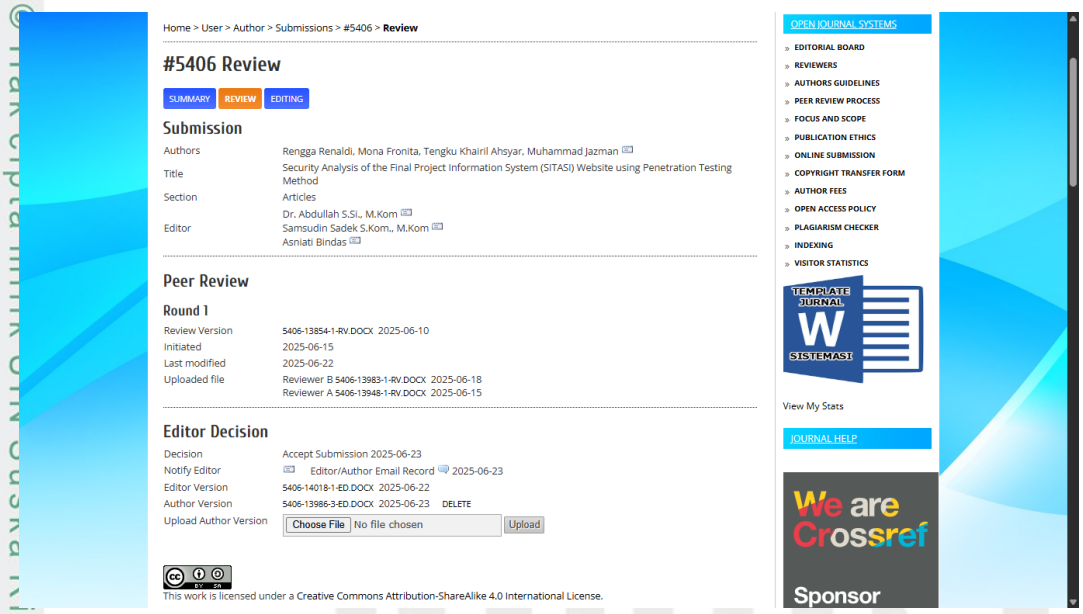
LAMPIRAN A

PROSES SUBMIT HINGGA ACCEPTED

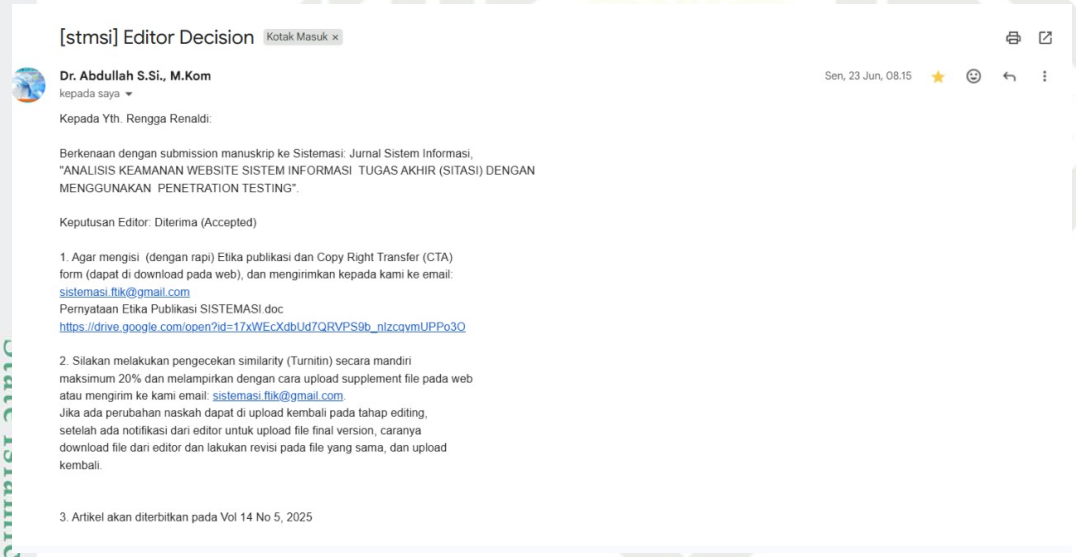
Gambar A.1. Bukti *Submission* Paper



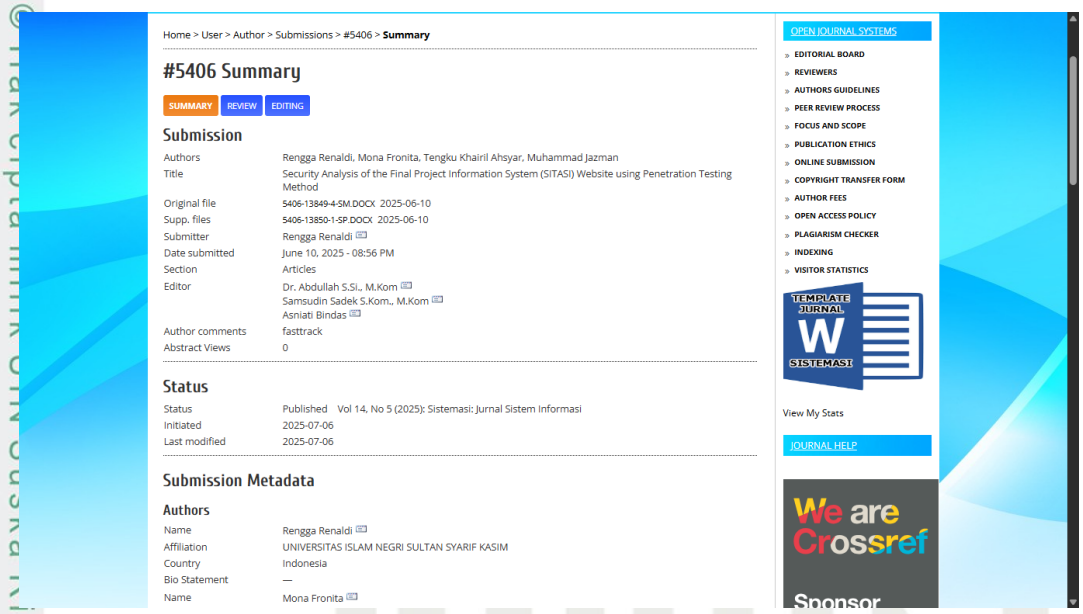
Gambar A.2. Bukti Review Paper



Gambar A.3. Bukti Review dan Hasil Revisi



Gambar A.4. Bukti Paper *Accepted*



Gambar A.5. Bukti *Published* Paper

SISTEMASI: JURNAL SISTEM INFORMSI
PROGRAM STUDI SISTEM INFORMASI
FAKULTAS TEKNIK DAN ILMU KOMPUTER
UNIVERSITAS ISLAM INDRAGIRI
INDONESIA

Letter of Acceptance

23 June 2025

Dear Rengga Renaldi,

Congratulations, We are pleased to inform you that your following manuscript has been accepted and will be published in SISTEMASI, Vol. 14 No. 5, 2025 pISSN: 2302-8149 eISSN: 2540-9719.

Title : **Analisis Keamanan Website Sistem Informasi Tugas Akhir (SITASI) menggunakan Metode Penetration Testing**

: **Website Security Analysis of Final Project Information System (SITASI) using Penetration Testing Method**

Authors : Rengga Renaldi, Mona Fronita, Tengku Khairil Ahsyar & Muhammad Jazman

Email : renggagggg6@gmail.com

Received on : 10 June 2025

Revised on : 22 June 2025

Accepted on : 23 June 2025

Thank you very much for submitting your article to "SISTEMASI"

Best Regards,

Dr. Abdullah Husin, S.Si., M.kom
Chief Editor

Gambar A.6. *Letter of Acceptance* (LOA)

DAFTAR RIWAYAT HIDUP

Rengga Renaldi lahir di Tembilahan pada tanggal 21 Juni 2001. Peneliti merupakan anak ketiga dari 5 bersaudara Bapak Rahmadi dan Ibu Rina Defriati. Pada tahun 2007 Peneliti memulai pendidikan di Sekolah Dasar Negeri di 007 Sekip Hulu. Kemudian setelah menyelesaikan pendidikan Sekolah Dasar, peneliti melanjutkan pendidikan di SMP Negeri 1 Tembilahan Kota pada tahun 2013 sampai tahun 2016. Kemudian Peneliti melanjutkan pendidikan di SMK Negeri 2 Tembilahan Kota pada tahun 2016 sampai tahun 2019. Pada tahun 2020 Peneliti melanjutkan Strata Satu (S1) di Universitas Islam Negeri Sultan Syarif Kasim Riau pada Fakultas Sains dan Teknologi Jurusan Sistem Informasi melalui jalur Seleksi Bersama Masuk Perguruan Tinggi Negeri (SBMPTN). Selama perkuliahan peneliti aktif dalam mengikuti kegiatan yang berada di dalam kampus maupun di luar kampus, Seperti mengikuti Kegiatan Kemah Bakti Mahasiswa pada tahun 2021 dan menjadi panitia Kemah Bakti Mahasiswa pada tahun 2022. Peneliti juga melaksanakan Kerja Praktek (KP) di Desa Rimbo Panjang, Kecamatan Tambang, Kabupaten Kampar. Kemudian pada tahun 2023 peneliti melaksanakan Kuliah Kerja Nyata (KKN) di Kelurahan Sungai Beringin, Kecamatan Tembilahan, Kabupaten Indragiri Hilir, Provinsi Riau. Terkait dengan pertanyaan kepada peneliti tentang penelitian yang dikerjakan dapat menghubungi kontak melalui *e-mail* 12050313320@students.uin-suska.ac.id untuk menjalin komunikasi yang lebih baik.