ANALYSIS AND OPTIMIZATION OF APPLICATION SECURITY SYSTEM FOR PREVENTION OF ILLEGAL CONTENT INTRUSION AT THE DIRECTORATE GENERAL OF LAND TRANSPORTATION

UNDERGRADUATE THESIS

Informatics Engineering Study Program

BY:

NAMA : THOMAS BRIMA EKAPUTRA

NIM : 190170006

FACULTY OF ENGINEERING

UNIVERSITY OF SATYA NEGARA INDONESIA

JAKARTA

2025

ANALISIS DAN OPTIMISASI SISTEM KEAMANAN APLIKASI PERIZINAN UNTUK PENCEGAHAN PENYUSUPAN KONTEN ILEGAL DI DIREKTORAT JENDERAL PERHUBUNGAN DARAT

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar

Sarjana Komputer

Disusun Oleh:

NAMA : THOMAS BRIMA EKAPUTRA

NIM : 190170006

FAKULTAS TEKNIK

UNIVERSITAS SATYA NEGARA INDONESIA

JAKARTA

2025

ANALYSIS AND OPTIMIZATION OF APPLICATION SECURITY SYSTEM FOR PREVENTION OF ILLEGAL CONTENT INTRUSION AT THE DIRECTORATE GENERAL OF LAND TRANSPORTATION

UNDERGRADUATE THESIS

Submitted as One of the Requirements to Obtain the Degree of

Bachelor Of Computer Science

BY:

NAMA : THOMAS BRIMA EKAPUTRA

NIM : 190170006

FACULTY OF ENGINEERING

UNIVERSITY OF SATYA NEGARA INDONESIA

JAKARTA

2025

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Alhamdulillah, Puji dan Syukur penulis panjatkan kehadirat Allah SWT karena atas rahmat dan karunia-Nya yang diberikan kepada penulis sehingga dapat menyelesaikan skripsi ini dengan judul "Analisis Dan Optimisasi Sistem Keamanan Aplikasi Perizinan Untuk Pencegahan Penyusupan Konten Ilegal Di Direktorat Jenderal Perhubungan Darat". Skripsi ini merupakan syarat untuk memperoleh gelar sarjana pada Program Studi Teknik Informatika Fakultas Teknik Universitas Satya Negara Indonesia.

Penulis mengucapkan terima kasih sebesar-besarnya kepada semua pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan bantuan bimbingan serta dukungan secara moril maupun materil sehingga skripsi ini dapat selesai sesuai dengan harapan. Selain itu, peneliti mengucapkan terima kasih secara khusus kepada:

1. Bapak Dr. Sihar P.H Sitorus, B.S.B.A., M.B.A. Selaku Rektor Universitas Satya Negara Indonesia.
2. Bapak Hernalom Sitorus, S.Kom., M.Kom. Selaku Dekan Fakultas Teknik Universitas Satya Negara Indonesia, sekaligus Dosen Pembimbing I yang meluangkan waktu serta pikiran untuk memberikan pengarahan dalam penulisan skripsi ini.

3. Bapak Abdul Kholiq, S.Kom., M.Kom. Selaku Dosen Pembimbing II atas semua bimbingan, dukungan serta masukan yang telah diberikan.
4. Seluruh Dosen Fakultas Teknik beserta Staff TU Universitas Satya Negara Indonesia yang tidak dapat disebutkan satu persatu.
5. Kedua orang tua dan mertua yang telah memberikan doa, kasih sayang dan bimbingan kepada penulis.
6. Istri tercinta penulis Siti Nurhasanah, yang selalu sabar memberikan kasih sayang, perhatian dan motivasi serta memberikan dukungan penuh untuk penyelesaian skripsi ini
7. Anak-anak penulis Ghassani Fildzah Syafna, Ghaisan Athafariz Hideo Toshi dan Ghania Lashira Hikari Hoshi, yang selalu memberikan pengertian dan perhatian, selama penulis menyelesaikan skripsi ini.
8. Pimpinan dan rekan kerja Kementerian Perhubungan, Direktorat Jenderal Perhubungan Darat Apip Ramdlani, S.Kom, MT., Joko Pitoyo, ST., M.M.Tr., Wisnu Dwi Sampurno, S.T., Fredy Yoseph Marianto, S.Stat., Fuad Naufal Ryan, A.md., Sahru Ardiansyah, S.Kom., atas dukungan moril dan materill yang diberikan kepada penulis.

Penulis berharap semoga skripsi ini dapat bermanfaat dan memberikan kebaikan ilmu pengetahuan bagi kita semua.

Jakarta, Februari 2025

Penulis

(Thomas Brima Ekaputra)

ABSTRAK

Penelitian ini dilakukan untuk memperoleh pemahaman yang lebih lengkap tentang analisis dan optimisasi sistem keamanan aplikasi perizinan untuk pencegahan penyusupan konten ilegal. Penelitian menggunakan pendekatan kualitatif dan kuantitatif dengan desain deskriptif analitis. Analisis keamanan dilakukan berdasarkan kerangka kerja NIST Cybersecurity Framework (CSF) 2.0 dan pedoman OWASP Top 10 yang mencakup identifikasi aset kritis, evaluasi risiko serta formulasi strategi mitigasi. Optimalisasi arsitektur server dilakukan dengan implementasi teknologi container berbasis docker swarm, pipeline otomatis melalui CI/CD, serta integrasi monitoring real-time. Implementasi ini berhasil meningkatkan kemampuan deteksi ancaman siber dan memberikan perlindungan lebih baik terhadap serangan modern seperti XSS, SQL Injection dan URL Redirection.

Hasil penelitian ini, telah membuktikan bahwa pendekatan holistik yang mengintegrasikan NIST CSF 2.0 dan OWASP Top 10 dapat meningkatkan perlindungan terhadap potensi risiko keamanan siber pada aplikasi perizinan. Selain itu optimalisasi infrastruktur sever dengan docker swarm dan CI/CD pipeline dapat secara signifikan meningkatkan keamanan dan ketahanan aplikasi perizinan di Direktorat Jenderal Perhubungan Darat. Sistem menjadi lebih adaptif terhadap dinamika ancaman siber modern, serta mempertahankan efisiensi operasional dan ketersediaan layanan bagi pengguna.

Kata Kunci: Keamanan Aplikasi, Penyusupan Konten Ilegal, NIST CSF 2.0, OWASP Top 10, Deteksi Ancaman, Arsitektur Server

ABSTRAK

This research was conducted to obtain a more comprehensive understanding of security analysis and optimization for licensing application systems to prevent illegal content infiltration. The study employed a qualitative and quantitative approach with a descriptive-analytical design. Security analysis was performed based on the NIST Cybersecurity Framework CSF 2.0 and OWASP Top 10 guidelines, encompassing critical asset identification, risk evaluation, and mitigation strategy formulation. Server architecture optimization was achieved through docker swarm-based container technology implementation, automated pipelines via CI/CD, and real-time monitoring integration. This implementation successfully enhanced cyber threat detection capabilities and provided improved protection against modern attacks such as XSS, SQL Injection, and URL Redirection.

The research findings demonstrate that a holistic approach integrating NIST CSF 2.0 and OWASP Top 10 can enhance protection against potential cybersecurity risks in licensing applications. Furthermore, server infrastructure optimization using docker swarm and CI/CD pipeline can significantly improve the security and resilience of licensing applications in the Directorate General of Land Transportation. The system becomes more adaptive to modern cyber threat dynamics while maintaining operational efficiency and service availability for users.

Keywords: *Application Security, Illegal Content Intrusion, NIST CSF 2.0, OWASP Top 10, Threat Detection, Server Architecture*

DAFTAR ISI

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan informasi saat ini menjadi salah satu aspek krusial didalam penyelenggaraan layanan pemerintahan berbasis elektronik. Saat ini instansi pemerintah dihadapkan pada tantangan besar memastikan bahwa data yang dikelola tetap aman, autentik, dan hanya dapat diakses oleh pihak yang berwenang. Meningkatnya ancaman keamanan yang kompleks dan canggih, berpotensi mengeksploitasi kerentanan sistem untuk tujuan ilegal. Direktorat Jenderal Perhubungan Darat, Kementerian Perhubungan memiliki tanggung jawab besar dalam pengelolaan aplikasi berbasis teknologi informasi sebagai bagian dari Sistem Pemerintahan Berbasis Elektronik Nasional (SPBE), Direktorat Jenderal Perhubungan Darat mengoperasikan sejumlah aplikasi perizinan yang bersifat strategis dan sensitif selama 24 jam.

Aplikasi perizinan yang dikelola oleh Direktorat Jenderal Perhubungan Darat mencakup data penting seperti data pribadi pengguna jasa transportasi, data perizinan, dan data operasional lainnya. Pemenuhan prinsip-prinsip keamanan informasi yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), keaslian (*authenticity*), dan kenirsangkalan (*nonrepudiation*) menjadi prioritas utama dalam pengelolaan aplikasi perizinan Direktorat Jenderal Perhubungan Darat. Serangkaian insiden keamanan yang terjadi selama tahun 2024 menunjukkan masih adanya celah pada aplikasi perizinan yang memerlukan

penanganan.

Aplikasi perizinan Air-SDP (Aplikasi Informasi dan Registrasi Angkutan Sungai Danau dan Penyeberangan) mengalami penyusupan konten ilegal berupa situs judi online pada tanggal 19 Maret 2024. Insiden serupa kembali terjadi pada tanggal 8 November 2024, hal ini menunjukkan bahwa masalah tidak hanya bersifat insidental akan tetapi berulang terjadi. Selain itu aplikasi perizinan Spionam (Perizinan Angkutan Jalan) dilaporkan juga tersusupi konten ilegal pada tanggal 4 Oktober 2024. Insiden yang terjadi ini mengindikasikan adanya kerentanan sistemik yang belum sepenuhnya tertangani dengan baik. Dampak dari insiden tersebut tidak hanya terbatas pada risiko kebocoran atau manipulasi data, hal ini berpotensi merusak reputasi institusi, mengancam privasi pengguna, dan membahayakan keselamatan serta keamanan transportasi darat secara keseluruhan.

Mitigasi yang telah dilakukan oleh Direktorat Jenderal Perhubungan Darat adalah menerapkan beberapa lapisan keamanan, seperti pembatasan akses berbasis peran (role-based access control), penggunaan firewall, serta enkripsi SSL/TLS untuk melindungi komunikasi data. Serangkaian insiden yang terjadi menunjukkan bahwa langkah-langkah tersebut belum cukup efektif dalam menghadapi ancaman siber yang semakin canggih. Pola serangan yang berulang pada aplikasi perizinan mengindikasikan perlu pendekatan keamanan yang lebih komprehensif, terstandar, dan adaptif terhadap perkembangan ancaman siber.

Berdasarkan permasalahan yang ada, penelitian ini dibuat bertujuan melakukan analisis mendalam terhadap sistem keamanan yang diterapkan pada aplikasi perizinan oleh Direktorat Jenderal Perhubungan Darat, dengan fokus pada

identifikasi kerentanan dan formulasi strategi optimisasi keamanan. Pendekatan penelitian menggunakan metode kualitatif dan kuantitatif untuk menghasilkan analisis holistik dan berbasis data. Hasil penelitian diharapkan dapat memberikan kontribusi nyata dalam memperkuat keamanan aplikasi perizinan, menghasilkan rekomendasi teknis yang aplikatif, serta menjadi referensi bagi Direktorat Jenderal Perhubungan Darat dalam mengembangkan sistem keamanan informasi yang efektif dan terstandar.

1.2 Rumusan Masalah

Berdasarkan latar belakang dapat dirumuskan suatu permasalahan, yaitu bagaimana menganalisis dan mengoptimasi sistem keamanan pada aplikasi perizinan di Direktorat Jenderal Perhubungan Darat dalam mencegah penyusupan konten ilegal.

1.3 Batasan Masalah

Untuk memfokuskan penelitian ditetapkan batasan masalah sebagai berikut:

1. Penelitian ini hanya mencakup aplikasi perizinan yang dikelola secara langsung oleh Direktorat Jenderal Perhubungan Darat. Aplikasi pihak ketiga atau aplikasi yang tidak terkait dengan perizinan tidak termasuk dalam lingkup penelitian ini.
2. Analisis dan optimisasi sistem keamanan akan berfokus pada kerangka kerja NIST *Cybersecurity Framework* (CSF) 2.0 untuk pendekatan keamanan dan panduan OWASP untuk keamanan aplikasi web khususnya terkait pencegahan

Cross-Site Scripting (XSS), SQL *Injection*, dan URL *redirection*. Standar keamanan lain di luar NIST CSF 2.0 dan OWASP tidak akan dibahas dalam penelitian ini.

3. Analisis keamanan dibatasi pada ancaman penyusupan konten ilegal, termasuk serangan berbasis halaman judi *online*, *phishing*, dan pengalihan situs (*URL redirection*) yang dapat mengganggu fungsi dan integritas aplikasi. Ancaman keamanan lainnya, seperti serangan DDoS atau *malware*, tidak akan dibahas dalam penelitian ini.
4. Rekomendasi dalam penelitian ini difokuskan pada solusi yang dapat diimplementasikan dalam jangka waktu 1-2 tahun dan sesuai dengan kapabilitas sumber daya di Direktorat Jenderal Perhubungan Darat. Optimisasi jangka panjang atau solusi yang memerlukan perubahan besar pada infrastruktur tidak termasuk dalam ruang lingkup penelitian ini.

1.4 Tujuan dan Kegunaan Penelitian

3.3.1 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

1. Menganalisis kondisi sistem keamanan yang ada pada aplikasi perizinan di Direktorat Jenderal Perhubungan Darat dalam menghadapi ancaman penyusupan konten ilegal.
2. Mengevaluasi efektivitas sistem keamanan yang ada pada aplikasi perizinan menggunakan kerangka kerja NIST CSF 2.0 dan panduan OWASP.

3. Mengidentifikasi celah keamanan yang memungkinkan terjadinya penyusupan konten ilegal berulang pada aplikasi perizinan di Direktorat Jenderal Perhubungan Darat.
4. Merumuskan strategi optimisasi keamanan yang efektif dan sesuai dengan kebutuhan Direktorat Jenderal Perhubungan Darat, yang dapat diimplementasikan untuk meningkatkan ketahanan aplikasi perizinan terhadap ancaman penyusupan konten ilegal.

3.3.2 Kegunaan Penelitian

Dengan penelitian ini diharapkan dapat:

1. Mengidentifikasi kondisi keamanan aplikasi perizinan di Ditjen Perhubungan Darat, termasuk kelemahan dan risiko penyusupan konten ilegal.
2. Memberikan rekomendasi teknis untuk meningkatkan keamanan aplikasi.
3. Mencegah insiden serupa di masa depan dan memperkuat kepercayaan publik terhadap layanan perizinan transportasi darat.