PERANCANGAN *CYBER SECURITY* UNTUK MENANGKAL SERANGAN *CYBER* MENGGUNAKAN METODE *WEB* APLIKASI *PENETRATION TEST* PADA DINAS PENANAMAN MODAL DAN PERIZINAN TERPADU SATU PINTU KABUPATEN OGAN KOMERING ILIR

TESIS

JERRY HANSEN
ENTERPRISE IT INFRASTRUCTURE
212420036

PROGRAM STUDI TEKNIK INFORMATIKA – S2
PROGRAM PASCASARJANA
UNIVERSITAS BINA DARMA
PALEMBANG
2025

PERANCANGAN *CYBER SECURITY* UNTUK MENANGKAL SERANGAN *CYBER* MENGGUNAKAN METODE *WEB* APLIKASI *PENETRATION TEST* PADA DINAS PENANAMAN MODAL DAN PERIZINAN TERPADU SATU PINTU KABUPATEN OGAN KOMERING ILIR

Tesis ini diajukan sebagai salah satu syarat
untuk memperoleh gelar

MAGISTER KOMPUTER

JERRY HANSEN
ENTERPRISE IT INFRASTRUCTURE
212420036

PROGRAM STUDI TEKNIK INFORMATIKA – S2
PROGRAM PASCASARJANA
UNIVERSITAS BINA DARMA
PALEMBANG
2025

Halaman Pengesahan Pembimbing Tesis

Judul Tesis: PERANCANGAN CYBER SECURITY UNTUK MENANGKAL SERANGAN CYBER MENGGUNAKAN METODE WEB APLIKASI PENETRATION TEST PADA DINAS PENANAMAN MODAL DAN PERIZINAN TERPADU SATU PINTU KABUPATEN OGAN KOMERING ILIR

Oleh JERRY HANSEN, NIM 212420036, Tesis ini telah disetujui dan disahkan oleh Tim Penguji Program Studi Teknik Informatika – S2 konsentrasi *ENTERPRISE IT INFRASTRUCTURE*, Program Pascasarjana Universitas Bina Darma pada 28 Agustus 2025 dan telah dinyatakan LULUS.

Palembang, 28 Agustus 2025
Mengetahui,
Program Studi Teknik Informatika – S2
Universitas Bina Darma
Ketua,

Universitas Bina Darma
Magister Teknik Informatika

Dr. Usman Ependi, S.Kom., M.Kom.

Pembimbing,

Dr. Tata Sutabri, S.Kom., M.M.S.I.

Halaman Pengesahan Penguji Tesis

Judul Tesis: PERANCANGAN CYBER SECURITY UNTUK MENANGKAL SERANGAN CYBER MENGGUNAKAN METODE WEB APLIKASI PENETRATION TEST PADA DINAS PENANAMAN MODAL DAN PERIZINAN TERPADU SATU PINTU KABUPATEN OGAN KOMERING ILIR

Oleh JERRY HANSEN, NIM 212420036, Tesis ini telah disetujui dan disahkan oleh Tim Penguji Program Studi Teknik Informatika – S2 konsentrasi *ENTERPRISE IT INFRASTRUCTURE*, Program Pascasarjana Universitas Bina Darma pada 28 Agustus 2025 dan telah dinyatakan LULUS.

Palembang, 28 Agustus 2025
Mengetahui,
Program Pascasarjana
Universitas Bina Darma
Direktur,

Universitas Bina Darma
PROGRAM PASCASARJANA

Prof. Dr. Ir. Achmad Syarifudin, M.Sc.

Penguji I,

Dr. Tata Sutabri, S.Kom., M.M.S.I.

Penguji II,

Prof. Dr. Edi Surya Negara H., S.Kom., M.Kom.

Penguji III,

M. Izman Herdiansyah, M.M., Ph. D.

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : JERRY HANSEN

NIM : 212420036

Dengan ini menyatakan bahwa:

1. Karya tulis Saya (Tesis, Skripsi, Tugas Akhir) ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik baik (Magister, Sarjana, dan Ahli Madya) di Universitas Bina Darma;
2. Karya tulis ini murni gagasan, rumusan dan penelitian Saya sendiri dengan arahan tim pembimbing;
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukkan ke dalam daftar pustaka;
4. Karena yakin dengan keasliaan karya tulis ini, Saya menyatakan bersedia Tesis/Skripsi/Tugas Akhir, yang Saya hasilkan di unggah ke internet;
5. Surat Pernyataan ini Saya tulis dengan sungguh-sungguh dan apabila terdapat penyimpangan atau ketidakbenaran dalam pernyataan ini, maka Saya bersedia menerima sanksi dengan aturan yang berlaku di perguruan tinggi ini.

Demikian Surat Pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 28 Agustus 2025
Yang Membuat Pernyataan,

JERRY HANSEN
NIM: 212420036

ABSTRAK

Teknologi digital memberikan dampak signifikan pada efisiensi layanan publik, namun juga menghadirkan risiko kerentanan keamanan siber. DPMPTSP Kabupaten Ogan Komering Ilir sebagai instansi penyedia layanan perizinan digital rentan terhadap ancaman seperti kebocoran data dan serangan siber. Penelitian ini bertujuan menganalisis celah keamanan pada *web*site DPMPTSP Kab. OKI melalui metode *penetration test* dengan pendekatan *ZAP* (Zed Attack *Proxy*) dan *Black Box Testing*. Metode *ZAP* digunakan untuk pemindaian otomatis kerentanan dinamis, sementara *Black Box Testing* mensimulasikan serangan eksternal tanpa peng*et*ahuan internal sistem. Hasil penelitian mengidentifikasi kerentanan kritis seperti SQL *Injection* to RCE (skor CVSS 9.3) yang memungkinkan eksekusi kode jarak jauh, serta kerentanan tingkat sedang seperti *Directory Listing* dan Reflected XSS. Selain itu, ditemukan pula kerentanan tingkat tinggi pada *Hash Disclosure* dan ketiadaan *token CSRF*, serta masalah konfigurasi *cookie* (*HTTP*Only dan Secure Flag). Analisis menunjukkan bahwa kombinasi kedua metode mampu memberikan evaluasi komprehensif, dengan *ZAP* efektif dalam pemetaan kerentanan otomatis, sedangkan *Black Box Testing* memvalidasi dampak eksploitasi secara realistis. Rekomendasi perbaikan mencakup implementasi *parameterized queries*, penambahan *token CSRF*, konfigurasi *cookie* yang aman, dan peningkatan kesadaran keamanan SDM. Penelitian ini menekankan pentingnya pengujian keamanan berkala, pembaruan infrastruktur, serta penerapan kebijakan keamanan siber yang terstruktur untuk memitigasi risiko serangan dan menjamin keamanan data pengguna.

Kata Kunci: Keamanan Siber, *Penetration Test*, *ZAP*, *Black Box Testing,* Kerentanan *Web*

ABSTRACT

Digital technology has significantly enhanced the efficiency of public services but concurrently introduced substantial cybersecurity risks. The Department of Investment and One-Stop Integrated Services (DPMPTSP) of Ogan Komering Ilir Regency, as a digital licensing service provider, remains vulnerable to threats such as data breaches and cyberattacks. This study aims to analyze security gaps in the DPMPTSP Kab. OKI website through penetration testing methodologies, employing ZAP (Zed Attack Proxy) for dynamic vulnerability scanning and Black Box Testing to simulate external attacks without internal system knowledge. The ZAP methodology identified critical vulnerabilities, including Hash Disclosure (high risk) and the absence of CSRF tokens (medium risk), alongside Low-risk issues such as insecure cookie configurations (missing HTTPOnly and Secure Flags). Black Box Testing revealed severe vulnerabilities, notably SQL Injection to Remote Code Execution (RCE) with a CVSS score of 9.3, enabling unauthorized remote command execution, as well as medium-risk vulnerabilities like Directory Listing and Reflected Cross-Site Scripting (XSS). The combined application of both methods demonstrated complementary efficacy: ZAP provided automated, broad-spectrum vulnerability mapping, while Black Box Testing validated exploit impacts through realistic attack simulations. Key recommendations include adopting parameterized queries to mitigate SQL Injection, implementing CSRF tokens, enforcing secure cookie attributes (HTTPOnly, Secure, and SameSite), and enhancing cybersecurity awareness among personnel. The study underscores the necessity of periodic security assessments, infrastructure updates, and structured cybersecurity policies to mitigate attack risks and ensure robust protection of user data. These findings emphasize the critical role of proactive cybersecurity measures in safeguarding public service platforms against evolving digital threats.

Keywords: *Cybersecurity, Penetration Testing, ZAP, Black Box Testing, Web Vulnerabilities.*

MOTTO DAN PERSEMBAHAN

- ✓ ***"The only limit to our realization of tomorrow is our doubts of today."*** **— Franklin D. Roosevelt**
  (Batasan satu-satunya untuk mewujudkan masa depan kita adalah keraguan kita hari ini.)
- ✓ ***"Success is not the key to happiness. Happiness is the key to success. If you love what you are doing, you will be successful."*** **— Albert Schweitzer**
  (Kesuksesan bukan kunci kebahagiaan. Kebahagiaan adalah kunci kesuksesan. Jika Anda mencintai apa yang Anda lakukan, Anda akan sukses.)
- ✓ ***"What lies behind us and what lies before us are tiny matters compared to what lies within us."*** **— Ralph Waldo Emerson**
  (Apa yang ada di belakang kita dan apa yang ada di depan kita hanyalah hal kecil dibandingkan dengan apa yang ada di dalam diri kita.)

SAYA PERSEMBAHKAN TESIS INI UNTUK:

- Masyarakat Kabupaten Ogan Komering Ilir Tercinta
- Untuk almamaterku, Universitas Bina Darma Palembang

KATA PENGANTAR

Segala puji penulis ucapkan ke hadirat Allah SWT atas segala nikmat dan karunia yang telah diberikan, sehingga tesis yang berjudul "**PERANCANGAN *CYBER SECURITY* UNTUK MENANGKAL SERANGAN *CYBER* MENGGUNAKAN METODE *WEB* APLIKASI *PENETRATION TEST* PADA DINAS PENANAMAN MODAL DAN PERIZINAN TERPADU SATU PINTU KABUPATEN OGAN KOMERING ILIR**" bisa terselesaikan dengan baik.

Dalam penelitian tesis ini, tentunya masih jauh dari kata sempurna. Hal ini dikarenakan keterbatasannya peng*et*ahuan yang dimiliki. Oleh karena itu dalam rangka melengkapi kesempurnaan dari penulisan tesis ini diharapkan adanya saran dan kritik yang diberikan bersifat membangun. Pada kesempatan yang baik ini, tak lupa penulis menghaturkan terimakasih kepada semua pihak yang telah memberikan bimbingan, pengarahan, nasehat dan pemikiran dalam penulisan proposal tesis ini, terutama kepada:

1. Prof. Dr. Sunda Ariana, M.Pd., M.M. selaku Rektor Universitas Bina Darma Palembang.
2. Prof. Dr. Ir. H. Achmad Syarifudin, M.Sc. selaku Direktur Pascasarjana Universitas Bina Darma Palembang.
3. Dr. Usman Effendi, M. Kom. selaku Ketua Program Studi Pascasarjana Teknik In*form*atika.
4. Dr. Tata Sutabri, S. Kom., MMSI., MKM. selaku Pembimbing yang telah memberikan bimbingan tesis ini.
5. Pihak Sekretariat Pascasarjana Universitas Bina Darma Palembang yang telah memberikan bimbingan pelayanan dengan baik.

Palembang, 29 Agustus 2025

Penulis

DAFTAR ISI

HALAMAN

BAB III METODOLOGI PENELITIAN

BAB IV HASIL DAN PEMBAHASAN

BAB V KESIMPULAN DAN SARAN

DAFTAR PUSTAKA

DAFTAR RIWAYAT HIDUP

LAMPIRAN

LEMBAR PERBAIKAN TESIS

DAFTAR TABEL

DAFTAR GAMBAR