



**IMPLEMENTASI SISTEM AUTENTIKASI JWT DENGAN *REFRESH*
TOKEN PADA APLIKASI *MOBILE* PORTOFOLIO DIGITAL
MENGUNAKAN REACT NATIVE DI FIK UPN "VETERAN"
JAKARTA**

SKRIPSI

**IHSAN TRI MARSENO
2110511088**

**PROGRAM STUDI S1 INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA
2025**



**IMPLEMENTASI SISTEM AUTENTIKASI JWT DENGAN *REFRESH*
TOKEN PADA APLIKASI *MOBILE* PORTOFOLIO DIGITAL
MENGUNAKAN REACT NATIVE DI FIK UPN “VETERAN”
JAKARTA**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana
Komputer**

**IHSAN TRI MARSEN
2110511088**

**PROGRAM STUDI S1 INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
2025**

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar:

Nama : Ihsan Tri Marseno
NIM : 2110511088
Tanggal : 23 Juni 2025

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku

Jakarta, 23 Juni 2025

Yang Menyatakan



Ihsan Tri Marseno

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Ihsan Tri Marseno
NIM : 2110511088
Fakultas : Ilmu Komputer
Program Studi : S-1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas skripsi saya yang berjudul:

Implementasi Sistem Autentikasi JWT Dengan *Refresh Token* Pada Aplikasi *Mobile* Portofolio Digital Menggunakan React Native di FIK UPN “Veteran” Jakarta

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/memformatkan, mengelola dalam bentuk pangkalan data (basis data), merawat dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya

Dibuat di Jakarta

Pada tanggal: 23 Juni 2025

Yang Menyatakan



Ihsan Tri Marseno

LEMBAR PERSETUJUAN

LEMBAR PERSETUJUAN

Yang bertanda tangan di bawah ini :

Nama : Ihsan Tri Marseno

NIM : 2110511088

Program Studi : Informatika Program Sarjana/~~Sistem Informasi Program Sarjana/Sains~~

~~Data Program Sarjana/Sistem Informasi Program Diploma~~ (*Coret yang tidak perlu)

Jenis Tugas Akhir : Skripsi / ~~Proyek / Artikel Publikasi~~ (*Coret yang tidak perlu)

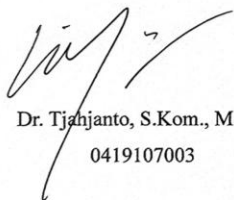
Judul Tugas Akhir : Implementasi Sistem Autentikasi JWT dengan *Refresh Token* pada Aplikasi *Mobile* Portofolio Digital menggunakan React Native di FIK UPN "Veteran" Jakarta

Dinyatakan telah memenuhi syarat dan menyetujui untuk mengikuti ujian sidang Tugas Akhir.

Jakarta, 09 Mei 2025

Menyetujui,

Dosen Pembimbing I,



Dr. Tjanjanto, S.Kom., M.M..
0419107003

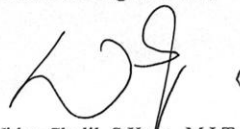
Dosen Pembimbing II,



I Wayan Rangga Pinastawa,
M.Kom
0007109404

Mengetahui,

Koordinator Program Studi,



Dr. Widya Cholil, S.Kom., M.I.T.
0218107101

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Judul : Implementasi Sistem Autentikasi JWT Dengan Refresh Token
Pada Aplikasi Mobile Portofolio Digital Menggunakan React
Native di FIK UPN "Veteran" Jakarta

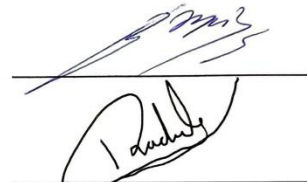
Nama : Ihsan Tri Marseno

NIM : 2110511088

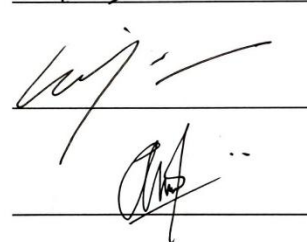
Program Studi : S1 Informatika

Disetujui Oleh:

Penguji 1:
Bayu Hananto S.Kom., M.Kom.



Penguji 2:
Radinal Setyadinsa S.Pd., M.T.I.



Pembimbing 1:
Dr. Tjahjanto S.Kom., M.M.

Pembimbing 2:
I Wayan Rangga Pinastawa S.Kom., M.Kom



Diketahui Oleh:

Koordinator Program Studi:
Dr. Widya Cholil, M.I.T
NIP. 197005212021212002



Dekan Fakultas Ilmu Komputer:
Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM
NIP. 197605082003121002



Tanggal Ujian Tugas Akhir:
18 Juni 2025

**IMPLEMENTASI SISTEM AUTENTIKASI JWT DENGAN REFRESH
TOKEN PADA APLIKASI MOBILE PORTOFOLIO DIGITAL
MENGUNAKAN REACT NATIVE DI FIK UPN “VETERAN”
JAKARTA**

IHSAN TRI MARSENO

ABSTRAK

Portofolio digital merupakan sarana penting bagi individu untuk mendokumentasikan pencapaian dan kompetensi, dengan keamanan data sebagai aspek krusial. Namun, saat ini keamanan aplikasi *mobile* portofolio digital menjadi tantangan besar, khususnya dalam melindungi data pribadi pengguna. Berbagai faktor internal dan eksternal turut mempengaruhi tingkat keamanan aplikasi *mobile*. Penelitian ini mengimplementasikan sistem autentikasi berbasis *JSON Web Token* (JWT) dengan mekanisme *refresh token* pada aplikasi *mobile* portofolio digital. Implementasi JWT dengan *refresh token* berhasil meningkatkan keamanan aplikasi melalui validitas masa berlaku *token* yang berbeda, integritas tanda tangan dengan algoritma HMAC SHA-256, dan pengalaman pengguna yang *seamless* tanpa *login* ulang. Sistem ini efektif mengamankan operasi CRUD pada fitur portofolio digital dan mengintegrasikan konversi portofolio menjadi CV berbasis *Applicant Tracking System*. Pengalaman pengguna yang mulus ini meningkatkan kontinuitas penggunaan aplikasi, mengurangi hambatan interaksi, dan menciptakan keseimbangan antara keamanan data dan kenyamanan pengguna. Implementasi yang dilakukan terbukti efektif meningkatkan keamanan aplikasi *mobile* portofolio digital dengan tetap mempertahankan pengalaman pengguna yang optimal.

Kata Kunci: *JSON Web Token*, *Refresh Token*, Autentikasi, Aplikasi *Mobile*, Portofolio Digital

**IMPLEMENTATION OF A JWT AUTHENTICATION SYSTEM WITH
REFRESH TOKEN ON A DIGITAL PORTFOLIO MOBILE
APPLICATION USING REACT NATIVE AT THE FACULTY OF
COMPUTER SCIENCE, UPN "VETERAN" JAKARTA**

IHSAN TRI MARSENO

ABSTRACT

Digital portfolios serve as essential tools for individuals to document their achievements and competencies, with data security being a crucial aspect. However, currently, the security of mobile digital portfolio applications presents a significant challenge, particularly in protecting users' personal data. Various internal and external factors influence the security level of mobile applications. This research implements an authentication system based on JSON Web Token (JWT) with a refresh token mechanism in a mobile digital portfolio application. The implementation of JWT with refresh tokens successfully enhances application security through different token validity periods, signature integrity using the HMAC SHA-256 algorithm, and a seamless user experience without requiring repeated logins. This system effectively secures CRUD operations on digital portfolio features and integrates portfolio conversion into CV based on Applicant Tracking Systems. This smooth user experience increases application usage continuity, reduces interaction barriers, and creates a balance between data security and user convenience. The implementation proves effective in enhancing the security of mobile digital portfolio applications while maintaining optimal user experience.

Keywords: *JSON Web Token, Refresh Token, Authentication, Mobile Application, Digital Portfolio*

KATA PENGANTAR

Bismillahirrahmanirrahim. Segala puji dan syukur penulis panjatkan kepada Allah SWT atas limpahan rahmat, karunia, dan kehendak-Nya sehingga penulis dapat menyelesaikan proposal skripsi berjudul “IMPLEMENTASI SISTEM AUTENTIKASI JWT DENGAN *REFRESH TOKEN* PADA APLIKASI *MOBILE PORTOFOLIO DIGITAL* MENGGUNAKAN REACT NATIVE DI FIK UPN VETERAN JAKARTA” dengan baik. Shalawat serta salam juga penulis sampaikan kepada junjungan kita, Nabi Muhammad SAW, yang selalu menjadi teladan dalam menjalani kehidupan. Proposal skripsi ini merupakan rancangan penelitian yang disusun sebagai bagian dari penyelesaian studi di Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta.

Dalam proses penyusunan proposal ini, penulis menerima banyak bantuan dan dukungan, baik secara moral maupun materiil. Oleh karena itu, melalui kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang mendalam kepada:

1. Ibunda tercinta yang telah memberikan dukungan kepada penulis dalam bentuk tenaga, biaya, waktu, dan lain sebagainya.
2. Almarhum Bapak tercinta yang sebelumnya telah mendukung penuh penulis untuk terus menyelesaikan kuliahnya.
3. Adik dan Kakak tercinta yang turut membantu dalam memberikan beberapa ide dan juga dukungan dari belakang.
4. Bapak Dr. Tjahjanto, S.Kom., M.M., selaku dosen pembimbing I yang membantu dalam pengarahan penelitian ini. Membantu mengarahkan visi proposal skripsi yang baik, dukungan, ide, dan lain sebagainya.
5. Bapak I Wayan Ranga Pinastawa, S.Kom., M.Kom. selaku dosen pembimbing II sekaligus dosen pembimbing akademik yang juga telah membimbing penulis dalam menyelesaikan proposal skripsi dalam bentuk dukungan, ide, dan juga penulisan skripsi dengan benar.
6. Rekan-rekan dan seluruh pihak yang terlibat dalam pembuatan proposal skripsi.

Jakarta, 9 Mei 2025

A handwritten signature in black ink, consisting of stylized, cursive letters that appear to read 'ITM' followed by a flourish.

Ihsan Tri Marseno

DAFTAR ISI

PERNYATAAN ORISINALITAS	i
PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	ii
LEMBAR PERSETUJUAN.....	iii
LEMBAR PENGESAHAN	iv
ABSTRAK	v
<i>ABSTRACT</i>	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xvii
DAFTAR LAMPIRAN	xviii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Tujuan dan Manfaat Penelitian	6
1.4.1 Tujuan	6
1.4.2 Manfaat Penelitian	7
1.5 Sistematika Penulisan	8
BAB II TINJAUAN PUSTAKA.....	9
2.1 Kajian Teoretis	9
2.1.1 Portofolio Digital	9
2.1.2 <i>JSON Web Token (JWT)</i>	10
2.1.3 Algoritma HMAC SHA-256.....	11
2.1.4 <i>Refresh Token</i>	12
2.1.5 <i>Aplikasi Mobile</i>	13
2.1.6 <i>Curriculum Vitae</i>	14
2.1.7 <i>Framework React Native</i>	15
2.1.8 <i>Framework Express.js</i>	15
2.1.9 <i>PostgreSQL Database</i>	16
2.1.10 <i>Unified Modeling Language (UML)</i>	17
2.1.10.1 <i>Use Case Diagram</i>	17
2.1.10.2 <i>Activity Diagram</i>	19

2.1.11	<i>Entity Relationship Diagram (ERD)</i>	21
2.1.12	<i>Metode Rapid Application Development (RAD)</i>	22
2.1.13	<i>Black Box Testing</i>	23
2.2	Penelitian Terdahulu	23
BAB III METODE PENELITIAN.....		30
3.1	Tahapan Penelitian	30
3.1.1	Identifikasi Masalah	30
3.1.2	Studi Literatur	31
3.1.3	Pengumpulan Data	32
3.1.4	Perancangan	33
3.1.5	<i>Development (Pengembangan)</i>	36
3.1.6	<i>Testing (Pengujian)</i>	36
3.1.7	Implementasi	37
3.2	Alat dan Bahan Penelitian.....	38
3.2.1	Alat Penelitian.....	38
3.2.1.1	Perangkat Keras (<i>Hardware</i>)	38
3.2.1.2	Perangkat Keras (<i>Hardware</i>)	39
3.2.2	Bahan Penelitian.....	39
3.2.2.1	Data Primer	39
3.2.2.2	Data Sekunder	39
3.3	Jadwal Penelitian.....	40
BAB IV HASIL DAN PEMBAHASAN		41
4.1	Profil Perusahaan	41
4.2	Analisis Sistem Berjalan	41
4.2.1	Proses Pengelolaan Portofolio Mahasiswa Saat Ini	41
4.2.2	Identifikasi Permasalahan dan Kebutuhan	42
4.3	Rancangan Sistem Usulan.....	43
4.3.1	Analisis Rancangan Sistem	43
4.3.2	Analisis Kebutuhan Data.....	46
4.3.3	Penyusunan <i>Product Backlog</i>	46
4.3.4	Penyusunan Iterasi <i>Backlog</i>	48
4.3.5	Perancangan Sistem Aplikasi.....	52
4.3.5.1	<i>Use Case Diagram</i>	53
4.3.5.2	<i>Activity Diagram</i>	55
4.3.5.3	Pembuatan <i>Database</i>	73
4.3.5.3.1	Tabel Pengguna (<i>Users</i>)	74

4.3.5.3.2	Tabel Peran (<i>Roles</i>)	75
4.3.5.3.3	Tabel List (<i>ListGenericEntity</i>)	76
4.3.5.3.4	Tabel <i>Attachments</i>	77
4.3.5.3.5	Tabel Prestasi (<i>Achievements</i>).....	78
4.3.5.3.6	Tabel Kegiatan (<i>Activities</i>).....	79
4.3.5.3.7	Tabel Sertifikasi (<i>Certifications</i>).....	80
4.3.5.3.8	Tabel Organisasi (<i>Organizations</i>)	81
4.3.6	Pembuatan <i>Backend</i> Serta Penerapan <i>Refresh Token</i> JWT.....	82
4.3.6.1	Konfigurasi Teknis <i>Backend Service</i>	83
4.3.6.2	Modul Otentikasi dan JWT	83
4.3.6.3	Modul Admin.....	98
4.3.6.4	Modul Verifikator (<i>Verifier</i>)	99
4.3.6.5	Modul Kegiatan (<i>Activities</i>)	100
4.3.6.6	Modul Prestasi (<i>Achievements</i>)	102
4.3.6.7	Modul Organisasi (<i>Organizations</i>)	103
4.3.6.8	Modul Sertifikasi (<i>Certifications</i>)	105
4.3.6.9	Modul <i>Search</i> dan <i>Validation CV ATS</i>	106
4.3.6.10	Modul General	107
4.3.7	Implementasi Keamanan Pada JWT	108
4.3.7.1	<i>Confidentiality</i> (Kerahasiaan)	108
4.3.7.2	<i>Integrity</i> (Integritas)	109
4.3.7.3	<i>Availability</i> (Ketersediaan).....	110
4.3.8	Pembuatan Aplikasi <i>Frontend</i>	111
4.3.8.1	Konfigurasi Teknis <i>Frontend</i>	112
4.3.8.2	<i>Login</i>	113
4.3.8.3	<i>Register</i>	116
4.3.8.4	<i>Axios</i>	119
4.3.8.5	Halaman Aktivitas.....	121
4.3.8.6	Halaman Prestasi.....	126
4.3.8.7	Halaman Sertifikasi.....	131
4.3.8.8	Halaman Organisasi	136
4.3.8.9	Halaman <i>Search</i>	140
4.3.8.10	Halaman Profil	141
4.3.8.11	Halaman Admin	145
4.3.8.12	Halaman Verifikator.....	147
4.3.9	Hasil Tampilan Antarmuka Aplikasi	153

4.3.9.1	Halaman <i>Onboarding</i>	154
4.3.9.2	Halaman <i>Login</i>	155
4.3.9.3	Halaman Daftar	156
4.3.9.4	Halaman Utama.....	157
4.3.9.5	Halaman Kegiatan Mahasiswa	160
4.3.9.6	Halaman Prestasi Mahasiswa	164
4.3.9.7	Halaman Organisasi Mahasiswa	168
4.3.9.8	Halaman Sertifikasi Mahasiswa	173
4.3.9.9	Halaman <i>Search</i> (Mahasiswa dan Tamu)	178
4.3.9.10	Halaman Profil	179
4.3.9.11	Halaman Admin	183
4.3.9.12	Halaman Verifikator.....	184
4.3.10	Pengujian.....	189
4.3.11	Pengujian Aplikasi Menggunakan <i>Black Box</i>	189
4.3.11.1	Pengujian Aplikasi <i>Backend</i>	189
4.3.11.2	Pengujian Aplikasi <i>Frontend</i>	193
4.3.12	Pengujian Waktu Respons <i>Refresh Token</i> Algoritma HS256 vs HS512 195	
4.3.13	Pengujian Keamanan Akses Operasi CRUD	196
4.3.14	Pengujian Simulasi Keamanan Sesi Ganda.....	197
4.3.15	Implementasi	202
4.4	Hasil dan Rekomendasi	203
4.4.1	Hasil Penelitian	203
4.4.2	Rekomendasi	204
BAB V PENUTUP.....		206
5.1	Kesimpulan	206
5.2	Saran.....	207
DAFTAR PUSTAKA		210
LAMPIRAN.....		214

DAFTAR GAMBAR

Gambar 2.1 <i>Header, Payload, dan Signature</i> pada JWT (Arvindpdmn, 2022)....	11
Gambar 2.2 Proses <i>Hash</i> Menggunakan SHA-256 (Darmawan et al., 2023).....	12
Gambar 2.3 Proses <i>Refresh Token</i> antara <i>client</i> dan <i>server</i> (GeeksforGeeks, 2024)	13
.....	
Gambar 3.1 Diagram Alir Penelitian	30
Gambar 3.2 Ilustrasi JWT dengan Metode <i>Refresh Token</i>	33
Gambar 3.3 Contoh UI/UX <i>Login</i> dan <i>Logout</i>	35
.....	
Gambar 4.1 Fungsi <i>Hash Token</i>	44
Gambar 4.2 <i>Use Case Diagram</i>	53
Gambar 4.3 <i>Activity Diagram</i> Daftar	56
Gambar 4.4 <i>Activity Diagram</i> Login	57
Gambar 4.5 <i>Activity Diagram</i> JWT	58
Gambar 4.6 <i>Activity Diagram</i> Kegiatan (Mahasiswa)	60
Gambar 4.7 <i>Activity Diagram</i> Prestasi (Mahasiswa)	61
Gambar 4.8 <i>Activity Diagram</i> Organisasi	63
Gambar 4.9 <i>Activity Diagram</i> Sertifikasi Keahlian (Mahasiswa).....	64
Gambar 4.10 <i>Activity Diagram</i> Profil (Mahasiswa)	65
Gambar 4.11 <i>Activity Diagram</i> Verifikasi Dokumen (Verifikator dan Admin) ...	67
Gambar 4.12 <i>Activity Diagram</i> Verifikasi <i>User</i> (Verifikator)	68
Gambar 4.13 <i>Activity Diagram</i> Pengelolaan <i>Token</i>	70
Gambar 4.14 <i>Activity Diagram</i> Pencarian (Tamu dan Mahasiswa).....	71
Gambar 4.15 Skema <i>Database</i>	73
Gambar 4.16 Tabel Pengguna	74
Gambar 4.17 Tabel Peran.....	75
Gambar 4.18 Tabel List.....	76
Gambar 4.19 Tabel <i>Attachments</i>	77
Gambar 4.20 Tabel Prestasi	78
Gambar 4.21 Tabel Kegiatan	79
Gambar 4.22 Tabel Sertifikasi	80
Gambar 4.23 Tabel Organisasi.....	81
Gambar 4.24 Fungsi Pengecekan <i>Request Register</i>	84
Gambar 4.25 Fungsi Pengecekan <i>Existing User</i>	84
Gambar 4.26 Fungsi <i>Hashing Password</i> Dan <i>Store Data</i>	85
Gambar 4.27 Fungsi <i>Store Attachment</i> Dan <i>Success Response</i>	86
Gambar 4.28 Fungsi Pengecekan <i>Request Body</i>	86
Gambar 4.29 Fungsi Pengecekan <i>Existing User</i>	87
Gambar 4.30 Fungsi Pengecekan <i>Password, Decode Token, Store Token, Dan Final Response</i>	88
Gambar 4.31 Integrasi API UPNVJ	89
Gambar 4.32 <i>Store Data</i> Hasil Hit API UPNVJ Ke Sistem.....	89
Gambar 4.33 Fungsi <i>Generate Access Token</i> dan <i>Refresh Token</i>	91
Gambar 4.34 Fungsi Pengecekan dan <i>Decode Token</i>	92
Gambar 4.35 Fungsi Pengecekan <i>Token</i>	92
Gambar 4.36 Fungsi Proses <i>Refresh Token</i>	93

Gambar 4.37 Fungsi <i>Logout</i>	94
Gambar 4.38 Fungsi <i>Middleware JWT</i>	96
Gambar 4.39 Fungsi <i>Scheduling Cron</i>	96
Gambar 4.40 Fungsi Proses Menghapus <i>Token</i>	97
Gambar 4.41 Fungsi Menghapus <i>Token</i> Dengan Paramater <i>Expired</i>	98
Gambar 4.42 Fungsi <i>Router Admin</i>	99
Gambar 4.43 Fungsi <i>Router Verifier (User)</i>	100
Gambar 4.44 Fungsi <i>Router Verifier</i> (Dokumen)	100
Gambar 4.45 Fungsi <i>Router Kegiatan</i>	102
Gambar 4.46 Fungsi <i>Router Prestasi</i>	103
Gambar 4.47 Fungsi <i>Router Organisasi</i>	105
Gambar 4.48 Fungsi <i>Router Sertifikasi</i>	106
Gambar 4.49 Fungsi <i>Router Search</i>	107
Gambar 4.50 Fungsi <i>Router General</i>	108
Gambar 4.51 Fungsi <i>Generate Access Token</i> Dengan <i>Secret Key</i> Dan Algoritma	109
Gambar 4.52 Fungsi <i>Middleware JWT</i> Dengan Verifikasi Dengan Kunci	110
Gambar 4.53 Contoh <i>Response</i> Pada Login Terdapat <i>Expired</i>	111
Gambar 4.54 Fungsi <i>handleClick</i> Untuk Validasi	113
Gambar 4.55 Fungsi <i>Hooks Login</i>	114
Gambar 4.56 Fungsi Ketika <i>Login Success</i> dan <i>Set Tokens</i>	115
Gambar 4.57 Fungsi <i>Redirect After Login</i> dan <i>onError</i>	116
Gambar 4.58 Fungsi <i>handleClick</i> untuk <i>Validasi Form Register</i>	117
Gambar 4.59 Fungsi <i>Convert To FormData</i>	117
Gambar 4.60 Fungsi <i>POST Endpoint Register</i>	118
Gambar 4.61 Fungsi <i>Interceptors Request Axios</i>	119
Gambar 4.62 Fungsi <i>Interceptors Response Axios</i>	119
Gambar 4.63 Fungsi <i>Refresh Stats</i>	121
Gambar 4.64 Fungsi <i>GET Request Aktivitas</i>	122
Gambar 4.65 Fungsi <i>POST Endpoint Aktivitas</i>	123
Gambar 4.66 Fungsi <i>PUT Endpoint Aktivitas</i>	124
Gambar 4.67 Fungsi <i>Hooks DELETE Endpoint Aktivitas</i>	125
Gambar 4.68 Fungsi <i>handleDelete</i> Pada <i>Endpoint DELETE Aktivitas</i>	126
Gambar 4.69 Fungsi <i>GET Endpoint Prestasi</i>	127
Gambar 4.70 Fungsi <i>POST Endpoint Prestasi</i>	128
Gambar 4.71 Fungsi <i>PUT Endpoint Prestasi</i>	129
Gambar 4.72 Fungsi <i>Hooks DELETE Prestasi</i>	130
Gambar 4.73 Fungsi <i>handleDelete</i> pada <i>Endpoint DELETE Prestasi</i>	131
Gambar 4.74 Fungsi <i>GET Endpoint Sertifikasi</i>	132
Gambar 4.75 Fungsi <i>POST Endpoint Sertifikasi</i>	133
Gambar 4.76 Fungsi <i>PUT Endpoint Sertifikasi</i>	134
Gambar 4.77 Fungsi <i>Hooks DELETE Endpoint Sertifikasi</i>	135
Gambar 4.78 Fungsi <i>handleDelete</i> pada <i>Endpoint Sertifikasi</i>	136
Gambar 4.79 Fungsi <i>GET Endpoint Organisasi</i>	137
Gambar 4.80 Fungsi <i>POST Endpoint Organisasi</i>	138
Gambar 4.81 Fungsi <i>PUT Endpoint Organisasi</i>	139
Gambar 4.82 Fungsi <i>Hooks DELETE Endpoint Organisasi</i>	140
Gambar 4.83 Fungsi <i>handleDelete</i> pada <i>Endpoint Organisasi</i>	140

Gambar 4.84 Fungsi GET <i>Endpoint Search</i>	141
Gambar 4.85 Fungsi POST <i>Endpoint Profil</i>	142
Gambar 4.86 Fungsi POST <i>Endpoint Profil</i>	144
Gambar 4.87 Fungsi <i>Generate QR Code</i>	145
Gambar 4.88 Fungsi <i>Save Dan Share PDF</i>	145
Gambar 4.89 Fungsi GET <i>Endpoint User Aktif (Admin)</i>	146
Gambar 4.90 Fungsi <i>Hooks PUT Endpoint Reject User</i>	146
Gambar 4.91 Fungsi <i>handleReject pada PUT Endpoint Reject User</i>	147
Gambar 4.92 Fungsi GET <i>Endpoint User Not Verified (Verifikator)</i>	148
Gambar 4.93 Fungsi <i>Hooks PUT Endpoint Verifikasi User (Verifikator)</i>	149
Gambar 4.94 Fungsi <i>handleVerify pada PUT Endpoint Verifikasi User</i>	149
Gambar 4.95 Fungsi <i>Hooks PUT Endpoint Reject User (Verifikator)</i>	150
Gambar 4.96 Fungsi <i>handleReject pada PUT Endpoint Reject User (Verifikator)</i>	150
Gambar 4.97 Fungsi GET <i>Endpoint Documents Not Verified</i> dan Parameter <i>Type</i>	151
Gambar 4.98 Fungsi <i>handleVerify pada PUT Endpoint Verifikasi User (Verifikator)</i>	152
Gambar 4.99 Fungsi <i>handleReject pada PUT Endpoint Reject Document (Verifikator)</i>	153
Gambar 4.100 Halaman <i>Onboarding</i>	154
Gambar 4.101 Halaman <i>Login</i>	155
Gambar 4.102 Halaman <i>Daftar</i>	156
Gambar 4.103 Halaman <i>Utama Mahasiswa</i>	157
Gambar 4.104 Halaman <i>Utama Admin</i>	158
Gambar 4.105 Halaman <i>Utama Verifikator</i>	159
Gambar 4.106 Halaman <i>Melihat Data Kegiatan Mahasiswa</i>	160
Gambar 4.107 Halaman <i>Tambah Data Kegiatan Mahasiswa</i>	161
Gambar 4.108 Halaman <i>Edit Data Kegiatan Mahasiswa</i>	162
Gambar 4.109 <i>Modal Konfirmasi Hapus Data Kegiatan Mahasiswa</i>	163
Gambar 4.110 Halaman <i>Melihat Data Prestasi Mahasiswa</i>	165
Gambar 4.111 Halaman <i>Tambah Data Prestasi Mahasiswa</i>	166
Gambar 4.112 Halaman <i>Edit Data Prestasi Mahasiswa</i>	167
Gambar 4.113 <i>Modal Konfirmasi Hapus Data Prestasi Mahasiswa</i>	168
Gambar 4.114 Halaman <i>Melihat Data Organisasi Mahasiswa</i>	169
Gambar 4.115 Halaman <i>Tambah Data Organisasi Mahasiswa</i>	170
Gambar 4.116 Halaman <i>Edit Data Prestasi Mahasiswa</i>	171
Gambar 4.117 <i>Modal Konfirmasi Hapus Data Organisasi Mahasiswa</i>	172
Gambar 4.118 Halaman <i>Melihat Data Sertifikasi Mahasiswa</i>	174
Gambar 4.119 Halaman <i>Tambah Data Sertifikat Mahasiswa</i>	175
Gambar 4.120 Halaman <i>Edit Sertifikat Mahasiswa</i>	176
Gambar 4.121 <i>Modal Konfirmasi Hapus Data Sertifikat Mahasiswa</i>	177
Gambar 4.122 Halaman <i>Search, Portfolio Digital, dan Verifikasi CV ATS</i>	178
Gambar 4.123 Halaman <i>Melihat Data Profil Mahasiswa</i>	179
Gambar 4.124 Halaman <i>Mengubah Data Profil Mahasiswa</i>	180
Gambar 4.125 Halaman <i>Melihat Data Portofolio Digital Mahasiswa</i>	181
Gambar 4.126 <i>Hasil Konversi Portofolio Digital Ke PDF</i>	182
Gambar 4.127 Halaman <i>Pengelolaan Token (Admin)</i>	183

Gambar 4.128 Modal Konfirmasi Hapus <i>Session User</i>	184
Gambar 4.129 Halaman Melihat Data Verifikasi Dokoumen, Modal Konfirmasi Verifikasi Dokumen, dan Modal Konfirmasi Tolak Verifikasi Dokumen	185
Gambar 4.130 Halaman Detail Kegiatan	186
Gambar 4.131 Halaman Melihat Data Verifikasi <i>User</i> , Modal Konfirmasi Verifikasi User, dan Modal Konfirmasi Tolak Verifikasi User	187
Gambar 4.132 Halaman Detail Verifikasi User	188
Gambar 4.133 Topologi Simulasi Sesi Ganda	198
Gambar 4.134 Tampilan Login Ponsel Pixel 5	199
Gambar 4.135 <i>Console Response</i> Hasil Login.....	199
Gambar 4.136 <i>Row</i> Hasil Login Di <i>Database</i>	199
Gambar 4.137 Tampilan Utama Pada Ponsel Pixel 5	200
Gambar 4.138 Tampilan Login Pada Ponsel Poco F4	201
Gambar 4.139 <i>Console</i> Keterangan Revoke Sesi Di Ponsel Pixel 5.....	201
Gambar 4.140 Row atau Sesi Baru Terbuat Di Ponsel Poco F4.....	201
Gambar 4.141 <i>Console Response</i> Mendapatkan Token Baru Hasil Login Di Poco F4	202
Gambar 4.142 <i>Console Response</i> Aplikasi Ketika <i>Token Expired</i>	202
Gambar 4.143 <i>Console</i> Bahwa <i>Token</i> Sudah Dicabut	202
Gambar 4.144 Pengecekan Ketika Sesi Login Sudah Dicabut	202

DAFTAR TABEL

Tabel 2.2 Simbol-simbol pada <i>Use Case Diagram</i> (Intern, 2024)	18
Tabel 2.3 Simbol-simbol pada <i>Activity Diagram</i> (Intern, 2021b)	19
Tabel 2.1 Penelitian Terdahulu	23
Tabel 3.1 Spesifikasi Perangkat Keras Laptop	38
Tabel 3.2 Spesifikasi Perangkat Keras <i>Smartphone</i>	38
Tabel 3.3 Spesifikasi Perangkat Lunak	39
Tabel 3.4 Jadwal Penelitian.....	40
Tabel 4.1 <i>Product Backlog</i>	47
Tabel 4.2 Iterasi 1	49
Tabel 4.3 Iterasi 2.....	50
Tabel 4.4 Iterasi 3.....	50
Tabel 4.5 Iterasi 4.....	51
Tabel 4.6 Konfigurasi Teknis Backend Service.....	83
Tabel 4.7 Konfigurasi Teknis <i>Frontend</i>	112
Tabel 4.8 Pengujian Aplikasi <i>Backend</i>	189
Tabel 4.9 Pengujian Aplikasi <i>Frontend</i>	193
Tabel 4.10 Perbandingan Waktu Respons <i>Refresh Token</i> HS256 vs HS512.....	195
Tabel 4.11 Hasil Pengujian Skenario Keamanan Akses	196
Tabel 4.12 Tabel Spesifikasi Minimum	203

DAFTAR LAMPIRAN

- Lampiran 1. Pertanyaan Wawancara
- Lampiran 2. Transkrip Wawancara
- Lampiran 3. Dokumentasi Wawancara
- Lampiran 4. Surat Permohonan Riset Mahasiswa
- Lampiran 5. Surat Permintaan Data
- Lampiran 6. Pakta Integritas
- Lampiran 7. *Schema Database* PRESMA UPNVJ
- Lampiran 8. Dokumentasi Foto bersama Narasumber, Bapak Asep Saeful Ridwan, S.Kom (Kepala UPA TIK UPNVJ)
- Lampiran 9. Dokumentasi *Console* Pengujian Waktu Respons *Refresh Token* HS256
- Lampiran 10. Dokumentasi *Console* Pengujian Waktu Respons *Refresh Token* HS256
- Lampiran 11. Repository Github *Frontend*
- Lampiran 12. Repository Github *Backend*
- Lampiran 13. *Output* Pengujian Keamanan Akses Operasi CRUD (Nomor 1)
- Lampiran 14. *Output* Pengujian Keamanan Akses Operasi CRUD (Nomor 2)
- Lampiran 15. *Output* Pengujian Keamanan Akses Operasi CRUD (Nomor 3)
- Lampiran 16. *Output* Pengujian Keamanan Akses Operasi CRUD (Nomor 4)
- Lampiran 17. Hasil Turnitin
- Lampiran 17. Daftar Riwayat Hidup