

DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN	xii
INTISARI.....	xiii
<i>ABSTRACT</i>	xiv
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	5
C. Batasan Masalah	5
D. Tujuan Penelitian	6
E. Manfaat Penelitian	6
BAB II TINJAUAN PUSTAKA.....	7
A. Landasan Teori.....	7
B. Penelitian Sebelumnya.....	15
BAB III METODE PENELITIAN.....	21
A. Tempat dan Waktu Penelitian.....	21
B. Metode Pengumpulan Data.....	21
C. Alat dan Bahan Penelitian.....	23
D. Konsep Penelitian	24
BAB IV HASIL DAN PEMBAHASAN	32
A. Gambaran Sistem	32
B. Perancangan Sistem	33

C. Implementasi.....	43
D. Pengujian.....	56
BAB V PENUTUP.....	78
A. Kesimpulan	78
B. Saran	78

DAFTAR PUSTAKA

LAMPIRAN



DAFTAR TABEL

Tabel 2.1 Penelitian Sebelumnya	18
Tabel 4.1 Daftar <i>Endpoint</i>	33
Tabel 4.2 Hasil uji kerentanan <i>Broken Object Level Authorization</i>	58
Tabel 4.3 Hasil uji kerentanan <i>Broken Authentication</i>	60
Tabel 4.4 Hasil uji kerentanan <i>Broken Object Property Level Authorization</i>	62
Tabel 4.5 Hasil uji kerentanan <i>Unrestricted Resource Consumption</i>	64
Tabel 4.6 Hasil uji kerentanan <i>Broken Function Level Authorization</i>	66
Tabel 4.7 Hasil uji kerentanan <i>Unrestricted Access to Sensitive Business Flows</i>	68
Tabel 4.8 Hasil uji kerentanan <i>Server-Side Request Forgery</i>	70
Tabel 4.9 Hasil uji kerentanan <i>Security Misconfiguration</i>	72
Tabel 4.10 Hasil uji kerentanan <i>Improper Inventory Management</i>	74
Tabel 4.11 Hasil uji kerentanan <i>Unsafe Consumption of APIs</i>	76
Tabel 4.12 Rekapitulasi hasil pengujian	77

DAFTAR GAMBAR

Gambar 1.1 Statistik kerentanan REST API pada Organisasi (2024-2025).	1
Gambar 2.1 Alur REST.....	8
Gambar 2.2 OWASP Foundation.....	12
Gambar 2.3 <i>Gray-box testing</i>	14
Gambar 3.1 Alur Penelitian.....	24
Gambar 3.2 <i>Gray-box testing</i>	30
Gambar 4.1 Arsitektur sistem	32
Gambar 4.2 Struktur JSON Web Token	39
Gambar 4.3 Alur Bcrypt.....	41
Gambar 4.4 Alur <i>Rate Limiting</i>	42
Gambar 4.5 Alur proses <i>Middleware</i>	43
Gambar 4.6 Kode <i>endpoint</i> POST/register	44
Gambar 4.7 Kode <i>endpoint</i> POST/login	45
Gambar 4.8 Kode <i>endpoint</i> GET /users	46
Gambar 4.9 Kode <i>endpoint</i> GET users/{id}	47
Gambar 4.10 Kode <i>endpoint</i> DELETE users/{id}	47
Gambar 4.11 Kode <i>endpoint</i> POST /notes.....	48
Gambar 4.12 Kode <i>endpoint</i> PUT /notes/{id}	49
Gambar 4.13 Kode <i>endpoint</i> GET notes/{id}	50
Gambar 4.14 Kode <i>endpoint</i> DELETE notes/{id}.....	51
Gambar 4.15 Kode <i>endpoint</i> GET /me	51
Gambar 4.16 Kode <i>endpoint</i> POST /refresh	52
Gambar 4.17 Kode <i>endpoint</i> POST /fetch-url.....	53
Gambar 4.18 Kode fungsi Validasi JWT	54
Gambar 4.19 Kode fungsi <i>Middleware</i>	55
Gambar 4.20 Daftar <i>endpoint</i> pada SwaggerUI.....	56
Gambar 4.21 Hasil uji akses tidak sah terhadap /users/6 oleh User B.....	58
Gambar 4.22 Hasil uji akses <i>endpoint</i> /me dengan token <i>invalid</i>	60
Gambar 4.23 Hasil uji memperbarui isi notes.....	62

Gambar 4.24 Hasil uji Fetch-url API	64
Gambar 4.25 Hasil uji akses <i>endpoint</i> khusus admin dengan token user biasa	66
Gambar 4.26 Hasil uji spam POST /register.....	68
Gambar 4.27 Hasil uji fetch URL umum untuk <i>baseline</i>	70
Gambar 4.28 Hasil uji akses <i>endpoint</i> tidak dikenal /.env	72
Gambar 4.29 Hasil scan otomatis <i>endpoint</i> menggunakan ZAP	74
Gambar 4.30 Hasil uji XSS pada URL simulasi	76



DAFTAR LAMPIRAN

Lampiran 1. Dokumentasi Proses Pengujian

Lampiran 2. Dokumentasi Isi *Database* Users

Lampiran 3. Kartu Bimbingan Skripsi Pembimbing 1

Lampiran 4. Kartu Bimbingan Skripsi Pembimbing 2

