

DAFTAR ISI

| | |
|---|-------------------------------------|
| LEMBAR PENGESAHAN TUGAS AKHIR..... | Error! Bookmark not defined. |
| PENGESAHAN PENGUJI SIDANG TUGAS AKHIR..... | Error! Bookmark not defined. |
| LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR..... | Error! Bookmark not defined. |
| ABSTRACT..... | iii |
| ABSTRAK..... | v |
| MOTTO DAN PERSEMBAHAN..... | vi |
| KATA PENGANTAR..... | vii |
| DAFTAR ISI..... | ix |
| DAFTAR GAMBAR..... | xiii |
| DAFTAR TABEL..... | xv |
| DAFTAR LAMPIRAN..... | xvii |
| DAFTAR PSEUDOCODE..... | xviii |
| BAB I PENDAHULUAN..... | I-1 |
| 1.1 Latar Belakang..... | I-1 |
| 1.2 Rumusan Masalah..... | I-6 |
| 1.3 Tujuan Penelitian..... | I-6 |
| 1.4 Manfaat Penelitian..... | I-7 |
| 1.5 Batasan Masalah..... | I-7 |

| | |
|--|-------|
| BAB II LANDASAN TEORI | II-1 |
| 2.1 Keamanan Aplikasi Web | II-1 |
| 2.2 <i>Penetration Testing</i> | II-2 |
| 2.3 <i>SQL Injection</i> | II-3 |
| 2.4 <i>Blind SQL Injection</i> | II-6 |
| 2.4.1 <i>Time Based blind SQL Injection</i> | II-7 |
| 2.5 <i>Penetration Testing Execution Standard (PTES)</i> | II-8 |
| 2.6 Algoritma Pencarian | II-9 |
| 2.6.1 <i>Algoritma Linear Search</i> | II-9 |
| 2.6.2 <i>Algoritma Binary Search</i> | II-11 |
| 2.6.3 <i>Algoritma Ternary search</i> | II-13 |
| 2.7 <i>Database</i> | II-16 |
| 2.8 <i>State of the art</i> | II-17 |
| BAB III METODOLOGI PENELITIAN..... | III-1 |
| 3.1 Tahapan Penelitian..... | III-1 |
| 3.1.1 <i>Studi Literatur</i> | III-2 |
| 3.2 <i>Penetration Testing Execution Standard (PTES)</i> | III-2 |
| 3.2.1 <i>Pre-engagement interaction</i> | III-2 |
| 3.2.2 <i>Information Gathering</i> | III-3 |
| 3.2.3 <i>Vulnerability Analysis</i> | III-4 |

| | |
|---|-------|
| 3.2.4 <i>Exploitation</i> | III-5 |
| 3.2.5 <i>Post Exploitation</i> | III-5 |
| 3.3 Penyusunan Kesimpulan & Saran | III-6 |
| BAB IV HASIL DAN PEMBAHASAN..... | IV-1 |
| 4.1 <i>Pre-engagement interaction</i> | IV-1 |
| 4.1.1 Perizinan dan Persetujuan..... | IV-1 |
| 4.1.2 Perangkat Lunak dan Perangkat Keras | IV-3 |
| 4.1.3 Etika dan batasan teknis..... | IV-4 |
| 4.2 <i>Information Gathering</i> | IV-5 |
| 4.2.1 <i>Scanning IP Address Web Target</i> | IV-6 |
| 4.2.2 <i>Scanning Informasi menggunakan WHOIS</i> | IV-7 |
| 4.2.3 <i>Port Scanning menggunakan NMAP</i> | IV-9 |
| 4.3 <i>Vulnerability Analysis</i> | IV-11 |
| 4.4 <i>Exploitation</i> | IV-16 |
| 4.4.1 Inisialisasi dan Konfigurasi | IV-17 |
| 4.4.2 Implementasi Eksploitasi..... | IV-21 |
| 4.4.3 Eksekusi dan analisis hasil..... | IV-33 |
| 4.4.4 Mekanisme Eksekusi Otomatisasi Eksploitasi | IV-34 |
| 4.4.5 Hasil eksploitasi..... | IV-37 |

| | |
|---|-------|
| 4.4.6 Konsep Otomatisasi Ekstraksi Karakter pada <i>Time-Based Blind SQLi</i> | IV-43 |
| 4.5 <i>Post Exploitation</i> | IV-46 |
| 4.5.1 Hasil Eksperimen Seluruh Algoritma Pencarian | IV-47 |
| 4.5.2 Hasil Analisis Performa Algoritma | IV-57 |
| 4.6 Rekomendasi Mitigasi <i>Time Based Blind SQL Injection</i> | IV-62 |
| 4.6.1 Penerapan <i>Parameterized Query</i> atau <i>Prepared Statements</i> | IV-63 |
| 4.6.2 Validasi dan sanitasi input..... | IV-64 |
| 4.6.3 Melakukan Monitoring dan Pemindaian kerentanan | IV-65 |
| BAB V KESIMPULAN DAN SARAN..... | V-1 |
| 5.1 Kesimpulan..... | V-1 |
| 5.2 Saran | V-2 |
| DAFTAR PUSTAKA | 1 |
| LAMPIRAN..... | L-1 |