

DAFTAR ISI

| | |
|--|-----------|
| LEMBAR PENGESAHAN | i |
| LEMBAR PERNYATAAN ORISINALITAS | ii |
| ABSTRAK | iii |
| ABSTRACT | iv |
| Kata Pengantar | v |
| Daftar Isi..... | vi |
| Daftar Gambar..... | ix |
| Daftar Tabel | x |
| Daftar Lampiran | xi |
| Daftar ISTILAH..... | xii |
| BAB I PENDAHULUAN..... | 14 |
| I.1 Latar Belakang..... | 14 |
| I.2 Perumusan Masalah..... | 15 |
| I.3 Tujuan Penelitian..... | 15 |
| I.4 Batasan Penelitian | 16 |
| I.5 Manfaat Penelitian..... | 16 |
| BAB II TINJAUAN PUSTAKA | 17 |
| <i>II.1 Security Hardening.....</i> | <i>17</i> |
| <i>II.2 Vulnerability</i> | <i>18</i> |
| <i>II.3 Penetration testing.....</i> | <i>19</i> |
| <i>II.4 Information security</i> | <i>20</i> |
| <i>II.4.1 Asset</i> | <i>20</i> |
| <i>II.4.2 Vulnerabilities</i> | <i>20</i> |
| <i>II.4.3 Risks</i> | <i>20</i> |

| | | |
|---------|---|----|
| II.4.4 | <i>Security Objectives</i> | 20 |
| II.4.5 | <i>Threats</i> | 21 |
| II.4.6 | <i>Countermeasures</i> | 21 |
| II.5 | <i>OWASP</i> | 21 |
| II.6 | Penelitian Sebelumnya | 22 |
| BAB III | Metodologi Penelitian..... | 25 |
| III.1 | Pengembangan Model Konseptual | 25 |
| III.2 | Sistematika Penyelesaian Masalah | 26 |
| III.2.1 | Perumusan Masalah | 27 |
| III.2.2 | Tahap <i>Access</i> | 27 |
| III.2.3 | Tahap <i>Analyze</i> | 27 |
| III.2.4 | Tahap <i>Remediate</i> | 27 |
| III.2.5 | Tahap <i>Manage</i> | 28 |
| III.2.6 | Tahap Akhir | 28 |
| III.3 | Alasan Pemilihan Metode..... | 28 |
| BAB IV | Analisis dan Perancangan | 29 |
| IV.1 | Perencanaan Sistem | 29 |
| IV.1.1 | <i>Hardware</i> | 29 |
| IV.1.2 | <i>Software</i> | 30 |
| IV.1.3 | Topologi..... | 33 |
| IV.2 | Skenario Pengujian..... | 34 |
| IV.2.1 | Skenario Pengujian <i>Scanning Tools</i> | 34 |
| IV.2.2 | Skenario Penetration testing Menggunakan <i>Penetration Tool</i> Metasploit dan Wireshark..... | 36 |
| IV.2.3 | Skenario Penetration testing Menggunakan <i>Penetration Tool</i> Metasploit | 38 |

| | |
|--|----|
| IV.2.4 Skenario Penetration testing Menggunakan <i>Penetration Tool</i> Burpsuite..... | 39 |
| IV.2.5 Skenario Penetration testing Menggunakan <i>Penetration Tool</i> Sqlmap..... | 40 |
| BAB V Implementasi dan Pengujian | 42 |
| V.1 Analisis Hasil <i>Vulnerability Scanning</i> | 42 |
| V.1.1 Analisis <i>Vulnerability</i> Berdasarkan Data dari Nessus | 42 |
| V.1.2 Analisis <i>Vulnerability</i> Berdasarkan Data dari Arachni..... | 48 |
| V.1.3 Analisis <i>Vulnerability</i> Berdasarkan Data dari Acunetix Web Vulnerability Scanner | 50 |
| V.1.4 Analisis <i>Vulnerability</i> Berdasarkan Data dari Nikto | 54 |
| V.2 Analisis Hasil <i>Penetration Testing</i> | 55 |
| V.2.1 Hasil Pengujian Eksploitasi DoS | 55 |
| V.2.2 Hasil Pengujian Eksploitasi Drupalgeddon | 58 |
| V.2.3 Hasil Pengujian <i>Penetration Testing Interception</i> | 59 |
| V.2.4 Hasil Pengujian <i>Penetration Testing SQL Injection</i> | 60 |
| V.3 Rekomendasi Pengamanan..... | 62 |
| V.3.1 <i>High Risk</i> | 62 |
| V.3.2 <i>Medium Risk</i> | 63 |
| V.3.3 <i>Low Risk</i> | 64 |
| BAB VI Kesimpulan dan Saran | 65 |
| VI.1 Kesimpulan | 65 |
| VI.2 Saran | 66 |
| Daftar Pustaka | 67 |
| LAMPIRAN | 69 |