

DAFTAR ISI

PERNYATAAN KEASLIAN LAPORAN TESIS	i
PERSETUJUAN TESIS	ii
PENGESAHAN TESIS.....	iii
KATA PENGANTAR.....	iv
Abstrak.....	v
<i>Abstract</i>	vi
DAFTAR ISI.....	vii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xiii
DAFTAR GRAFIK.....	xvi
1. BAB I. PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Identifikasi Masalah.....	7
1.3. Rumusan Masalah.....	8
1.4. Batasan Masalah	9
1.5. Tujuan Penelitian	10
1.6. Manfaat Penelitian	10
1.7. Sistematika Penulisan	11
2. BAB II. LANDASAN TEORI	13
2.1. Penelitian Sebelumnya.....	13
2.1.1. <i>Research Trend</i> Terkait Deteksi dan Mitigasi <i>Cyber Attack</i>	25
2.1.2. Formulasi, Urgensi, dan Kebaruan Penelitian	26
2.2. Keamanan Siber (<i>Cyber Security</i>)	28
2.3. Ancaman Siber (<i>Cyber Threats</i>)	28
2.3.1. Jenis-Jenis Ancaman Siber	29
2.3.1.1. Serangan Siber (<i>Cyber Attack</i>).....	29
2.3.1.2. Kejahatan Siber (<i>Cyber Crime</i>)	30
2.3.1.3. Terorisme Siber (<i>Cyber Terrorism</i>)	30
2.3.2. Teknik Serangan Siber	31
2.3.2.1. <i>Cross-Site Scripting (XSS)</i>	31

2.3.2.2.	<i>SQL Injection</i>	32
2.3.2.3.	<i>Remote Code Execution (RCE)</i>	32
2.4.	Celah Keamanan Berdasarkan OWASP	33
2.4.1.	<i>Broken Access Control</i>	33
2.4.2.	<i>Cryptographic Failures</i>	33
2.4.3.	<i>Injection</i>	34
2.4.4.	<i>Insecure Design</i>	34
2.4.5.	<i>Security Misconfiguration</i>	34
2.4.6.	<i>Vulnerable and Outdated Components</i>	35
2.4.7.	<i>Identification and Authentication Failures</i>	35
2.4.8.	<i>Software and Data Integrity Failures</i>	35
2.4.9.	<i>Security Logging and Monitoring Failures</i>	36
2.4.10.	<i>Server-Side Request Forgery (SSRF)</i>	36
2.5.	Pemetaan Serangan dan Celah Keamanan OWASP Top-10	36
2.6.	Deteksi Serangan Siber	38
2.7.	Pembelajaran Mesin (<i>Machine Learning</i>)	39
2.7.1.	Jenis-Jenis Pembelajaran Mesin	39
2.7.1.1.	<i>Supervised Learning</i>	40
2.7.1.2.	<i>Unsupervised Learning</i>	40
2.7.1.3.	<i>Reinforcement Learning</i>	41
2.7.2.	Pembelajaran Mesin bagi Keamanan Siber	41
2.7.3.	Pemrosesan dan Pengenalan Teks untuk Deteksi Serangan	42
2.7.3.1.	Natural Language Processing Kit (NLTK)	43
2.7.3.2.	<i>Scikit-Learn</i>	43
2.8.	Mitigasi Serangan Siber	43
2.8.1.	Zed Attack Proxy (ZAP).....	46
2.8.2.	Arachni.....	47
2.9.	<i>Multi-Layer Security</i>	47
2.9.1.	OWASP Mod Security Firewall	49
2.9.2.	<i>HTTP Middleware</i>	50
2.9.3.	<i>Template Engine</i>	51
2.9.4.	<i>Data Sanitizer</i>	52
2.9.5.	<i>Framework/CMS Built-In Security</i>	53
2.9.6.	Skenario Implementasi Berdasarkan Karakteristik <i>Website</i>	56

3.	BAB III. METODE PENELITIAN	59
3.1.	Alat dan Bahan Penelitian.....	59
3.1.1.	Alat Penelitian.....	59
3.1.2.	Bahan Penelitian	63
3.2.	Tahapan Penelitian.....	66
3.2.1.	Skema Tahapan Metode Deteksi	66
3.2.2.	Skema Tahapan Metode Mitigasi	71
3.3.	Metode Penelitian	72
3.3.1.	Metode Deteksi	73
3.3.1.1.	Model Deteksi.....	74
3.3.1.2.	<i>Detection Placement</i> (Penempatan Deteksi).....	77
3.3.2.	Metode Mitigasi	78
3.3.2.1.	<i>OWASP Mod Security Firewall</i>	79
3.3.2.2.	<i>HTTP Middleware</i>	79
3.3.2.3.	<i>Template Engine</i>	80
3.3.2.4.	<i>Data Sanitizer</i>	81
3.3.2.5.	<i>CMS/Framework Built-in Security</i>	81
3.3.2.6.	Komparasi Data Mitigasi	81
3.4.	Evaluasi Metode.....	82
3.4.1.	Evaluasi Metode Deteksi	82
3.4.2.	Evaluasi Metode Mitigasi	83
3.5.	<i>Timeline</i> Penelitian.....	83
4.	BAB IV. HASIL PENELITIAN DAN PEMBAHASAN	85
4.1.	Hasil Penelitian	85
4.1.1.	Metode Deteksi Menggunakan <i>Machine Learning</i>	85
4.1.1.1.	Teknik Serangan <i>Cross Site Scripting</i> (XSS)	85
4.1.1.2.	Teknik Serangan <i>SQL Injection</i> (SQLi).....	91
4.1.1.3.	Teknik Serangan <i>Remote Code Execution</i> (RCE)	97
4.1.2.	Metode Mitigasi Menggunakan <i>Multi-Layer Security</i>	103
4.1.2.1.	Teknik Serangan <i>Cross Site Scripting</i> (XSS)	103
4.1.2.2.	Teknik Serangan <i>SQL Injection</i> (SQLi).....	106
4.1.2.3.	Teknik Serangan <i>Remote Code Execution</i> (RCE)	108
4.2.	Analisa Pembahasan	110
4.2.1.	Implementasi Metode Deteksi Menggunakan <i>Machine Learning</i>	110

4.2.1.1.	Teknik Serangan <i>Cross Site Scripting</i> (XSS)	111
4.2.1.2.	Teknik Serangan <i>SQL Injection</i> (SQLi)	147
4.2.1.3.	Teknik Serangan <i>Remote Code Execution</i> (RCE)	179
4.2.2.	Implementasi Metode Mitigasi <i>Multi-Layer Security</i>	208
4.2.2.1.	Teknik Serangan <i>Cross Site Scripting</i> (XSS)	210
4.2.2.2.	Teknik Serangan <i>SQL Injection</i> (SQLi)	221
4.2.2.3.	Teknik Serangan <i>Remote Code Execution</i> (RCE)	229
4.2.3.	Relevansi dan Komparasi dengan Hasil Penelitian Sebelumnya.....	238
4.2.3.1.	Metode Deteksi	238
4.2.3.2.	Metode Mitigasi	241
5.	BAB V. KESIMPULAN DAN SARAN.....	243
5.1.	Simpulan	243
5.1.1.	Tingkat Akurasi Metode Deteksi	243
5.1.2.	Tingkat Efektivitas Metode Mitigasi	245
5.1.3.	Implementasi Metode Deteksi dan Metode Mitigasi	247
5.2.	Saran	248
5.2.1.	Penelitian Selanjutnya.....	248
5.2.2.	Praktisi Keamanan Siber.....	248
5.2.3.	Keterbatasan Penelitian.....	249