

## DAFTAR ISI

	Hal.
<b>HALAMAN JUDUL.....</b>	<b>i</b>
<b>HALAMAN PERSETUJUAN .....</b>	<b>iii</b>
<b>HALAMAN PENGESAHAN .....</b>	<b>iv</b>
<b>HALAMANAN PERSEMBAHAN.....</b>	<b>v</b>
<b>INTISARI .....</b>	<b>vi</b>
<b>KATA PENGANTAR.....</b>	<b>vii</b>
<b>DAFTAR ISI.....</b>	<b>ix</b>
<b>DAFTAR TABEL.....</b>	<b>xiii</b>
<b>DAFTAR GAMBAR .....</b>	<b>xiv</b>
<b>BAB I PENDAHULUAN .....</b>	<b>1</b>
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah .....	3
1.3 Ruang Lingkup.....	3
1.4 Tujuan .....	4
<b>BAB II TINJAUAN PUSTAKA DAN DASAR TEORI .....</b>	<b>5</b>
2.1 Tinjauan Pustaka .....	5
2.2 Dasar Teori.....	5
2.2.1 PHP.....	5

2.2.2 MySQL .....	6
2.2.3 Htmlebrities .....	7
2.2.4 Escapeshellarg .....	7
2.2.5 Brute Force .....	7
2.2.6 SQL Injection .....	8
2.2.7 Cross Site Scripting.....	8
2.2.8 Command Execution .....	8
2.2.9 File Inclusion .....	9
2.2.10 Arbitrary File Upload .....	9
<b>BAB III ANALISIS DAN PERANCANGAN SISTEM .....</b>	<b>10</b>
3.1 Analisis Sistem.....	10
3.1.1 Analisis Kebutuhan Data .....	10
3.1.2 Analisis Kebutuhan Perangkat Lunak .....	11
3.1.3 Analisis Kebutuhan Perangkat Keras .....	11
3.2 Perancangan Sistem .....	11
3.2.1 Arsitektur Sistem.....	11
3.2.2 Flowchart Diagram.....	14
3.2.3 Perancangan Input.....	16

## **BAB VI IMPLEMENTASI DAN PEMBAHASAN**

<b>SISTEM .....</b>	<b>18</b>
4.1 Implementasi Program .....	18
4.1.1 Pengamanan Serangan Brute Force .....	18
4.1.2 Pengamanan Serangan XSS dan SQLi .....	20
4.1.3 Pengamanan Serangan File Inclution .....	21
4.1.4 Pengamanan Serangan Command Execution .....	22
4.1.5 Pengamanan Serangan Arbitrary File Upload .....	22
4.1.6 Penulisan Log .....	24
4.1.7 Report Log .....	24
4.2 Pembahasan dan Pengujian Sistem .....	26
4.2.1 Pengujian Pengaman Celah Brute Force .....	27
4.2.2 Pengujian Pengaman Celah SQL Injection .....	29
4.2.3 Pengujian Pengaman Celah XSS .....	31
4.2.4 Pengujian Pengaman Celah File Inclution .....	33
4.2.5 Pengujian Pengaman Celah Command Exectuion ..	34
4.2.6 Pengujian Pengaman Celah Arbitrary File Upload ..	36
4.2.7 Report Serangan .....	37
<b>BAB V KESIMPULAN DAN SARAN.....</b>	<b>39</b>
5.1 Kesimpulan .....	39

5.2 Saran-saran .....	40
<b>DAFTAR PUSTAKA .....</b>	<b>41</b>
<b>LAMPIRAN :</b>	
• LAMPIRAN 1 : RANCANGAN TABEL .....	42

## DAFTAR TABEL

	<b>Hal.</b>
<b>Tabel 4.1</b> Tabel Pengaturan Modul Pengaman .....	26
<b>Tabel 4.2</b> Tabel Pengujian Brute Force .....	27
<b>Tabel 4.3</b> Tabel Pengujian SQL Injection .....	29
<b>Tabel 4.4</b> Tabel Pengujian XSS .....	31
<b>Tabel 4.5</b> Tabel Pengujian File Inclution .....	33
<b>Tabel 4.6</b> Tabel Pengujian Command Execution .....	35
<b>Tabel 4.7</b> Table Pengujian Arbitrary File Upload .....	36

## DAFTAR GAMBAR

	<b>Hal.</b>
<b>Gambar 3.1</b> Block Diagram .....	12
<b>Gambar 3.2</b> Flowchart Diagram .....	15
<b>Gambar 3.3</b> Input Cheat Sheet .....	16
<b>Gambar 3.4</b> Input Alamat IP .....	16
<b>Gambar 3.5</b> Input Data User .....	16
<b>Gambar 3.6</b> Input Setting Brute Force .....	17
<b>Gambar 4.1</b> Log Pemblokiran IP .....	28
<b>Gambar 4.2</b> Log Serangan <i>SQL Injection</i> .....	31
<b>Gambar 4.3</b> Log Serangan XSS .....	32
<b>Gambar 4.4</b> Log Serangan <i>File Inclusion</i> .....	34
<b>Gambar 4.5</b> Log Serangan <i>Command Execution</i> .....	35
<b>Gambar 4.6</b> Log Serangan Arbitrary File Upload .....	37
<b>Gambar 4.7</b> Contoh Chart Report .....	38
<b>Gambar 4.1.</b> Jumlah Serangan Yang Terjadi .....	38