

KATA PENGANTAR

Puji dan syukur senantiasa penulis panjatkan kehadirat Allah SWT, karena hanya dengan izin dan ridho-Nya penulis dapat menyelesaikan laporan proyek akhir ini dengan baik dan lancar. Tujuan penulisan laporan ini adalah untuk menambah wawasan bagi penulis khususnya tentang **“Pengujian Keamanan JDefender Untuk Menangkal Serangan SQL Injection, Flooding dan PHP Injection pada sebuah Web-site Berbasis Joomla”**, serta sebagai bukti tertulis pembuatan laporan untuk memenuhi syarat kelulusan pada Program Studi Teknik Komputer di Politeknik Telkom.

Pada kesempatan yang baik ini penulis mengucapkan terima kasih kepada Allah SWT yang telah memberikan rahmat dan hidayahnya, sehingga dapat terselesaikannya laporan proyek akhir ini tepat pada waktunya. Yang kedua kepada orang tua yang tak henti-hentinya memberikan semangat serta dukungan, sehingga dapat terselesaikannya laporan akhir ini dengan lancar.

Penulis menyadari bahwa isi yang terkandung dalam laporan ini masih sangat sederhana dan jauh dari kesempurnaan, untuk itu kritik dan saran yang bersifat konstruktif sangatlah penulis harapkan demi kesempurnaan lebih lanjut. Namun demikian penulis berharap semoga yang sederhana ini bermanfaat bagi penulis sendiri khususnya maupun bagi para pembaca pada umumnya. Dan semoga Allah SWT mencatatnya sebagai bagian dari ilmu yang bermanfaat.

Bandung, 16 Oktober 2010

Penulis

DAFTAR ISI

KATA PENGANTAR	i
ABSTRAK	ii
ABSTRACT	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	ix
DAFTAR TABEL	xiii
DAFTAR ISTILAH	xiv
DAFTAR SINGKATAN	xv

BAB I

PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan	2
1.4 Batasan Masalah.	2
1.5 Metodologi Penelitian	3
1.5.1 Studi Literatur	3
1.5.2 Wawancara	3
1.5.3 Pembangunan Model	4
1.5.4 Implementasi	4
1.5.5 Analisis Hasil	5
1.5.6 Pembuatan Laporan	5
1.6 Jadwal Pelaksanaan	6

BAB II

TINJAUAN PUSTAKA	7
2.1 Joomla	7
2.1.1 Karakteristik Joomla	7
2.1.2 Bahasa Pemrograman Yang Digunakan	8
2.1.3 Database Yang Digunakan	9
2.1.4 Web Server Yang Digunakan	10
2.1.5 Aplikasi Untuk Pembuatan Database	11
2.1.6 Kebutuhan Minimum dari Joomla	12
2.1.7 Keuntungan Menggunakan Joomla	13
2.2 JDefender	13
2.3 Konsep Hacking Secara Umum	15
2.4 SQL Injection	15
2.4.1 Pengertian SQL Injection	15
2.4.2 Sebab Terjadinya SQL Injection	16
2.4.3 Celah Kerawanan dari Sebuah Websi-te	16
2.4.4 Karakteristik Teknik Serangan SQL Injection	16
2.5 Macam-Macam Serangan dari SQL Injection	17
2.5.1 Serangan Dengan String ‘ or 1 =1--	17
2.5.2 Mengambil Data Yang Diinginkan	17
2.5.3.Update atau Insert Data	18
2.5.4 Tabel Pola Attack Dari Serangan SQL Injection	19
2.5.5 Menghadapi SQL Injection	26
2.5.5.1 Filtering Data	26
2.5.5.2 Pengamanan Kode SQL Untuk Aplikasi Web	27
2.6 Flooding	28

2.6.1	Pengertian Flooding	28
2.6.2	Contoh Dari Serangan Flooding	28
2.6.2.1	Denial of Service	28
2.6.2.2	Cara Melakukan Serangannya	29
2.6.2.3	Cara Pencegahannya	31
2.7	PHP Injection	33
2.7.1	Pengertian PHP Injection	33
2.7.2	Cara Melakukan Serangannya	33
2.7.3	Cara Pencegahan PHP Injection	39
2.8	REGEX (Regular Expression)	40
2.8.1	Pengertian REGEX	40
2.8.2	Deskripsi REGEX	41
BAB III		
ANALISIS KEBUTUHAN DAN PERANCANGAN		
3.1	Kebutuhan Perangkat Keras	44
3.2	Kebutuhan Perangkat Lunak	45
3.3	Sistem yang Akan Dibuat	46
3.4	Perancangan Sistem	48
3.4.1	Flowchart Dari Sistem	48
3.5	Perancangan Antarmuka	49
3.5.1	Definisi Aktor	50
3.5.2	Definisi Use Case	51
3.6	Konsep Hacking JDefender	52

BAB IV

IMPLEMENTASI DAN PENGUJIAN	53
4.1 Instalasi Joomla Versi 1.0.15.....	53
4.2 Instalasi JDefender Versi 1.6	57
4.3 Instalasi Komponen DS_Syndicate	60
4.4 Implementasi dan Pengujian Keamanan JDefender	61
4.4.1.a Pengujian SQL Injection Pada Form Login	61
4.4.1.b Pengujian SQL Injection Pada Alamat URL	64
4.4.2.a Pengujian Keamanan JDefender Dengan Flooding	71
4.4.2.a.1 Pengujian Dengan Serangan ICMP PING	71
4.4.2.b.1 Pengujian Dengan Serangan NET SEND	75
4.4.3.a Pengujian Keamanan JDefender Dengan PHP Injection	79
4.4.3.a.1 Pengujian Dengan Mencuri Password	79
4.4.3.b.1 Pengujian Dengan Menggunakan /passwd%00.....	82
4.4.3.c.1 Pengujian Dengan Menggunakan /etc/passwd	85
4.5 Pola Pengujian Keamanan JDefender	88
4.5.1 Pengujian Dengan Serangan SQL Injection	88
4.5.2 Pengujian Dengan Serangan Flooding	89
4.5.3 Pengujian Dengan Serangan PHP Injection	90
4.6 Komparasi Keamanan CMS Joomla Dengan Keamanan CMS Lain	91
4.6.1 Fungsi Dari Keamanan Joomla	91
4.6.2 Fungsi Dari Keamanan Drupal	92

BAB V

PENUTUP93

5.1 Kesimpulan93

5.2 Saran93

REFERENSIxvi

DAFTAR GAMBAR

Gambar 2.1.1 Menu Control Panel Joomla.....	8
Gambar 2.1.2 phpinfo() pada XAMPP	9
Gambar 2.1.3 MySQL Database Configuration.....	10
Gambar 2.1.4 XAMPP Control Panel.....	11
Gambar 2.1.5 PHPMyAdmin.....	12
Gambar 2.2 Konfigurasi JDefender	14
Gambar 3.3 Sistem Yang Akan Dibuat.....	47
Gambar 3.4.1 Perancangan Sistem	48
Gambar 3.5 Use-Case Perancangan Antarmuka	49
Gambar 4.1.a Pre-Installation Check	53
Gambar 4.1.b Penjelasan dari GNU/GPL License.....	54
Gambar 4.1.c Konfigurasi Database MySQL	54
Gambar 4.1.d Penamaan Situs Joomla.....	55
Gambar 4.1.e Konfirmasi Site URL, Admin Email dan Password.....	55
Gambar 4.1.f Sukses Instalasi Joomla.....	56
Gambar 4.1.g Back End Joomla.....	56
Gambar 4.1.h Control Panel Joomla	57
Gambar 4.2.a Penginstalan Component	58
Gambar 4.2.b Sukses upload Component	58
Gambar 4.2.c Penginstalan bot atau plugin.....	59

Gambar 4.2.d Sukses upload mambot.....	59
Gambar 4.3.a Instalasi Komponen DS_Syndicate	60
Gambar 4.3.b Komponen DS_Syndicate sukses ter-upload	60
Gambar 4.4.1.a Pesan atau Alert Hasil dari Serangan SQL Injection.....	64
Gambar 4.4.1.b.1 RSS Feed Komponen DS_Synsicate.....	66
Gambar 4.4.1.b.2 Error Menggunakan Tanda Petik Tunggal	66
Gambar 4.4.1.b.3 Error Menggunakan ORDER BY di kolom 1	67
Gambar 4.4.1.b.4 Error Menggunakan ORDER BY di kolom 20	67
Gambar 4.4.1.b.5 Error Menggunakan ORDER BY di kolom 21	67
Gambar 4.4.1.b.6 Munculnya Kolom Ke 2.....	68
Gambar 4.4.1.b.7 Munculnya Versi dari Database MySQL	68
Gambar 4.4.1.b.8. Munculnya Username Administrator	69
Gambar 4.4.1.b.9 Munculnya Username, Password dan Email.....	69
Gambar 4.4.1.b.2.1 Error Ketika Tanda Komentar di plugin dicabut.....	70
Gambar 4.4.2.a.1 Serangan ICMP PING dari Komputer Client.....	71
Gambar 4.4.2.a.2 Web-site dari Komputer Client	72
Gambar 4.4.2.a.3 Bloking dari Web Client.....	72
Gambar 4.4.2.a.4 Bloking dari Web Client setelah di F5	73
Gambar 4.4.2.a.5 Pengaturan Antiflood dari Server	73
Gambar 4.4.2.a.6 IP Address Attacker di Log JDefender.....	74
Gambar 4.4.2.a.7 Bloking IP Address di JDefender	74
Gambar 4.4.2.b.1 Penyerangan NET SEND oleh Client	75

Gambar 4.4.2.b.2 Web-site dari Komputer Client	76
Gambar 4.4.2.b.3 Bloking dari Web Client	76
Gambar 4.4.2.b.4 Bloking dari Web Client setelah di F5	77
Gambar 4.4.2.b.5 Pengaturan Antiflood dari Server.....	77
Gambar 4.4.2.b.6 IP Address Attacker di Log JDefender	78
Gambar 4.4.2.b.7 Bloking IP Address di JDefender.....	78
Gambar 4.4.3.a.1 Sebelum Web-site diserang	79
Gambar 4.4.3.a.2 Bloking Web-site dari Client.....	80
Gambar 4.4.3.a.3 Bloking Web-site dari Client setelah di F5	80
Gambar 4.4.3.a.4 Pengaturan PHP Injection di JDefender	81
Gambar 4.4.3.a.5 Bloking User di JDefender	81
Gambar 4.4.3.b.1 Web-site Sebelum Diserang	82
Gambar 4.4.3.b.2 Blocking Web-site dari Client.....	83
Gambar 4.4.3.b.3 Bloking Web-site setelah di F5	83
Gambar 4.4.3.b.4 Pengaturan PHP Injection di JDefender.....	84
Gambar 4.4.3.b.5 Bloking User di JDefender	84
Gambar 4.4.3.c.1 Web-site Sebelum Diserang	85
Gambar 4.4.3.c.2 Bloking Web-site dari Client.....	86
Gambar 4.4.3.c.3 Bloking Web-site setelah di F5	86
Gambar 4.4.3.c.4 Pengaturan PHP Injection di JDefender	87
Gambar 4.4.3.c.5 Bloking User di JDefender	87
Gambar 4.5.1 Pengujian dengan Serangan SQL Injection.....	88

Gambar 4.5.2 Pengujian dengan Serangan Flooding	89
Gambar 4.5.3 Pengujian dengan Serangan PHP Injection.....	90

DAFTAR TABEL

Tabel 1.6 Jadwal pelaksanaan.....	6
Tabel 2.5.4 Tabel Pola Attack dari Serangan SQL Injection.....	19
Tabel 2.8.2 Tabel Deskripsi REGEX.....	41
Tabel 3.5.1 Definisi Aktor.....	50
Tabel 3.5.2 Definisi Use-Case.....	51
Tabel 4.4.1.a Pengujian Serangan SQL Injection Pada Form Login.....	61
Tabel 4.4.1.b Tabel Penyerangan SQL Injection.....	64
Tabel 4.5.1 Fungsi dari Keamanan Joomla.....	91
Tabel 4.5.2 Fungsi dari Keamanan Drupal.....	92

DAFTAR ISTILAH

<i>Administrator</i>	(Orang yang mempunyai hak akses penuh terhadap suatu sistem).
<i>Client</i>	(Orang yang mempunyai hak akses terbatas terhadap suatu sistem dan <i>client</i> hanya bisa melakukan manipulasi data, apabila diijinkan oleh <i>administator</i> sistem).
<i>Component</i>	(Inti dari program utama suatu <i>tools</i> yang berisi <i>script</i> yang menjalankan sistem dengan jalan saling berkesinambungan dengan <i>plugin</i>).
<i>Cracker</i>	(Orang yang jahat dan selalu memanipulasi <i>sript coding</i> untuk dapat dijadikan alat untuk melakukan tindak kejahatan)
<i>DS_Syndicate</i>	(Komponen dari <i>joomla 1.0.15</i> untuk <i>RSS_FEED</i>).
<i>Flooding</i>	(Membanjiri Komputer korban dengan <i>request</i> paket yang berlebihan dan tiada hentinya, sehingga menyebabkan komputer korban <i>crash</i> atau <i>hang</i>).
<i>JDefender</i>	(Keamanan untuk melindungi suatu <i>web-site</i> dari serangan <i>cracker</i>).
<i>Joomla</i>	(<i>Content Management System</i> sebagai pembuat <i>web-site</i>).
<i>PHP Injection</i>	(Serangan dengan metode menyisipkan <i>script PHP</i> ke dalam alamat <i>URL</i> dan <i>menu</i> navigasi pencarian pada suatu situs atau <i>web-site</i>).
<i>Plugin</i>	(<i>File</i> berisi <i>script</i> yang mempunyai fungsi untuk mengecek setiap parameter yang lewat melalui <i>component</i>).
<i>SQL Injection</i>	(Aksi <i>hacking</i> yang dilakukan di komputer <i>client</i> dengan cara memanipulasi <i>query sql</i> di memori aplikasi <i>client</i> untuk menyerang komputer korban).

DAFTAR SINGKATAN

Com	(Component)
Email Address	(Electronic Mail Address)
JDefender	(Joomla Defender)
Passwd	(Password)
PHP Injection	(Hypertext Processor Injection)
Plg	(Plugin)
PMA	(PHPMyAdmin)
SQL Injection	(Structure Query Language Injection)
URL	(Uniform Resource Locator)