

TUGAS AKHIR

**ANALISA KEAMANAN INFORMASI PADA APLIKASI BERBASIS WEB
MENGUNAKAN TEKNIK WEB APPLICATION FIREWALL
MODSECURITY**



Oleh:

Albi Alamsyah
1210651199

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER

2016

TUGAS AKHIR

ANALISA KEAMANAN INFORMASI PADA APLIKASI BERBASIS WEB MENGUNAKAN TEKNIK WEB APPLICATION FIREWALL MODSECURITY

Disusun Untuk Melengkapi Dan Memenuhi Syarat Kelulusan
Guna Meraih Gelar Sarjana Komputer
Teknik Informatika Universitas Muhammadiyah Jember



Oleh:

Albi Alamsyah
1210651199

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER

2016

HALAMAN PENGESAHAN

ANALISA KEAMANAN INFORMASI PADA APLIKASI BERBASIS WEB MENGUNAKAN TEKNIK WEB APPLICATION FIREWALL MODSECURITY

Oleh:

Albi Alamsyah
1210651199

Telah disetujui bahwa Laporan Tugas Akhir ini untuk diajukan pada sidang Tugas Akhir tanggal sebagai salah satu syarat kelulusan dan mendapatkan gelar Sarjana Komputer (S.Kom) di Universitas Muhammadiyah Jember

Disetujui oleh,

Pembimbing I

Pembimbing II

Triawan Adi Cahyanto, M.Kom
NPK.12 03 719

.....
NPK.....

HALAMAN PENGESAHAN

ANALISA KEAMANAN INFORMASI PADA APLIKASI BERBASIS WEB MENGUNAKAN TEKNIK WEB APPLICATION FIREWALL MODSECURITY

Oleh:

Albi Alamsyah
1210651199

Telah Mempertanggung Jawabkan Laporan Tugas Akhirnya Pada sidang Tugas Akhir tanggal
..... Sebagai Salah Satu
Syarat Kelulusan dan Mendapatkan Gelar Sarjana Komputer (S.Kom)
di
Universitas Muhammadiyah Jember

Disetujui oleh,

Dosen Penguji :
Penguji I

Dosen Pembimbing :
Pembimbing I

Daryanto, M.Kom
NPK.11 03 589
Penguji II

Triawan Adi Cahyanto, M.Kom
NPK.12 03 719
Pembimbing II

Deni Arifianto, M.Kom
NPK. 11 03 588
Mengesahkan,
Dekan Fakultas Teknik

.....
NPK.....
Mengetahui,
Ketua Program Studi Teknik Informatika

Ir. Suhartinah, MT
NPK. 95 05 246

Yeni Dwi Rahayu, M.Kom
NPK.11 03 590

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Albi Alamsyah

Nim : 1210651199

Tempat Tanggal Lahir : Jember, 25-09-1994

Alamat : Dusun Tegal Banteng RT 006/RW 005 Kesilir Wuluhan Jember

Dengan ini menyatakan bahwa Skripsi dengan judul: “ANALISA KEAMANAN INFORMASI PADA APLIKASI BERBASIS WEB MENGGUNAKAN TEKNIK WEB APPLICATION FIREWALL MODSECURITY” adalah hasil pekerjaan saya dan seluruh ide, pendapat, atau materi dari sumber lain telah dikutip dengan cara penulisan referensi yang sesuai.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa ada tekanan dan paksaan dari pihak mana pun serta bersedia mendapatkan sanksi akademik jika ternyata di kemudian pernyataan ini tidak benar

Jember, Juni 2016

Yang menyatakan,

Albi Alamsyah
NIM 1210651199

KATA PENGANTAR

Puji dan syukur kehadiran Allah SWT atas berkat rahmat serta kasih-Nya sehingga penulis dapat menyelesaikan Proposal tugas akhir ini yang berjudul “ANALISA KEAMANAN INFORMASI PADA APLIKASI BERBASIS WEB MENGGUNAKAN TEKNIK WEB APPLICATION FIREWALL MODSECURITY”.

Penyusunan laporan proposal tugas akhir ini untuk memenuhi sebahagian syarat memperoleh gelar Sarjana Komputer (S.Kom).

Ucapan terima kasih kepada pihak-pihak yang telah membantu penulis, selama penyusunan laporan proposal tugas akhir ini diantaranya:

1. Ibu Ir Suhartinah, MT selaku Dekan Fakultas Teknik Universitas Muhammadiyah Jember.
2. Ibu Yeni Dwi Rahayu, M.Kom selaku Kaprodi Teknik Informatika Universitas Muhammadiyah Jember.
3. Bapak Triawan Adi Cahyanto, M.Kom selaku Dosen Pembimbing laporan tugas akhir ini yang telah memberikan bimbingan dan pengarahan sehingga laporan tugas akhir ini bisa selesai.
4. Para Dosen Penguji yang telah memberikan arahan dalam penyusunan laporan tugas akhir ini.
5. Para Dosen Fakultas Teknik Universitas Muhammadiyah Jember, terima kasih semua ilmu yang telah diberikan
6. Terima kasih juga kepada semua pihak yang telah membantu dalam penyelesaian tugas akhir ini yang tidak dapat disebutkan satu per satu.

Akhir kata penulis mengucapkan terimakasih kepada semua pihak yang telah membantu dan penulis berharap semoga skripsi ini dapat bermanfaat bagi kita semua dan menjadi bahan masukan.

Jember, 14 Januari 2016

Penulis,

DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN KEASLIAN.....	v
ABSTRAK.....	vi
ABSTRACT	vii
KATA PENGANTAR.....	ix
DAFTAR ISI	xi
DAFTAR GAMBAR.....	
DAFTAR TABEL.....	
BAB 1. PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
BAB 2. TINJAUAN PUSTAKA.....	5
2.1 Keamanan Informasi	4
2.2 Keamanan Web.....	5
2.3 Apikasi web dan keamanan aplikasi web	5
2.3.1 Aplikasi Web.....	5
2.3.2 Keamanan aplikasi web	7
2.4 Celah keamanan.....	7
2.4.1 Celah keamanan pada aplikasi web	8
2.5 Identifikasi jenis serangan pada aplikasi web.....	9
2.5.1 SQL Injections.....	10
2.5.2 Cros Site Scripting	11
2.5.3 Remote file Inclusions.....	13

2.6 Firewall	15
2.6.1 Fungsi Firewall	16
2.6.2 Serangan	16
2.7 Linux	17
2.8 Metode Pengamanan	21
2.8.1 Fitur WAF	21
2.8.2 Modsecurity	21
2.8.2.1 Fitur Modsecurtu	22
2.8.2.2 OWASP Modsecurity	22
2.6 BAB 3. METODE PENELITIAN	23
3.1 Studi Literatur	23
3.2 Analisis Kebutuhan sistem	24
3.2.1 Analisis Perangkat Keras	24
3.2.2 Analisis Perangkat Lunak	24
3.3 Desain Infrastruktur	25
3.4 Pengujian Serangan	26
3.5 Analisa	27
3.5.1 Analisa Uji coba serangan	27
BAB 4. IMPLEMENTASI DAN PENGUJIAN	29
4.1 Implementasi Modsecurtu	29
4.2 Pengujian	29
4.2.1 Pengujian SQL Injections	29
4.2.2 Pengujian Cros Site Sciptions	31
4.2.3 Pengujian Remote File Inclusion	32
BAB 5. KESIMPULAN DAN PENUTUP	34
5.1 Kesimpulan	34
5.2 Penutup	34
DAFTAR PUSTAKA	35
LAMPIRAN	
AUTOBIOGRAFI PENULIS	

DAFTAR GAMBAR

Gambar	Judul	Halaman
2.1	Contoh <i>Web</i> Tradisional yang Hanya Berisi Informasi Statis	6
2.2	Arsitektur Sederhana 3 tier.....	10
2.3	Contoh Kode PHP.....	11
2.4	Contoh Halaman Terinfeksi	12
2.5	ilustrasi firewall.....	15
2.6	Bagan Firewall	16
3.1	Desain dengan <i>WAF Modesecurity</i>	25
3.2	Desain Web server tanpa <i>WAF Modesecurity</i>	26
4.1	Serangan SQL Injection 1 dengan <i>WAF</i>	30
4.2	mengubah Rule /deteksi serangan.....	30
4.3	Serangan SQL Injection 2 tanpa <i>WAF</i>	31
4.4	Serangan SQL Injection 2 dengan <i>WAF</i>	31
4.5	Serangan XSS tanpa <i>WAF</i>	32
4.6	Serangan XSS dengan <i>WAF</i>	32
4.7	Serangan RFI 1 tanpa <i>WAF</i>	33
4.8	Serangan RFI 1 dengan <i>WAF</i>	33
4.9	Serangan RFI 2 tanpa <i>WAF</i>	33
4.10	Serangan RFI 2 dengan <i>WAF</i>	33

DAFTAR TABEL

Tabel	Judul	Halaman
2.1	WHID top 10 attacks methods	9
3.1	Spesifikasi Perangkat Keras	24

DAFTAR PUSTAKA

- Ahmad Muammar. W. K.2004. *FireWall*. Ilmukomputer.com
- Ande. 2011. Local File Inclusion (LFI). [https://evilzone.org/tutorials/localfile-inclusion-\(lfi\)](https://evilzone.org/tutorials/localfile-inclusion-(lfi)). (02 April 2016)
- Chan, Y.B., Yoke, C.A., & Yousefi, D. 2013. An Exploratory of Airline E-ticker Purchasing Intention among Foreign Undergraduates in Malaysia. *Journal of Human and Social Science Research Vol. 1, No. 1 (2013), 51-61*.
- Clarke, J. 2009. *SQL Injection Attacks dan Defense*. Burlington : Syngress Publishing, Inc.
- Christopher Alfeld et al. Ironbee Open Source WAF. <https://www.ironbee.com/docs/manual/ironbee-reference-manual.html>. (10 april 2016)
- Ellysa. R, Husni. Muchammad, Baskoro Adi Pratomo(2013). Pendeteksi Serangan SQL Injection Menggunakan Algoritma SQL Injection Free Secure pada Aplikasi Web, Institut Teknologi Sepuluh Nopember (ITS) Surabaya.
- Grossman, J., Hansen, R., Petkov, D.P., & Rager, A. 2007. *XSS Attacks: Cross Site Scripting Exploits and Defense*. Burlington: Syngress Publishing, Inc.
- Garfinkel, S. & Howard, S.E. 2001. *Web Security & Commerce*. United States: O'Reilly & Associates.
- Herrmann, S.D. 2002. *A Pratical Guide to Security Engineering And Information Assurance*. New York: Auerbach Publications.
- ISO/IEC (2005). Information technology — Security techniques — Code of practice for information security management. [http://www.specon.ru/files/ISOIEC%2017979%20\(second%20edition\).pdf](http://www.specon.ru/files/ISOIEC%2017979%20(second%20edition).pdf). (10 april 2016)
- Krawczyk, P. 2013. Most common attacks on web applications. <http://ipsec.pl/webapplication-security/most-common-attacks-web-applications.html>. (diakses 02 April 2016).
- Pribadi, Harijanto.2008. *Firewall melindungi jaringan dari DdoS menggunakan LINUX+MIKROTIK*. Penerbit Andi : Yogyakarta.
- Rahmat. Fajri, Mazharuddin S. Ary, Studiawan. H (2013). sistem Pendeteksi dan Pencegah Peretasan Terhadap Aplikasi Berbasis Web dengan Teknik Web Application Firewall (WAF), Institut Teknologi Sepuluh Nopember (ITS) Surabaya. ISSN: 2337-3539 (2301-9271 Print).

Stuttard, D., Pinto, M. 2011. *The Web Application Hacker's Handbook: Finding And Exploiting Security Flaws*. 2 nd Edition. Canada: John Wiley & Sons, Inc

Sarno, R. & Iffano, I. 2009. *Keamanan Sistem Informasi*. ITS press..