

**MEMBANGUN APLIKASI PEMBELAJARAN SECURE
WEB PROGRAMMING
BERBASIS OWASP TOP 10**

Diajukan Untuk Memenuhi Salah Satu Syarat Mencapai
Gelar Sarjana Komputer (S.Kom.)
Program Studi Teknik Informatika Pada Sekolah Tinggi Manajemen
Informatika Dan Komputer AKAKOM Yogyakarta

Disusun Oleh :

SRI SETIA BELLA

No. Mhs. : 075410151

Jurusan : Teknik Informatika

Jenjang : Strata Satu (S1)

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN
KOMPUTER
AKAKOM
YOGYAKARTA
2012**

HALAMAN PERSETUJUAN

Judul : MEMBANGUN APLIKASI PEMBELAJARAN SECURE WEB
PROGRAMMING BERBASIS OWASP TOP 10

Nama : Sri Setia Bella

No. Mhs : 075410151

Jenjang : Strata Satu (S1)

Jurusan : Teknik Informatika

Mata Kuliah : Skripsi

Selesai diperiksa dan disetujui,

Yogyakarta, Januari 2012

Mengetahui dan Menyetujui,

Dosen Pembimbing

Badiyanto, S.Kom., M.Kom.

HALAMAN PENGESAHAN
MEMBANGUN APLIKASI PEMBELAJARAN SECURE WEB
PROGRAMMING BERBASIS OWASP TOP 10

Dipertahankan Di Depan Dewan Penguji Skripsi
Sekolah Tinggi Manajemen Informatika Dan Komputer
AKAKOM Yogyakarta
Dan Dinyatakan Diterima Untuk Memenuhi Syarat-Syarat
Guna Memperoleh Gelar Sarjana Komputer

Hari : Kamis
Tanggal : 9 Februari 2012

Mengesahkan,

Dosen Penguji :

1. Dra. Hj. Syamsu Windarti, M.T., Apt. 1.....
2. Erna Hudianti Pujiarini, S.Si., M.Si. 2.....
3. Badiyanto, S.Kom., M.Kom. 3.....

Mengetahui,

Ketua Jurusan Teknik Informatika Strata Satu

Febri Nova Lenti, S. Si., M.T.

HALAMAN MOTTO

Try Harder... !!!!!!!!!!!

Untuk menjadi yang terbaik, tidak cukup hanya dengan bersikap baik
(Irriducibili)

HALAMAN PERSEMBAHAN

Karya tulis ini ku persembahkan untuk :

Tuhanku Allah SWT yang telah memberikan hikmat, kekuatan,
pertolongan dan perlindungan.

Kepada kedua orang tua ku Ayah dan Ibu yang selalu memberikan do'a
dan telah membesarkan aku.

Kepada Keluarga Besar ku di Jambi dan Situbondo yang selalu
memberi semangat dan dukungan kepadaku.

Buat semua teman-teman Himpunan Mahasiswa Jurusan Teknik
Informatika STMIK AKAKOM Yogyakarta.

Buat semua Bapak-Ibu karyawan dan teman-teman di STMIK AKAKOM
Yogyakarta. Yang selalu membagikan Ilmu-ilmunya dan selalu
memberikan semangat serta pelengkap dalam kehidupanku.

Teman - teman sekaligus tim 9tails dan Mas Mada Rambu Perdana yang
selalu berbagi ilmu dan membantu saya ketika mengalami kesulitan.

Teman-teman Bonek Korwil Jogja yang menjadi keluarga kecilku
Selama tinggal di Jogja. Salam Satu Nyali, WANI..!!!!

INTISARI

Saat ini tingkat serangan terhadap aplikasi web semakin tinggi dengan makin banyaknya tools-tools hacking yang semakin canggih dalam membantu penyerang melakukan penyusupan atau hacking, sehingga OWASP merilis sepuluh serangan yang paling sering dilakukan yaitu OWASP Top 10.

Web Aplikasi ini dirancang untuk pembelajaran keamanan web aplikasi, dimana didalamnya terdapat 10 celah berdasarkan OWASP Top 10. Tujuannya untuk mengetahui bagaimana sebuah celah bisa dieksploitasi dan bagaimana cara menutup celah tersebut. Tools-tools yang digunakan untuk melakukan serangan antara lain : Burpsuite dan sqlmap.

Setelah mengetahui jenis-jenis serangan dan cara memperbaiki, akan diketahui ada dua level keamanan yaitu level berbahaya dan sedang. Sehingga Web Aplikasi ini sudah layak untuk di jadikan pembelajaran keamanan web aplikasi.

Kata kunci : Hacking, Keamanan Web Aplikasi, OWASP Top Ten, Web Aplikasi, Web Developer.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Tuhan Yang Maha Esa, yang telah memberikan segala hikmat dan rahmat-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul **MEMBANGUN APLIKASI PEMBELAJARAN SECURE WEB PROGRAMMING BERBASIS OWASP TOP 10** yang digunakan untuk memenuhi salah satu persyaratan memperoleh gelar Sarjana Komputer.

Dengan segala kerendahan dan ketulusan hati, penulis menyampaikan penghargaan dan ucapan terima kasih yang sedalam - dalamnya kepada semua pihak yang telah membantu memberikan arahan, bimbingan, dan motivasi, baik secara langsung maupun tidak langsung, sehingga skripsi ini dapat diselesaikan, yaitu kepada :

- 1. Bapak Sigit Anggoro, S.T., M.T.,** selaku Ketua Sekolah Tinggi Manajemen informatika dan Komputer AKAKOM Yogyakarta.
- 2. Bapak Drs. Berta Bednar, M.T.,** selaku Pembantu Ketua I Sekolah Tinggi Manajemen Informatika dan Komputer AKAKOM Yogyakarta
- 3. Ibu Febri Nova Lenti, S.Si., M.T.,** selaku Ketua Jurusan Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer AKAKOM Yogyakarta.

4. **Bapak Badiyanto, S.Kom., M.Kom.,** selaku dosen pembimbing I, yang telah memberikan bimbingan serta pengarahan dalam penulisan skripsi ini.
5. Seluruh staf dan karyawan Sekolah Tinggi Manajemen Informatika dan Komputer AKAKOM Yogyakarta.
6. Kedua orang tua serta seluruh keluarga tercinta yang telah memberikan doa dan dukungan selama ini tanpa kenal lelah.
7. Teman-teman di HMJ Teknik Informatika STMIK AKAKOM Yogyakarta.
8. Temen-teman di 9tails dan teman-teman di Information Security Shinobi Camp, terutama mas Mada Rambu Perdana yang telah membimbing saya selama ini.
9. Semua pihak yang telah memberikan bantuan baik tenaga maupun pikiran dalam penyelesaian skripsi ini.

Penulis menyadari bahwa dalam penulisan karya tulis ini masih terdapat kekurangan, baik dalam analisis maupun cara penyajian materi. Oleh karena itu, kritik dan saran sangat penulis harapkan demi sempurnanya skripsi ini. Semoga skripsi ini dapat memberikan manfaat kepada pembaca.

Yogyakarta, Januari 2012

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERSEMBAHAN	iv
HALAMAN MOTTO	v
INTISARI	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xi

BAB 1 PENDAHULUAN

1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Ruang Lingkup	2
1.4 Tujuan Penelitian	3

BAB 2 TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka.....	4
2.2 Dasar Teori.....	4
2.2.1 OWASP (Open Web Application Security Project)	4
2.2.2 OWASP Top 10.....	5
2.2.3 Aplikasi Web	8
2.2.4 Secure Coding.....	9

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

3.1 Analisis Sistem	10
3.1.1 Analisis Kebutuhan Perangkat Keras.....	10
3.1.2 Analisis Kebutuhan Perangkat Lunak.....	10

3.1.3 Analisis Kebutuhan Perangkat Lunak Pengujian.....	10
3.2 Perancangan Sistem.....	12
3.2.1 Perancangan Web Aplikasi	12
3.2.2 Perancangan Proses Penetrasi dan Pengamanan.....	12
3.2.3 Blok Diagram Serangan.....	16
3.2.4 Flowchart Sistem.....	19

BAB 4 IMPLEMENTASI DAN PEMBAHASAN SISTEM

4.1 Implementasi Sistem.....	30
4.1.1 Implementasi Proses Panetrasi (Hacking).....	30
4.1.2 Implementasi Proses Pengamanan.....	47
4.2 Pembahasan Sistem.....	56
4.2.2 Analisa Pengujian Aplikasi.....	56

BAB 5 KESIMPULAN DAN SARAN

5.1 Kesimpulan	58
5.2 Saran	59

DAFTAR PUSTAKA

DAFTAR GAMBAR

Gambar 3.1	Blok Diagram Serangan Injeksi.....	16
Gambar 3.2	Blok Diagram Serangan XSS.....	16
Gambar 3.3	Blok Diagram Serangan Manajemen Sesi.....	16
Gambar 3.4	Blok Diagram Serangan Referensi Objek.....	17
Gambar 3.5	Blok Diagram Serangan CSRF	17
Gambar 3.6	Blok Diagram Serangan Konfig. Keamanan.....	17
Gambar 3.7	Blok Diagram Serangan Penyimpanan Kriptografi.....	17
Gambar 3.8	Blok Diagram Serangan Akses URL.....	18
Gambar 3.9	Blok Diagram Serangan SSL.....	18
Gambar 3.10	Blok Diagram Serangan Redireksi.....	18
Gambar 3.11	Flowchart Sistem.....	19
Gambar 3.12	Flowchart Sistem Pengujian Celah Injeksi.....	20
Gambar 3.13	Flowchart Sistem Pengujian Celah XSS.....	21
Gambar 3.14	Flowchart Sistem Pengujian Celah Manajemen Sesi...	22
Gambar 3.15	Flowchart Sistem Pengujian Celah Referensi Objek....	23
Gambar 3.16	Flowchart Sistem Pengujian Celah CSRF	24
Gambar 3.17	Flowchart Sistem Pengujian Celah Konfig. Keamanan.	25
Gambar 3.18	Flowchart Sistem Pengujian Celah Penyimpanan.....	26
Gambar 3.19	Flowchart Sistem Pengujian Celah Akses URL.....	27
Gambar 3.20	Flowchart Sistem Pengujian Celah SSL.....	28
Gambar 3.21	Flowchart Sistem Pengujian Celah Redireksi.....	29

Gambar 4.1	Halaman Login.....	30
Gambar 4.2	Analisa Proses Login Dengan Burpsuite.....	31
Gambar 4.3	Proses SQL Injection Dengan sqlmap.....	31
Gambar 4.4	Hasil SQL Injection Dengan sqlmap.....	32
Gambar 4.5	Halaman Admin.....	33
Gambar 4.6	Halaman Isi Buku Tamu.....	33
Gambar 4.7	Tampilan Serangan XSS.....	34
Gambar 4.8	Halaman Admin.....	35
Gambar 4.9	Halaman Admin Terproteksi.....	35
Gambar 4.10	Halaman Admin Tidak Terproteksi.....	36
Gambar 4.11	Tampilan File robots.txt.....	37
Gambar 4.12	Proses Ganti Password.....	38
Gambar 4.13	Analisa Proses Ganti Password Dengan Burpsuite.....	38
Gambar 4.14	Berhasil Ganti Password Dengan CSRF.....	39
Gambar 4.15	Proses Upload File Gambar.....	40
Gambar 4.16	Proses Upload File php.....	40
Gambar 4.17	Proses Upload File Backdoor.....	40
Gambar 4.18	Proses Bypass Proteksi File Gambar.....	41
Gambar 4.19	Akses Backdoor.....	42
Gambar 4.20	Data Hasil SQL Injection.....	43
Gambar 4.21	Direktori Transversal.....	43
Gambar 4.22	Direktori Transversal 2.....	44

Gambar 4.23 Tampilan Ebook.....45

Gambar 4.24 Celah Local File Inclusion.....46