

ANALISIS SERANGAN SQL INJECTION PADA CELAH KEAMANAN WEBSITE STUDI KASUS PT. ABC

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan Program Strata 1,
Program Studi Teknik Informatika, Universitas Pasundan Bandung

Oleh

Fauzi Abdurrachman Muttaqien
NRP : 12.304.0353



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
SEPTEMBER 2019**

LEMBAR PENGESAHAN
LAPORAN TUGAS AKHIR

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal sidang sesuai berita acara sidang, tugas akhir dari :

Nama : Fauzi Abdurrahman Muttaqien
NRP : 123040353

Dengan judul :

**“ANALISIS SERANGAN SQL INJECTION PADA CELAH KEAMANAN WEBSITE
STUDI KASUS PT. ABC”**

Bandung, 30 September 2019

Menyetujui,

Pembimbing Utama

(Doddy Ferdiansyah, S.T, M.T)

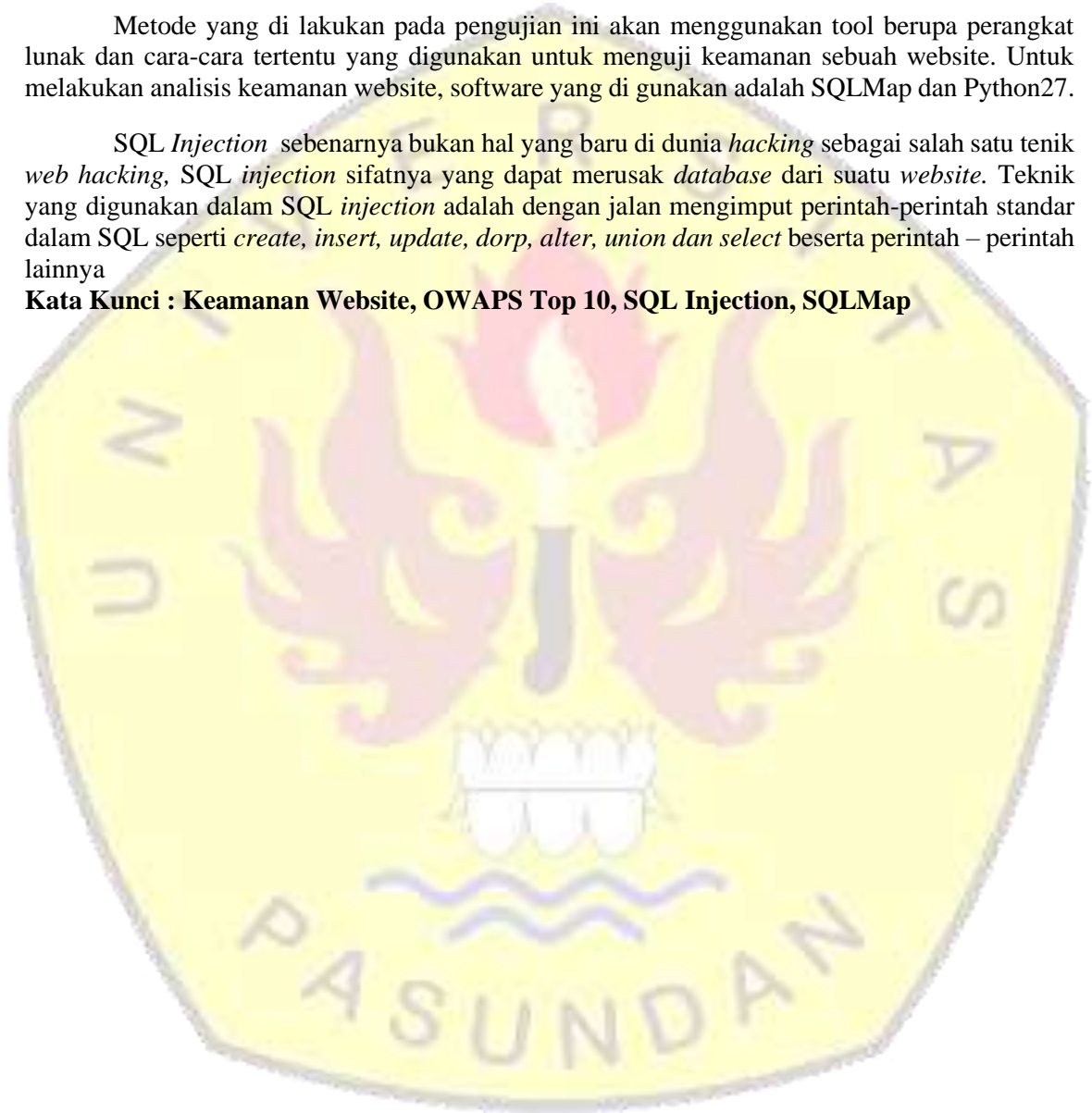
ABSTRAK

Pada saat ini website menjadi salah satu media informasi modern yang berkembang sangat cepat. Dalam pembuatan website tidak hanya sisi desain dan informasi yang dipentingkan tetapi aspek keamanan dari sebuah website itu sendiri mempunyai peranan yang sangat penting dalam sebuah website. Kebutuhan keamanan sebuah website timbul dari kebutuhan untuk melindungi data. Pertama, dari kehilangan dan kerusakan data. Kedua, adanya pihak yang tidak hendak mengakses dan merubah data. Permasalahan lainnya mencakup perlindungan data dari delay yang berlebihan pada saat mengakses atau menggunakan data.

Metode yang dilakukan pada pengujian ini akan menggunakan tool berupa perangkat lunak dan cara-cara tertentu yang digunakan untuk menguji keamanan sebuah website. Untuk melakukan analisis keamanan website, software yang digunakan adalah SQLMap dan Python27.

SQL Injection sebenarnya bukan hal yang baru di dunia *hacking* sebagai salah satu teknik *web hacking*, *SQL injection* sifatnya yang dapat merusak *database* dari suatu *website*. Teknik yang digunakan dalam *SQL injection* adalah dengan jalan mengimput perintah-perintah standar dalam SQL seperti *create*, *insert*, *update*, *dorp*, *alter*, *union* dan *select* beserta perintah – perintah lainnya

Kata Kunci : Keamanan Website, OWAPS Top 10, SQL Injection, SQLMap



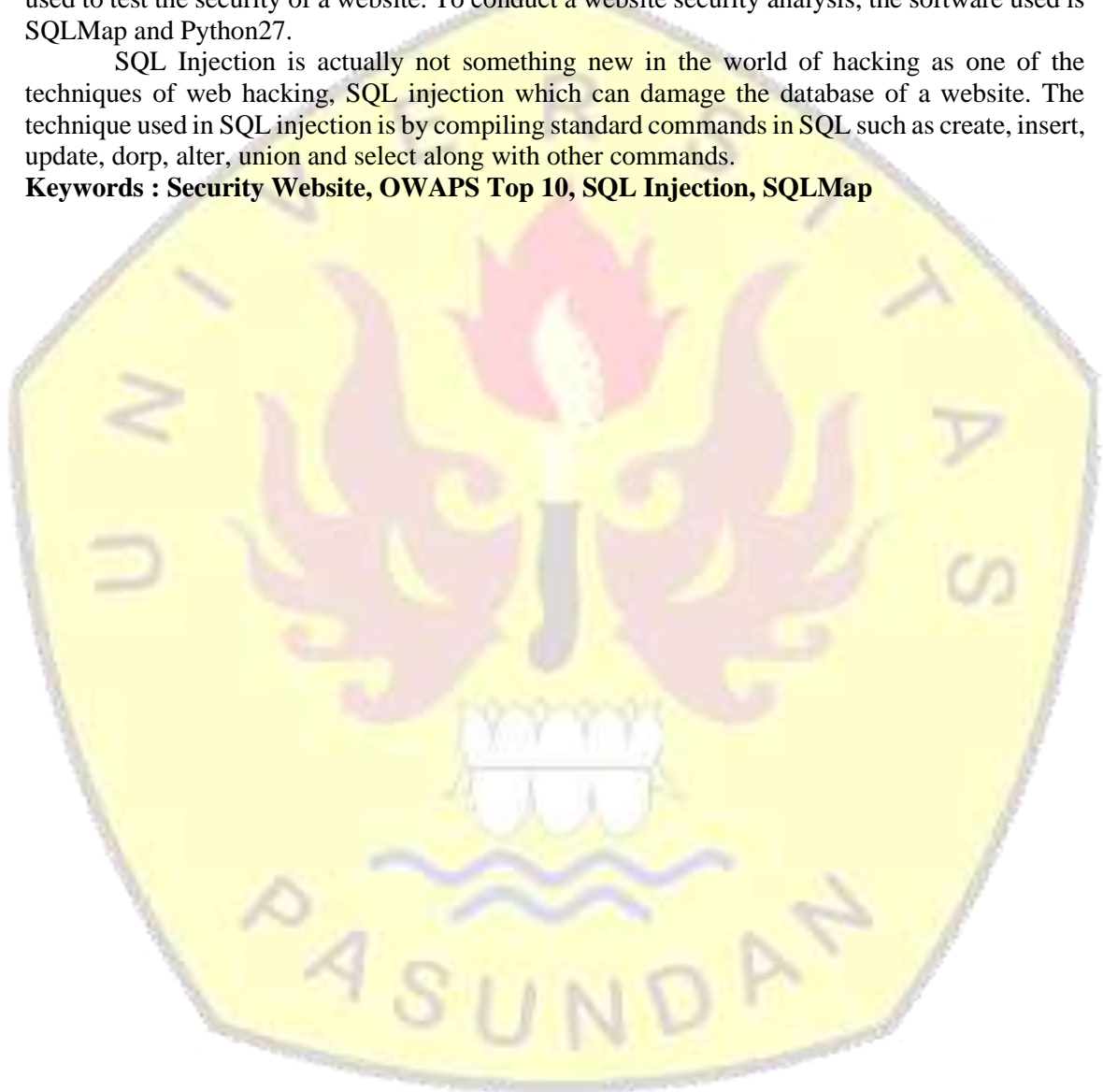
ABSTRACT

At this time the website is becoming one of the modern information media that is developing very fast. In making a website not only the design and information aspects are important but the security aspect of a website itself has a very important role in a website. The security needs of a website arise from the need to protect data. First, from data loss and damage. Second, there are parties who do not want to access and change data. Other problems include protecting data from excessive delay when accessing or using data.

The method used in this test will use tools in the form of software and certain methods used to test the security of a website. To conduct a website security analysis, the software used is SQLMap and Python27.

SQL Injection is actually not something new in the world of hacking as one of the techniques of web hacking, SQL injection which can damage the database of a website. The technique used in SQL injection is by compiling standard commands in SQL such as create, insert, update, drop, alter, union and select along with other commands.

Keywords : Security Website, OWAPS Top 10, SQL Injection, SQLMap



DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	iv
DAFTAR TABEL	vii
DAFTAR GAMBAR	ix
DAFTAR ISTILAH	xi
DAFTAR LAMPIRAN	xii
BAB 1 PENDAHULUAN	1-1
1.1. Latar Belakang	1-1
1.2. Identifikasi Masalah	1-2
1.3. Tujuan Tugas Akhir	1-2
1.4. Lingkup Tugas Akhir	1-2
1.5. Metodologi Tugas Akhir	1-2
1.6. Sistematika Penulisan Tugas Akhir	1-3
BAB 2 LANDASAN TEORI	2-1
2.1. Pengertian Website	2-1
2.2. OWASP Top 10 2013	2-1
2.3. Protokol HTTP	2-3
2.4. HTTPS (Hyper Text Transfer Protocol Secure)	2-4
2.5. SSL (Secure Socket Layer)	2-4
2.6. XAMPP	2-5
2.7. PhpMyAdmin	2-6
2.8. CMD (Command Prompt)	2-7
2.9. SQLMap	2-8
2.10. SQL Injection	2-8
2.11. Mekanisme SQL Injection	2-9
2.12. Penelitian Terdahulu	2-10
BAB 3 SKEMA PENELITIAN	3-1
3.1. Alur Penyelesaian Tugas Akhir	3-1
3.2. Skema analisis	3-2
3.2.1. Langkah – langkah analisis	3-4
3.3. Kerangka Pemikiran Teoritis	3-3

3.3.1. Analisis dan solusi tugas akhir	3-4
3.3.2. Manfaat.....	3-5
3.4. Profile Penelitian.....	3-6
3.4.1. Objek penelitia	3-6
BAB 4 ANALISIS DAN PENGUJIAN.....	4-1
4.1. Langkah-Langkah Analisis Keamanan Website	4-1
4.1.1. Kesiapan implementasi software pengujian sql	4-1
4.1.1.1 XAMPP	4-1
4.1.1.2 SQLMap	4-2
4.1.2. Informasi dari sebuah website yang akan di ujikan	4-5
4.2. Langkah-Langkah Mencari Celah Keamanan Website.....	4-10
4.3. Pengujian Keamanan Beberapa Website.....	4-11
4.4. Tata cara Pengujian SQL Injection	4-11
BAB 5 PENUTUP	5-1
5.1. Kesimpulan	5-1
5.2. Saran	5-1
DAFTAR PUSTAKA	
LAMPIRAN	

BAB 1

PENDAHULUAN

Bab ini menjelaskan latar belakang, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi penelitian tugas akhir dan sistematika penulisan tugas akhir.

1.1 Latar Belakang

Website adalah keseluruhan halaman – halaman yang terdapat dalam sebuah domain yang mengandung informasi. Sebuah *website* biasanya di bangun atas banyak halaman web yang saling berhubungan. Hubungan antara satu halaman web dengan halaman web yang lainnya disebut dengan hyperlink. Sedangkan yang dijadikan media penghubung di sebut hypertext. [HID10]

Keamanan *website* sangat di perlukan bagi suatu organisasi ataupun perusahaan tersebut. *Website* yang tidak menawarkan keamanan akan sangat berpotensi hilangnya integritas data dan kepercayaan konsumen akan perusahaan tersebut. Namun kebanyakan pemilik *website* mengabaikan *security system* pada *website* tersebut. Salah satu serangan yang paling sering digunakan oleh para *cracker* tersebut adalah *SQL Injection*. [ANL02]

Penulis juga melihat kejahatan di dunia teknologi dan informasi terutama pada aplikasi web semakin marak terjadi. Salah satu faktor yang menyebabkan kurangnya tingkat keamanan pada aplikasi web adalah kesalahan penulisan kode program. Berdasarkan hasil riset OWASP Top 10 tahun 2013, terdapat 10 risiko keamanan yang paling kritis pada aplikasi berbasis web. [OWA13]

SQL Injection sebenarnya bukan hal yang baru di dunia *hacking* sebagai salah satu teknik *web hacking*, *SQL injection* sifatnya yang dapat merusak *database* dari suatu *website*. Teknik yang digunakan dalam *SQL injection* adalah dengan jalan mengimput perintah-perintah standar dalam SQL seperti *create, insert, update, dorp, alter, union dan select* beserta perintah – perintah lainnya. [ANL02]

Harapannya setelah dilakukan nya analisis terhadap *website* PT.ABC bisa menjadi referensi untuk menambah fitur-fitur keamanan *website* nya demi menjaga data yang ada. Maka *website* PT. ABC akan terjamin keamanannya. Sehingga pelanggan merasa aman bahwa data profil pelanggan dan komplain gangguan terjaga kerahasiaanya, perusahaan juga mendapatkan kepercayaan lebih dari pelanggannya dan meningkatkan kemampuan bersaing dari perusahaan lainnya.

1.2 Identifikasi Masalah

Berdasarkan latar belakang di atas dapat dirumuskan beberapa permasalahan sebagai berikut:

1. Bagaimana mengetahui celah keamanan *website*?

1.3 Tujuan Tugas Akhir

Tujuan dari penelitian skripsi ini adalah sebagai berikut:

1. Mencari celah keamanan dari suatu *website*.

1.4 Lingkup Tugas Akhir

Agar tidak terlampaui luas dan menyimpang pembahasannya, penulis membuat batasan-batasan masalah sebagai berikut:

1. Pengujian terhadap serangan *SQL Injection*

1.5 Metodologi Tugas Akhir

Metodologi penelitian yang digunakan dalam penulisan skripsi ini adalah sebagai berikut:

1. Identifikasi Masalah

Pada tahap ini dilakukan identifikasi masalah yang terjadi pada sebuah website serta solusi sementara yang diusulkan untuk menyelesaikan masalah tersebut.

2. Pengumpulan Data

Pada tahapan ini merupakan suatu tahapan yang dilakukan untuk mengumpulkan data mengenai website yang akan di uji. Di dalam tahapan ini ada tiga tahapan yang dilakukan yaitu:

- a) Observasi

Merupakan suatu tahapan yang dilakukan untuk mencari informasi terkait hal-hal yang di butuhkan dengan cara melakukan observasi secara langsung.

- b) Studi Literatur

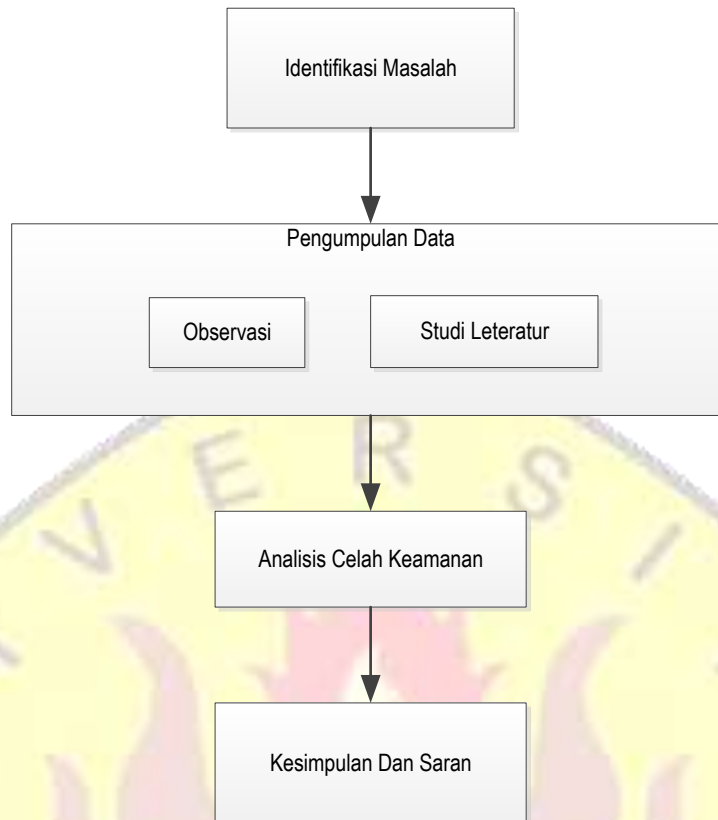
Merupakan pemanfaatan hasil dari pencarian dari referensi seperti internet, buku dan jurnal untuk mendapatkan materi yang berkaitan dengan tugas akhir yang di buat.

3. Analisis Celah Keamanan

Pada tahapan ini merupakan pengujian melakukan analisis terhadap suatu website dengan celah keamanan atau kerentanan yang di peroleh yang memiliki tingkat resiko paling tinggi dan di sertai pengujian yang mengacu pada literatur yang sudah ada.

4. Kesimpulan dan Saran

Pada tahapan ini merupakan tahapan penjelasan mengenai kesimpulan dari hasil pengujian yang telah dilakukan pada sebuah website yang di uji serta sebagai saran bagi penelitian selanjutnya.



Gambar 1.1 Metodologi Tugas Akhir

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan skripsi adalah:

BAB 1 PENDAHULUAN

Menguraikan tentang latar belakang permasalahan, merumuskan inti permasalahan yang dihadapi, menentukan tujuan penelitian, diikuti dengan pembatasan masalah, metodologi penelitian, serta sistematika penulisan.

BAB 2 LANDASAN TEORI

Pada bab ini membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang pernah dilakukan sebelumnya termasuk sintesisnya. Membahas tentang tinjauan perusahaan dan konsep dasar serta teori-teori yang berkaitan dengan topik penelitian dan yang melandasi perancangan sistem keamanan website.

BAB 3 SKEMA PENELITIAN

Pada bab 3 ini menjelaskan mengenai alur tugas akhir dari awal hingga akhir, rancangan penelitian, peta analisis, analisis masalah dan kerangka berpikir teoritis yang ditunjang dari sumber literatur yang sesuai.

BAB 4 ANALISIS DAN PENGUJIAN

Pada bab ini menguraikan bagaimana mengimplementasikan setiap prosedur pada bab sebelumnya ke dalam bentuk bahasa pemrograman untuk membuat sistem. Kemudian akan dilakukan pengujian terhadap prosedur tersebut dan melakukan pembahasan tentang kemampuan terhadap prosedur tersebut.

BAB V KESIMPULAN DAN SARAN

Pada bab terakhir ini akan memberikan suatu kesimpulan dan saran terhadap hasil pengujian yang dilakukan pada perancangan sistem keamanan webiste.



DAFTAR PUSTAKA

- [ANL02] Anley C “Advanced SQL Injection in SQL Server Applications. An NGSSoftware Insight Scurity Research (NISR) Publications” Tersedia : 2002
- [BIN18] pengertian, Tutorial dan Tools SQL Injection, Tersedia : 2018
<http://www.binushacker.net/tutorial-pentest-hacking-dengan-sqlmap.html>
- [BUN07] Bunafit Nugroho “ Buku Latihan : Konfigurasi & Manipulasi Registry Windows Xp”, Tersedia : 2007
- [CLA09] Clarke, J “ SQL Injection Attack and Defense “, Tersedia : 2009
- [DAD14] Dadan “ Membuat CMS Multifitur”, Tersedia : 2014
- [JAM09] Jamiludin, Jaja M, “ Best Tools Hacking and Recovery Password”, Tersedia : 2009
- [MAD15] Made, I Suartana “ Sistem Pengamanan Web Server Dengan Web Application Firewall (WAF)” Tersedia : Februari 2015.
- [MHI15] M. Hilmi Masruri “ Membangun SMS Gateway dengan Gammu & Kalkun”, Tersedia : 2015
- [OWA13] OWAPS top 10 2013 tersedia : 21 Agustus 2015
- [RAH10] Rahmat Hidayat “ Cara Praktis Membangun Website Gratis” , Tersedia : 2010
- [RAH13] Rahman, Arief Hakim “ pendeteksi SQL Injection menggunakan algoritma SQL Injection Free Secure Pada Aplikasi Web”, Tersedia November 2013
- [SRI14] Sritrusta Sukaridhoto, ST. Ph.D. “ Buku Jaringan Komputer 1”, Tersedia : 2014
- [SUR17] Su Rahman “ Rahasia Membuat Website Dan Seo Paling Mudah Dengan Rvsitebuilder Pro”, Tersedia : 2017
- [YOG08] Yogi wicaksono “Membangun bisnis online dengan mambo”, Tersedia : 2008