STUDI KEAMANAN SISTEM INFORMASI BERBASIS *WORDPRESS* TERHADAP SERANGAN SQL *INJECTION* DI SITUS CAHUNNES.COM

SKRIPSI

Skripsi ini ditulis sebagai Salah Satu Syarat

untuk Memperoleh Gelar Sarjana Pendidikan

Program Studi Pendidikan Teknik Informatika dan Komputer S1

Oleh

Mars Dwika Aulia

NIM 5302410176

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS NEGERI SEMARANG

2017

LEMBAR PERSETUJUAN PEMBIMBING

Nama	: Mars Dwika Aulia
NIM	: 5302410188
Program Studi	: Pendidikan Teknik Informatika dan Komputer
Judul	: Studi Keamanan Sistem Informasi Berbasis Wordpress Terhadap Serangan SQL Injection di Situs cahunnes.com.

Skripsi ini telah disetujui oleh pembimbing untuk diajukan ke sidang panitia ujian Skripsi Program Studi Pendidikan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Semarang.

Semarang, 1 Agustus 2017

Dosen Pembimbing,

Drs. Djoko Adi Widodo, M.T

NIP. 195909271986011001

LEMBAR PENGESAHAN KELULUSAN

Skripsi dengan judul "Studi Keamanan Sistem Informasi Berbasis *Wordpress* Terhadap Serangan *SQL Injection* di Situs cahunnes.com". telah dipertahankan di depan sidang Panitia Ujian Skripsi/TA Fakultas Teknik UNNES pada tanggal 4 bulan Agustus tahun 2017

Oleh

Nama : Mars Dwika Aulia
NIM : 5302410176
Program studi : Pendidikan Teknik Informatika dan Komputer S1

Panitia

Ketua

Dr.-Ing. Dhidik Prastiyanto, S.T., M.T.
NIP. 197805312005011002

Sekretaris

Ir. Ulfah Mediaty Arief, M.T
NIP. 196605051998022001

Penguji I

Drs. Sri Sukamta,M.Si
NIP. 196505121991031003

Penguji II

Drs. Yohanes Primadiyono, M.T
NIP. 196209021987031002

Penguji III/Pembimbing

Drs. Djoko Adi Widodo, M.T
NIP. 195909271986011001

Mengetahui,
Dekan Fakultas Teknik

Dr. Nur Qudus, M.T.
NIP. 196911301994031001

LEMBAR PERNYATAAN KEASLIAN KARYA ILMIAH

Dengan ini saya menyatakan bahwa:

1. Skripsi/TA ini, adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, magister, dan/atau doktor), baik di Universitas Negeri Semarang (UNNES) maupun di perguruan tinggi lain.
2. Karya tulis ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan Pembimbing dan masukan Tim Penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya ini, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi ini.

Semarang, 20 Juni 2017
Yang membuat pernyataan,

Mars Dwika Aulia
NIM. 5302410176

MOTTO

1. Dan tidaklah Aku ciptakan Jin dan Manusia kecuali untuk beribadah kepadaku" (QS Adz-Dzaariyaat : 56).
2. Ingatlah bahwa di dalam jasad itu ada segumpal daging. Jika ia baik, maka baik pula seluruh jasad. Jika ia rusak, maka rusak pula seluruh jasad. Ketahuilah bahwa ia adalah hati (HR. Bukhari no. 52 dan Muslim no. 1599).
3. Maha Suci Allah Yang di tangan-Nya-lah segala kerajaan, dan Dia Maha Kuasa atas segala sesuatu (QS Al-mulk : 1)

SARI

Aulia, Mars Dwika. 2017. "Studi Keamanan Sistem Informasi Berbasis Wordpress Terhadap Serangan SQL Injection di Situs cahunnes.com". Skripsi. Jurusan Teknik Elektro Program Studi Pendidikan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Semarang.
Pembimbing : Drs. Djoko Adi Widodo, M.T.

Kata kunci : , Wordpress, Sql Injection, keamanan sistem informasi, *White Box testing*

Wordpress merupakan penyedia *Content Management System*(CMS) yang paling banyak digunakan saat ini dalam pengembangan situs web. Selain kemudahan, sistem keamanan adalah hal utama yang harus dperhatikan dalam pengembangan situs web. Salah satu teknik *hacking* yang paling populer adala *sql injection.* Penelitian ini dilakukan untuk mengetahui bagaimana dan apa saja yang dapat dilakukan oleh serangan berbasis *sql injection,* serta apakah sistem informasi berbasis wordpress aman terhadap serangan *sql injection.*

Penelitian dilakukan dengan melakukan serangan *sql injection* kepada *dummy website*, hal ini bertujuan untuk mendapatkan metode penyerangan yang valid dan mendapatkan gambaran tentang dampak dari *sql injection*. Setelah melakukan *sql injection* pada *dummy website* selanjutnya dilakukan pula *sql injection* pada *real website*, hal ini bertujuan untuk menganalisa perilaku *cms wordpress* terhadap *sql injection*.

Penyerangan pada *dummy website* menunjukan bahwa, dengan metode yang benar *sql injection* memungkinkan penyerang untuk mengakses database dan mendapatkan data dari *website target*. Pada penyerangan terhadap situs cahunnes.com, teknik *sql injection* yang dikenal secara umum, tidak berhasil menembus sistem keamanan cahunnes.com, hal ini disebabkan karena situs cahunnes.com melakukan konversi pada *url* sehingga *id* tidak tampak pada *url,*dan cahunnes.com juga melakukan *blocking* terhadap penggunaan *syntax sql* pada url. Melalui penelitian ini dapat disimpulkan bahwa sistem informasi berbasis wordpress relatif aman dari serangan *sql injection.*

PRAKATA

Alhamdulillahirrabil'alamin. Puji syukur penulis panjatkan kehadirat Allah SWT, yang telah memberikan rahmat dan hidayahnya sehingga skripsi yang berjudul "Studi Keamanan Sistem Informasi Berbasis Wordpress Terhadap Serangan SQL Injection di Situs cahunnes.com" dapat diselesaikan dengan baik.

Penulis menyadari bahwa penyusunan skripsi ini tidak lepas dari bantuan berbagai pihak, maka pada kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Prof. Dr. Fahrur Rokhman, M.Hum Rektor Universitas Negeri Semarang.
2. Dr. Nur Qudus, M.T Dekan Fakultas Teknik Universitas Negeri Semarang.
3. Dr.-Ing. Dhidik Prastiyanto, S.T., M.T.. Ketua Jurusan Teknik Elektro Fakultas Teknik Universitas Negeri Semarang.
4. Ir. Ulfah Mediaty Arief, M.T., Kaprodi Pendidikan Teknik Informatika dan Komputer.
5. Drs. Djoko Adi Widodo, M.T, selaku dosen pembimbing.. dosen pembimbing yang telah memberikan bimbingan, motivasi, dan arahan dalam menyelesaikan skripsi ini.
6. Bapak, ibu dosen dan staf di Jurusan Teknik Elektro UNNES yang telah memberikan ilmu pengetahuan kepada penulis.
7. Semua rekan seperjuangan di Prodi Pendidikan Teknik Informatika dan Komputer angkatan 2010 atas dukungan, bantuan dan kebersamaannya selama ini.

Semarang, 20 Juni 2017

Penulis

Mars Dwika Aulia

NIM 5302410176

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

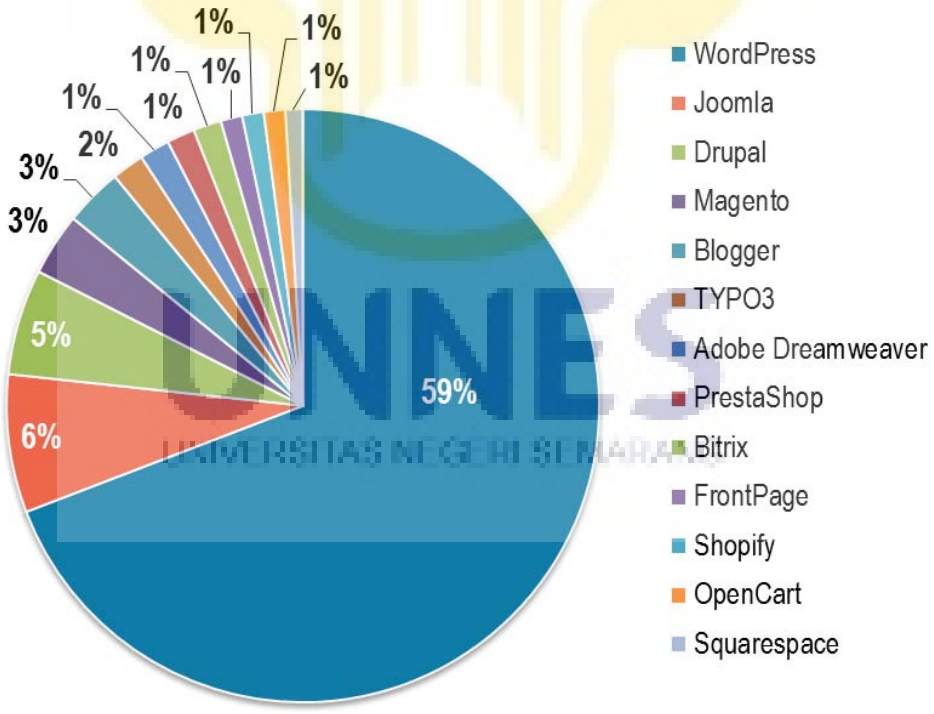
Teknologi internet di era saat ini telah berkembang dengan begitu cepat dan juga pesat. Internet yang diawal pembuatannya dimaksudkan untuk kepentingan militer saat ini telah banyak digunakan masyarakat untuk berbagai kebutuhan. Kebutuhan masyarakat terhadap teknologi internet telah bergeser dari hanya kebutuhan sekunder menjadi kebutuhan yang bersifat primer. Tingginya minat masyarakat dibidang internet dapat terlihat dari banyaknya jumlah pengguna aktif internet di Indonesia, berdasarkan survey yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia pengguna internet Indonesia pada 2016 mencapai 132,7 juta. Artinya, ada peningkatan signifikan, bila dibandingkan dengan dua tahun lalu yang mencapai 88,1 juta pengguna saja.

Salah satu fitur utama dalam teknologi internet adalah website. website memungkinkan penggunanya untuk saling berbagi informasi kapanpun dan dimanapun dibutuhkan. Sebuah website bisa berupa hasil kerja dari perorangan atau individu, atau menunjukkan kepemilikan dari suatu organisasi, perusahaan. biasanya pembahasan dalam sebuah situs web merujuk pada sebuah ataupun beberapa topik khusus, atau kepentingan tertentu.

Secara umum dalam membangun sebuah website ada dua alternatif cara yang dapat digunakan, yaitu yang berbasis CMS(*Content Management System*) dan yang berbasis CSS (*Cascading Style Sheets*). Perbedaan yang mendasar dari

kedua cara diatas adalah, dalam CSS perancang website membangaun situsnya dari awal dengan menggunakan bahasa pemrograman baik HTML,PHP,dan juga SQL. Sedangkan dalam CMS pembuat situs hanya perlu untuk meilih elemen – elemen apa saja yang ingin ada dalam websitenya tanpa perlu memahami lebih jauh terkait bahasa pemrograman.

Salah satu aplikasi yang popular dalam pembuatan website berbasis CMS adalah WordPress. Dalam penelitian yang dilakukan oleh w3techs Wordpress menempati urutan pertama aplikasi CMS yang paling banyak digunakan. Wordpress memperoleh presentase sebesar 59%, dan disusul oleh Joomla ditempat kedua yang memperoleh presentase sebesar 6 %.



Gambar 1.1 : Presentase penggunaan CMS (w3tech, 2016)

WordPress memungkinkan penggunanya untuk memodifikasi dan menyesuaikan website yang dibuatnya sesuai dengan kebutuhan., Pengguna WordPress dapat mengunduh aplikasi beserta seluruh berkas CMS WordPress. Selanjutnya, CMS ini dapat diubah ulang selama seseorang menguasai PHP, CSS dan skrip lain yang menyertainya.

Pengunaan Wordpress sebagai *platform* sebuah website tidak hanya digunakan pada website – website personal saja. Banyak instansi – instansi di Indonesia yang merancang website nya dengan menggunakan WordPress. Hal ini dikarenakan selain karena kemudahan yang ditawarkan, Wordpress juga menawarkan kecepatan dalam pembuatan.

Salah satu lembaga yang menggunakan wordpress sebagai aplikasi pembuatan sistem informasi adalah situs cahunnes.com. Cahunnes.com merupakan situs yang menyajikan berita seputar kampus Universitas Negeri Semarang sebagai konten utamanya. Sebagai situs dengan konten berita, kredibilitas dan nama baik merupakan hal yang sangat penting bagi pengelola situs cahunnes.com.

Maka berdasarkan paparan di atas, penulis tertarik untuk meneliti keaman system informasi yang berbasis CMS dalam skripsi yang berjudul **"Studi Keamanan System Informasi Berbasis Wordpress Terhadap Serangan SQL Injection di Situs cahunnes.com"**..

1.2 Identifikasi Masalah

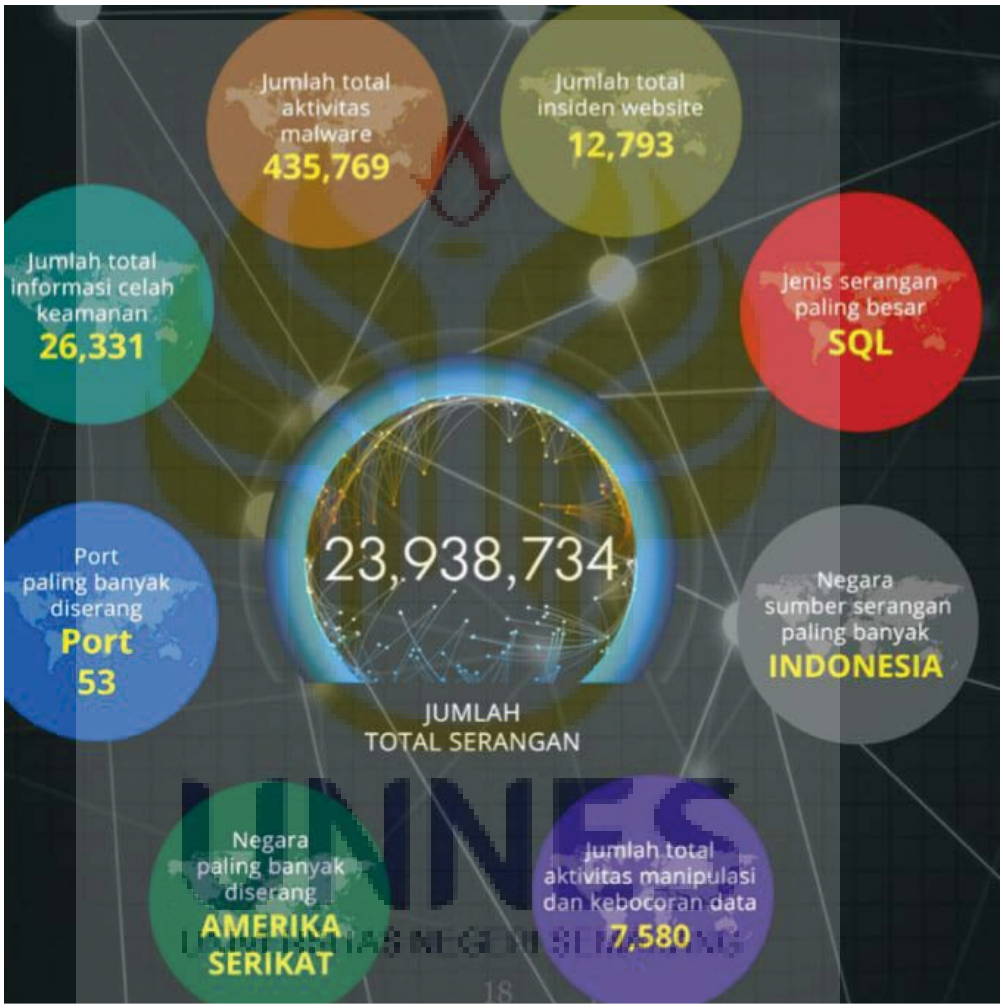
Komputer dalam perkembangannya saat ini, telah menjadi bagian yang penting dalam kehidupan penggunanya. Sudah bukan merupakan hal yang aneh bila sebuah proses produksi maupun pelayanan jasa menjadi terganggu karena jaringan komputer yang tidak bekerja dengan semestinya.

Kemajuan teknologi yang begitu pesat menuntut komputer untuk memiliki tingkat kompleksitas yang semakin tinggi, namun dengan tingkat penggunaan yang semakin mudah Para pengembang berlomba-lomba membuat produk yang mudah digunakan namun pada akhirnya sering tidak memperhatikan factor keamanan. Dengan tuntutan waktu dan target yang ketat, para pengembang tidak jarang hanya melakukan pengetesan terhadap fungsi suatu program dan masalah keamanan kurang mendapatkan perhatian

Tidak jarang dijumpai banyaknya perbaikan yang perlu dilakukan dari sebuah produk perangkat lunak yang sudah digunakan oleh masyarakat. Hal ini menandakan bahwa proses *quality control* tidak berkjalan secara maksimal, karena tidak dapat mendeteksi permasalahan secara dini. Hal ini juga menandakan bahwa semakin komplek sebuah produk perangkat lunak semakin berbahaya pula ancaman terhadap produk perangkat lunak tersebut

Masalah timbul dikarenakan, melakukan penyerangan terhadap suatu system atau biasa disebut hacking ternyata tidak membutuhkan proses yang begitu sulit. Disebabkan oleh semakin pesatnya perkembangan teknologi, diikuti juga oleh semakin berkembangnya peralatan – peralatan untuk melakukan *hacking*. Saat ini hanya dengan menekan tombol pada *mouse*, para

pelaku penyerangan atau biasa disebut *hacker* dapat dengan mudah mendapatkan akses terhadap sebuah sistem. Akibatnya adalah secara umum kemampuan *hacker* semakin menurun namun potensi ancaman yang dapat ditimbulkan justru semakin meningkat.



Gambar 1.2 : statistik aktivitas *hacking* tahun 2015 (Asosiasi Pengelola Jasa Internet Indonesia, 2016)

Dalam penelitian yang dilakukan oleh Asosiasi Pengelola Jasa Internet Indonesia (Lumanto, 2016), yang merupakan lembaga yang bertugas dalam menjaga dan mengawasi keamanan infrastruktur internet di Indonesia. Dikatakan

bahwa ditahun 2015 terdapat 23.938.734 aktifitas hacking di Indonesia, dimana sasaran terbesarnya adalah Negara Amerika Serikat dan jenis serangan paling besar adalah jenis serangan berbasis SQL.

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

Gambar 1.3 : Riset OWASP 2017 (OWASP, 2017)

Permasalahan tentang ancaman *sql injection* terhadap sistem informasi kembali dijelaskan oleh OWASP (*The Open Web Application Security Project*) melalui hasil riset yang dipublikasikan pada bulan juli 2017. Dalam rilis tersebut dikatakan bahwa serangan berbasis *injection* masih merupakan serangan dengan resiko paling tinggi dibandingkan dengan metode srangan lainnya. OWASP sendiri merupakan sebuah komunitas terbuka yang fokus pada keamanan aplikasi web.

Permasalah keamanan sitem terhadap *sql injection* juga terjadi dalam dunia pendidikan khususnya pada sistem informasi universitas. Berdasarkan penelitian yang dialkukan oleh Resi Utami Putri dan Jazi Eko Isriyanto, dikatakan bahwa pada tahun 2012 terdapat 68 *ip address* yang melakukan *sql injection* pada laman www.ugm.ac.id (Putri & Isriyanto, 2012)

1.3 Pembatasan Masalah

Dalam pembuatan skripsi ini, penulis membatasi masalah yang akan dianalisis yaitu:

1. Menggunakan serangan yang berbasis SQL Injection untuk menganalisa keaman sistem informasi pada situs cahunnes.com.
2. Penulis tidak melakukan implementasi peningkatan keamanan sistem informasi yang sudah ada dan hanya memberikan solusi terkait bagaimana mengantisipasi serangan berbasis SQL Injection.

.

1.4 Rumusan Masalah

Sesuai dengan identifikasi masalah dan pembatasan masalah yang telah dikemukakan, maka permasalahan dalam penelitan ini adalah,

1. Bagaimana *SQL Injection* dapat menyerang sebuah sistem informasi
2. Apakah Sistem Informasi Berbasis *Wordpress* aman terhadap serangan berbasis *sql injection*

1.5 Tujuan Penelitan

Tujuan penelitian yang hendak dicapai dalam penelitan ini adalah,

1. Mendapatkan serangkaian *syntaq sql* yang berfungsi dalam melakukan serangan pada sebuah sistem informasi
2. Melakukan analisa sistem keamanan situs cahunnes.com terhadap serangan *sql injection*

1.6 Manfaat Penelitan

Hasil kegiatan penelitan ini diharapkan dapat memberikan manfaat kepada, mahasiswa, pengelola situs cahunnes.com, dan praktisi dibidang pengembangan *website,* adapun manfaatnya antara lain:

1. Bagi mahasiswa, sebagai gambaran secara umum tentang sistem informasi dan elemen keamanannya
2. Bagi pengelola situs cahunnes.com, sebagai bahan referensi terkait keamanan sistem informasi yang dikelola.
3. Bagi pengembang *website*, sebagai bahan pertimbangan dalam menentukan *platform website* yang hendak dikembangkan.

BAB II

KAJIAN PUSTAKA DAN LANDASAN TEORI

5.1 Kajian Pustaka

Penelitian yang relevan dalam penulisan skripsi ini adalah penelitian yang diladilakukan oleh Alifandi Yudistira (2012) dengan judul Anilisis Kemanan Otentikasi dan Basis Data pada Web Simple-O Menggunakan SQL Injection. Penelitian yang dilakukan adalah menguji sistem keamanan website Simple-O dengan menggunakan sintaks *sql injection* . Website Simple-O yang mana merupakan sebuah website yang dirancang untuk melakukan ujian essay secara online, akan dimasukan sintaks – sintaks sql pada form login. Contoh sintaks yang digunakan adalah "or", "1=1", "0=0"

Penelitian lain yang relevan dan menjadi referensi adalah penelitian yang dilakukan oleh Bayu Arie Nugroho (2012) dengan judul Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Terhadap Serangan Packet Sniffing. Penelitian ini membahas evaluasi tingkat keamanan fasilitas wifi di PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta dengan menggunakan aplikasi netstumbler, inSSIDer dan ettercap. Netstumbler adalah tools wifi hacking yang digunakan untuk mendeteksi dan mengidentifikasi sinyal wireless yang terbuka. inSSIDer adalah software alternatif yang fungsinya sama persis dengan netstumbler. Ettercap adalah tools packet sniffer yang dipergunakan

untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan, yang juga memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum. Dalam penelitian ini dilakukan dua tahap, yang pertama mengidentifikasi keberadaan dan keamanan wifi yang dipakai menggunakan software inSSIDer. Tahap kedua melakukan serangan packet sniffing menggunakan software ettercap sebagai langkah pengujian keamanan di PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta.

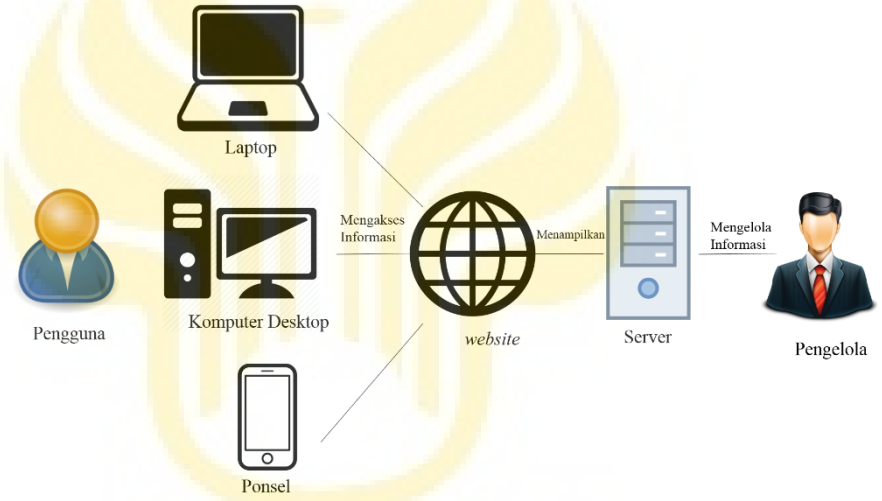
Penelitian yang dilakukan oleh Moh dahlan dkk (2014) dengan judul Pengujian Dan Analisa Keamanan Website Terhadap Serangan *Sql Injection* (Studi Kasus : Website UMK). Penelitian yang dilakukan adalah dengan melakukan serangan berbasis *sql injection* terhadap*website* Universitas Muria Kudus (UMK). Penelitian dilakukan dengan menggunakan dua pendekatan yaitu pendekatan proses forensik untukmenganalisa teknis keamanan website dan studi pustaka sebagai referensi kajiandan teori. Pada awal penelitian, peneliti melakukan identifikasi terhadap kebutuhan-kebutuhan, baikkebutuhan fungsional sistem maupun identifikasi kondisi jaringan website Universitas Muria Kudus. Pada tahapan selanjutnya peneliti mulai melakukan serangan*sqlinjection* terhadap website UMK. Serangan disini hanya dilakukan untuk melihat apakah penyerang dapat memasuki database website UMK tanpa melakukan manipulasi terhadap database yang ada, sehingga tidak akanmengganggu kondisi website yang sedang berjalan

Penelitian yang dilakukan oleh Resi Utami Putri dan Jazi Eko Istiyanto (2012) dengan judul Analisis Forensik Jaringan Studi Kasus Serangan *Sql Injection* pada *Server* Universitas Gadjah Mada. Penelitian yang dilakukan bertujuan untuk menemukan sumber serangan berbasis *sql injection* terhadap*server* Universitas Gajah Mada. Metode yang digunakan adalah model proses forensik (*The Forensic Process Model*) sebuah model proses investigasi forensik digital, yang terdiri dari tahap pengkoleksian, pemeriksaan, analisis dan pelaporan. Penelitian dilakukan selama lima bulan dengan mengambil data dari *Intrusion Detection System* (IDS) Snort. Beberapa *file* log digabungkan menjadi satu file log, lalu data dibersihkan agar sesuai untuk penelitian

2.2 Landasan Teori

2.2.1 Sistem Informasi

Sitem informasi adalah suatu sistem buatan manusia yang secara umum terdiri atas sekumpulan komponen berbasis komputer dan manual yang dibuat untuk menghimpun, menyimpan dan mengelola data serta menyediakan informasi keluaran kepada pemakai (Celinas et al, 1990).



Gambar 2.1 : Desain sistem informasi

Gambar 2.1 merupakan contoh sederhana dari arsitektur sebuah sistem informasi. Pada gambar tersebut dapat dilihat bahwa pengelola sistem informasi mengimpun dam menyimpan informasi dalam sebuah server. Kemudian dengan media berupa *website* pengelola sistem informasi menampilkan informasi yang telah dikelola sebelumnya. Sedangkan dari sisi pengguna, dapat mengakses informasi melalui

*website*dengan bantuan perangkat yang tersedia, seperti komputer *desktop,* laptop, maupun telepon genggam.

2.2.2 Situs Web

Web merupakan kumpulan dokumen-dokumen multimedia yang saling terhubung satu sama lain yang menggunakan protokol HTTP dan untuk mengaksesnya menggunakan browser (Charolina, 2011).Sejarah web sendiri dimulai pada tahun 1989 ketika Tim Berner Lee Fisikawan CERN (*Consei European pour la Recherce Nuclaire*) mengajukan protokol sistem distribusi informasi internet yang digunakan untuk berbagai informasi diantara para fisikawan. Protokol inilah yang selanjutnya dikenal sebagai Protokol*World Wide Web* dan dikembangkan oleh *World Wide Web Consortium*.(Jogiyanto,2005:284)

Pada mulanya aplikasi web dibangun hanya dengan menggunakan bahasa yang disebut HTML *(Hyper Text Markup Language*) dan protokol yang digunakan dinamakan HTTP (*HyperText Transfer Protokol*). Pada perkembangan berikut, sejumlah skrip dan objek dikembangkan untuk memperluas kemampuan HTML, antara lain PHP . Dengan memperluas kemampuan HTML, yakni dengan menggunakan perangkat lunak tambahan, perubahan informasi dalam halaman-halaman web dapat ditangani melalui perubahan data, bukan melalui perubahan program. Sebagai implementasinya, aplikasi web dikoneksikan ke basis data. Dengan demikian perubahan informasi dapat dilakukan oleh operator atau

yang bertanggung jawab terhadap kemutakhiran data, dan tidak menjadi tanggung jawab programer atau webmaster.

2.2.3 Content Management System

Sistem manajemen konten (*content management system*, disingkat CMS), adalah perangkat lunak yang digunakan untuk menambahkan atau memanipulasi isi dari suatu situs web.CMS merupakan*platform* situs web yang menerapkan sistem yang berorientasi terhadap konten. Karena sifat CMS yang berorientasi terhadap konten inilah saat ini sudah bukan merupakan kendala yang berarti bagi manajemen atau humassuatu perusahaan atau institusi untuk memperbaharui situs webnya. Dengan hak akses dan otoritas masing-masing, setiap bagian dari perusahaan/intitusi/organisasi dapat memberikan kontribusinya kedalam website tanpa prosedur yang sulit (Amin, 2014).

2.2.4 Structure Query Language

Berdasarkan ANSI (American National Standar Institute), maka SQL adalah bahasa standar untuk sistem manajemen database rasional. SQL merupakan kependekan dari *Structured Query Language*, bahasa pemrograman yang sering dipergunakan untuk mengelola database relasional.

Pernyataan-pernyataan SQL digunakan untuk melakukan beberapa tugas seperti update data pada database, atau menampilkan data dari

database. Beberapa software yang menggunakan SQL diantaranya,Oracle, Sybase, Microsoft SQL Server, Microsoft Access, dan Ingres. Setiap software database mempunyai bahasa perintah / sintaks yang berbeda, namun pada prinsipnya mempunyai arti dan fungsi yang sama. Perintah-perintah tersebut antara lain, "Select", "Insert", "Update", "Delete", "Create", dan "Drop", yang dapat digunakan untuk mengerjakan hampir semua kebutuhan untuk memanipulasi sebuah database (Irmansyah, 2003).

2.2.5 Structure Query Language Injection

Sql injection merupakan salah satu teknik *hacking* dengan cara memanipulasi sintaks SQL. Pada *sql injection* dilakukan dengan memasukan perintah – perintah yang digunakan dalam database melalui url(Efvy, 2015).

Pada dasarnya SQL Injection merupakan cara mengeksploitasi celah keamanan yang muncul pada level atau “layer” database dan aplikasinya. Celah keamanan tersebut ditunjukkan pada saat penyerang memasukkan nilai “string” dan karakter-karakter contoh lainnya yang ada dalam instruksi SQL. Dikatakan sebagai sebuah “injeksi” karena aktivitas penyerangan dilakukan dengan cara “memasukkan” string (kumpulan karakter) khusus untuk melewati filter logika hak akses pada website atau sistem komputer yang dimaksud.

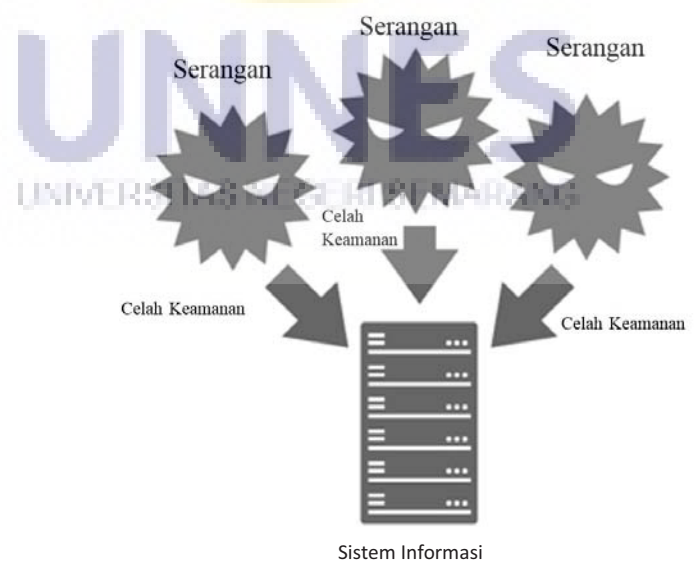
2.2.6 Terminologi – Terminologi Dasar dalam Keamanan Sistem

2.2.6.1 Vulnerability

Vulnerability adalah Kelemahan dari sebuah aset atau sekumpulan aset yang dapat dimanfaatkan oleh satu atau lebih ancaman (ISO 27005). Sedangkan menurut definisi dariIETF (Internet Engineering Task Force) melalui RFC 2828*vulnerability* adalah sebuah celah atau kelemahan dalam sebuah system, baik dalam desain, implementasi, atau operasional dan manajemen yang dapat dimanfaatkan untuk menyerang sebuah system informasi

2.2.6.2 Threat

Dalam definisi yang diungkapkan oleh Id-SIRTII/CC (2016) *threat* atau ancaman adalah segala sesuatu yang memiliki potensi untuk mengganggu jalannya operasi, fungsi, integritas atau ketersediaan sistem informasi.



Gambar 2.2 : Ilustrasi Ancaman Pada Sistem Informasi

2.2.7 Elemen – elemen keamanan

S'to.(2009) menyatakan bahwa keamanan dalam sistem terdiri dari tiga elemen yang seringkali disingkat menjadi CIA (*confidentiality, integrity, dan aviability*). Ancaman dari para penyerang adalah serangan terhadap ketiga elemen tersebut dan mengancam ketiga elemen tersebut.

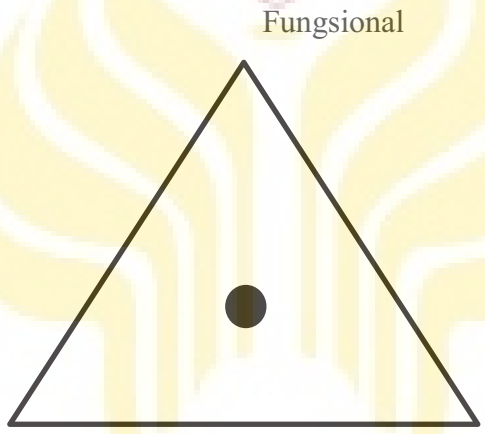
Confidentiality secara mudah dapat diartikan sebagai faktor kerahasiaan. Kerahasiaan dalam hal ini adalah kerahasiaan data, baik perusahaan seperti perbankan, korporasi dan lain lain, maupun kerahasiaan dari pengguna atau pelanggan seperti nasabah.

Integrity atau integritas dalam hal ini terkait dengan integritas perorangan maupun perusahaan terhadap sistem yang dimiliki maupun terhadap data yang dikirim. Dalam faktor data contohnya, penyerang bisa saja membajak sebuah pesan elektronik yang dikirim oleh suatu perusahaan terhadap perusahaan rekanannya. Dengan membajak pesan tersebut penyerang bisa mengganti pesan yang dikirimkan semau keinginan penyerang, dan hal seperti menjadi sangat berbahaya, karena perushaan tersebut akan kehilangan integritasnya terhadap perusahaan rekanannya.

Aviability terkait dengan dengan ketersediaan sistem, baik secara layanan sistem maupun secara personal sabg pembuat sistem. Jika seorang penyerang menyerang elemen keamanan sebuah sistem dan mengubahnya atau bahkan mematikan sebuah sistem, maka sistem tersebut akan terganggu elemen ketersediannya, bahkan bias saja sampai ke tahapa tidak dapat dihubungi sama sekali, yang berarti penyerang telah menghilangkan secara

penuh elemen ketersediaan dari korbannya. Itulah yang dimaksud dengan *aviability* atau elemen ketersediaan/ keberadaan.

Sebuah sistem pastilah diharapkan mempunyai kemudahan untuk digunakan oleh semua orang, fungsional, dan juga memiliki keamanan yang baik pula. Namun dalam kenyataanya, sebuah sistem hampir tidak mungkin memiliki ketiga poin diatas. Hubungan antara ketiga poin diatas akan digambarkan dalam segitiga dibawah ini.



Gambar 2.3 : Ilustrasi posisi suatu sistem informasi

Dalam segitiga diatas dapat dilihat bahawa ketika seorang perancang sistem ingin membuat sistem dengan mengutamakan sistem keamanan maka fungsi sebuah sistem dan kemudahan penggunaanya harus dikorbankan. Demikian pula jika sistem ingin diutamakan akan mudah digunakan, maka elemen keamanan dan fungsional akan dikorbankan.

Menentukan dimana letak sistem diletakan dalam segitiga tersebut sangatlah tergantung pada situasi dan kondisi yang ada. Dalam hal ini seorang perancang sistem dituntut unutk dapat menentukan keseimbangan antara ketiga elemen tersebut.

2.2.8 Analisis Keamanan Sistem Informasi

Secara umum dalam melakukan analisis pada sebuah elemen dalam sistem informasi ada dua metode yang digunakan, yaitu metode *white box testing* dan metode *black box testing*

2.2.8.1 White Box Testing

White box testing atau metode pengujian *white box* merupakan proses pengujian perangkat lunak dari sisi desain dan kode program (Trianjaya, 2013). Program diuji apakah mampu menghasilkan fungsi-fungsi yang sesuai dengan kebutuhan dan tidak mengalami kesalahan dari sisi program. Pengujian ini dilakukan dengan melakukan pemeriksaan logic dari kode program. Pengujian ini dilakukan secara langsung pada saat proses implementasi atau pengkodean. Dalam arti lain metode pengujian *white box* dapat dikatakan sebagai pengujian sistem dari dalam sistem.

2.2.8.2 Black Box Testing

Black boxtesting atau metode pengujian *black box* merupakan suatu strategi testing yang hanyamemperhatikan kepada faktor fungsionalitas dan spesifikasi dari perangkat lunak(Sunarya dan Destiani, 2016).Pengetahuan khusus dari kode aplikasi / struktur internal dan pengetahuan pemrograman pada umumnya tidak diperlukan. Dalam istilah lain, dapat dikatakan bahwa metode *black box testing* adalah sebuah metode pengujian sistem yang dilakukan diluar sistem.

BAB V

SIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian analisis keamanan sistem informasi berbasis wordpress terhadap serangan *sql injection* (studi kasus cahunnes.com) dapat disimpulkan bahwa :

1. Terdapat celah keamanan berupa *sql injection* terhadap situs – situs website di dunia
2. Serangan berbasis *sql injection* dapat membuat seorang penyerang mengetahui isi dari database walaupun tanpa akses yang legal
3. Dengan pengaman yang baik serangan berbasis *sql injection* dapat dicegah.
4. Situs berbasis wordpress terbukti memiliki keamanan yang baik dalam menghadapi serangan berbasis *sql injection*
5. Situs berbasis wordpress melakukan modifikasi pada *url* situs, sehingga tidak menampilkan *id* dalam database.
6. Situs berbasis wordpress melakukan *blocking* terhadap perintah *sql* pada alamat situs

5.2 Saran

Berdasarkan hasil penelitian, maka dapat diajukan beberapa saran untuk masyarakat, baik seorang *web developer* maupun masyarakat awam, adapun sarannya adalah sebagai berikut :

1. Memberikan perhatian yang lebih terhadap keamanan *website* yang dikembangkan
2. Mengganti alamat dari halaman admin, agar walupun keamanan situs berhasil ditembus, penyerang tetap kesulitan dalam melanjutkan penyerangan
3. Untuk para profesional maupun awam, dapat menggunakan fasilitan CMS wordpress dalam mengbangun situsnya, karena wordpress memiliki sistem keamanan yang baik.

DAFTAR PUSTAKA

Amin,F.2014.**Rekayasa Website Teater Institut Seni Indonesia (Isi) Yogyakarta Dengan Content Management System (Cms) Wordpress**.*Jurnal Dinamika Informatika* 16(2).

Jogiyanto. 2008. **Sistem Teknologi Informasi. Penerbit** ANDI. Jakarta

Lumanto, R. 2016. **Internet *Protection & Safety***. *APJII Open Policy Meeting.* 30 Mei. Batam

Nugroho, B.A. 2012. **Analisis Keamanan Jaringan Pada Fasilitas Internet(Wifi) Terhadap Serangan Packet Sniffing**, *skripsi*.Program S1 Teknik Informatika Universitas Muhammadiyah Surakarta.Sukoharjo.

Putri,R.U, dan J.E. Istiyanto. 2012. **Analisis Forensik Jaringan Studi Kasus Serangan *SQL Injection* pada Server Universitas Gadjah Mada**. *Jurnal Teknik Informatika.* 6(2) : 101-112.

S'to. 2009. ***Certified Ethical Hacker 100% illegal***. Penerbit Jasakom. Jakarta

Yudistira, A. 2012. **Analisis Keamanan Otentikasi dan Basis Data pada Web Simple-o Menggunakan Sql Injection**.*skripsi*, Program S1 Teknik KomputerUniversitas Indonesia, Depok.

Zam, E. 2015. ***Hacking Aplikasi Web : Uncensored***. Penerbit Jasakom. Jakarta