JURNAL SISTEM INFORMASI DAN TEKNOLOGI
(S I N T E K)

Situs Jurnal
https://sintek.stmikku.ac.id/index.php/home

PENGEMBANGAN MANAJEMEN KEAMANAN INFORMASI DATABASE DAN APLIKASI DENGAN OPTIMASI KEAMANAN WEBSITE

Willy Andrian[1] , Dedy Prasetya Kristiadi[2]

[1]Departemen Sistem Informasi,
·STMIK Kuwera, Jl. Kalideres Permai Jakarta Barat
,[2]Computer Systems Department
Raharja University
[1]andrianwilly33@gmail.com,[2]dedy.prasetya@raharja.info

Abstrak

Sistem Informasi yang taerdapat pada perusahaan memiliki pengaruh besar dalam kemajuan perusahaan maupun instansi lainnya. Sistem informasi ini berkontribusi sebagai *supplier* sekaligus pengolah yang menghasilkan keluaran berupa data penting sebagai bahan kajian maupun analisis yang terusdiproses untuk menghasilkan sesuatu yang berkualitas. Misalnya,informasi penjualan,produksi dan bahan yang berpengaruh terhadap keberlangsungan hidup perusahaan. Oleh karna itu, keamanan informasi *Virtual Private Server* atau VPS pada database dan aplikasi penting perusahaan yang berisi data dan aplikasi untuk customer atau client menjadi sangat penting untuk dipelajari dan selalu dikembangkan agar system informasi tetap terjamin. Model penelitian ini adalah penelitian eksperimen dimana aplikasi SQLMap dan Shell.php digunakan sebagai alat untuk pencobaan penetrasi website yang selanjutnya akan diteruskan sampai pembobolan VPS Penelitian ini bertujuan untuk menganalisis celah sekuritas VPS dan website yang dapat dimanfaatkan oleh para pembobol atau hacker untuk melakukan tindakan yang bersifat merusak atau tindak pencurian data. Penelitian ini diawali dengan analisis yang akan digunakan sebagai acuan atau parameter dalam pengamanan server oleh developer maupun security tester. Hasil dari penelitian ini adalah identifikasi permasalahan utama yang menjadi kendala perusahaan dalam mengamankan website dan VPS, celah keamanan yang teridentifikasi, langkah-langkah pengamanan serta dampak yang ada oleh karena pengamanan dan tanpa pengamanan
.

Kata kunci: keamanan informasi, *virtual private server, sql injection, sqlmap, shell php*

1. PENDAHULUAN

Persaingan bisnis pada bidang teknologi informasi terus meningkat sejalan dengan perkembangan teknologi itu sendiri. Teknologi informasi yang digunakan pada sebuah perusahan dapat menjadi indiator perkembangan perusahaan dan kemampuan

perusahaan dalam melindungi infrastruktur yang berupa teknolgi informasi dalam menstabilkan keunggulan bisnis.
Keunggulan terhadap daya saing diyakini telah dimiliki oleh suatu perusahaan jika seluruh kegiatan yang dilakukan melibatkan teknologi informasi yang baik dan mendapatkan informasi sebanyak-banyaknya untuk kebutuhan perusahaan[1]. Namun demikian, perusahaan juga memiliki pesaing yang terus menerapkan strateginya demi mendapatkan keuntungan yang lebih besar. Strategi yang diterapkan tak jarang merujuk pada investasi teknologi dan informasi[2]. Pada umumnya perusahaan tidak dapat mempertahankan keunggulan tersebut dalam suatu periode tertentu hal ini disebabkan oleh beberapa faktor. Salah satunya adalah teknologi dan sistem informasi yang tidak mendukung percepatan proses perusahaan dalam menghadapi persaingan.

Perusahaan dianggap mampu mencapai tujuan utamanya yaitu memperoleh penghasilan di atas rata-rata, jika dalam mencapai keunggulan daya saing tersebut berhasil mengeksploritasikan keunggulannya. Penghasilan di atas rata-rata adalah penghasilan berupa keuntungan yang diharapkan oleh seorang investor harapkan dari sebuah investasi dengan resiko yang sama. Resiko adalah ketidak pastian investor secara ekonomis apakah keuntungan atau kerugian yang dihasilkan dari sejumlah investasi [3].

Sementara itu,sejalan dengan perkembangan teknologi informasi dan komunikasi maka segala bentuk data dan informasi serta perangkatnya yang berkaitan dengan pengembangan perusahaan menjadi investasi yang penting[4]. Pengembangan tersebut dapat berupa infrastruktur jaringan,aplikasi,alat komunikasi dll. Peningkatan peralatan komunikasi dan aplikasi sebagai akibat meningkatnya kebutuhan mausia dalam berinteraksi kepada sesamanya dalam bentuk transaksional maupun sosial. Kehadirnn teknologi juga mendukung peradaban manusia menuju modernisasi yang memberikan peluang akan lahirnya ide-ide bisnis baru. Selanjutnya,muncul ide-ide seputar penyedia jasa pengadaan infrastruktur teknologi informasi dan komunikasi berupa jaringan sekaligus maintenance[5]. Hal ini menggambarkan bahwa betapa penntingnya infrastruktur system informasi pada suatu perusahaan sebagai asset yang harus dijaga dan dikembangkan.

Dengan adanya teknologi yang memadai, bisnis-bisnis berbasis teknologi informasi pun banyak bermunculan seperti startup, dimana mereka menggunakan teknologi informasi yang ada untuk dapat memberikan layanan ataupun produk dalam bentuk digital guna meningkatkan nilai jual dari suatu perusahaan[6]. Salah satu jenis bidang usaha yang cukup sering dilakukan oleh startup adalah bidang software house. Dalam operasionalnya, bisnis bidang software house selalu menggunakan teknologi database sebagai tempat penyimpanan data transaksi secara digital serta server sebagai tempat penyimpanan aplikasi dan data. Server sendiri terbagi menjadi *cloud server* dan *physical server*. Namun, terlebih dari semua itu, keamanan data dan aplikasi merupakan hal penting yang harus dijaga dan dikembangkan agar bisnis ini dapat terus berjalan[7].

Penelitian ini akan membahas analisa keamanan data dan aplikasi yang ada pada perusahaan ini, identifikasi masalah-masalah yang menjadi kendala dalam melakukan pengamanan dan bagaimana cara untuk mengatasi masalah keamanan tersebut serta dampak yang ditimbulkan.

2. Teori dan Literatur

2.1 Informasi

Informasi adalah data yang berupa gambar,suara,tulisan yang telah diolah menjadi sesuatu yang bermanfaat bagi penerima sekaligus dalam pengambilan keputusan. Dengan demikian informasi adalah gabungan data yang memiliki berbagai bentuk sebagai bahan untuk pengambilan keputusan.
Menurut Sutabri (2012:29) “Teori informasi lebih tepat disebut sebagai teori matematis dan komunikasi, sumber informasi adalah data”. Informasi adalah

sebuah istilah yang tepat dalam pemakaian umum, mengenai data mentah, data tersusun, kapasitas sebuah saluran komunikasi, dan lain sebagainya. Informasi juga mencakup mengenai data yang telah diklasifikasikan atau diinterpretasi untuk digunakan dalam proses pengambilan keputusan.

2.2 Database

Database adalah sekumpulan data tersebar yang berhubungan secara logis, dan penjelasan dari data ini dirancang untuk memenuhi kebutuhan informasi dari suatu organisasi. *Database* merupakan "kumpulan dari data yang saling berhubungan satu dengan yang lainnya, tersimpan di simpanan luar komputer dan digunakan perangkat lunak tertentu untuk memanipulasinya". *Database* merupakan salah satu komponen yang penting di sistem informasi, karena berfungsi sebagai basis penyedia informasi bagi para pemakainya. Penerapan *database* dalam sistem informasi disebut dengan *database system*[8].

3. Metode

Metode penelitian merupakan komponen yang penting untuk mendapatkan data hasil penelitian. Metode penelitian yang digunakan adalah metode kualitatif. Dengan metode ini penulis melakukan observasi dan wawancara secara langsung dengan tujuan mendapatkan informasi yang dibutuhkan secara akurat. Metode observasi Melakukan peninjauan langsung dengan mempelajari sistem informasi yang sudah berjalan.Studi Pustaka mempelajari referensi jurnal, buku, dan *e-book* yang berkaitan langsung .Metode Wawancara Mengadakan tanya jawab kepada pengguna dan pembuat aplikasi untuk mendapatkan informasi lebih lanjut tentang pengambilan data.

Metode prototipe (*Prototyping*) adalah sebuah metode dimana penulis dapat menggambarkan sistem yang akan dibuat sehungga dapat mudah dimengerti oleh calon pengguna. Metode prototipe yang digunakan untuk menunjang penelitian ini adalah metode *sketching* dimana penulis membuat sebuah sketsa dari sistem yang diusulkan ke calon pengguna.

Identifikasi masalah dalam penelitian ini adalah: (1) Aplikasi website yang tidak aman, cenderung mudah ditembus dan rentan dibobol sampai ke database hingga server penyimpanan itu sendiri. Beberpapa perusahaan atau institusi tidak memiliki prosedur untuk melakukan quality check pada sekuritas website. (2) Aplikasi live atau production untuk client disimpan dalam satu Virtual Private Server yang sama. Jika terdapat salah satu saja website yang dibobol, maka dapat saja terjadi pencurian atau perusakan data pada keseluruhan isi VPS. (3) Enterprise tidak memiliki staff yang expertise dalam menjaga sekuritas website.

4. PEMBAHASAN

VPS atau *Virtual Private Server* berawal dari sebuah server yang dibagi menjadi beberapa virtual server yang dapat digunakan untuk berbagai keperluan layaknya server fisik, seperti penginstalan sistem operasi, tempat penyimpanan database ataupun sebagai server hosting (dedicated hosting). Manajemen VPS dapat dilakukan dengan menggunakan software seperti WinSCP. Pada perusahaan umumya VPS dimanfaatkan sebagai media penyimpanan database serta aplikasi web yang akan digunakan oleh client dalam operasionalnya. Oleh karena itu, pengamanan website dan server menjadi hal yang sangat kritis agar dapat memastikan data dan aplikasi client tidak bocor kepada pihak yang tidak bertanggung jawab. Namun berdasarkan penelitian yang dilakukan, keadaan yang terjadi justru sebaliknya, dimana bisnis telah berjalan sebelum aplikasi melewati masa security check. Hal ini jika dibiarkan akan mengakibatkan pencurian data oleh pihak luar, kerusakan data dan beberapa akibat lainnya. Dari penelitian yang dilakukan, juga ditemukan alasan-alasan yang menjadi permasalahan dalam membuat prosedur pengamanan website dan server, yaitu sebagai berikut:

(1) Belum ditetapkannya prosedur atau standar

dalam pengamanan aplikasi.
(2) Tidak memiliki karyawan yang mengerti dasar pengamanan aplikasi berbasis cloud.
(3) Jumlah karyawan yang sedikit mengakibatkan karyawan harus mengerjakan banyak hal dan kekurangan waktu dalam mempelajari pengetahuan baru mengenai sekuritas.
(4) Tidak adanya knowledge management system sebagai dokumentasi untuk kemudian hari.

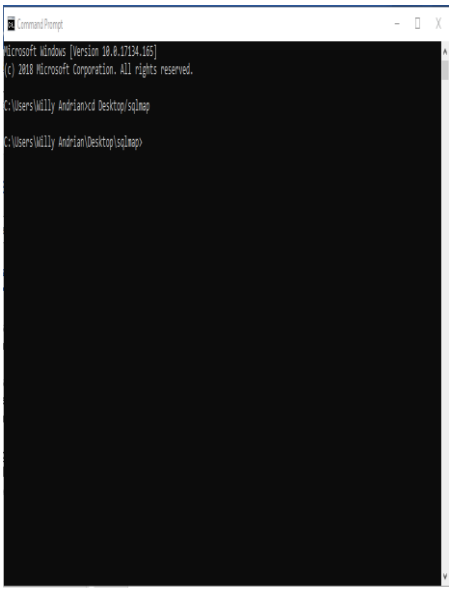
Sementara itu, informasi-informasi penting yang terdapat pada server adalah sebagai berikut:

(1) Database: Database client yang telah terintegrasi dengan aplikasi, memuat transaksi operasional client.
(2) Konfigurasi server: Merupakan data yang menentukan bagaimana suatu aplikasi dapat mengkakses database yang ada serta manajemen server lainnya.
(3) Aplikasi / Produk: Merupakan aplikasi live yang dihosting dalam server untuk digunakan oleh client / user.
(4) Dokumen: Dokumen pendukung bisnis seperti MOU (Memorandum of Understanding).

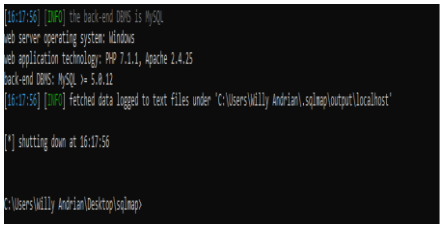
Dalam konteks PT. XYZ, server yang aman tidak sepenuhnya menjamin tidak akan terjadi pembobolan. Server yang digunakan sebagai hosting website dapat saja bobol jika website yang dihosting tidak aman. Penelitian yang dilakukan pada PT. XYZ menunjukkan bahwa aplikasi atau website perusahan tersebut rentan mengalami serangan berikut dari pembobol:

(1) **XSS (Cross Site Scripting):** Merupakan cara penyerangan keamanan website dengan menginjeksi atau memasukkan script pada website melalui form yang ada.
(2) **SQL Injection:** Merupakan serangan keamanan yang memanfaatkan statement SQL yang tidak tepat.
(3) **Shell Injection:** Merupakan serangan keamanan yang memanfaatkan kesalahan code atau memanfaatkan celah validasi pada file upload.

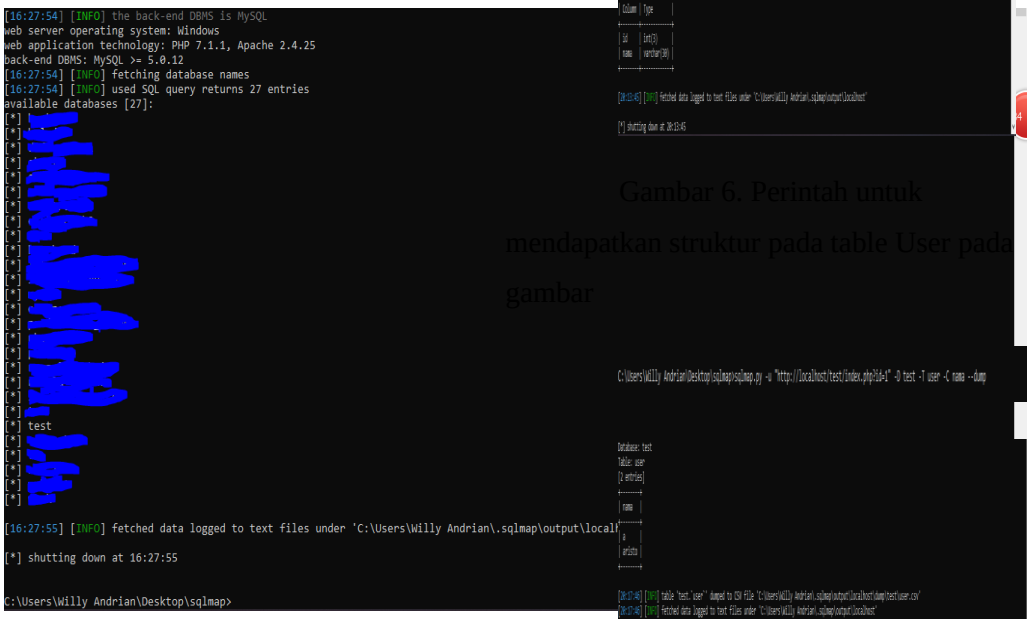
Berikut merupakan salah satu contoh proses eksperimen untuk mengeksploitasi keamanan website dan server pada PT. XYZ menggunakan teknik SQL Injection dengan menggunakan bantuan aplikasi SQLMap:



Gambar 1. Posisi awal pada command prompt.



Gambar 2. Melakukan Pengecekan Spesifikasi Terhadap Server.



Gambar 4 Perintah untuk mendapatkan list database pada server target.

Gambar 5. Perintah untuk mendapatkan list table pada database yang telah didapatkan pada gambar

Gambar 6. Perintah untuk mendapatkan struktur pada table User pada gambar

Gambar 7. Perintah untuk mendapatkan isi tabel yang telah didapatkan sebelumnya

Berdasarkan proses diatas, dapat disimpulkan bahwa keamanan website yang lemah dapat mengakibatkan terjadinya pencurian data yang dapat merugikan perusahaan hingga terjadi pengrusakan lanjutan. Secara teknis, pembobolan dimungkinkan karena form pada website belum disanitasi atau belum diberi validasi agar tidak membaca tanda petik yang masuk ke form sebagai bagian dari perintah SQL. Hal ini dapat diatas dengan menggunakan fungsi *MYSQL_REAL_ESCAPE_STRING*.

Namun secara garis besar, berikut merupakan hal-hal yang dapat dilakukan

untuk meningkatkan keamanan website dan server

(1) Melakukan *training* pada karyawan agar pengetahuan tentang sekuritas dapat ditingkatkan.
(2) Membuat prosedur testing sekuritas aplikasi sebagai bagian dari *quality control.*
(3) Memasang f*irewall* pada VPS.
(4) Melakukan validasi kelayakan code seperti memastikan bahwa fungsi mengupload gambar hanya dapat digunakan untuk mengupload file berekstensi .jpg, .png ataupun ekstensi file gambar lainnya.
(5) Melakukan backup database secara berkala agar dapat melakukan restorasi jika terjadi kerusakan data.
(6) Membuat password dengan kombinasi unik.

5. PENUTUP

Keamanan system informasi menjadi kebutuhan yang harus segera diselesaikan agar pengguna dapat dengan nyaman menggunakan aplikasi yang telah disediakan oleh perusahaan. Persaingan bisnis maupun dan pengelolaan keamanan system yang buruk dapat menyebabkan data dicuri maupun sabotase. Oleh karena itu pengaanan terhadap system informasi yang meliputi system database,jaringan dan hak pengguna menjadi prioritas dalam system informasi. Selain itu keamanan data juga salah satu jaminan kepercayaan terhadap perusahaan. Selain itu keamanan informasi dan kenyamanan pengguna menjadi kunci penentu perusahaan dalam menjaga kualitasnya.

DAFTAR PUSTAKA

[1] Azwar Aziz.2011.' Pemanfaatan Teknologi Informasi dalam Pengembangan Bisnis Pos information technology utilization in business post development, https://media.neliti.com/media/publications/41157-ID-pemanfaatan-teknologi-informasi-dalam-pengembangan-bisnis-pos.pdf. Di download tanggal 22-11-2022
[2] Daryanto. 2010. "*Teknologi Jaringan Internet*". Bandung: Satu Nusa.
[3] Tolle, Herman. 2008. *"Pengantar Sistem Pakar*

[3] Safaat, Nazruddin. 2012. "Pemrograman aplikasi *mobile smartphone* dan tablet PC berbasis *Android*". Bandung: Informatika.
[4] Kusrini. 2010. *"Sistem Pakar Teori Dan Aplikasi"*. Yogyakarta: Andi.
[5] Kusrini. 2009. *"Menentukan Faktor Kepastian Pengguna Dengan Metode Kuantifikasi Pertanyaan"*. Yogyakarta: Andi.
[6] Nugroho, Adi. 2010. *"Analisis Perancangan Sistem Informasi dengan Metodologi Berorientasi Object".* Bandung: Informatika.
[7] Henderi. 2009. "*Unified Modeling Language".* Tangerang.
[8] Iwan Sofana. 2012. "*CISCO CCNA & Jaringan Komputer*," Bandung : Informatika. Jadibaru. 2015. "*Pengenalan Android Studio*". http://www.jadibaru.com/android/pengenalan-android-studio-2/. Diakses tanggal 11 Nov 2021.
[9] Yuliana, O. Y. Penggunaan Teknologi Internet. J. Akunt. Dan Keuang. 2, 36–52 (2000)