ANALISIS KEAMANAN WEB SERVER TERHADAP WEBSITE PT. VICTORY INTERNASIONAL FUTURES MALANG DENGAN TEKNIK SQL INJECTION

Nurhayati Rumaf[1)], Khoerul Anwar [2)], Dwi Safiroh Utsalina [3)]
[1,2]Program Studi Teknik Informatika [1)], STIMIK PPKIA Pradnya Paramita Malang
rumafnurhayati@yahoo.co.id, aqhoir@stimata.ac.id
[3]Program Studi Sistem Informasi STIMIK PPKIA Pradnya Paramita Malang
utsalina@stimata.ac.id

Abstract:
SQL injection is an activity insert the SQL command to an existing SQL statement in the application that is running . In other words, SQL injection is a technique exploiting the web apilikasi which also uses a database for data storage . SQL injection technique allows one to log into the system without having to have an account. The method used in the analysis of web server security on the website PT.Victory International Futures with SQL Injection technique is the method of qualitative data collection through library are like a book , which contains information and theory as well as journal articles and similar studies are published on the website - the official site and reliable as supporting the completion of the study , berexplorasi in identifying weaknesses or loopholes in websites or web server that allow SQL Injection attacks. The results of the study of security analysis techniques webserver with " SQL Injection " aims to determine whether the webserver or the website is vulnerable to SQL Injection attacks , or vice versa , so that website owners can perform maintenance and repairs so that website owners be wary of internet crime.

***Keywords** : web server , website , security , SQL Injection*

Pendahuluan

Keamanan suatu webserver atau web *security* system merupakan salah satu prioritas yang utama bagi aplikasi berbasis web. Jika seorang administrator jaringan mengabaikan keamanan suatu web server, maka *hacker* dapat mengambil data-data penting pada server tersebut dan bahkan pula dapat mengacak-acak isi dari web tersebut. Web Server yang merupakan host yang paling banyak menjadi sasaran target serangan dalam teknologi internet saat ini. Web server merupakan hal yang berperan penting pada sebuah website karena Web Server berisi Web Pages di dalamnya mengandung informasi atau dokumen yang ingin disebarluaskan oleh para Pengguna. Ancaman keamanan secara spesifik terhadap Web server umumnya terbagi menjadi beberapa kategori diantaranya : Entitas *malicious*, serangan *Denial of Service* (DoS), Informasi sensitif pada Web server, Informasi sensitif di database, Informasi sensitif yang ditransmisikan tanpa di enkripsi antara Webserver, *Command Injection, SQL (Structrured Query Language), lightweight Directory Access Protocol(LADP),* dan *cross sites cripting (XSS),* Serta *Defacement* (penggantian tampilan). Serangan *hacker* diakibatkan kurangnya perhatian tentang sistem keamanan web server oleh pembuat website, dan atau pemilik website. Serangan terhadap web server dapat juga dialami oleh PT. Victory Internasional Futures perusahaaan yang bergerak di bidang investasi Foreign Exchange (Forex), Index Futures, dan Comodity. Dengan demikian, perusahaan ini menggunakan website sebagai media interaksi dan sarana promosi. Untuk itu dilakukan analisis terhadap keamanan website PT. Victory Internasional Futures Malang dimana aspek keamanan yang diteliti adalah *Web Server* dengan metoda Kualitatif menggunakan teknik *SQL Injection*. *SQL Injection* adalah suatu teknik mengeksploitasi web aplikasi yang di dalamnya menggunakan database sebagai penyimpanan datanya. *SQL Injection* mengijinkan *user* tidak sah (penyerang) untuk mengakses *database*. *SQL Injection* juga memungkinkan seorang *attacker* merubah, menghapus, maupun menambahkan data–data

pada *website* tanpa harus memiliki *account* sebagai admin.

Rumusan Masalah

Rumusan masalah yang dapat diambil dari latar belakang yang telah diuraikan diatas adalah :

1. Bagaimana menganalisis sistem keamanan Web server pada website PT.Victory Internasional Futures Malang dengan teknik SQL Injection ?
2. Bagaimana menginformasikan hasil analisis penelitian kepada PT. Victory Internasional Futures Malang ?

Tujuan Penelitian

Tujuan penelitian ini adalah :

1. Menganalisis kelemahan dan kelebihan sistem keamanan *Web Server* pada *website* PT.Victory Internasional Futures Malang dengan teknik *SQL Injection*.
2. Menginformasikan hasil analisis penelitian kepada PT.Victory Internasional Futures Malang.

Manfaat Penelitian

Manfaat penelitian ini terdiri dari dua jenis diantaranya sebagai berikut :

a. Manfaat bagi PT.Victory Internasional Futures Malang :
   PT.Victory Internasional Futures Malang dapat memperoleh informasi tentang serangan – serangan yang mungkin terjadi pada *web server* mereka, dan aman atau tidak amannya *web server* tersebut. Sehingga PT. Victory Internasional Futures Malang dapat melakukan percegahan dan pemeliharaan terhadap *website*, untuk menjaga kerahasian data nasabah, data penting perusahaan, dan Pemilik *website* lebih waspada terhadap kejahatan di internet.
b. Manfaat Bagi Dunia Pendidikan
   Teknik *SQL injection* dan *SQL Map* ini dapat dikembangkan sebagai Ilmu, Referensi, dan Metode Analisis permasalahan keamanan internet, hasil analisis dapat digunakan sebagai literatur atau perbandingan dalam penelitian selanjutnya.

Web server

teknologi web berkembang menjadi alat bantu yang tidak hanya mampu menyediakan informasi, namun juga mampu untuk mengolah informasi. Proses pengolahan informasi dengan memanfaatkan web menyebabkan web menjadi media informasi yang dinamis. Hal ini membutuhkan sarana teknis yang bergantung pada penggunaan perangkat lunak yang kuat, aman, terpercaya, dan cepat. Perangkat lunak penentu yang dibutuhkan antara lain adalah sebuah *Web server* yang disebut juga sebagai *HTTP server*, karena menggunakan *protocol HTTP* sebagai basisnya.

Web server adalah sebuah bentuk server yang khusus digunakan untuk menyimpan halaman *website* atau *homepage*. Web adalah jaringan *client server* interaktif yang menggunakan teknologi *World Wide Web* (pengguanaan *hypetext* dan *graphic* secara bersamaan untuk menampilkan informasi (abdul kadir, 2008 : 2).

Website

Website (Situs Web) merupakan alamat (*URL*) yang berfungsi sebagai tempat penyimpanan data dan informasi dengan berdasarkan topik tertentu situs atau web dapat dikategorikan menjadi 2 yaitu :

Web Statis, yaitu : Web yang berisi atau menampilkan informasi – informasi yang sifatnya statis (tetap)

Dan web dinamis, yaitu : Web yang menampilkan informasi serta dapat berinteraksi dengan *user* yang bersifat dinamis.

Aplikasi Web

Aplikasi web adalah aplikasi yang disimpan dan dieksekusi dilingkungan *webserver* Setiap permintaan yang dilakukan oleh *user* melalui aplikasi *client (web browser)* akan direspon oleh aplikasi web dan hasilnya akan dikembalikan lagi ke hadapan *user* dengan aplikasi web, halaman yang tampil di layar *web browser* dapat bersifat dinamis, tergantung dari nilai data atau parameter yang dimasukan oleh *user* (Budi Raharjo, Imam Heryanto, Ejang RK, 2010 : 40).

Http

HTTP (*Hypertext Transfer Protocol*) merupakan protokol yang digunakan untuk mendistribusikan sistem informasi yang berbasis *hypertext* Protokol ini merupakan protokol standar yang digunakan untuk mengakses *HTML*. *HTTP* diprakarsai oleh *World Wide Web* sistem informasi yang menyeluruh sejak tahun 1990. Apabila pada penjelajahan web dan pada alamat tertulis *http://www.google.com* ini merupakan salah satu penggunaan protokol *HTTP* dalam web.

Internet

Internet atau *Interconnected Networking* merupakan dua komputer atau lebih yang saling berhubungan membentuk jaringan komputer hingga meliputi jutaan komputer di dunia, yang saling berinteraksi dan bertukar informasi.

Situs dapat diartikan sebagai kumpulan halaman-halaman yang digunakan untuk menampilkan informasi, gambar gerak, suara, dan atau gabungan dari semuanya itu baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan *link-link*. Unsur-Unsur *Website* atau Situs yang harus ada agar situs dapat berjalan dengan baik dan sesuai yang diharapkan situs antara lain:

Domain Name.

Domain name atau biasa disebut nama domain adalah alamat permanen situs di dunia *internet* yang digunakan untuk mengidentifikasi sebuah situs atau dengan kata lain *domain name* adalah alamat yang digunakan untuk menemukan situs kita pada dunia *internet*. Istilah yang umum digunakan adalah *URL*. Contoh sebuah *URL* adalah *http://www.yahoo.com* (dapat juga tanpa www). *domain name* yang berakhiran dengan *.Com .Net .Org .Edu .Mil* atau *.Gov*. Jenis *domain* ini sering juga disebut *top level domain* dan *domain* ini tidak *berafiliasi* berdasarkan negara, sehingga siapapun dapat mendaftar. (*.com)* merupakan *top level domain* yang ditujukan untuk kebutuhan "*commercial*". (*.edu)* merupakan *domain* yang ditujukan untuk kebutuhan dunia pendidikan "*education* ", (*.gov)* merupakan *domain* untuk pemerintahan "*government*", (*.mil*) merupakan *domain* untuk kebutuhan angkatan bersenjata "*military*", (*.org* : domain untuk organisasi atau lembaga *non profit* "*Organization*".

Country-Specific Domains. *domain* yang berkaitan dengan dua huruf ekstensi, dan sering juga disebut *second level domain*, seperti *.id* (Indonesia), *.au*(Australia), *.jp*(Jepang) dan lain lain. *Domain* ini dioperasikan dan di daftarkan disetiap negara. Di Indonesia, *domain-domain* ini berakhiran, *.co.id*, *.ac.id*, *.go.id*, *.mil.id*, *.or.id*, dan pada akhir-akhir ini ditambah dengan *war.net.id*, *.mil.id,* dan *web.id*. Penggunaan dari masing-masing akhiran tersebut berbeda tergantung pengguna dan pengunaannya, antara lain: *(.co.id),* untuk Badan Usaha yang mempunyai badan hukum sah, *(.ac.id),* untuk Lembaga Pendidikan, *(.go.id)* Khusus untuk Lembaga Pemerintahan Republik Indonesia *(.mil.id)*, Khusus untuk Lembaga Militer Republik Indonesia, (*.or.id*) untuk segala macam organisasi yand tidak termasuk dalam kategori (*ac.id, co.id, go.id, mil.id*), (*.war.net.id*), untuk industri warung *internet* di Indonesia (*.sch.id)* khusus untuk Lembaga Pendidikan yang menyelenggarakan pendidikan seperti SD, SMP dan atau SMU, (*.web.id*) Ditujukan bagi badan usaha, organisasi ataupun perseorangan yang melakukan kegiatannya di *Worl Wide Web.* Nama *domain* dari tiap-tiap situs di seluruh dunia tidak ada yang sama sehingga tidak ada satupun situs yang akan dijumpai tertukar nama atau tertukar halaman situsnya. Untuk memperoleh nama dilakukan penyewaan *domain*, biasanya dalam jangka waktu tertentu (tahunan).

Hosting

Hosting dapat diartikan sebagai ruangan yang terdapat dalam harddisk tempat menyimpan berbagai data, file-file, gambar dan lain sebagainya yang akan ditampilkan disitus. besarnya data yang bisa dimasukkan tergantung dari besarnya *hosting* yang disewa/dipunyai, semakin besar *hosting* semakin besar pula data yang dapat dimasukkan dan ditampilkan dalam situs.

***Scripts*/Bahasa Program**

Scripts adalah bahasa yang digunakan untuk menerjemahkan setiap perintah dalam situs yang pada saat diakses. Jenis *scripts* sangat menentukan statis, dinamis atau interaktifnya sebuah situs. Semakin banyak ragam *scripts* yang digunakan maka akan terlihat situs semakin dinamis, dan interaktif serta terlihat bagus. Bagusnya situs dapat terlihat dengan tanggapan pengunjung serta frekwensi kunjungan. Jenis - jenis *scripts* yang banyak dipakai para *designer* antara lain *HTML, ASP, PHP, JSP, Java Scripts, Java applets* dsb.

Design Web

Setelah melakukan penyewaan *domain* dan *hosting* serta penguasaan *scripts*, unsur situs yang paling penting dan utama adalah *design. Design* web sangat menentukan kualitas dan keindahan situs. *Design* sangat berpengaruh kepada penilaian pengunjung akan bagus tidaknya sebuah *web site.*

MySQL

MySQL adalah salah satu jenis database server yang menggunakan *SQL* sebagai bahasa dasar untuk mengakses databasenya. Selain itu, ia bersifat open source (tidak perlu membayar untuk menggunakannya) pada berbag *platform* kecuali untuk jenis *enterprise*, yang bersifat komersial (Abdul Kadir, 2008 : 348).

MySQL termasuk jenis *RDBMS* (*relational database management system*). Itulah sebabnya istilah seperti tabel, baris dan kolom digunakan pada *MySQL*. Pada *MySQL*, sebuah database mengandung satu atau lebih beberapa kolom. *MySQL* merupakan sebuah implementasi dari sistem manajemen basis data *relasional* (*RDBMS*) yang didistribusikan secara gratis dibawah *lisensi GPL* (*General Public License*). *Menurut* (Budi Raharjo, Imam Heryanto, Ejang RK, 2010 : 216) *SQL* (*Structured Query Language*) adalah sebuah konsep pengoperasian basisdata, terutama untuk pemilihan atau seleksi dan pemasukan data, yang memungkinkan pengoperasian data dikerjakan dengan mudah secara otomatis.

SQL Injection

SQL injection adalah kegiatan menyisipkan perintah *SQL* kepada suatu *statement SQL* yang ada pada aplikasi yang sedang berjalan. Dengan kata lain *SQL injection* ini merupakan suatu tehnik pengeksploitasi pada web apilikasi yang didalamnya menggunakan database untuk penyimpanan datanya. Terjadinya *SQL injection* tersebut dikarenakan *security* atau keamanan pada level aplikasi (dalam hal ini aplikasi web) masih kurang sempurna. Kurang sempurnanya adalah pada cara aplikasi meng-*handle* inputan yang boleh diproses ke dalam *database*. Misalnya pada suatu web yang terdapat fasilitas *login*, terdapat dua buah inputan pada umumnya, yaitu *username* dan *password*. Jika karakter yang masuk melalui dua buah inputan tersebut tidak disaring dengan baik maka bisa menimbulkan efek *SQL injection*, ini dikarenakan biasanya inputan tersebut secara sistem akan menjadi bagian dari kriteria dari suatu perintah *SQL* di dalam aplikasi web-nya. Secara garis besar terjadinya *SQL injection* tersebut adalah sebagai berikut:

1) Tidak adanya penyaringan terhadap karakter – karakter tanda petik satu (**'**) dan juga karakter *double minus* (--) yang menyebabkan suatu aplikasi dapat disisipi dengan perintah *SQL*.

2) Sehingga seorang *Hacker* dapat menyisipkan perintah *SQL* kedalam suatu parameter maupun pada *text area* suatu *form*

Default Setting SQL

Seperti yang kita ketahui bahwa tehnik *SQL injection* ini memungkinkan seseorang dapat *login* kedalam sistem tanpa harus memiliki *account*. Salah satunya yaitu *default setting SQL*. *Default setting SQL* yang paling berbahaya adalah menggunakan *adminID = sa* dan *password blank alias* (kosong), apabila ada direktori sebuah situs yang disitu ada *input* untuk adminnya, maka jika kita isi *id*-nya dengan = *'sa'* dan *password*nya =*' '* maka kita langsung masuk sebagai *admin*, ini kalau *default setting*-nya belum diubah. Namun ada lagi *string* yang bisa kita *input* untuk akses sebagai web *admin* yaitu dengan *string ' OR 1=1--* apabila ada *input* web *admin* yang *input box*-nya adalah *User* dan *Password* maka apabila kita masukan *string ' OR 1=1--* di *input box user* dan masukan *foobar* di *input box password*, maka akan membuat *SQL query*-nya bingung diakibatkan jadi *SQL Query*

membacanya sebagai : **SELECT * from users where User ='' or 1=1-- and Password ='foobar'** yang artinya *SQL*nya men-*SELECT* semua *query* dari *user* yang *user*-nya **''** (kosong) atau (**OR**) **1=1 (true) --** (tanda **--** adalah *mark* dari *SQL* seperti halnya di *C/C++ marknya // atau /*)*

Gambar 1. Contoh ilustrasi SQL injection Pada admin login area

Jadi kalau diuraikan logikanya adalah bahwa *SQL*-nya menganggap ***1=1*** sebagai *true* sehingga kolom itu di-*bypass* lalu kolom *password*-nya diabaikan karena setelah **1=1** terdapat *mark SQL* (--), sehingga *password* itupun diabaikan. Lalu apakah hanya itu *string*-nya dalam menginjeksi sebuah situs? Tentu saja tidak. Inti dari injeksi dalam langkah awalnya adalah memaksa keluar sebuah *error page* yang berisi informasi struktur *database* situs itu dan kalau kita ingin melihatnya kita harus men-*debug*-nya. Jadi yang kita masukkan adalah *string debugging SQL code,* yaitu **' having 1=1--** , ini adalah *string* yang harus dimasukkan kalau kita ingin melihat *error page* dari situs sasaran. Sehingga dapat dikatakan bahwa teknik ini memungkinkan seseorang dapat *login* kedalam sistem tanpa harus memiliki *account*. Selain itu *SQL injection* juga memungkinkan seseorang merubah, menghapus, maupun menambahkan data–data yang berada didalam *database*. Bahkan yang lebih berbahaya lagi yaitu mematikan *database* itu sendiri, sehingga tidak bisa memberi layanan kepada *web server*.

Nmap

Nmap ("*Network Mapper*") adalah sebuah *tool open source* untuk eksplorasi dan audit keamanan jaringan. *Nmap* menggunakan paket IP *raw* untuk mendeteksi *host* yang terhubung dengan jaringan dilengkapi dengan layanan (nama aplikasi dan versi) yang diberikan, sistem operasi (dan versi), apa jenis *firewall*/*filter* paket yang digunakan, dan sejumlah karakteristik lainnya. *Output Nmap* adalah sebuah daftar target *host* yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan. Berikut layanan – layanan yang dapat diberikan *Nmap* diantaranya nomor *port*, nama layanan, status *port* : terbuka (*open*), difilter (*filtered*), tertutup (*closed*), atau tidak difilter (*unfiltered*), nama *reverse DNS,* prakiraan sistem operasi, jenis *device*, dan alamat *MAC*.

Tipe-tipe pemindaian dengan *Nmap*

connect scan (-sT)

Jenis *scan* ini konek ke *port* sasaran dan menyelesaikan *three-way handshake (SYN, SYN/ACK, dan ACK). Scan* jenis ini mudah terdeteksi oleh sistem sasaran.

TCP SYN scan (-sS)

Paling populer dan merupakan *scan default nmap. SYN scan* juga sukar terdeteksi, karena tidak menggunakan *3 way handshake* secara lengkap, yang disebut sebagai teknik *half open scanning*. *SYN scan* juga efektif karena dapat membedakan *3 state port*, yaitu *open*, *filterd* ataupun *close*. Teknik ini dikenal sebagai *half-opening scanning* karena suatu koneksi penuh *TCP* tidak sampai terbentuk. Sebaliknya, suatu paket *SYN* dikirimkan ke *port* sasaran. Bila *SYN/ACK* diterima dari *port* sasaran, kita dapat mengambil kesimpulan bahwa *port* itu berada dalam status *LISTENING*. Suatu *RST/ACT* akan dikirim oleh mesin yang melakukan *scanning* sehingga koneksi penuh tidak akan terbentuk. Teknik ini bersifat siluman dibandingkan *TCP connect* penuh, dan tidak aka tercatat pada log sistem sasaran.

TCP FIN scan *(-sF)*

Teknik ini mengirim suatu paket *FIN* ke *port* sasaran berdasarkan *RFC 793*, sistem sasaran akan mengirim balik suatu *RST* untuk setiap *port* yang tertutup. Teknik ini hanya dapat dipakai pada *stack TCP/IP* berbasis *UNIX.*

TCP Xmas Tree scan (*-sX*)

Teknik ini mengirimkan suatu paket *FIN, URG*, dan *PUSH* ke *port* sasaran. Berdasarkan *RFC 793*, sistem sasaran akan mengembalikan suatu *RST* untuk semua *port* yang tertutup.

TCP Null scan *(-sN*)

Teknik ini membuat *off* semua *flag*. Berdasarkan *RFC 793*, sistem sasaran akan mengirim balik suatu *RST* untuk semua *port* yang tertutup.

***TCP ACK scan** (-sA*)
Teknik ini digunakan untuk memetakan set aturan *firewall*. Dapat membantu menentukan apakah *firewall* itu merupakan suatu *simple packet filter* yang membolehkan hanya koneksi-koneksi tertentu (koneksi dengan *bit* set *ACK*) atau suatu *firewall* yang menjalankan *advance packet filtering.*

***TCP Windows scan** (-sW*)
Teknik ini dapat mendeteksi port-port terbuka maupun terfilter/tidak terfilter pada sistem sistem tertentu (sebagai contoh, *AIX* dan *FreeBSD*) sehubungan dengan anomali dari ukuran *windows TCP* yang dilaporkan.

TCP RPC scan
Teknik ini spesifik hanya pada *system UNIX* dan digunakan untuk mendeteksi dan mengidentifikasi *port RPC (Remote Procedure Call)* dan program serta normor versi yang berhubungan dengannya.

Permasalahan
SQL injection adalah salah satu teknik mengeksploitasi website atau web server yang sedang marak saat ini, dan Webserver merupakan host yang paling banyak menjadi sasaran target serangan dalam teknologi internet karena Webserver berperan penting pada website, Webserver berisi *webpages* yang di dalamnya mengandung informasi atau dokumen yang ingin disebarluaskan dan diperlukan oleh para pengguna. Ancaman keamanan secara spesifik terhadap Webserver umumnya terbagi menjadi beberapa kategori diantaranya : Entitas *malicious*, serangan *Denial of Service* (DoS), Informasi sensitif pada Webserver, Informasi sensitif di database, Informasi sensitif yang ditransmisikan tanpa dienkripsi antara Webserver, *Command Injection, Structrured Query Language (SQL), lightweight Directory Access Protocol (LADP),* dan *cross site scripting (XSS),* serta *Defacement* (penggantian tampilan).

Sehingga serangan terhadap webserver dapat juga dialami oleh website atau webserver PT. Victory Internasional Futures perusahaan yang bergerak di bidang investasi *Foreign Exchange (Forex), Index Futures (Index),* dan *Comodity Exchange (Gold)* yang juga menggunakan *website* sebagai sarana promosi dan media komunikasi antara perusahaan dengan nasabah.

Analisis Masalah
untuk mengetahui masalah keamanan Webserver tersebut, maka dilakukan analisis terhadap keamanan Webserver PT. Victory Internasional Futures menggunakan metoda kualitatif dengan langkah – langkah dalam menentukan kebutuhan dan kriteria analisis dalam bentuk tabel prosedur dan kebutuhan serta kriteria berdasarkan teori yang digunakan dalam penelitian. Contoh prosedur dan kebutuhan analisis serta kriteria analisis seperti yang terlihat pada tabel 1.

Tabel 1 Tabel Kebutuhan Analisis Dan Kriteria Analisis

Prosedur	**Kebutuhan**	**Kriteria Analisis**
1.Information Gathering	*-Server Spy -Netcraft.com - Whois dan Whatweb*	*Standart Information*
2. Service Enumeration	*- Nmap -SQL Injection*	*Information Access Service*
3.Vulnebrality Identification	*- Acunetix -Backtrack*	*Information vulnebrality*
4. penetration	*-exploite*	Simulasi serangan

Pemodelan Sistem
Pemodelan sistem untuk menganalisis keamanan *website (www.vifcorps.com)* dengan teknik *SQL Injection*, menggunakan metode Kualitatif yang terdiri dari 4 langkah seperti yang dijelaskan pada tabel 1 :

Information Gathering* menggunakan *server spy* dan *netcraft.
Information Gathering, untuk teknologi *server spy*, langkah – langkahnya adalah sebagai berikut : Buka *web browser*, masuk ke *http://browserspy.dk/webserver.php,* kemudian

masukan alamat *website* atau *URL* yang ingin diketahui informasi web sever dan sistem operasinya, ke dalam kotak seperti yang terlihat pada gambar 2.

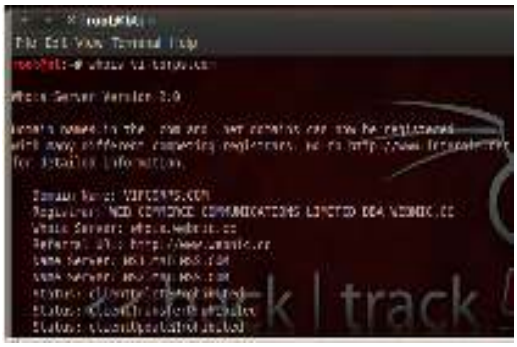
Gambar 2. kotak *URL website server spy*

Untuk teknologi *netcraft*, Buka *web browser*, masuk ke *http://netcraft.com/* kemudian masukan alamat *website* atau *URL* yang ingin diketahui informasi web sever, sistem operasinya, hosting, keyword, ip address, dll ke dalam kotak seperti yang terlihat pada gambar 3

Gambar 3. kotak *URL/website netcraft.com*

Information Gathering* menggunakan *whois* dan *whatweb

Whois dan *whatweb* digunakan agar dapat melengkapi informasi yang di dapatkan dari *server spy* dan *netcraft.com*. Untuk dapat menggunakan *whois* dan *whatweb***,** langkah – langkahnya adalah sebagai berikut *: install OS backtrack* di *computer Linux*, atau di *virualbox* (*computer windows*), kemudian masuk keterminal dan ketikkan ***apt-get install whois*,** setelah selesai menginstall, ketikkan *whois* IP address atau alamat *website* yang ingin diketahui informasinya Contoh : ***Whois vifcorps.com,*** maka akan keluar informasi seperti yang terlihat pada gambar 4.



Gambar 4.*whois vifcorps.com* pada terminal Backtrack

Seperti halnya dengan *whois,* masuk ke terminal backtrack, ketikkan ***apt-get install whatweb***, setelah selesai, ketikkan ***whatweb –v www. vifcorps.com,*** maka akan keluar informasi seperti yang terlihat pada gambar 5.

Gambar 5. ***whatweb –v www. vifcorps.com*** pada terminal backtrack

Service Enumeration yaitu mencari sumber data yang menyediakan akses ke database, server, dll. Melakukan *scanning port* yang terbuka, dengan menggunakan *Nmap,* dan *SQL Injection* untuk mengetahui, apakah ada pesan *error* dari *database*.

Service Enumeration* menggunakan *Nmap

Langkah – langkah *scanning port* menggunakan *Nmap* adalah sebagai berikut: seperti pada *whois* dan *whatweb*, *Nmap* juga menggunakan backtrack, dan perlu diinstall juga. Masuk ke terminal backtrack, ketikkan ***apt-get install Nmap,*** ada beberapa teknik *Nmap* yang akan dilakukan, diantarannya : ***Nmap –O***, ***Nmap _sU***, ***Nmap –sO***, serta ***Nmap –sV***. kemudian setelah selesai, ketikkan *Nmap*

-*O*/-sU/-sO/-sV IP address, atau alamat *website*, untuk mencari port apa saja yang terbuka, Contoh : ***Nmap –O vifcorps.com***, maka akan keluar informasi seperti yang terlihat pada gambar 6.

Gambar 6. scanning port *Nmap* –O *vifcorps.com*

Nmap* –sU *vifcorps.com

Gambar 7. *Nmap* -sU *vifcorps.co*

Nmap* –sO *vifcorps.com

Gambar 8. *Nmap* -sO *vifcorps.com*

Nmap* -sV *vifcorps.com

Gambar 9. *Nmap* -sV *vifcorps.com*

Service Enumeration* menggunakan teknik *SQL Injection

Untuk mengetahui apakah ada pesan error dari database, maka perlu diperiksa *website* *www.vifcorps.com* dengan menggunakan teknik *SQL Injection* diantaranya : teknik *SQL Injection* dengan *single quote,(')*, *SQL Injection* dengan *double quote(")*, *or*, *order*, *limit.* Langkah – langkah melakukan teknik *SQL Injection* adalah sebagai berikut : ***SQL Injection*** dapat dilihat pada gambar 11, 12, dan 13.

Gambar 10.

http://www.vifcorps.com/about- vif/company-profile'

out-

Gambar 12. *http://www.vifcorps.com/about-vif/**'company-profile***

Pengujian Sistem

Pengujian sistem dilakukan dengan membuat beberapa rencana awal pengujian. Untuk menjelaskan bagian – bagian sistem yang akan diuji. Rencana pengujian sistem pada penelitian ini dapat dilihat pada table 2.

Tabel 2. Rencana Pengujian

no	***Class* Uji**	***Tools/Item* pengujian**	**Keterangan**
1.	*Information Gathering*	*Server spy*, *netcraft*, *whois*, dan what web.	*informational*
2.	*Service Enumerat*	Scanning Port, *SQL Injection*,	*Inform*
3	*Vulnebrality Identification*	*Acunetix*vulnerability web*scaner*,(blind_injection, *SQL Injection*), backtrack OS(joomscan).	*Default*
4	*Penetration*	Teknik*SQL Injection*	*Penetrasi akan dilakukan jika ditemu*

Kegiatan Pengujian

Kegiatan pengujian dijelaskan dalam tabel 3

Tabel 3. Kegiatan pengujian

Kebutuhan	Eksplorasi
-Server Spy *-Netcraft.com* *- Whois dan Whatweb*	*- http://www.vifcorps.com-* *- www.vifcorps.com* *- Whois vifcorps.com* *- whatweb –v www. vifcorps.com*
- Nmap *-SQL Injection*	*- Nmap -O*/-sU/-sO/-sV vifcorp.com *single quote,(‘), double quote(“), or, order, limit, having, double minus(--),* dll
- Acunetix *-Backtrack*	*- www.vifcorp.com* *- Joomscan.PL –u vifcorps.com -x*
-exploite	*-Bruteforce,* *- Both* *- Disclosure* *- flag on the cookie* *- Malicious* *-inject JavaScript or DHTML code* *- inject JavaScript code in a URL* *Dll.*

Hasil Pengujian

berdasarkan pengamatan yang dilakukan, maka didapatkan hasil seperti *www.vifcorps.com* menggunakan *Backtrack OS* terhadap 26 isi dari *website* atau webserver tersebut diantaranya terdapat 5 temuan yang di exploite dengan teknik *SQL Injection* dan *Blind SQL Injection,* akan tetapi tidak ditemukan kelemahannya. Dan acunetix menetapkan skala 1 sampai yang menyatakan tingkat *vurnerability* atas sistem yang di-*scan*. Seperti yang dijelaskan pada table 4 dan 5.

tabel 4 hasil scaning

pengamatan vulnerabliti dari backtrack OS
12
Info -> CoreComponent: com_content *SQL Injection* Vulnerability
Exploit: /index.php?option=com_content&task=blogcategory&id=60&Itemid=99999+UNION+SELECT+1,concat(0x1e,username,0x3a,password,0x1e,0x3a,usertype,0x1e),3,4,5+FROM+jos_users+where+userty

pe=0x53757065722041646d696e6973747261746f72--
No
Tidak Lemah
14
Info -> CoreComponent: MailTo *SQL Injection* Vulnerability
Exploit: /index.php?option=com_mailto&tmpl=mailto&article=550513+and+1=2+union+select+concat(username,char(58),password)+from+jos_users+where+usertype=0x5375706572041646d696e6973747261746f72--&Itemid=1
NO
Tidak Lemah
15
Info -> CoreComponent: com_content Blind *SQL Injection* Vulnerability
Exploit: /index.php?option=com_content&view=%'+'a'='a&id=25&Itemid=28
NO
Tidak Lemah
19
Info -> CoreComponent: com_content view=archive *SQL Injection* Vulnerability
Exploit: Unfiltered POST vars - filter, month, year to /index.php?option=com_content&view=archive
NO
Tidak Lemah
24
Info -> CoreComponent: com_banners Blind *SQL Injection* Vulnerability
Exploit:/index.php?option=com_banners&task=archivesection&id=0'+and+'1'='1::/index.php?option=com_banners&task=archivesection&id=0'+and+'1'='2 No
Tidak Lemah

Table 5. hasil scaning menggunakan Acunetix

Scan of http://www.vifcorps.com:80/

Scan details

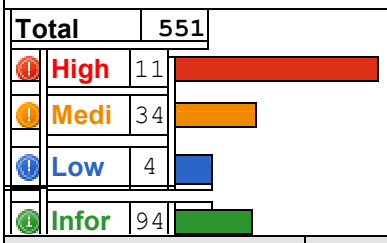
Scan information	
Starttime	6/3/2013 10:17:56 PM
Finish time	6/4/2013 4:14:44 AM
Scan time	5 hours, 56 minutes
Profile	Default
Server information	
Responsiv	True
Server	Apache/2.2.22
Server OS	Unknown
Server	PHP

Threat level

***Acunetix* Threat Level 3**

One or more high-severity type vulnerabilities have been discovered by the *scanner*. A malicious user can exploit these vulnerabilities and

Alerts distribution



Alert group	Severity	Alert count
Blind *SQL Injection*	High	2
Cross Site Scripting	High	108
Script source code	High	1
HTML form without	Medium	214
User credentials are	Medium	128
Login page password-	Low	1
Possible Virtual Host	Low	3
Broken links	Information	12
Content type is not	Information	3
GHDB	Information	3
Password type input	Information	76

Vulnerablity Identification untuk *website* atau *web server* pada *website Acunetix*

Kesimpulan

Berdasarkan data dan eksplorasi yang telah dilakukan, vulnebrality identification Webserver pada situs www.vifcorps.com tidak menemukan kelemahan atau celah untuk serangan bebasis *script* seperti *SQL Injection, Xross site scripting (XSS),blind injection,* demikian juga serangan terhadap *entitas malcious, brute force,* sehingga dapat dikatakan webserver tersebut aman dari serangan *SQL Injection.*

Saran

Penelitian mengenai analisis keamanan *web server* ini memerlukan saran – saran untuk pengembangan sistem lebih lanjut. Adapun saran tersebut adalah sebagai berikut :

Diharapkan pada penelitian berikutnya, dapat meneliti lebih luas lagi, tentang bagaimana mengamankan suatu webserver, dan *website* dari serangan *Blind Injection, Cgi tester, Directory file, File checks, Google Hacking testing Database (GHDB), Parameter manipulation, SQL Injection, Text search, Version checks, Web application xfs, Entity encode heap overflow, cross site scripting,* dll. dan dapat memberikan solusi terkait dengan lemahnya sistem.

Daftar Pustaka

1. Sadewosury. *2007.* ***Landasan Teori Webserver*** http://elib.unikom.ac.id/files/disk1/305/jbptunikompp-gdl-sadewosury-15211-3-babii.pdf/ tanggal 03 April 2013 pukul 22. 11)

2. Sasongko, Ashwin., Tjahjono, Heru, Bambang., Chendramata, Aidil. Dkk. *2011.* ***Panduan Keamanan Webserver***. Jakarta : Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika

3. storageSkripsi. *2013.* ***Landasan Teori Internet, dan TCP/IP*** http://storage.jakstik.ac.id/students/paper/skripsi/10401209/BAB%20II.pdf/ tanggal 05 April 2013 pukul 22.02)

4. Supardi, Yuniar. 2010. ***Web My Profile Dengan Joomla 1.5x*** Jakarta : PT. Elex Media Komputindo.

5. Temamaulia. *2006.* ***Pengertian Analisis dan Analisis Sistem***. http://elib.unikom.ac.id/files/disk1/57/jbptunikompp-gdl-s1-2006-temamaulia-2813-12.-bab--i.pdf/ tanggal 03 April 2013 pukul 19.45

6. Thesisbinus. *2007.* ***Pengertian Analisis dan Perancangan*** (http://library.binus.ac.id/eColls/eThesis/Bab2/2007-2-00421-MNSI-Bab%202.pdf/ tanggal 03 April 2013 pukul 19.45)

7. unsri. 2010. ***SQL Injection dan cara penangananya*** http://*www.*google.co.id/*URL*?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&sqi=2&ved=0CEkQFjAG&*URL*=http%3A%2F%2F*www.*unsri.ac.id%2Fupload%2Farsip%2FSQL%2520Injection.doc&ei=0vNeUcv5NsSlrQfTgoHwAw&usg=AFQjCNG6h6D4xlzIjOEcYAATsdyAbaO0Pw&bvm=bv.44770516,d.bmk / tanggal 05 April 2013 pukul 22.58).

8. Usurepository. *2007.* ***Landasan Teori Internet, Webserver*** (http://repository.usu.ac.id/bitstream/123456789/16955/4/Chapter%20II.pdf/ tanggal 05 April 2013 pukul 21.29)

9. Usurepository. *2007.* ***Landasan Teori Internet, Webserver*** (http://repository.usu.ac.id/bitstream/123456789/16955/4/Chapter%20II.pdf/ tanggal 05 April 2013 pukul 21.36)

10. Usurepository. *2007.* ***Landasan Teori Internet, Webserver*** (http://repository.usu.ac.id/bitstream/123456789/16955/4/Chapter%20II.pdf/ tanggal 05 April 2013 pukul 21.29)