ANALISIS HACKING TERHADAP SISTEM KEAMANAN WEB SITE

Elyyani
Pusat Pemanfaatan Sains Antariksa - LAPAN
Jl. Dr. Djundjunan 133 Bandung 40173
elyyani@bdg.lapan.go.id

Abstrak

Keunggulan web adalah kemudahan untuk mengakses informasi, yang dihubungkan satu dengan lainnya melalui konsep hypertext. Informasi dapat tersebar dimana-mana dan terhubung melalui hyperlink . Pergerakkan sistem informasi tersebut menyebabkan web dan internet makin berkembang. Untuk itu, keamanan sistem informasi yang berbasis web dan internet sangat tergantung pada keamanan sistem web itu sendiri. Adanya kelemahan terhadap website baik dari sisi scripting, lubang pada situs tetangga maupun tempat hosting yang bermasalah akan menjadi faktor penyebab terjadinya beberapa tindakan/serangan hacking. Untuk melindungi atau memproteksi website adalah dengan melakukan strategi dasar pengamanan mulai dari pemilihan sistem operasi (OS), setting Server, desain aplikasi, instalasi patch, kontrol akses, audit dan log file. Ada 3 level yang dapat diterapkan yaitu berdasarkan sistem operasi (OS) dan hardware, level akses host dan level direktori dan file.

Kata Kunci : scripting, hosting, file log, kontrol akses.

1.LATAR BELAKANG

Belakangan ini, dunia Teknologi Informasi underground sudah semakin marak. Beberapa media cetak , elektronik dan dunia maya banyak berita yang memuat aksi-aksi penyerangan terhadap web bahkan web pemerintahpun sudah banyak yang menjadi korbannya.

Demikian pula halnya dalam melindungi informasi pada situs web yang merupakan media dalam menyebarluaskan informasi penelitian sains antariksa, atmosfer dan iklim. Informasi merupakan sumber daya atau harta-kekayaan terpenting pada suatu perusahaan yang sifatnya sangat pribadi dan integritas dari situs web itu sendiri sehingga perlu perlindungan agar tidak diacak-acak oleh hacker. Dari banyak kasus yang ditemukan, hacker cenderung untuk melakukan

penyerangan terhadap data, sumber daya serta reputasi perusahaan *(Stiawan Deris, 2005)*.

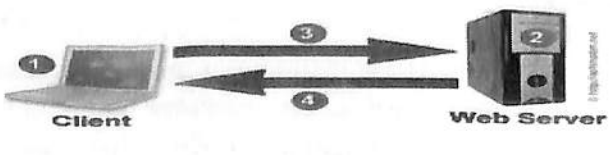
Dengan melihat kenyataan yang ada para pengelola website tidak bisa berdiam diri, berbagai upaya dilakukan dengan memperbaiki pengamanan terhadap web yang dibangunnya. Meskipun demikian tidak ada sistem keamanan yang dapat menjamin 100% bahwa web kita aman, hanya kita sebagai pengelola bisa meminimalisir berbagai kemungkinan yang akan terjadi.

Untuk dapat mengamanankan informasi pada sebuah web site tentunya kita sebagai pengelola harus paham betul tentang berbagai sistem proteksi dan serangan-serangan terhadap web site. Ini dilakukan dengan mengenal prinsip dan cara kerja web server, faktor penyebab serangan, mengenal tindakan-tindakan *hacking*, serta strategi dasar pengamanan web

2. PRINSIP DAN CARA KERJA WEB SERVER

Menurut Wikipedia, Web Server merupakan sebuah perangkat lunak server yang berfungsi menerima permintaan HTTP atau HTTPS dari klien yang dikenal dengan browser web dan mengirimkan kembali hasilnya dalam bentuk halaman-halaman web yang umumnya berbentuk dokumen HTML. Karena web server hanyalah suatu perangkat lunak, saat ini banyak pilihan yang dapat kita pilih. Mulai dari yang gratis (free) sampai yang bayar, mulai dari yang kompleks sampai yang bisa berjalan di CD. Beberapa diantaranya yang cukup banyak digunakan adalah Apache Web Server, Internet Information Services (IIS), Xitami, PWS dan lain-lain.

Web server bertanggung jawab penuh untuk menerima request HTTP dari beragam klient dan mengirimkan jawaban HTTP kepadanya *(McClure, 2003)*. Pada dasarnya tugas web server hanya menerima permintaan(request) dari client dan mengirimkan apa yang diminta oleh client (response).



Gambar 2-1:Cara kerja web server

Keterangan pada gambar 2-1 adalah:

1. Client disini dapat berupa komputer desktop dengan minimal memiliki browser dan terhubung ke web server melalui jaringan (intranet atau internet).
2. Komputer yang berfungsi sebagai server, dimana didalamnya terdapat perangkat lunak web server. Agar komputer ini dapat diakses oleh client maka komputer harus terhubung ke jaringan (intranet atau internet).
3. Pertama-tama, client (user) akan meminta suatu halaman ke (web) server untuk ditampilkan di komputer client. Misalnya client mengetikkan suatu alamat (biasa disebut URL). Client menekan tombol Enter atau klik tombol Go pada browser. Melalui media jaringan (bisa internet, bisa intranet) dan melalui protokol http, akan dicarilah alamat URL yang dicari tersebut. Inilah yang disebut request.
4. Sekarang dari sisi server (web server), mendapat permintaan dari client kemudian server akan mencari di komputernya halaman sesuai permintaan. Jika ditemukan, maka halaman yang diminta akan dikirimkan ke client (si peminta), namun jika tidak ditemukan, maka server akan memberi pesan "*404. Page Not Found*", yang artinya halaman tidak ditemukan.

3. ANALISA TERHADAP FAKTOR PENYEBAB SERANGAN TERHADAP WEB SITE

Analisa dilakukan terhadap banyak faktor dintaranya dari sisi scripting, situs tetangga yang tidak aman (jika disimpan pada hosting yang sama) serta tempat hosting yang bermasalah.

1. Analisa dari sisi scripting

Kesalahan dalam scripting pada saat pembuatan web adalah hal terbanyak yang dimanfaatkan oleh para *attacker*, sehingga melalui lubang ini rata-rata web berhasil diserang. Kelemahan-kelemahan scripting yang ditemukan pada proses *vulnerabilities scanning* misalnya, XSS, SQL Injection, PHP Injection, HTML Injection, dan lain sebagainya. CMS seperti Mambo, Joomla, WordPress tersebut memiliki banyak komponen pendukung di internet yang bisa kita download, install dan konfigurasi. Sehingga sangat memungkinkan sekali terdapat bug pada scriptingnya. Untuk itu penting dilakukan pembedahan terhadap script tersebut serta melakukan pengujian sebelum komponen tersebut kita gunakan pada web yang sebenarnya.

2. Analisa dari sisi situs tetangga

Jika sebuah website disimpan pada salah satu hosting maka kita perlu waspada terhadap lubang pada situs tetangga artinya web tetangga dalam satu hosting sedang dihacked. Dalam hal ini para attacker bisa menanam program yang dijadikan backdoor, dengan *backdoor* inilah *attacker* bisa masuk ke dalam web kita bahkan web lainnya. Bukan itu saja, tidak mustahil *attacker* melakukkan defacing massal, termasuk web yang sedang kita kelola

3. Analisa dari sisi hosting

Faktor penyebab lain adalah tempat hosting yang bermasalah, ini menjadi sebab dihackednya banyak situs yang berada di bawah pengelolaannya. Web hosting dengan administrasi yang kurang baik dan jarang diupdate akan memberikan ketidaknyamanan bagi pelanggannya sehingga tidak mudah diserang.

Sebagai pengelola web site beberapa tindakan hacking ini wajib diketahui sebagai bahan referensi dalam membenahi sistem proteksi terhadap web. Beberapa tindakan hacking adalah:

- **Memodifikasi Validasi Input**
  Dalam melakukan proses *attacking* biasanya para attacker mencoba menguji validasi-validasi input yang diterapkan pada form dan parameter buangan pada *address bar*. Penanganan yang harus diperhatikan adalah memperhatikan validasi yang terdapat pada form, baik itu validasi angka maupun validasi string, batasi jumlah karakter yang bisa dimasukkan, batasi kegiatan-kegiatan injeksi dengan : strip_tags(), htmlspecialchars(), gunakan variabel global sebagaimana mestinya dan gunakan *wordfilter* untuk memfilter berbagai inputan yang berbahaya.

- **Cross-Site Scripting (XSS)**
  Salah satu *vulnerabilities* dalam website adalah *Cross-Site Scripting* (XSS). Ada 2 jenis aksi yang biasa dilakukan dalam XSS, yaitu

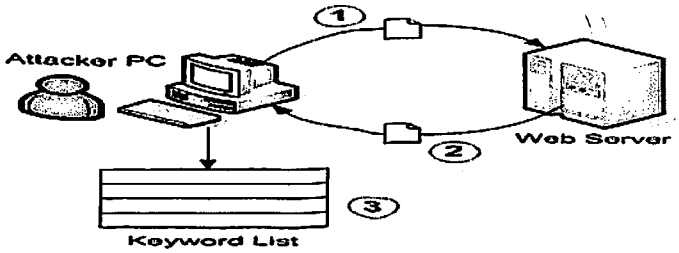
  - *Direct Action,* merupakan injeksi kode yang dilakukan oleh *attacker*, tetapi hasil injeksinya hanya ditampilkan pada komputer user bersangkutan.

  - *Stored Action*, merupakan injeksi kode yang dilakukan oleh *attacker* dan hasil injeksinya bisa dinikmati oleh banyak pengunjung.

Cara mengatasinya adalah dengan mengusahakan semua kode-kode spesial yang mempunyai arti dalam scripting HTML seperti < (kurang dari), > (lebih dari), & (ampersand), " (kutip dua) dan ' (kutip satu) tidak dieksekusi sebagai karakter spesial. Semua karakter spesial tersebut harus diubah dan dikonversi ke entitas HTML.

- **SQL Injection**

  SQL Injection merupakan teknik hacking yang sudah tersebar luas dan relatif mudah dipahami. *Attacker* melakukan proses *attacking* dengan menyisipkan perintah-perintah SQL pada form ataupun pada address bar. Untuk mengatasi hal ini, sebaiknya kita membatasi input dengan : htmlspecialchars(), mysql_escape_string() dan hubungi administrator hosting untuk merubah : magic_quotes_gpc=on.



Gambar 3-1: SQL Injection

- **PHP Injection**

  Dengan PHP Injection, *Attacker* mempergunakan sploit yang sudah ditanam di remote server miliknya dan hanya dengan mengeksekusi script sploit tersebut melalui address bar dan melakukan *connect back*, maka web tersebut dapat dikuasai.

4. HASIL DAN PEMBAHASAN

Untuk meminimalisir ataupun mengurangi serangan para hacking maka ada beberapa strategi dalam mengamankan sebuah web site. Strategi ini dapat dilihat berdasarkan pemilihan sistem operasi (OS), Setting Server, dan desain aplikasi yang digunakan. Penentuan kebijakan dalam menerapkan sistem pengamanan merupakan kunci utama yang harus diperhatikan. Salah satunya adalah pemilihan sistim operasi yang merupakan salah satu hal penting karena berhubungan dengan kontrol akses sehingga dibutuhkan berbagai setting dan konfigurasi yang memadai serta tidak mengandalkan default sistem yang ada.

Faktor yang kedua adalah instalasi Patch, instalasi patch ini dibutuhkan untuk memperbaiki kesalahan pada software aplikasi yang akan dipasang. Penerapan patch ini harus dilakukan pada sistem operasi, server web, *add on*, maupun file-file komponen lain yang terintegrasi dengan sebuah website.

Selain itu proses validasi identitas harus juga diperhatikan, sehingga perlu dilakukan cara autentifikasi dan otorisasi pada bagian kontrol aksesnya. Autentikasi yaitu dengan proses validasi identitas yang dilakukan dengan membandingkan data user yang dikirim dengan data yang terdapat dalam database, misalnya autentikasi password. Setelah melakukan autentikasi, langkah selanjutnya yaitu melakukan otorisasi yang merupakan proses untuk menentukan apakah pengguna memiliki ijin untuk melakukan tindakan yang diminta, misalnya penggunaan hostname.

Faktor yang terakhir adalah audit dan log file, proses yang dapat memonitor aktivitas tertentu seperti usaha login (berhasil atau gagal), dan kemudian menuliskannya ke dalam log ini merupakan proses audit. Sebagai contoh, kita dapat menganalisa dengan mengaudit kegagalan usaha login dalam log, memungkinkan kita menentukan saat seseorang berusaha menyerang server.

Dalam hasil/implementasinya ada 3 level keamanan yang dapat diterapkan diantaranya: sistem operasi (OS) dan hardware, level akses host dan level direktori dan file.

Level sistem operasi dan hardware ini meliputi perangkat keras server, network dan sistem operasi yang dipakai. Level akses host yaitu level yang digunakan untuk memperkuat keamanan web yaitu mengaktifkan restriksi akses level host yaitu dengan melakukan proteksi pada direktori yang dianggap penting dan bukan untuk konsumsi umum, seperti direktori administrator, login. Keamanan direktori tersebut yang umum hanya 1 level keamanan tetapi bisa ditingkatkan menjadi 2 level keamanan dengan menambah 1 level akes keamanan lagi yaitu autentifikasi akses direktori, sehingga ketika akan melakukan login sebelum masuk ke menu login administrator akan muncul terlebih dahulu jendela autentikasi yang berisi user dan password. Dimana sebaiknya user dan passwordnya berbeda dengan user dan password untuk login pada direktori web. Pengamanan yang terakhir adalah level akses direktori dan level akses file. Pada level akses direktori dilakukan dengan memproteksi pada direktori yang dianggap penting seperti direktori administrator dan login.

5. KESIMPULAN

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, hal ini seringkali kurang mendapat perhatian dari para pengelolanya. Sistem proteksi pada sebuah web site berfungsi untuk melindungi data dan informasi yang ada didalamnya agar informasi tersebut tidak dimanfaatkan oleh orang yang tidak bertanggung jawab. Dalam hal ini para hacker bisa dengan leluasa melakukan berbagai serangan seperti aktivitas mengubah halaman depan atau isi suatu website yang memanfaatkan kelemahan dari sisi web server selain itu juga dapat memanfaatkan kelemahan dari sisi layanan (*vulnerability*) yang bisa diatasi dengan melakukan instalasi patch serta meng-update server.

DAFTAR RUJUKAN

McClure, Stuart., Web Hacking Serangan Dan Pertahanannya, Andi Yogyakarta, 2003.

Stiawan, D., Sistem Keamanan Komputer, Elek Media Komputindo, Jakarta, 2005.

http://computer.howstuffworks.com/web-server1.htm pada tanggal 17 Mei 2009