

Keamanan Sistem WWW

WWW security



Sejarah WWW



- Dikembangkan oleh Tim Berners-Lee ketika sedang berada di CERN
- Kemudahan untuk mengakses informasi melalui sistem hypertext
- Mula-mula dikembangkan dengan NeXT, kemudian muncul Mosaic (Windows, Mac, Unix), dan ... akhirnya Netscape. Kemudian meledak

Sejarah WWW

- Bahan bacaan
 - <http://ensiklonesia.insan.co.id>
 - Buku Tim Berners-Lee, "Weaving the Web"
 - <http://www.w3.org>

Sistem WWW

- Arsitektur sistem WWW
 - Server (apache, IIS)
 - Client (IE, Netscape, Mozilla, Firefox, Opera, Galeon, kfm, arena, amaya, lynx)
 - Terhubung melalui jaringan
- Program dapat dijalankan di server (CGI, [java] servlet) atau di sisi client (javascript, java applet)

Asumsi [Sisi Pengguna]

- Server dimiliki dan dikendalikan oleh organisasi yang mengaku memiliki server tersebut
- Dokumen yang ditampilkan bebas dari virus atau itikad jahat lainnya
- Server tidak mencatat atau mendistribusikan informasi tentang user (misalnya kebiasaan browsing)

Asumsi [Sisi Webmaster]

- Pengguna tidak beritikad untuk merusak web server atau mengubah isinya
- Pengguna hanya mengakses dokumen² yang diperkenankan diakses (dimana dia memiliki ijin)
- Identitas pengguna benar

Asumsi Kedua Pihak

- Network dan komputer bebas dari penyadapan pihak ketiga
- Informasi yang disampaikan dari server ke pengguna (dan sebaliknya) terjamin keutuhannya dan tidak dimodifikasi oleh pihak ketiga

Keamanan Server WWW

- Server WWW (httpd) menyediakan informasi (statis dan dinamis)
- Halaman statis diperoleh dengan perintah GET
- Halaman dinamis diperoleh dengan
 - CGI (Common Gateway Interface)
 - Server Side Include (SSI)
 - Active Server Page (ASP), PHP
 - Servlet (seperti Java Servlet, ASP)

Eksplorasi server WWW

- Tampilan web diubah (*deface*)
 - dengan eksploitasi skrip / privilege / OS di server
 - Situs yang dideface dikoleksi di <http://www.alldas.org>
- Informasi bocor
 - (misal laporan keuangan semestinya hanya dapat diakses oleh orang/ bagian tertentu)

Eksplorasi server WWW [2]

- Penyadapan informasi
 - URLwatch: melihat siapa mengakses apa saja. Masalah privacy
 - SSL memproteksi, namun tidak semua menggunakan SSL karena komputasi yang tinggi
- DoS attack
 - Request dalam jumlah yang banyak (bertubi-tubi)
 - Request yang memblokir (lambat mengirimkan perintah GET)

Eksplorasi server WWW [3]

- Digunakan untuk menipu firewall (*tunelling* ke luar jaringan)
- Port 80 digunakan untuk identifikasi server (karena biasanya dibuka di router/firewall)
 - telnet ke port 80 (dibahas di bagian lain)

Membatasi Akses

- Access Control
 - Hanya IP tertentu yang dapat mengakses server (konfigurasi web server atau firewall)
 - Via userid & password (htaccess)
 - Menggunakan enkripsi untuk menyandikan data-data

htaccess di Apache

- Isi berkas ".htaccess"

```
AuthUserFile /home/budi/.passme
AuthGroupFile /dev/null
AuthName "Khusus untuk Tamu Budi"
AuthType Basic
<Limit GET>
    require user tamu
</Limit>
```
- Membatasi akses ke user "tamu" dan password
- Menggunakan perintah "`htpasswd`" untuk membuat password yang disimpan di ".passme"

Secure Socket Layer (SSL)

- Menggunakan enkripsi untuk mengamankan transmisi data
- Mulanya dikembangkan oleh Netscape
- Implementasi gratis pun tersedia
 - openssl
- Beberapa masalah dengan SSL
 - ASN.1 compiler yang bermasalah menimbulkan masalah di beberapa implementasi SSL

Cari info server

- Informasi tentang server digunakan sebagai bagian dari casing the joint
- Dapat dilakukan dengan
 - Memberikan perintah HTTP langsung via telnet
 - Menggunakan program netcat

Keamanan CGI

- CGI digunakan sebagai *interface* dengan sistem informasi lainnya (gopher, WAIS)
- Diimplementasikan dengan berbagai bahasa (perl, C, C++, python, dll.)
- Skrip CGI dijalankan di server sehingga membuka potensi lubang keamanan

Lubang Keamanan CGI

- Beberapa contoh
 - CGI dipasang oleh orang yang tidak berhak
 - CGI dijalankan berulang-ulang untuk menghabiskan resources (CPU, disk): DoS
 - Masalah *setuid* CGI di sistem UNIX, dimana CGI dijalankan oleh userid web server
 - Penyisipan karakter khusus untuk shell expansion
 - Kelemahan ASP di sistem Windows
 - Guestbook abuse dengan informasi sampah (pornografi)
 - Akses ke database melalui perintah SQL (SQL injection)

Keamanan Client WWW

- Berhubungan dengan masalah privacy
 - Cookies untuk tracking kemana saja browsing
 - Pengiriman informasi pribadi
- Attack (via active script, javascript, java)
 - Pengiriman data-data komputer (program apa yang terpasang, dsb.)
 - DoS attack (buka windows banyak)
 - Penyusupan virus, trojan horse, spyware