Copyright © September 2023

Pertemuan XI

Keamanan Web Server

11.1 WEB HACKING

Secara umum pengertian WWW adalah kumpulan sumber daya internet (seperti FTP, telnet, Usenet), teks hyperlink, file audio, dan video, dan situs jarak jauh yang dapat diakses dan dicari oleh browser berdasarkan standar seperti HTTP dan TCP / IP. Disebut juga web, itu dibuat pada tahun 1989 oleh fisikawan Inggris Tim Berners-Lee saat bekerja di Laboratorium Fisika Partikel Eropa. Disebut CERN setelah inisial Prancisnya Conseil Europeen de Reserches Nucleaires di Swiss, sebagai cara yang lebih mudah untuk mengakses informasi yang tersebar di internet. Definisi yang lebih luas berasal dari Konsorsium World Wide Web (W3C): "World Wide web adalah semesta informasi yang dapat diakses jaringan, perwujudan pengetahuan manusia."

Pada walnya Berners-Lee hanya ingin menemukan cara untuk menyusun arsip-arsip risetnya. Dan untuk itu, ia mengembangkan suatu sistem untuk keperluan pribadinya. Sistem tersebut adalah program peranti lunak yang dinamai Equire. Dengan program itu, Berners-Lee telah berhasil menciptakan jaringan terkait antara berbagai arsip-arsip sehingga memudahkan informasi yang dibutuhkan. Inilah yang kemudian menjadi sebuah dasar dari sebuah revolusi yang dikenal sebagai web.

Copyright © September 2023

World Wide Web menurut para ahlim diantaranya :

1. MCLeod (Pearson)

Pengertian Www menurut MCLeod ialah suatu informasi yang dapat diakses dengan melalui internet di mana berbagai dokumen hypermedia/ file-file komputer disimpan serta juga kemudian diambil dengan cara-cara yang menggunakan metode penentuan alamat yang unik.

2. V. Djong

Definisi WWW menurut V. Djong ialah fasilitas di internet untuk dapat layanan website yang menggunakan protocol http, sering kita lihat sebuah nama domain itu ditulis dengan secara lengkap, misalnya www.google.co.id.

3. Akbar Kaelola

Pengertian WWW menurut Akbar Kaelola ialah sebagai media bagi manusia dalam kegiatan atau aktivitas berbagi dokumen, gambar, film, musik serta informasi, dan juga menjual barang maupun jasa di internet.

4. Lisa Kuswayatno

Pengertian WWW / World Wide Web dikemukakan oleh Lisa Kuswayatno ialah suatu layanan internet dengan menggunakan konsep hypertext antar dokumen yang saling berkaitan.

5. Yuhefizar

Definisi WWW menurut Yuhefizar merupakan suatu metode untuk menampilkan informasi di internet yang dapat diakses dengan melalui sebuah paladen/ browser.

11.1.1 Manfaat World Wide Web, diantaranya sebagai berikut :

1. Web Mail Service

Web mail service ini digunakan untuk mengirimkan surat elektronik kepada orang lain. Layanan ini juga bisa didapatkan secara gratis maupun berbayar.

Copyright © September 2023

Layanan email gratis ini misalnya seperti Gmail.com, Yahoo.com, dan hotmail.com. Sedangkan untuk email berbayar ini biasanya untuk keperluan perusahaan itu dengan menggunakan domain sendiri.

2. Search Engine

Search engine atau mesin pencari ini merupakan layanan gratis untuk mencari informasi itu dengan berdasarkan kata kunci tertentu. Search engine yang cukup populer saat ini ialah Google, dan Bing.

3. Web Hosting

Ini merupakan tempat untuk menyimpan data base dari sebuah website. Sebuah website itu hanya bisa diakses apabila domain website tersebut terhubung dengan web hosting tempat ia menyimpan data base.

4. Portal

Portal ini merupakan sebuah layanan di internet yang mana terdapat beberapa layanan sekaligus, contohnya seperti email, news, chatting, tanya jawab. Salah satu portal yang cukup populer itu diantaranya Yahoo.com.

11.1.2 Contoh WWW / World Wide Web

Tentunya para pengguna internet ini sudah tidak asing lagi dengan istilah dari World Wide Web (WWW). Sebagian besar website yang terdapat di internet itu menggunakan WWW pada awal nama domainnya.

Dibawah ini merupakan beberapa contoh WWW:

www.google.com

www.yahoo.com

www.facebook.com

www.twitter.com

www.youtube.com Dan lain-lain

World Wide Web merupakan bagian dari Internet yang paling populer, sehingga serangan paling banyak terjadi lewat **port 80** atau yang dikenal sebagai **Web hacking,** berupa :

1. **Deface situs**
2. **SQL injection**
3. **M**emanfaatkan kelemahan **scripting** maupun **HTML form**.

11.2 Deface

Deface adalah suatu aktivitas mengubah halaman depan atau isi suatu situs Web sehingga tampilan atau isinya sesuai dengan yang anda kehendaki.

Deface banyak terjadi pada situs *e-commerce web* yang menggunakan Microsoft IIS. Ini dikarenakan adanya bug pada IIS yang dikenal sebagai unicode bug. Dengan adanya bug ini seseorang dapat mengakses *command line shell* cmd.exe pada server keluarga Windows NT.

Deface website adalah ulah peretas yang masuk ke sebuah website dan mengubah tampilannya. Perubahan tersebut bisa meliputi semua halaman atau di bagian tertentu saja. Contohnya, font website diganti, muncul iklan mengganggu, hingga perubahan konten halaman secara keseluruhan.

Secara sederhana, cara kerja deface website dapat digambarkan sebagai sejumlah langkah strategis yang digunakan untuk mengganti tampilan dari website yang menjadi target.

Untuk bisa 'menguasai' website yang menjadi korban defacing ini tentu tidaklah sederhana. Diperlukan kemampuan untuk bisa masuk ke dalam website ataupun mengakses server sehingga berbagai hal bisa dilakukan termasuk mengganti tampilan dan juga data-data yang ada pada website. Ketika ingin melakukan defacing suatu website, terlebih dahulu Anda perlu 'masuk' ke dalam sistem tempat situs tersebut berada untuk bisa mengakses sejumlah fitur seperti data SQL, server, dan atau yang lain sebagainya sebelum kemudian memanfaatkannya untuk mengganti tampilan website korban sesuai dengan selera defacer yang bersangkutan.

Teknik-teknik Deface Situs Web

Secara garis besarnya deface ini dapat dilakukan dengan 3 cara yaitu :

1. Secara umum, ***Memasukkan Input Illegal***

Tujuan adalah agar user terlempar keluar dari direktori file-file web server dan masuk ke root directory untuk kemudian menjalankan cmd.exe dan mengamati struktur direktori pada NT server sasaran.

2. Dengan TFTP (Trivial File Transfer Protocol) adalah protokol berbasis UDP yang listen pada port 69 dan sangat rawan keamanannya dan kebanyakan web server menjalankan servis TFTP ini.

3. Dengan FTP dengan Web yang telah diisi bahan deface. Setiap NT server memiliki file ftp.exe untuk melakukan FTP upload ataupun FTP download (dari dan ke sever itu).

11.2.1 NETCAT

Netcat memungkinkan anda membentuk port filter sendiri yang memungkinkan file transfer tanpa menggunakan FTP. Lebih jauh lagi, Netcat dapat digunakan untuk menghindari port filter pada kebanyakan firewall, men-spoof IP address, sampai melakukan session hijacking.

11.2.2 Mengamankan server IIS dari deface

Selalu mengupdate dengan service pack dan hotfix terbaru.

Melindungi dengan oleh firewall dan IDS (intrusion detection system).

Menghilangkan Opsi Tulis pada Protokol HTTP (HTTP 1.0 atau HTTP 1.1)

Perintah-perintah yang didukung HTTP 1.0 dan HTTP 1.1

CONNECT*, DELETE*, GET, HEAD, OPTIONS, POST, PUT,TRACE

Copyright © September 2023

11.3 SQL Injection

SQL Injection attack merupakan salah satu teknik dalam melakukan web hacking untuk menggapai akses pada sistem database berbasis Microsoft SQL Server.

Teknik ini memanfaatkan kelemahan dalam bahasa pemograman scripting pada SQL dalam mengolah suatu sistem database yang memungkinkan seseorang tanpa account dapat masuk dan lolos verifikasi dari MS SQL server.

Contoh : Memasukkan karakter ‘ OR ‘ ‘= pada username dan password pada suatu situs.

Lanjutan

SQL Injection adalah salah satu teknik yang menyalahgunakan celah keamanan yang ada di SQL pada lapisan basis data suatu aplikasi. Celah ini terjadi karena input dari user tidak difilter secara benar dan dalam pembuatannya menggunakan form yang salah. Jadi sampai saat ini SQL Injection masih menjadi favorit hacker untuk melakukan serangan pada website. Apalagi sekarang ini hacking melalui jaringan internet sudah tidak semudah zaman dulu.

Untuk mengatasi hal ini, atur agar:

• Hanya karakter tertentu yang boleh diinput.

• Jika terdeteksi adanya *illegal character*, langsung tolak

permintaan.

11.3.1 Tujuan SQL Injection

1. Bypass Otentikasi

Jika berhasil masuk kedalam sistem, hacker akan mudah melakukan bypass tanpa perlu menggunakan username dan password yang benar untuk bisa mendapatkan akses. Cukup dengan memasukan script SQL Injection pada form yang masih terbuka.

2. Pencurian Informasi

Hacker memungkinkan untuk mengambil semua informasi yang ada pada website terutama informasi yang bersifat sensitif seperti username dan password.

3. Delete Data

Copyright © September 2023

SQL Injection memungkinkan untuk hacker menghapus semua data yang tersimpan di database, jika sudah terjadi seperti ini dan tidak ada backup database maka akan sangat berbahaya. Jadi Anda perlu melakukan backup data secara berkala untuk tujuan keamanan data.

4. Modify Data

Selain menghapus data, hacker dengan mudah mengubah data yang tersimpan di database sehingga menyebabkan data tidak valid. Jadi Anda perlu memiliki backup data jika sewaktu-waktu data dirubah oleh orang yang tidak bertanggung jawab.

5. Command Execution

Pada beberapa database, Anda sebagai user bisa mengakses operating system menggunakan server database, kalau sudah seperti ini hacker bisa dengan mudah menyerang semua yang ada pada website Anda.

6. Compromised Integritas Data

Serangan ini melibatkan perubahan isi database, seorang penyerang bisa menggunakan serangan ini untuk deface halaman web atau memasukkan konten berbahaya ke dalam halaman web.

7. Compromised Ketersediaan Data

Serangan ini memungkinkan penyerang untuk menghapus informasi dengan maksud untuk merusak atau menghapus log atau audit informasi dalam database.

11.3.2 sejarah java script

Ketika World Wide Web pertama kali dibuat pada awal 1990, semua halaman website bersifat statis. Halaman yang ditampilkan kepada pengunjung tidak dapat berubah, apalagi menyediakan navigasi ke halaman lain. Alhasil, pengunjung tidak dapat melakukan interaksi apapun selain menyimak apa yang ada di halaman tersebut.

Agar bisa membuat sebuah halaman di website dapat berinteraksi dengan pengunjung atau merespon permintaan, kamu perlu menambahkan beberapa bentuk bahasa pemrograman. Selain itu, agar bisa merespon tanpa harus memuat ulang halaman website, bahasa pemrograman ini harus berjalan di komputer yang sama dengan browser yang menampilkan halaman.

Saat itu, ada dua browser yang cukup populer, yang pertama adalah Netscape Navigator dengan LiveScript yang memungkinkan interaksi dapat terjadi di sebuah website. Cara kerjanya, browser akan menafsirkan perintah secara langsung tanpa memerlukan tambahan kode atau plugin. Siapa pun yang menggunakan Netscape bisa berinteraksi dengan halaman yang menggunakan LiveScript.

Namun, mengingat saat itu bahasa pemrograman Java (yang memerlukan plugin terpisah) sedang marak digunakan, akhirnya Netscape memutuskan untuk mengganti nama bahasa yang ada di browser mereka, yaitu "LiveScript", menjadi "JavaScript". Tak mau ketinggalan, browser Internet Explorer juga melakukan update sehingga tak hanya mendukung satu, tapi dua bahasa pemrograman yang terintegrasi.

Salah satunya disebut "VBScript" dan didasarkan pada bahasa pemrograman Basic. Bahasa pemrograman lainnya disebut dengan "JScript" yang terlihat sangat mirip dengan kata "JavaScript". Sebenarnya, jika pengguna bisa sangat berhati-hati dengan perintah yang digunakan, mereka bisa menulis kode yang dapat diproses oleh JavaScript dan JScript sekaligus.

Ketika penggunaan Internet Explorer sedang melejit, JavaScript menjadi standar bahasa pemrograman yang berlaku untuk menulis proses interaktif yang selanjutnya akan dijalankan di web browser. Kemudian, di tahun 1996, JavaScript diserahkan ke asosiasi internasional ECMA (European Computer Manufacturers Association) dan secara resmi namanya berubah menjadi "ECMAScript" atau "ECMA-262".

11.3.3 JavaScript: Client Side Scripting

JavaScript adalah bahasa pemrograman web yang bersifat Client Side Programming Language. Client Side Programming Language adalah tipe bahasa pemrograman yang pemrosesannya dilakukan oleh client. Aplikasi client yang dimaksud merujuk kepada web browser seperti Google Chrome dan Mozilla Firefox.

Bahasa pemrograman Client Side berbeda dengan bahasa pemrograman Server Side seperti PHP, dimana untuk server side seluruh kode program dijalankan di sisi server. Untuk menjalankan JavaScript, kita hanya membutuhkan aplikasi text editor dan web browser. JavaScript memiliki fitur: high-level programming language, client-side, loosely tiped dan berorientasi objek.

JavaScript adalah bahasa scripting yang paling populer di internet dan bekerja pada banyak browser seperti Internet Explorer, Mozilla, Firefox, Netscape, Opera.

Copyright © September 2023

Pada dasarnya, pengertian JavaScript adalah suatu bahasa kode atau pemrograman yang digunakan untuk menciptakan sekaligus mengendalikan konten website agar menjadi dinamis

Menggunakan sintaks seperti C++/Java

Contoh scripting language yang bekerja di sisi client:

• JavaScript

• Client side VB Script

Adapun scripting language di sisi server:

• ASP (Active Server Pages)

• JSP (Java Server Pages)

• PHP (Personal Home Page)

11.3.3 fungsi JavaScript.

1. Membuat situs tampak lebih interaktif dan menarik karena akan lebih dari sekadar laman statis yang penuh tulisan.
2. Berfungsi untuk mobile app development atau menciptakan aplikasi yang beroperasi di smartphone dan tablet.
3. Menciptakan game berbasis web browser.
4. Meskipun JavaScript umumnya digunakan untuk menciptakan bagian frontend pada sebuah situs, bahasa pemrograman ini sangat serbaguna sehingga bisa digunakan untuk bagian backend situs.

Kelemahan Dasar HTML Form

- Formulir dalam format HTML (HTML Form) adalah tampilan yang digunakan untuk menampilkan jendela untuk memasukkan *username* dan *password*.
- Setiap HTML form harus menggunakan salah satu metode pengisian formulir, yaitu GET atau POST.
- Melalui kedua metode HTTP ini (GET atau POST) parameter disampaikan ke aplikasi di sisi server.
- Masalahnya dengan menggunakan GET, variabel yang digunakan akan terlihat pada kotak URL, yang memungkinkan pengunjung langsung memasukkan karakter pada form

Copyright © September 2023

process, selain juga perintah GET dibatasi oleh string sepanjang 2047 karakter. Variabel juga dapat diambil dengan Request.QueryString.

- POST biasa digunakan untuk mengirim data dalam jumlah besar ke aplikasi di sisi server, sehingga tidak menggunakan URL query string yang terbatas. POST juga lebih aman sebab variabel tidak terlihat oleh pengunjung, sehingga lebih sulit dimainkan lewat perubahan nama variabel. Namun variabel tetap dapat diambil dengan RequestForm.

Mencari informasi mengenai Web Server

- Menggunakan www.google.com

Memasukan keyword allinurl dengan memodifikasi ke berbagai bentuk karena Google akan mencari semua URL dalam sebuah situs.

Contoh :

- allinurl:.co.nz/admin.asp
- allinurl:.co.id atau net atau org, or.id
- allinurl:.fr/admin.asp

Tool untuk memeriksa Vulnerabilities

Happy Browser adalah *Software* yang digunakan sebagai *tool* untuk memeriksa, mencari, atau melacak komputer-komputer server yang security-nya sangat lemah (vulnerabilities). Di ciptakan pada akhir tahun 1999 oleh Doc Holiday dan Ganymed.

- www.computec.ch/software/webserver
- www16.brinkster.com/erytricky/Software/thc.zip

Hacking Tools:

Instant Source, Wget, WebSleuth, Black Widow, Window Bomb