



KEAMANAN SISTEM INFORMASI

Pertemuan VI

Keamanan World Wide Web

Rianto, S.Kom., M.Eng.

Fakultas Sains dan Teknologi

Universitas Teknologi Yogyakarta

Email : me@rianto.com Website : <http://www.rianto.com>

Mobile : 0815 787 02873

Daftar Isi

- Deface
- SQL Injection
- Kelemahan Form HTML

Web Hacking

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. **XSS**

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

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 (Lanjutan)

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).

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**.

SQL Injection

- SQL Injection attack merupakan salah satu teknik dalam melakukan web hacking untuk menggapai akses pada sistem database.
- Teknik ini memanfaatkan kelemahan dalam scripting pada SQL dalam mengolah suatu sistem yang memungkinkan seseorang tanpa account dapat masuk dan lolos verifikasi.

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

Untuk mengatasi hal ini, atur agar:

- Hanya karakter tertentu yang boleh diinput.
- Jika terdeteksi adanya *illegal character*, langsung tolak permintaan.

Java Script Scripting

JavaScript sendiri merupakan suatu *scripting language* yang dieksekusi di sisi client (komputer pengguna), sehingga suatu transaksi yang menggunakan JavaScript sebagai *scripting language*-nya dapat dipastikan sangat rawan terhadap manipulasi dari sisi pemakai.

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)

Kelemahan Dasar Form HTML

- 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.

Kelemahan Dasar Form HTML

- Masalahnya dengan menggunakan GET, variabel yang digunakan akan terlihat pada kotak URL, yang memungkinkan pengunjung langsung memasukkan karakter pada form 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.

Kelemahan Dasar Form HTML

- Masalahnya dengan menggunakan GET, variabel yang digunakan akan terlihat pada kotak URL, yang memungkinkan pengunjung langsung memasukkan karakter pada form 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.

Studi Kasus dan Bahan Diskusi

- Buku Tamu pada sebuah situs dan HTML Special Character

Daftar Pustaka

- Keamanan Sistem Informasi
Dr. Budi rahardjo