# Deteksi Malicious Code Javascript Pada Browser Internet

Sholeh Umar, mafia@student.eepis-its.edu

*Abstract*---- Pada suatu web page sering ditemukan website yang di dalamnya tersisipi *code* Java *Script* yang terdapat bermacam-macam fungsi dari *script* itu .Tidak dapat dipungkiri bahwa *code Java Script* lebih fleksibel dan menarik.Namun didalam Java Script itu terdapat *code-code* yang baik untuk memperindah tampilan tersebut,agar tampilan web nyaman,bagus,menarik untuk diliat dan juga ada kode yang buruk (*Malicious Code*) yang digunakan untuk kejelekan contoh kecilnya untuk mengganggu pengunjung serta kenyamanan pada pengunjung pada web yang disisipi *code Malicious* tersebut,ataupun pencurian cookies user.

Alangkah baiknya jika pengunjung tahu bahwa ada script yang tidak baik untuk diakses sehingga pengunjung diberi saran untuk tidak mengakses website tersebut atau meniggalkan website tersebut untuk keamanan pribadi pengunjung serta keamanan *computer* tersebut.Dan agar pula demi menjaga privasi pengunjung dan terhindar dari gangguan orang lain juga.Oleh karena itu kita gunakan aplikasi pendeteksi *code-code Malicious* tersebut agar tehindar dari bermacam-macam gangguan yang lain.

.

*Index Terms*----*Malicious code, Java Script*.

## I. PENDAHULUAN

Penelitian yang dilakukan pada tugas akhir ini adalah untuk membuat sebuah aplikasi yang berfungsi mencegah adanya Malicious Code javascript pada browser internet.

Diharapkan aplikasi yang dibangun dapat mengenali jenis-jenis *malicious code* sehingga dapat membedakan script yang berbahaya dan tidak berbahaya untuk di akses,yang kemudian bila ada script berbahaya aplikasi tersebut dapat memberikan *alert*,sehingga user tahu bahwa ada script berbahaya yang sedang diakses.

Selain memberikan alert dan dapat membaca script berbahaya,aplikasi ini diharapkan juga dapat memberikan solusi diantaranya memfilter data yang masuk kedalam computer user dan juga memberikan solusi terbaik apa yang harus dilakukan oleh user yang sedang browswing nantinya.

Proyek ini dilakukan untuk membangun aplikasi keamanan jaringan.Dan nantinya aplikasi ini diharapkan dapat membantu keamanan user untuk browsing.

## II. DATA DAN TINJAUAN PUSTAKA

Pada Project ini terdapat tinjauan pustaka yang akan membahas tentang teori – teori yang menunjang dalam menyelesaikan proyek akhir ini. Beberapa teori penunjang pada proyek akhir ini adalah sebagai berikut :

### A. AVG LINK SCANNER


Baru saja AVG merilis salah satu fitur (fasilitas) bawaan Antivirusnya, AVG LinkScanner sebagai software terpisah dan gratis. AVG LinkScanner bertujuan menganalisis dan mengecek halaman web atau link sebelum dibuka akan kemungkinan adanya bahaya.

Dengan banyaknya jutaan alamat di Internet, diperkirakan oleh AVG bahwa ada lebih dari 2 juta alamat situs yang disusupi oleh ancaman tersembunyi, baik diketahui atau tidak dan terjadi 100.000 sampai 150.000 ancaman dalam sehari.

AVG LinkScanner memberikan 2 fitur utama, yaitu :

1. Search-Shield, yang menyecan hasil pencarian, misalnya di google, dan memberikan rating untuk tiap hasil link

yang diberikan. Sehingga user bisa lebih tahu apakah link tersebut aman untuk di klik.

2. Active Surf-Shiled, akan menyecan halaman website ketika kita klik atau memasukkan alamat website di web browser. Jika Halaman tersebut terinfeksi, maka akan dihentikan membukanya

Dikutip dari:
http://ebsoft.web.id/2009/04/21/avg-merilis-avg-linkscanner-sebagai-software-gratis-terpisah/
Namun contoh aplikasi diatas berbeda dengan aplikasi yang akan dibuat nantinya,diantara perbedaannya ialah:

a. Aplikasi ini melakukan stream untuk semua packet data port 80,dan sebelum masuk ke level applikasi(browser)
b. Aplikasi ini tidak berpengaruh user menggunakan browser apapun,akan tetapi AVG LinkScanner ini dapat digunakan bagi pengguna Internet Explorer dan Mozilla Firefox.

Mungkin ini perbedaan dan sedikit pembanding aplikasi yang akan di buat dengan aplikasi yang sudah ada

.

## B. MALICIOUS CODE

*Malicious Code* disingkat (malcodes) atau bisa disebut Kode jahat/perusak, didefinisikan sebagai program, atau script yang dapat dieksekusi dan dibuat dengan tujuan untuk merusak sistem komputer. Oleh karena itu script yang dibuat secara tidak sengaja oleh programer, tidak termasuk dalam kategori ini. Tetapi untuk script yang benar-benar mengganggu, banyak orang mengkategorikannya sebagai malcode.

**Klasifikasi**

Kode perusak dapat digolongkan dalam 3 macam golongan: virus, worm dan Trojan Horses..

**Virus**

Virus memiliki kemampuan jahat untuk mereproduksi diri mereka sendiri dan terdiri dari kumpulan *code* yang dapat memodifikasi target *code* yang sedang berjalan.

**Worm**

Worm ditujukan kepada program yang mengkopi dirinya sendiri ke hanya memory *computer*.

**Trojan Horse**

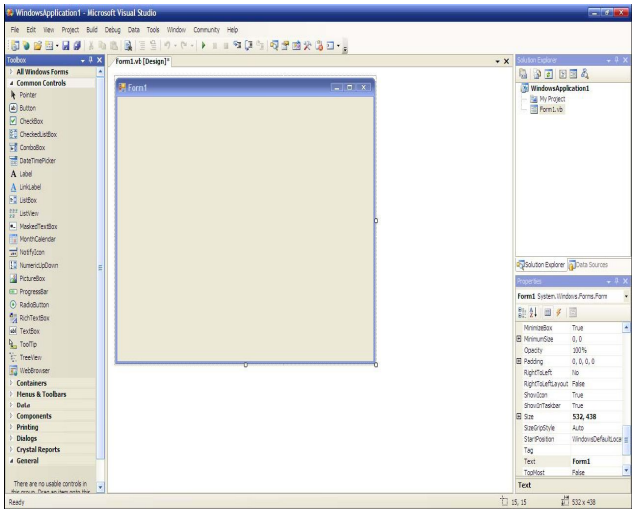
Trojan Horse diproduksi dengan tujuan jahat. Berbeda dengan virus, Trojan Horse tidak dapat memproduksi diri sendiri.

## C. Visual Basic .Net

Visual Studio.Net merupakan versi kelanjutan dari Visual Basic dimana pada .Net sudah menyertakan teknologi .Net Framework, juga adanya fasilitas windows form designer memungkinkan memperoleh aplikasi desktop dalam waktu yang sinakat dan fasilitas penyusunan kode otomatis sehingga terlihat lebih rapi dan menyediakan model pemrograman data akses berbasis *ActiveX Data Object* (ADO) ditambah dengan XML baru yang berbasis Microsoft ADO.NET :

- **Tampilan Dasar Visual Basic .Net**

Lingkungan besar yang terdiri dari beberapa bagian kecil ini menyediakan tool untuk mendesain, menjalankan dan mencari kesalahan program dari aplikasi yang dibuat.



**Gambar Utama Visual Basic .NET**

## D. REGULAR EXPRESSION

Regular expression atau biasa disingkat regex, merupakan suatu notasi fleksibel dan ringkas untuk menemukan dan menggantikan pola teks. Notasi regular expression terdiri dari dua jenis karakter dasar,yaitu karakter teks literal (normal) dan metakarakter. Karakter normal menyatakan bahwa teks harus eksis di string target, sedangkan metakarakter menyatakan teks dapat bermacam-macam di string target.

Regular expression memungkinkan kita menguraikan sejumlah teks guna menemukan pola karakter spesifik. Selain itu, Anda juga bisa mengganti, memodifikasi, atau menghapus suatu substring dengan cepat dan akurat, sesuai kriteria yang kita inginkan. Hampir semua bahasa pemrograman mengimplementasikan regular

expression, begitu pula halnya dengan Visual Basic .NET. Di .NET Framework disediakan namespace System.Text.RegularExpression
yang berisi delapan kelas untuk mendukung penggunaan regular expression. Namespace ini menyediakan fungsionalitas yang dapat digunakan pada berbagai platform atau bahasa yang berjalan di .NET Framework,termasuk C#, C++, dan J#.
Dikutip dari:
http://ilmukomputer.com
Fungsi regex pada Visual Basic.Net disini untuk mendaptakan script javascript pada TCP stream packet data yang melalui port 80,yang kemudian akan di bandingkan dengan script yang ada dalam Data Text aplikasi berikut

**E.JavaScript**

JavaScript adalah bahasa pemrograman yang khusus untuk halaman web agar halaman web menjadi lebih hidup. Kalau dilihat dari suku katanya terdiri dari dua suku kata, yaitu Java dan Script. Java adalah Bahasa pemrograman berorientasi objek, sedangkan Script adalah serangkaian instruksi program

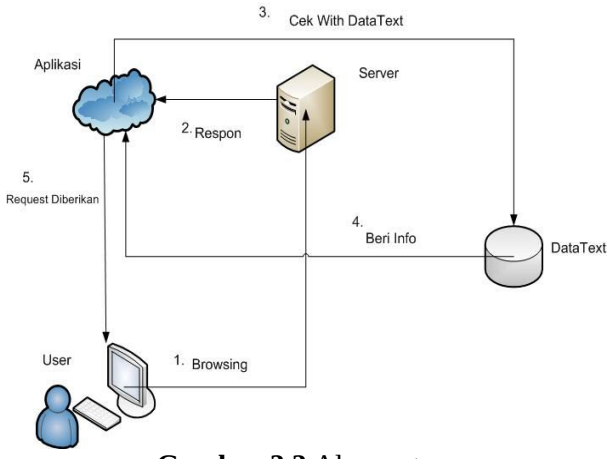
## III. PERANCANGAN SISTEM

Perancangan proyek akhir ini adalah bagaimana merancang suatu aplikasi perangkat lunak Deteksi Malicious Code JavaScript pada Browser yang secara optimal dapat melakukan proses pencegahan Script jahat yang tidak di inginkan pada saat browsing,dan lain-lain,

Perancangan sistem juga memerlukan referensi yang berhubungan dengan Deteksi Malicious Code,jenis-jenis Malicious Code yang sudah pernah ada,dan literatur lain yang mendukung baik dari buku, internet dan media lainnya.

Pengumpulan data berupa data-data yang diperlukan di aplikasi ini, khususnya datateks contoh malicious code.

### 3.1.4 DESAIN SISTEM




**Gambar 3.3** Alur system

Penjelasan alur sistem di atas :

1. User sedang browsing/request pada server,
2. Server merespon dan memberikan semua request kepada user yang sedang *request*,
3. Aplikasi menangkap hasil respon dari server,
4. kemudian aplikasi mengecek dengan data text yang sudah ada
5. jika terdapat script yang bahaya,maka memberikan *warning*,dan memberikan solusi,
6. jika tidak ada *code* yang berbahaya maka ditampilkan semua hasil respon dari server kepada user,
7. selesai

## IV. SOFTWARE DEVELOPMENT

Disini ada contoh interface yang di harapkan nantinya: :


**Gambar 4.1** Interface

REFERENCES


[1] Hallaraker, Vigna. (2004). *Detecting Malicious Javascript Code in Mozilla*. University of California, Santa Barbara.

[2] Michael Zalewski. Google browser security handbook

[3] http://en.wikipedia.org/wiki/Malicious_code_detection <diakses pada tanggal 29-Januari-2009,pukul 16.00>

[4] http://www.webopedia.com/TERM/M/malicious_code.html <diakses pada tanggal 29-Januari-2009,pukul 16.00>

[5] WAHDI 'S BLOG: Kode Jahat/Perusak (Malicious Codes) http://wahdisblog.blogspot.com/2007/07/kode-jahatperusak-malicious-codes.html <diakses pada tanggal 29-Januari-2009,pukul 16.00>