Kelvin Samarvin

172101763 / C4

1. XSS Attack
   Cross site scripting adalah serangan injeksi kode pada sisi klien dengan menggunakan sarana halaman website atau web aplikasi. Peretas akan mengeksekusi skrip berbahaya di browser korban dengan cara memasukkan kode berbahaya ke halaman web atau web aplikasi yang sah. Serangan ini dapat dilakukan menggunakan JavaScript, VBScript, ActiveX, Flash, dan bahasa sisi klien lainnya.

   Adapun tujuan digunakannya *Script* XSS (Cross-Site Scripting) adalah sebagai berikut:

   - Untuk menyamar sebagai atau menyamar sebagai pengguna korban.
   - Melakukan tindakan apa pun yang dapat dilakukan pengguna.
   - Untuk membaca data apa pun yang dapat diakses pengguna.
   - Menangkap kredensial login pengguna.
   - Melakukan perusakan virtual situs web.
   - Menyuntikkan fungsionalitas trojan ke situs web.

Tahapan dalam XSS:

A. Menjalankan Kode JavaScript

Untuk menjalankan kode JavaScript berbahaya di browser korban, penyerang harus terlebih dahulu menemukan cara untuk menyuntikkan kode berbahaya (payload) ke halaman web yang dikunjungi korban.

B. Memulai Akses

Setelah itu, korban harus mengunjungi dan mengakses halaman web dengan kode berbahaya. Jika serangan diarahkan pada korban tertentu, penyerang dapat menggunakan rekayasa sosial dan / atau phishing untuk mengirim URL jahat ke korban.Agar langkah pertama dimungkinkan, situs web yang rentan perlu memasukkan input pengguna secara langsung ke halaman-halamannya. Seorang penyerang kemudian dapat memasukkan string jahat yang akan digunakan dalam halaman web dan diperlakukan sebagai kode sumber oleh browser korban. Ada juga varian serangan XSS di mana penyerang memikat pengguna untuk mengunjungi URL menggunakan rekayasa sosial dan payload adalah bagian dari tautan yang diklik pengguna.

2. Backdoor
   Istilah backdoor sekarang digunakan oleh hacker-hacker untuk merujuk kepada mekanisme yang mengizinkan seorang peretas sistem dapat mengakses kembali sebuah sistem yang telah diserang sebelumnya tanpa harus mengulangi proses eksploitasi terhadap

sistem atau jaringan tersebut, seperti yang ia lakukan pertama kali. Umumnya, setelah sebuah jaringan telah diserang dengan menggunakan exploit (terhadap sebuah kerawanan/vulnerability), seorang penyerang akan menutupi semua jejaknya di dalam sistem yang bersangkutan dengan memodifikasi berkas catatan sistem (log) atau menghapusnya, dan kemudian menginstalasikan sebuah backdoor yang berupa sebuah perangkat lunak khusus atau menambahkan sebuah akun pengguna yang memiliki hak akses sebagai administrator jaringan atau administrator sistem tersebut. Jika kemudian pemilik jaringan atau sistem tersebut menyadari bahwa sistemnya telah diserang, dan kemudian menutup semua kerawanan yang diketahui dalam sistemnya (tapi tidak mendeteksi adanya backdoor yang terinstalasi), penyerang yang sebelumnya masih akan dapat mengakses sistem yang bersangkutan, tanpa ketahuan oleh pemilik jaringan, apalagi setelah dirinya mendaftarkan diri sebagai pengguna yang sah di dalam sistem atau jaringan tersebut. Dengan memiliki hak sebagai administrator jaringan, ia pun dapat melakukan hal yang dapat merusak sistem atau menghilangkan data. Dalam kasus seperti di atas, cara yang umum digunakan adalah dengan melakukan instalasi ulang terhadap sistem atau jaringan, atau dengan melakukan restorasi dari cadangan/backup yang masih bersih dari backdoor.

Tujuan backdoor pada web server digunakan untuk melakukan aktivitas berbahaya, seperti:

- Pencurian data
- Pembajakan server
- Merusak situs web
- Menaruh virus pada pengunjung website

3. DDoS Attack

DDoS adalah serangan yang sangat populer digunakan oleh hacker. Selain mempunyai banyak jenis, DDoS memiliki konsep yang sangat sederhana, yaitu membuat lalu lintas server berjalan dengan beban yang berat sampai tidak bisa lagi menampung koneksi dari user lain (overload). Salah satu cara dengan mengirimkan request ke server secara terus menerus dengan transaksi data yang besar.

Cara kerja dan tujuan dilakukannya DDoS attack:

- Request flooding merupakan teknik yang digunakan dengan membanjiri jaringan menggunakan banyak request. Akibatnya, pengguna lain yang terdaftar tidak dapat dilayani.
- Traffic flooding merupaka teknik yang digunakan dengan membanjiri lalu lintas jaringan dengan banyak data. Akibatnya, pengguna lain tidak bisa dilayani.
- Mengubah sistem konfigurasi atau bahkan merusak komponen dan server juga termasuk tipe denial of service, tetapi cara ini tidak banyak digunakan karena cukup sulit untuk dilakukan.

Tujuan dari serangan DDoS ini adalah menghabiskan semua bandwidth yang tersedia antara target dengan jaringan internet. Caranya adalah dengan membuat lalu lintas yang sangat padat, seperti penggunaan botnet.