Nama : MUHAMMAD ZULFIKRAN

Nim : 22650174

JenisJenis Serangan Siber di Aplikasi Web dan Contoh Penyerangannya

A. Serangan Siber di Aplikasi Web

1. SQL Injection (SQLi)

   Definisi Serangan yang mengeksploitasi kerentanan dalam input aplikasi web untuk menjalankan perintah SQL berbahaya pada database backend. Contoh Penyerang memasukkan perintah SQL seperti `' OR '1'='1` pada kolom login untuk mendapatkan akses tanpa otorisasi.

2. CrossSite Scripting (XSS)

   Definisi Serangan yang memungkinkan penyerang menyisipkan skrip berbahaya ke dalam situs web yang kemudian dijalankan di browser pengguna lain. Contoh Penyerang memasukkan kode JavaScript berbahaya pada formulir komentar untuk mencuri cookie pengguna.

3. CrossSite Request Forgery (CSRF)

   Definisi Serangan yang memaksa pengguna untuk menjalankan tindakan yang tidak diinginkan di aplikasi web yang sudah diautentikasi. Contoh Penyerang mengirimkan tautan yang mengarahkan pengguna untuk mengirimkan permintaan transfer dana tanpa sepengetahuan mereka.

4. Distributed Denial of Service (DDoS)

   Definisi Serangan yang berupaya membuat aplikasi web tidak tersedia dengan membanjiri server dengan lalu lintas yang berlebihan. Contoh Serangan menggunakan botnet untuk membanjiri server aplikasi web dengan jutaan permintaan per detik.

5. File Inclusion

Definisi Serangan yang mengeksploitasi kelemahan pada aplikasi web untuk memasukkan file berbahaya dari server lokal atau eksternal. Contoh Penyerang menggunakan parameter URL untuk memasukkan file berisi skrip berbahaya seperti `http//example.com/index.php?page=../../evil.php`.

6. ManintheMiddle (MITM)

Definisi Serangan di mana penyerang mencegat komunikasi antara pengguna dan server untuk mencuri data sensitif. Contoh Penyerang menggunakan jaringan WiFi publik tanpa enkripsi untuk mencuri kredensial login pengguna.

7. Brute Force Attack

Definisi Serangan yang mencoba berbagai kombinasi username dan password secara otomatis hingga menemukan yang benar. Contoh Penyerang menggunakan skrip otomatis untuk mencoba ribuan kombinasi kata sandi pada formulir login aplikasi web.

8. Remote Code Execution (RCE)

Definisi Serangan yang memungkinkan penyerang menjalankan kode berbahaya pada server aplikasi web. Contoh Penyerang mengunggah file PHP berbahaya melalui fungsi unggah file tanpa validasi yang memadai.

9. Directory Traversal

Definisi Serangan yang mengeksploitasi kerentanan untuk mengakses direktori atau file yang tidak dimaksudkan untuk diakses oleh pengguna.Contoh Penyerang menggunakan URL seperti `http//example.com/index.php?file=../../etc/passwd` untuk membaca file sistem.

10. ZeroDay Exploits

Definisi Serangan yang memanfaatkan kerentanan yang belum diketahui oleh pengembang perangkat lunak atau vendor keamanan. Contoh

Penyerang mengeksploitasi kerentanan baru dalam framework aplikasi web sebelum ada patch keamanan yang dirilis.

B. Cara Mencegah Serangan Siber

1. Validasi Input Selalu lakukan validasi dan sanitasi data yang dimasukkan oleh pengguna.
2. Gunakan HTTPS Enkripsi komunikasi antara server dan pengguna.
3. Perbarui Sistem Secara Berkala Terapkan pembaruan keamanan untuk aplikasi, framework, dan server.
4. Gunakan Firewall Aplikasi Web (WAF) Lindungi aplikasi web dari ancaman umum.
5. Gunakan Teknik Otentikasi yang Kuat Implementasikan autentikasi dua faktor (2FA).
6. Monitoring dan Logging Pantau aktivitas aplikasi web untuk mendeteksi anomali.

C. Kasus Nyata

1. **SQL Injection (SQLi)**

   Pada tahun 2012, sebuah situs kartu kredit di AS diserang melalui SQL Injection. Penyerang berhasil mencuri data pelanggan termasuk nomor kartu kredit dengan memanfaatkan input login yang tidak divalidasi.

2. **Cross-Site Scripting (XSS)**

   Pada tahun 2017, XSS ditemukan di aplikasi web milik Yahoo! Mail. Penyerang bisa menyisipkan skrip berbahaya untuk mencuri cookie pengguna yang memungkinkan mereka mengakses akun email korban.

3. **Cross-Site Request Forgery (CSRF)**

   Pada 2008, CSRF menyerang platform media sosial MySpace. Penyerang membuat pengguna secara tidak sadar memposting pesan ke profil mereka hanya dengan mengunjungi halaman tertentu.

4. **Distributed Denial of Service (DDoS)**

   Pada Oktober 2016, serangan DDoS besar-besaran terhadap penyedia DNS Dyn menyebabkan gangguan akses ke situs besar seperti Twitter, Reddit, dan Netflix. Serangan dilakukan melalui botnet Mirai.

5. **File Inclusion**

   Pada tahun 2010, sebuah situs komunitas online diserang melalui **Local File Inclusion (LFI)**. Penyerang membaca file konfigurasi server yang mengandung informasi sensitif, seperti kredensial database.

6. **Man-in-the-Middle (MITM)**

   Pada 2015, serangan MITM dilakukan melalui jaringan Wi-Fi publik. Penyerang berhasil mencuri kredensial login bank pengguna yang tidak menggunakan HTTPS untuk enkripsi data.

7. **Brute Force Attack**

   Pada tahun 2017, sebuah situs WordPress besar menjadi target serangan brute force untuk login admin. Ribuan kombinasi username dan password dicoba hingga akun admin berhasil ditembus.

8. **Remote Code Execution (RCE)**

   Pada tahun 2021, kerentanan **Log4Shell** di library Log4j menyebabkan RCE di banyak aplikasi web populer. Penyerang dapat mengontrol server hanya dengan menyisipkan input tertentu.

9. **Directory Traversal**

   Pada tahun 2018, platform e-commerce menemukan eksploitasi Directory Traversal. Penyerang mengakses file konfigurasi server dan mencuri kunci API yang digunakan untuk integrasi pembayaran.

10. **Zero-Day Exploits**

    Pada tahun 2020, sebuah eksploitasi zero-day ditemukan di aplikasi Zoom. Kerentanan ini memungkinkan penyerang mengambil alih kontrol komputer pengguna hingga Zoom merilis patch keamanan.