Keamanan Siber

Pertemuan # Web App Security

Always The First

Web Application Security

- Pentingnya Keamanan: Aplikasi web terhubung ke internet dan rentan terhadap berbagai serangan.
- Ancaman Utama: Serangan seperti XSS, SQL Injection, dan CSRF dapat membahayakan pengguna dan data.
- Data Sensitif: Pengguna sering kali berbagi data pribadi yang perlu dijaga keamanannya.
- Peran Developer: Pengembang bertanggung jawab mengimplementasikan keamanan pada aplikasi.
- Tujuan Keamanan: Mengurangi risiko dan melindungi kepercayaan pengguna terhadap aplikasi.

World Wide Web (WWW)

- Definisi WWW: Sistem jaringan yang menghubungkan dokumen melalui internet.
- Sejarah WWW: Dikembangkan oleh Tim Berners-Lee pada akhir 1980-an.
- HTTP dan HTTPS: Protokol dasar yang digunakan untuk transfer data di WWW.
- Akses Global: WWW memungkinkan pengguna di seluruh dunia untuk mengakses informasi.
- Teknologi Pendukung: HTML, CSS, dan JavaScript untuk pembuatan halaman web.

Cara Kerja WWW

- Protokol HTTP/HTTPS: HTTP untuk komunikasi umum, HTTPS untuk komunikasi terenkripsi.
- Model Client-Server: Klien (browser) meminta data, server merespons dengan konten.
- Browser sebagai Klien: Browser mengirimkan permintaan dan menampilkan hasil.
- Peran Server: Server menyimpan dan menyediakan data atau aplikasi untuk diakses.
- Keamanan dalam Pertukaran Data: HTTPS membantu melindungi data dalam transmisi.

Struktur Dasar Aplikasi Web

- Client (Browser): Mengakses aplikasi web dan menampilkan halaman.
- Server: Tempat aplikasi dan data disimpan dan diproses.
- Basis Data: Menyimpan data yang dibutuhkan oleh aplikasi web.
- Arsitektur Tiga Tingkat: Klien, server, dan basis data membentuk arsitektur ini.
- Interaksi Client-Server-DB: Mengalirkan data untuk pengalaman pengguna yang dinamis.

Jenis Situs Web

- Situs Statis: Konten tetap, tidak berubah sesuai permintaan.
- Situs Dinamis: Menyesuaikan konten berdasarkan interaksi pengguna.
- Teknologi Dinamis: PHP, ASP.NET, dan JavaScript untuk konten interaktif.
- Keunggulan Dinamis: Dapat disesuaikan dan responsif terhadap kebutuhan pengguna.
- Contoh Situs Statis vs Dinamis: Blog vs e-commerce.

Mengapa Keamanan Penting di Aplikasi Web

- Lingkungan Terbuka: Internet adalah tempat terbuka, memudahkan akses dan risiko.
- Risiko Serangan: Data dapat dicuri, disalahgunakan, atau disusupi malware.
- Contoh Kasus: Situs e-commerce tanpa HTTPS berisiko terhadap pencurian data.
- Pengaruh Terhadap Reputasi: Situs yang rentan dapat kehilangan kepercayaan pengguna.
- Tanggung Jawab Developer: Developer harus menjaga keamanan pengguna dengan optimal.

Cross-Site Scripting (XSS)

- Definisi XSS: Serangan yang memasukkan skrip berbahaya ke dalam halaman web.
- Cara Kerja: Skrip berbahaya dieksekusi di browser pengguna tanpa sepengetahuan mereka.
- Jenis XSS: Stored, Reflected, dan DOM-based.
- Dampak: Pencurian data pribadi dan pembajakan akun pengguna.
- Pencegahan: Validasi input, CSP, dan hindari data pengguna langsung dalam HTML.

SQL Injection (SQLi)

- Definisi SQLi: Serangan di mana perintah SQL berbahaya dimasukkan ke dalam input.
- Cara Kerja: Penyerang memasukkan kode SQL untuk akses tidak sah ke database.
- Dampak: Dapat melihat, menghapus, atau mengubah data sensitif.
- Contoh Kasus: Aplikasi yang tidak memvalidasi input rentan terhadap serangan ini.
- Pencegahan: Parameterized queries dan prepared statements untuk input.

Cross-Site Request Forgery (CSRF)

- Definisi CSRF: Serangan di mana penyerang membuat pengguna melakukan tindakan tanpa sadar.
- Cara Kerja: Permintaan dibuat dari situs lain saat pengguna telah login.
- Dampak: Pengubahan data pengguna atau pengambilalihan akun.
- Contoh: Pengguna mengklik tautan berbahaya yang memodifikasi akun mereka.
- Pencegahan: Token anti-CSRF, otentikasi dua faktor, dan verifikasi identitas.

Remote & Local File Inclusion (RFI/LFI)

- Definisi: RFI menyertakan file eksternal, LFI menggunakan file lokal dalam aplikasi.
- Cara Kerja: Penyerang memuat file jahat melalui input aplikasi.
- Dampak: Eksekusi kode tidak sah, pencurian data, akses tidak sah ke server.
- Contoh Kasus: Aplikasi yang menerima jalur file dari pengguna tanpa validasi.
- Pencegahan: Batasi input file dan hanya izinkan file dari sumber terpercaya.

Scanning Vulnerability Tools

- Pentingnya Scanning: Deteksi dini kerentanan mencegah serangan.
- Acunetix: Alat scanning otomatis untuk SQLi, XSS, dll.
- W3AF: Framework open-source untuk audit keamanan aplikasi web.
- WPScan: Alat khusus untuk scanning kerentanan pada WordPress.
- Penggunaan: Identifikasi dan perbaikan kerentanan sebelum eksploitasi.

Server Hardening

- Definisi: Menguatkan keamanan server dengan konfigurasi optimal.
- Langkah: Menonaktifkan layanan tidak perlu untuk mengurangi risiko.
- Firewall: Membatasi lalu lintas dan akses dari luar.
- Kontrol Akses: Izin terbatas untuk mencegah akses tidak sah.
- Keamanan Konfigurasi: Pengaturan tambahan untuk keamanan data di server.

Kontrol Akses

- Prinsip Least Privilege: Memberikan hak akses minimum sesuai kebutuhan.
- Role-Based Access Control (RBAC): Akses berdasarkan peran pengguna.
- Separation of Duties: Memisahkan tugas penting untuk mengurangi risiko.
- Contoh: Hanya admin yang memiliki hak untuk mengelola akun pengguna.
- Pentingnya: Menghindari penyalahgunaan akses pada aplikasi web.

Session Management

- Pentingnya Manajemen Sesi: Mencegah session hijacking atau pembajakan sesi.
- Penggunaan Token: Menggunakan token yang aman dan unik untuk setiap sesi.
- Batas Waktu Sesi: Menetapkan kedaluwarsa sesi untuk keamanan.
- Single Session Per User: Membatasi pengguna hanya satu sesi aktif.
- Best Practice: Gunakan token yang sulit ditebak dan amankan sesi pengguna.

SSL/TLS dan HTTPS

- Definisi SSL/TLS: Protokol keamanan yang mengenkripsi data antara klien dan server.
- HTTPS: HTTP dengan enkripsi SSL/TLS untuk komunikasi aman.
- Cara Kerja: Sertifikat SSL memastikan enkripsi dan identifikasi server.
- Jenis Sertifikat: DV, OV, EV – tingkat validasi yang berbeda.
- Manfaat: Meningkatkan keamanan data dan kepercayaan pengguna.

Keamanan Sisi Klien

- Risiko Sisi Klien: Ancaman XSS, CSRF, Clickjacking dapat terjadi di browser.
- Keamanan Browser: Selalu gunakan browser terbaru dan aman.
- CSP: Content Security Policy mencegah XSS dengan membatasi sumber skrip.
- SameSite Cookies: Mencegah CSRF dengan mengatur cookie lintas situs.
- Pentingnya Edukasi: Pengguna perlu memahami ancaman umum.

Edukasi Pengguna & Keamanan Sandi

- Kesadaran Keamanan: Mengedukasi pengguna tentang ancaman siber.
- Sandi Unik: Menghindari penggunaan kata sandi yang sama di beberapa situs.
- Pengelola Kata Sandi: Alat untuk menyimpan kata sandi dengan aman.
- Klik yang Aman: Hindari klik tautan atau unduhan dari sumber tidak dikenal.
- Dampak: Edukasi membantu mengurangi risiko serangan terhadap pengguna.

Kesimpulan

- Perlunya Keamanan: Melindungi aplikasi web dan data pengguna sangat penting.
- Kepercayaan Pengguna: Keamanan yang baik membangun kepercayaan pengguna.
- Pencegahan Dini: Implementasi keamanan sejak awal pengembangan.
- Keamanan Berkelanjutan: Update, patch, dan pemantauan rutin sangat penting.
- Kesadaran Developer: Pentingnya kesadaran keamanan untuk aplikasi modern.

INSTITUT TEKNOLOGI DAN BISNIS STIKOM BALI

Kampus Merdeka INDONESIA JAYA

Single Degree Program

S2 - Sistem Informasi (M.Kom.)
S1 - Sistem Komputer (S.Kom.)
S1 - Sistem Informasi (S.Kom.)
S1 - Teknologi Informasi (S.Kom.)
S1 - Bisnis Digital (S.Bns.)
D3 - Manajemen Informatika (A.Md.Kom.)

Dual Degree International Program

S1 - Sistem Informasi (S.Kom., B.IT.)
(collaboration with HELP University)
S1 - Bisnis Digital (S.Bns., B.M.)
(collaboration with DNUI University)

Dual Degree National Program

S1 - Sistem Informasi (S.Kom., S.Ds.)
(collaboration with Universitas Teknologi Bandung)

www.stikom-bali.ac.id info@stikom-bali.ac.id (0361) 244445

STIKOMERS TV STIKOM Bali @stikombali

Always The First