ISSN 2962–5688
Website :
jurnal.umj.ac.id/index.php/TripleA
Email : triplea@umj.ac.id

TRIPLE A
Jurnal Pendidikan Teknologi Informasi

PROTOKOL SECURE SOCKET LAYER UNTUK KEAMANAN BERBASIS WEB

Muhammad Azwan[1*)], Ahmad Fikri Adriansyah[2*)], Muhammad Rifki Al Fauzan[3*)]
[1)] Pendidikan Teknologi Informasi, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Muhammadiyah Muara Bungo, Jl. Rang Kayo Hitam, Cadika, Kec. Rimbo Tengah, Kabupaten Bungo, Jambi 37211
[2,3)]Pendidikan Teknologi Informasi, Fakultas Ilmu Pendidikan, Universitas Muhammadiyah Jakarta, Jl. K.H. Ahmad Dahlan, Cireundeu, Kec. Ciputat Timur., Kota Tangerang Selatan, Banten 15419

[*]*azwanstarmimoor01@gmail.com*

ABSTRACT

Internet is defined as an interconnected network which can literally be interpreted as a connected network. Simply put, the Internet is Simply put, the Internet is a assembly of interconnected computers. Part of the Internet is the World Wide Web (WWW), or what is now commonly known as web technology. Information on the Web is one of the means of communicating information quickly, up-to-date, and efficiently. As web usage grows and diversifies, there are other things to consider. It's the security of the website itself. Often referred to as web security or web security, it basically means protecting a website or web application by detecting, preventing, and responding to cyberthreats. The research uses Secure Socket Layer as one of the security protocols that protects transactions on websites with advanced data encryption techniques..
Keywords*: Internet, Web, Secure Socket Layer*

ABSTRAK

Internet didefinisikan sebagai interconnected network yang secara harfiah dapat diartikan sebagai jaringan yang terhubung. Sederhananya, Internet adalah kumpulan komputer yang terhubung satu sama lain. Bagian dari Internet adalah World Wide Web (WWW) atau yang sekarang biasa dikenal dengan teknologi Web. Informasi melalui web merupakan salah satu sarana untuk menyampaikan informasi dengan cepat, terbaru dan efisien. Disamping penggunaan web yang terus meningkat dan beragam ada hal lain yang perlu diperhatikan yaitu mengenai keamanan situs web itu sendiri. Keamanan dunia maya, atau sering disebut dengan cyber-secure, pada dasarnya berarti melindungi situs web atau situs web dengan mengidentifikasi, mencegah, dan menanggapi ancaman dunia maya.
Kata Kunci: *Internet, Web, Lapisan Soket Aman*

DOI:https://

TRIPLE A: Jurnal Pendidikan Teknologi Informasi. Vol. 1 (2), pp: 81-85.

PENDAHULUAN

Dengan terus berkembangnya system teknologi informasi, sistem yang dapat memudahkan penggunaan dan pencarian informasi apapun dalam bentuk halaman web juga semakin meningkat. Sering kali pengguna hanya fokus terhadap penggunaan sebuah website tanpa memperhatikan tingkat keamanan yang harusnya juga menjadi perhatian. Keamanan merupakan aspek yang sangat penting dalam sebuah website. Menjaga keamanan dan kerahasiaan data online memerlukan suatu teknik enkripsi data yang digunakan untuk menyembunyikan data dari pihak ketiga. Metode yang cukup andal untuk melindungi data secara real-time adalah protokol Secure Socket Layer (SSL).

TINJAUAN PUSTAKA

Keamanan Website

Keamanan website adalah suatu aktivitas untuk melindungi website dan jaringannya dari berbagai ancaman. Mulai dari pencurian data, hingga perusakan software dan hardware. Umumnya, keamanan website disebut juga dengan cyber security. Keamanan website adalah salah satu prioritas utama pengembang web. Jika seseorang mengabaikan perlindungan ini, seorang peretas dapat memperoleh informasi penting dan bahkan mengubah format website tersebut.

Keamanan

Keamanan adalah suatu keadaan dimana tidak ada resiko atau bahaya. Dalam dunia TI keamanan berarti terbebasnya segala sesuatu yang mencakup semua permasalahan keamanan baik secara fisik ataupun non fisik.

Web

web adalah penyebaran informasi melalui Internet. Web, juga dikenal sebagai situs web, berisi berbagai informasi tekstual, tanggal, data. Gambar membisu atau bergerak, data animasi, suara, video atau kombinasi berdasarkan semuanya, baik tidak aktif juga dinamis, menciptakan rangkaian bangunan yg saling berhubungan, masing-masing dihubungkan oleh jaringan halaman atau hyperlink. Atau pengertian website adalah kumpulan halaman web yang berbeda dikelompokkan ke dalam domain atau subdomain. Tentu saja, ini lebih dari sekadar tempat di World Wide Web (WWW), yaitu Internet.

Internet

Internet adalah sistem global jaringan komputer Perangkat yang saling terhubung yang menggunakan TCP/IP (Transmission Control Protocol/Internet Protocol Suite) untuk menghubungkan perangkat di seluruh dunia.Internet umumnya digunakan untuk mencari sebuah informasi dan memudahkan komunikasi antar satu pihak ke pihak lain tanpa harus terhalang oleh jarak dan waktu.

***Secure Socket Layer* (SSL)**

SSL (Secure Socket Layer), sebuah protokol keamanan internet terenkripsi yang menyediakan privasi, otentikasi, dan integritas komunikasi Internet. Fitur keamanan Awalnya dikembangkan oleh Netscape pada tahun 1995. Dengan SSL, proses transmisi data website dienkripsi agar lebih aman.

METODE PENELITIAN

Peneletian ini menggunakan metode pengumpulan data dan informasi yang bertujuan untuk menambah pengetahuan dan mengembangkan keterampilan dalam dunia teknologi yang berfokus pada keamanan web(web security).

Pengumpulan data dilakukan dengan observasi dan studi pustaka, dilanjutkan dengan metode penelitian diawali dengan perencanaan, pemecahan masalah, dilanjutkan dengan analisis kebutuhan, dilanjutkan dengan tahap akhir desain, yang kemudian dapat diimplementasikan pada model yang sudah ada. masalah.

HASIL DAN PEMBAHASAN

Web/ Situs web adalah sekelompok halaman di domain Internet yang dibuat untuk tujuan tertentu dan dihubungkan bersama dan umumnya dapat diakses Melalui halaman awal browser melalui URL situs web. (Firmansyah, 2020).

Halaman web biasanya adalah dokumen yang ditulis dalam HTML (Hyper Text Markup Language) dan diakses melalui HTTP. HTTP adalah protokol untuk mengirimkan berbagai informasi dari server situs web dilihat oleh satu atau lebih pengguna melalui browser. (sora, 2014). Pada penelitian dengan observasi dan studi literature menunjukan bahwa web tanpa penggunaan protocol Secure Socket Layer(SSL)sangat rentan terhadap serangan(attack). Dengan adanya protocol Secure Socket Layer dipastikan situs web akan lebih aman terlindungi dari ancaman dan serangan dari pihak lain.

SSL atau Secure Sockets Layer adalah teknologi keamanan standar yang membuat koneksi terenkripsi antara server dan klien. Ini biasanya disebut sebagai server web dan browser, atau server email dan program email (seperti Microsoft Outlook). Secure Sockets Layer adalah server dan klien (biasanya server web dan browser, atau server email, program email (seperti Microsoft Outlook). SSL sendiri merupakan teknologi yang diperlukan untuk mengamankan komunikasi dan transmisi data antara web server dan user. SSL dapat digunakan melindungi informasi rahasia seperti nomor kartu kredit, kata sandi, dan informasi penting lainnya. Ini karena SSL sengaja mengenkripsi alias mengacak struktur data. Oleh karena itu, sulit bagi peretas untuk mendapatkan informasi yang benar.

Saat Browser Anda mencoba mengakses situs web yang diamankan dengan SSL, dan browser serta server web membuat koneksi menggunakan proses yang disebut "SSL handshake". Pada dasarnya 3 kunci digunakan untuk membuat koneksi SSL:

Kunci publik, kunci privat, dan kunci sesi. Apa pun yang dienkripsi dengan kunci publik hanya dapat didekripsi dengan kunci privat dan sebaliknya. Karena enkripsi dan dekripsi menggunakan kunci privat dan publik membutuhkan banyak daya pemrosesan, mereka digunakan untuk menghasilkan kunci sesi simetris hanya selama jabat tangan SSL. Jika koneksi aman, kunci sesi digunakan untuk mengenkripsi semua data yang dikirim. Sesi SSL selalu dimulai dengan pertukaran pesan yang disebut jabat tangan SSL. Dengan sesi

Handshake ini memungkinkan server untuk mengautentikasi dirinya sendiri ke klien menggunakan teknik kunci publik.

Langkah-langkah yang terlibat dalam pesan yang dipertukarkan selama jabat tangan SSL diringkas di bawah ini :

- Klien mengirimkan ke server nomor versi SSL klien, pengaturan enkripsi, informasi yang dihasilkan secara acak, dan informasi lain yang diperlukan server untuk berkomunikasi dengan klien melalui SSL.
- Server mengirimkan nomor versi SSL server kepada klien, pengaturan cipher, data yang dihasilkan secara acak.
- Klien menggunakan beberapa informasi yang dikirim oleh server untuk mengautentikasi server. Jika server tidak dapat diautentikasi, pengguna diperingatkan tentang masalah tersebut dan diberitahu bahwa koneksi terenkripsi dan terautentikasi tidak dapat dibuat. Jika server berhasil diautentikasi, klien akan pergi ke langkah berikutnya.
- Menggunakan semua data yang dihasilkan dalam jabat tangan sejauh ini, klien (dengan kerja sama server, tergantung pada sandi yang digunakan) membuat rahasia premaster Enkripsi sesi demi sesi menggunakan Enkripsi kunci publik server dan kirim rahasia premaster terenkripsi ke server.
- Jika server telah meminta otentikasi klien (langkah opsional dalam jabat tangan), klien juga menandatangani bagian lain dari data yang unik untuk Handshake ini dan dikenal oleh klien dan server. Dalam hal ini klien mengirimkan data yang ditandatangani dan sertifikat klien sendiri ke server bersama dengan rahasia premaster terenkripsi.
- Jika server telah meminta otentikasi klien, server mencoba untuk mengotentikasi klien. Jika klien tidak dapat diautentikasi, sesi dihentikan. Jika klien berhasil diautentikasi, server menggunakan kunci pribadinya untuk mendekripsi rahasia premaster, kemudian melakukan serangkaian langkah (yang juga dilakukan klien, mulai dari rahasia premaster yang sama) untuk menghasilkan rahasia master.
- Baik klien dan server menggunakan rahasia master untuk menghasilkan kunci sesi, yang simetri. Kunci yang digunakan untuk mengenkripsi dan mendekripsi informasi yang dipertukarkan selama sesi SSL dan untuk memverifikasi integritasnya - yaitu, untuk mendeteksi setiap perubahan dalam data antara waktu pengiriman dan waktu diterima melalui koneksi SSL.
- Klien mengirim pesan ke server yang menginformasikan bahwa pesan masa depan dari klien akan dienkripsi dengan kunci sesi. Kemudian mengirimkan pesan terpisah (terenkripsi) yang menunjukkan bahwa klien bagian handshake selesai.
- Server mengirim pesan ke klien yang menginformasikannya bahwa pesan masa depan dari server akan dienkripsi dengan kunci sesi. Kemudian mengirim pesan terpisah (terenkripsi) yang menunjukkan bahwa server bgian dari handshake selesai..
- Jabat tangan SSL sekarang selesai, dan sesi SSL telah dimulai. Klien & server memakai kunci sesi buat mengenkripsi & mendekripsi data yang mereka kirim satu sama lain dan untuk memvalidasi integritasnya.

SIMPULAN

Dari serangkaian penelitian maka disini dapat disimpulkan bahwa metode

pengamanan dengan protocol SSL(Secure Socket Layer) sangat memberi pengaruh terhadap keamanan situs web. SSL (Secure Socket Layer) merupakan lapisan keamanan yang melindungi transaksi situs web menggunakan teknologi enkripsi data tingkat lanjut. Situs web yang dilengkapi dengan enkripsi SSL beralih ke https dan simbol gembok muncul di bilah alamat browser, dan dapat ditekan untuk menampilkan Jenis SSL, teknologi enkripsi yang digunakan, dan identitas pemilik situs web. SSL memiliki banyak keunggulan, salah satunya adalah kemampuan untuk melindungi website atau website dari ancaman atau serangan yang ada.

DAFTAR PUSTAKA

Agustiara, W., Pratama, A., & Junaidi, S. (2022). "Security Analysis of Secure Socket Layer Protocol Against Packet Sniffing Attacks on the Website of the Padang Newspaper General Daily News Portal". JTIK (Journal of Informatics Engineering Kaputama), 6(1), 10-15.

Prasetyo, S. E., & Hassanah, N. (2021). "Website Security Analysis of Universitas Internasional Batam Using Issaf Method. SCIENTIFIC JOURNAL OF INFORMATICS", 9(02), 82-86.

Dastres R, & Soori M. (2020) "Secure Socket Layer (SSL) in the Network and Web Security". International Journal of Computer and Information Engineering, 14(10), 331-333.

Rachmawati R.F. (2021) "Sistem Informasi Penempatan Petugas Jaga Keamanan Berbasis Web Studi di Sekolah ACS Jakarta". Jurnal Ilmiah Teknologi Informasi Terapan, 26-34.

Mahardhika, M. A., Purwanto, Y., & Ruriawan, M. F. (2021). "Pengamanan Data Cloud Storage Dengan Menggunakan Advanced Encryption Standard Dan Elliptic Curve Digital Signature Algorithm Pada Secure Socket Layer Berbasis Website". eProceedings of Engineering, 8(2).

AHMAD, Z. M. (2021). "Pengamanan Cloud Storage dengan Penerapan Ssl (Secure Socket Layer) Menggunakan Metode Algoritma Kriptografi RSA Berbasis Aplikasi Website".

Suryawan, I. G. T., & Paramitha, I. G. D. (2021). "Analisis Kinerja Website Menggunakan Pendekatan Automated Software Testing". Jurnal Teknologi Informasi dan Komputer, 6(3).

Daud, G. S., & Maguid, M. A. (2022). "Secured Cotabato City State Polytechnic College Web-Based Student Clearance System". Randwick International of Social Science Journal, 3(1), 61-66.

Fauzan, F. Y., & Syukhri, S. (2021). "Analisis Metode Web Security PTES (Penetration Testing Execution And Standart) Pada Aplikasi E-Learning Universitas Negeri Padang". Voteteknika (Vocational Teknik Elektronika dan Informatika), 9(2), 105-111.