ANALISIS SISTEM KEAMANAN PADA APACHE WEB SERVER MENGGUNAKAN SELF SIGNED CA DI WEBMIN

SKRIPSI

FAUZAN NUGROHO **1807422024**

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2025

ANALISIS SISTEM KEAMANAN PADA APACHE WEB SERVER MENGGUNAKAN SELF SIGNED CA DI WEBMIN

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan

Untuk Memperoleh Diploma Empat Politeknik

FAUZAN NUGROHO

1807422024

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2025

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Fauzan Nugroho

NIM : 1807422024

Jurusan/Program Studi : T.Informatika dan Komputer / Teknik Multimedia dan Jaringan

Judul skripsi : Analisis Sistem Keamanan pada Apache Web Server Menggunakan Self-signed CA di Webmin

Menyatakan dengan sebenarnya bahwa skripsiini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung cirri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatantersebut.

Depok, 6 Juli 2025

Yang membuat pernyataan

Fauzan Nugroho

NIM 1807422024

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Fauzan Nugroho

NIM : 1807422024

Program Studi : Teknik Multimedia dan Jaringan

Judul Skripsi : Analisis Sistem Keamanan pada Apache Web Server Menggunakan Self-signed CA di Webmin

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Selasa,

Tanggal 8, Bulan Juli, Tahun 2025 dan

Dinyatakan **LULUS.**

Disahkan oleh

Pembimbing I : Defiana arnaldy, S. Tp., M.Si.

Penguji I : Dr. Prihatin Oktivasari, S.Si., M.Si

Penguji II : Fachroni Arbi Murad, S.Kom., M.Kom

Penguji III : Ariawan Andi Suhandana, S.Kom., M.Ti.

Mengetahui :

Jurusan Teknik Informatika dan Komputer

Ketua

Dr., Anita Hidayati , S.Kom., M.Kom.

NIP. 197908032003122003

KATA PENGANTAR

Puji syukur kepada Allah SWT berkat Rahmat, Hidayah, dan Karunia-Nya kepada kita semua sehingga penulis dapat menyelesaikan skripsi dengan judul 'Analisis Sistem Keamanan pada Apache Web Server Menggunakan Self-signed CA di Webmin' . Penulis menyadari dalam penyusunan skripsi ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Allah SWT tuhan yang maha esa, yang telah memberikan saya rizki berupa kesehatan dan akal pikiran yang sangat berharga bagi penulis sehingga laporan ini dapat terselesaikan dengan baik.
2. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan secara moral dan material.
3. Bapak Defiana arnaldy, S. Tp., M. Si. selaku pembimbing skripsi yang telah membimbing penulis dalam menyelesaikan skripsi ini.

Penulis menyadari skripsi ini tidak luput dari berbagai kekurangan. Penulis mengharapkan saran dan kritik demi kesempurnaan dan perbaikannya sehingga akhirnya laporan skripsi ini dapat memberikan manfaat bagi bidang pendidikan dan penerapan di lapangan serta bisa dikembangkan lagi lebih lanjut.

Depok, 6 Juli 2025

(Fauzan Nugroho)

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini :

Nama : Fauzan Nugroho

NIM : 1807422024

Jurusan/Program Studi : T.Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan , menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

Analisis Sistem Keamanan pada Apache Web Server Menggunakan Self-signed CA di Webmin.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta..

Demikian pernyatan ini saya buat dengan sebenarnya.

Depok, 6 Juli 2025

Yang Menyatakan

(Fauzan Nugroho)

1807422024

Analisis Sistem Keamanan pada Apache Web Server Menggunakan Self-signed CA di Webmin

Abstrak

Komunikasi data melalui protokol HTTP rentan terhadap serangan penyadapan, sementara penggunaan sertifikat dari Otoritas Sertifikat (CA) publik seringkali tidak praktis untuk lingkungan pengembangan lokal. Penelitian ini menganalisis efektivitas implementasi sertifikat yang ditandatangani sendiri (self-signed certificate) pada Apache Web Server yang dikelola melalui Webmin sebagai solusi keamanan. Metode penelitian yang digunakan adalah eksperimen dalam lingkungan virtual terisolasi yang mencakup server (Ubuntu), klien (Windows), dan penyerang (Kali Linux). Ketahanan sistem diuji melalui simulasi serangan Man-in-the-Middle (MITM) untuk membandingkan keamanan koneksi sebelum (HTTP) dan sesudah (HTTPS) implementasi sertifikat. Hasil pengujian menunjukkan bahwa koneksi HTTPS yang diamankan dengan sertifikat self-signed berhasil mengenkripsi seluruh lalu lintas data. Berbeda dengan koneksi HTTP yang memungkinkan data disadap dalam bentuk plaintext, koneksi terenkripsi ini memastikan data hanya terbaca sebagai ciphertext oleh penyerang, sehingga kerahasiaan dan integritasnya terjaga. Disimpulkan bahwa penggunaan sertifikat self-signed merupakan solusi keamanan untuk melindungi lingkungan pengembangan atau pengujian internal dari ancaman penyadapan data menggunakan metode MITM, meskipun tidak direkomendasikan untuk server produksi yang diakses publik.

Kata Kunci: *http, https, Self-signed CA, website.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi jaringan komputer berkembang dengan sangat pesat, perkembangan ini diawali oleh munculnya internet sebagai media informasi (terkoneksi dari seluruh belahan dunia). Pengaruh dari kehadiran teknologi ini yaitu mempermudah manusia untuk mengakses tugas ataupun informasi yang diinginkan dan dengan mudahnya menyelesaikan pekerjaan secara instan(Momin & Ali, 2023). Namun dengan perkembangan teknologi tersebut seperti komputer ke internet dapat membuka potensi adanya lubang keamanan (*security hole*). Hal ini menjadi masalah besar apabila tidak ditangani dengan benar karena dengan tereksploitasinya lubang keamanan, seperti *hacker* dan *intruder* (penyusup) dapat dengan mudah melakukan tindak kejahatan dalam dunia cyber yang dikenal dengan *cyber crime*.

Website adalah salah satu aplikasi yang berisikan protokol HTTP (*hyper transfer protocol*) dan untuk mengakses perangkat lunak yang disebut browser. Fungsi website diantaranya : media promosi, pemasaran, informasi, pendidikan dan komunikasi (Nurlailah & Nova Wardani, 2023). Pada pada dasarnya terdapat 4 elemen dasar dari sebuah website yaitu : browser, server, URL dan *pages*. Beberapa tahun terakhir keamanan merupakan pokok persoalan utama. Banyak diberitakan mengenai penyusupan di website dan perusahaan atau perusakan serta penghilangan aset perusahaan yang dalam bentuk digital (Mundt & Baier, 2023). *Web server* sering kali menjadi target dari berbagai jenis serangan baik yang sifatnya minor maupun major sehingga berakibat fatal. Akan tetapi, website dijadikan pintu oleh peretas (*hacker*) untuk menembus *web server* bahkan sampai ke root untuk kesenangan bahkan dengan sengaja menyerang website tersebut.

Keamanan *server website* biasanya merupakan masalah dari seorang administrator. Seorang administrator bertugas untuk mengawasi dan melakukan tindakan preventif ketika terjadi aksi penyusupan dan serangan. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima.

Terdapat berbagai cara untuk mengamankan *web server* dari serangan *hacker* salah *satunya* yaitu menggunakan SSL/TLS. *Secure Socket Layer* (SSL) adalah sebuah protokol keamanan digital yang memungkinkan proses komunikasi terenkripsi antara pengguna situs *web* dan *web browser*. *Sementara itu, Transport Layer Security* (TLS) adalah sebuah sistem keamanan yang berfokus pada perlindungan privasi dan integritas data selama transmisi informasi di jaringan. Dalam mengelola dan mengkonfigurasi web server Apache, khususnya terkait implementasi SSL/TLS, kompleksitas perintah baris seringkali menjadi tantangan bagi administrator.

Webmin hadir sebagai solusi berbasis web yang menyediakan antarmuka grafis intuitif untuk manajemen sistem UNIX, termasuk konfigurasi web server seperti Apache. Penggunaan Webmin secara signifikan mempermudah proses administrasi dan konfigurasi SSL/TLS, memungkinkan pengelolaan sertifikat, pengaturan virtual host, dan restart layanan dengan lebih efisien, bahkan bagi mereka yang kurang akrab dengan command line.

Namun, lingkungan pengujian local menghadapi kendala untuk memperoleh sertifikat dari Otoritas Sertifikat (CA) public karena memerlukan proses validasi domain yang harus dapat diakses secara publik. Sebagai solusinya, penelitian ini menggunakan sertifikat self-signed, yakni sertifikat yang ditandatangani oleh pembuatnya sendiri. Metode ini memungkinkan simulasi penuh lingkungan HTTPS terenkripsi di dalam jaringan lokal yang terisolasi untuk tujuan pengujian internal. Dengan demikian, penerapan self-signed CA menjadi langkah fundamental dalam penelitian ini untuk menganalisis cara kerja dan efektivitas SSL/TLS tanpa bergantung pada infrastruktur eksternal.

Berdasarkan permasalahan tersebut, maka penelitian yang akan dilakukan akan mengenai "Analisis Sistem Keamanan pada *Apache Web Server* Menggunakan *Self-Signed CA* di *Webmin*". Sebuah website yang sudah menggunakan SSL atau TLS, meskipun self-signed, akan menunjukkan notifikasi tertentu di browser bahwa komunikasi sudah terenkripsi. SSL atau TLS juga secara umum mempengaruhi SEO dan peringkat website di mesin pencarian karena sesuai dengan algoritma yang ditetapkan Google, di mana Google cenderung melarang penggunanya untuk mengunjungi website yang tidak memiliki atau menggunakan SSL atau TLS.

1.2 Perumusan Masalah

Berdasarkan latar belakang, perumusan masalah penelitian yang akan dikaji adalah sebagai berikut:

a. Bagaimana cara kerja Self-signed CA dalam mengamankan web server
b. Bagaimana analisis keamanan dari Self-signed CA pada Webmin
c. Seberapa efektif implementasi SSL/TLS dengan sertifikat self-signed pada Apache Web Server melalui Webmin dalam memitigasi serangan Man-in-the-Middle (MITM) di lingkungan pengujian?
d. Apa saja kelebihan dan keterbatasan teknis dari penggunaan sertifikat self-signed CA sebagai solusi enkripsi lapisan transportasi data untuk Apache Web Server dalam konteks lingkungan pengujian lokal?

1.3 Batasan Masalah

Batasan masalah yang ada dalam penelitian ini adalah :

1. Penelitian ini fokus pada implementasi dan analisis keamanan SSL/TLS menggunakan sertifikat self-signed CA. Penggunaan sertifikat dari Certificate Authority (CA) publik atau pihak ketiga tidak termasuk dalam ruang lingkup penelitian ini, karena tujuan utamanya adalah menguji lingkungan lokal.
2. Web server yang digunakan dalam penelitian ini adalah Apache Web Server.
3. Manajemen dan konfigurasi web server, khususnya terkait SSL/TLS, akan dilakukan melalui Webmin. Metode konfigurasi manual melalui command line atau tool manajemen lain di luar Webmin tidak menjadi fokus pembahasan.
4. Lingkungan pengujian SSL/TLS dan simulasi serangan Man-in-the-Middle (MITM) dilakukan dalam jaringan virtual yang terisolasi menggunakan VirtualBox, dengan mesin Ubuntu sebagai server, Windows sebagai client, dan Kali Linux sebagai attacker. Penelitian ini tidak melibatkan pengujian di lingkungan produksi atau jaringan publik.

5. Analisis keamanan difokuskan pada lapisan transportasi data (SSL/TLS) dan dampaknya terhadap kerahasiaan komunikasi serta ketahanan terhadap serangan MITM. Penelitian ini tidak membahas kerentanan aplikasi web secara spesifik seperti SQL Injection, XSS, dll. atau keamanan sistem operasi secara menyeluruh di luar konteks konfigurasi web server dan SSL/TLS.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan pembuatan skripsi ini adalah untuk:

1. Mengimplementasikan sertifikat self-signed CA pada Apache Web Server melalui Webmin di lingkungan lokal untuk mengaktifkan komunikasi HTTPS terenkripsi.
2. Menganalisis perbandingan tingkat keamanan komunikasi data pada Apache Web Server antara kondisi HTTP dan HTTPS setelah implementasi sertifikat self-signed CA, dengan mengamati indikator keamanan browser dan lalu lintas jaringan.
3. Mengevaluasi efektivitas implementasi SSL/TLS dengan sertifikat self-signed CA dalam memitigasi serangan Man-in-the-Middle (MITM) pada Apache Web Server di lingkungan pengujian yang terisolasi.
4. Menganalisis kelebihan dan keterbatasan teknis dari penggunaan sertifikat self-signed CA sebagai solusi enkripsi lapisan transportasi data untuk Apache Web Server dalam konteks lingkungan pengujian lokal.

1.4.2 Manfaat

Manfaat dari skripsi ini dapat diuraikan menjadi dua aspek utama, yaitu manfaat secara akademis dan manfaat praktis.

Secara akademis, penelitian ini memberikan pengaruh terhadap pengembangan pengetahuan di dalam bidang keamanan *web server*, khususnya terkait konfigurasi dan penerapan sertifikat enkripsi.

Secara praktis, penelitian ini bermanfaat bagi berbagai jenis pengguna, baik *end-user* maupun pemilik atau pengelola server, dalam memahami serta meningkatkan

tingkat keamanan saat mengakses atau mengelola sistem berbasis web. Indikator rasa aman yang dimaksud meliputi perlindungan terhadap akses tidak sah, integritas data, dan keandalan sistem yang digunakan.

1.5 Sistematika Penulisan

Sistematika penulisan berikut dibentuk untuk mempermudah dalam penyusunan skripsi penelitian ini dengan penulisan yang baik ketik sistematika penulisan yang digunakan dijabarkan sebagai berikut:

BAB I PENDAHULUAN

Bab pendahuluan mendeskripsikan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Definisi dan penjelasan pustaka yang dijadikan referensi dalam penelitian ini akan dijelaskan pada bab 2 titik teori yang dipaparkan diantaranya mengenai keamanan website kemudian aplikasi yang digunakan untuk memakai website serta terus yang digunakan untuk enkripsi.

BAB III METODE PENELITIAN

Bab metode penelitian memaparkan pendekatan-pendekatan yang dapat dilakukan dalam perancangan dan implementasi tujuan penelitian secara terstruktur.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi subtansi meliputi analisis kebutuhan, perancangan, implementasi, pengujian serta hasil analisis pengujian.

BAB V PENUTUP

Bab ini berisi simpulan dan saran.

BAB V
PENUTUP

5.1 Simpulan

Berdasarkan analisis dan pengujian yang telah dilakukan, dapat ditarik beberapa simpulan yang secara langsung menjawab tujuan penelitian:

1. Implementasi Sertifikat Self-Signed CA: Implementasi sertifikat self-signed CA pada Apache Web Server berhasil dilakukan dengan efektif di lingkungan lokal menggunakan kombinasi OpenSSL untuk pembuatan sertifikat dan Webmin sebagai antarmuka manajemen. Proses ini, mulai dari pembuatan Certificate Authority (CA) lokal hingga konfigurasi virtual host di Apache, dapat dikelola dengan lebih sederhana melalui antarmuka grafis Webmin, yang membuktikan kelayakan metode ini untuk lingkungan pengembangan.
2. Analisis Perbandingan Keamanan (HTTP vs. HTTPS): Terdapat peningkatan keamanan yang fundamental setelah implementasi sertifikat self-signed. Sebelum implementasi, koneksi melalui HTTP ditandai "Not Secure" oleh peramban dan rentan terhadap penyadapan plaintext. Setelah implementasi, protokol komunikasi berhasil diubah menjadi HTTPS. Meskipun peramban menampilkan peringatan keamanan karena sifat self-signed dari sertifikat, analisis lalu lintas jaringan membuktikan bahwa seluruh data telah ditransmisikan melalui jalur terenkripsi (SSL/TLS), sehingga kerahasiaan dan integritasnya terjaga.
3. Efektivitas Mitigasi Serangan Man-in-the-Middle (MITM): Implementasi SSL/TLS menggunakan sertifikat self-signed terbukti sangat efektif dalam memitigasi simulasi serangan Man-in-the-Middle di lingkungan pengujian yang terisolasi. Pada koneksi HTTPS, alat seperti Ettercap dan Wireshark tidak mampu menangkap kredensial atau data sensitif dalam bentuk plaintext. Data yang disadap hanya berupa ciphertext yang tidak dapat diinterpretasikan, yang menegaskan bahwa enkripsi pada lapisan transportasi berhasil melindungi komunikasi dari ancaman penyadapan.
4. Kelebihan dan Keterbatasan Teknis: Kelebihan utama dari metode ini adalah kemampuannya untuk mengaktifkan enkripsi HTTPS secara cepat

dan tanpa biaya di lingkungan pengembangan lokal yang terisolasi, tanpa memerlukan validasi domain publik. Namun, keterbatasan teknis yang paling signifikan adalah sertifikat self-signed tidak dipercaya secara otomatis oleh peramban publik, sehingga memunculkan peringatan keamanan yang mengharuskan impor CA lokal secara manual ke dalam trust store klien untuk pengujian yang mulus.

5.2 Milestone Penelitian

Selama pelaksanaan penelitian ini, beberapa tonggak pencapaian (milestone) teknis berhasil diraih, yang menjadi fondasi bagi kesimpulan akhir:

1. Penciptaan Lingkungan Laboratorium Virtual yang Fungsional: Berhasil membangun infrastruktur jaringan virtual yang terisolasi menggunakan VirtualBox, yang terdiri dari tiga mesin virtual dengan peran spesifik: Ubuntu sebagai Server, Windows sebagai Client, dan Kali Linux sebagai Attacker. Konfigurasi alamat IP dan jaringan internal yang tepat memastikan semua komponen dapat berkomunikasi sesuai skenario pengujian.
2. Implementasi Penuh Self-Signed Certificate via Webmin: Berhasil mengonfigurasi Apache Web Server untuk menggunakan protokol HTTPS dengan mengimplementasikan sertifikat yang dibuat dan ditandatangani sendiri (self-signed certificate). Proses ini berhasil dikelola seluruhnya melalui antarmuka Webmin, menunjukkan efisiensi Webmin dalam menyederhanakan tugas administrasi SSL/TLS yang kompleks.
3. Demonstrasi Keberhasilan Enkripsi Data: Berhasil membuktikan secara empiris bahwa lalu lintas data pada koneksi HTTPS terenkripsi. Melalui analisis paket menggunakan Wireshark, ditunjukkan bahwa data yang sebelumnya berupa plaintext pada koneksi HTTP kini berubah menjadi ciphertext yang tidak dapat dibaca, memvalidasi fungsi utama SSL/TLS.

4. Validasi Ketahanan Terhadap Serangan MITM: Berhasil melakukan simulasi serangan Man-in-the-Middle (MITM) dan membuktikan bahwa koneksi HTTPS yang diamankan dengan sertifikat self-signed mampu melindungi data dari penyadapan. Kegagalan dalam menangkap kredensial pada sesi HTTPS menjadi bukti nyata efektivitas mitigasi dari implementasi ini.

5.3 Saran

Berdasarkan simpulan dan hasil penelitian yang telah diperoleh, berikut adalah beberapa saran untuk pengembangan lebih lanjut dan penerapan praktis:

1. Studi Komparatif Berkelanjutan: Untuk analisis yang lebih komprehensif, disarankan untuk melakukan studi komparatif dengan Certificate Authority (CA) lain atau metode pengamanan web server lainnya misalnya Nginx dengan Self-signed CA, atau implementasi SSL/TLS manual dari sisi performa dan kemudahan manajemen dalam skala yang lebih besar. Ini dapat memberikan wawasan lebih lanjut mengenai efisiensi dan skalabilitas solusi yang ada.
2. Pengujian Keamanan yang Lebih Dalam: Melakukan pengujian penetrasi (pentest) yang lebih mendalam dan pemindaian kerentanan secara berkala pada web server dan aplikasi web adalah penting. Hal ini untuk mengidentifikasi celah keamanan yang mungkin tidak terdeteksi oleh pengujian standar, serta memastikan konfigurasi yang aman secara berkelanjutan.
3. Pemantauan Log Keamanan: Implementasi sistem pemantauan log keamanan yang proaktif pada Apache dan sistem Ubuntu dapat membantu mendeteksi anomali atau upaya serangan secara real-time, memungkinkan respons cepat dari administrator. Webmin dapat digunakan untuk mempermudah akses dan analisis log.
4. Edukasi dan Kesadaran Pengguna: Penting untuk terus meningkatkan kesadaran pengguna dan administrator mengenai praktik keamanan siber terbaik, termasuk pentingnya menggunakan HTTPS, memperbarui perangkat lunak secara rutin, dan memahami berbagai jenis ancaman siber.

DAFTAR PUSTAKA

Aayush, A., Aryan, Y., & Muniyal, B. (2022). Understanding SSL Protocol and Its Cryptographic Weaknesses. *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, 825–832. https://doi.org/10.1109/ICIEM54221.2022.9853153

Alby, M. F., Ruslan, I. F., & Muharman, M. L. (2022). Information Security Test on Websites and Social Media Using Footprinting Method. *Proceedings of the 8th International Conference on Industrial and Business Engineering*. https://doi.org/10.1145/3568834.3568868

Al-Shareeda, M., Anbar, M., Manickam, S., & Hasbullah, I. (2020). Review of Prevention Schemes for Man-In-The-Middle (MITM) Attack in Vehicular Ad hoc Networks. *International Journal of Engineering and Management Research*. https://doi.org/10.31033/ijemr.10.3.23

Arman, M., & Rachmat, N. (2020). Implementasi sistem keamanan web server menggunakan pfsense. *Jusikom: Jurnal Sistem Komputer Musirawas*, *5*(1), 13–23.

Bhargavan, K., Bichhawat, A., Huy, Q., Hosseyni, P., Küsters, R., Schmitz, G., & Würtele, T. (2021). An In-Depth Symbolic Security Analysis of the ACME Standard. *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3460120.3484588

Chen, C., Tian, C., Duan, Z., & Zhao, L. (2018). RFC-Directed Differential Testing of Certificate Validation in SSL/TLS Implementations. *2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE)*, 859–870. https://doi.org/10.1145/3180155.3180226

Fattah, H. (2021). Hypertext Transfer Protocol (HTTP). *LTE™ Cellular Narrowband Internet of Things (NB-IoT)*. https://doi.org/10.1201/9781003120018-15

Hu, Q., Asghar, M., & Brownlee, N. (2021). A large-scale analysis of HTTPS deployments: Challenges, solutions, and recommendations. *J. Comput. Secur.*, *29*, 25–50. https://doi.org/10.3233/jcs-200070

Kampourakis, V., Kambourakis, G., Chatzoglou, E., & Zaroliagis, C. (2022). Revisiting man-in-the-middle attacks against HTTPS. *Netw. Secur.*, *2022*. https://doi.org/10.12968/s1353-4858(22)70028-1

Khan, N., Khan, A., Kar, H., Ahmad, Z., Tarmizi, S., & Julaihi, A. (2022). Employing Public Key Infrastructure to Encapsulate Messages During Transport Layer Security Handshake Procedure. *2022 Applied Informatics International Conference (AiIC)*, 126–130. https://doi.org/10.1109/AiIC54368.2022.9914605

King, G., & Wang, H. (2021). *HTTPA: HTTPS Attestable Protocol*. 811–823. https://doi.org/10.1007/978-3-031-28073-3_54

Koch, J., & Hao, W. (2021). Apache and HTTP/2 in the Cloud: A Comparative Study of Apache Architecture in AWS. *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 673–680. https://doi.org/10.1109/iemcon53756.2021.9623230

Kponyo, J., Agyemang, J., & Klogo, G. (2020). Detecting End-Point (EP) Man-In-The-Middle (MITM) Attack based on ARP Analysis: A Machine Learning Approach. *Int. J. Commun. Networks Inf. Secur.*, *12*. https://doi.org/10.22541/au.158938565.57807215

Liu, J., & Cheng, W. (2024). Design and Implementation of a Web Application Firewall System based on OpenResty. *2024 9th International Symposium on Computer and Information Processing Technology (ISCIPT)*, 6–9. https://doi.org/10.1109/ISCIPT61983.2024.10673202

Mai, A., Schedler, O., Weippl, E., & Krombholz, K. (2022). *Are HTTPS Configurations Still a Challenge?: Validating Theories of Administrators' Difficulties with TLS Configurations*. 173–193. https://doi.org/10.1007/978-3-031-05563-8_12

Mallik, A. (2019). MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*. https://doi.org/10.22373/cj.v2i2.3453

Momin, M. M., & Ali, O. (2023). Comprehensive Review of the Impact of Advanced Technology Adoption on Work and Continuous Improvement. *HighTech and Innovation Journal*, *4*(3), 667–680. https://doi.org/10.28991/HIJ-2023-04-03-014

Mundt, M., & Baier, H. (2023). Threat-Based Simulation of Data Exfiltration Toward Mitigating Multiple Ransomware Extortions. *Digital Threats: Research and Practice*, *4*(4). https://doi.org/10.1145/3568993

Nugroho, F. R., Afiana, F. N., & Kuncoro, A. P. (2024). NIST Cyber Security Framework Development for Website Information Collection. *Jurnal Teknologi Sistem Informasi Dan Aplikasi*, *7*(3), 1335–1342. https://doi.org/10.32493/jtsi.v7i3.41541

Nurlailah, E., & Nova Wardani, K. R. (2023). PERANCANGAN WEBSITE SEBAGAI MEDIA INFORMASI DAN PROMOSI OLEH-OLEH KHAS KOTA PAGARALAM. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *8*(4), 1175–1185. https://doi.org/10.29100/jipi.v8i4.4006

Nyabuto, G. (2023). Client-server Architecture, a Review. *International Journal of Advanced Science and Computer Applications*. https://doi.org/10.47679/ijasca.v3i1.48

Poghosyan, I. (2024). ADVANTAGE OF INSTALLING MOODLE LEARNING MANAGEMENT SYSTEM UNDER IIS/MARIADB OVER APACHE/MYSQL. *Main Issues Of Pedagogy And Psychology*. https://doi.org/10.24234/miopap.v11i2.49

Tripathy, S. S. (2024). A comprehensive survey of cybercrimes in India over the last decade. *International Journal of Science and Research Archive*. https://doi.org/10.30574/ijsra.2024.13.1.1919

Westfall, J. (2021). *Basic Linux Administration via GUI (Webmin)*. 77–110. https://doi.org/10.1007/978-1-4842-6966-4_4

Xia, K., Zhang, L., Yuan, S., & Lou, Y. (2023). SCSS: An Intelligent Security System to Guard City Public Safe. *IEEE Access*, *11*, 76415–76426. https://doi.org/10.1109/ACCESS.2023.3297643

Zhang, X.-G., Yang, G., & Wasly, S. (2021). Man-in-the-middle attack against cyber-physical systems under random access protocol. *Inf. Sci.*, *576*, 708–724. https://doi.org/10.1016/j.ins.2021.07.083