

Security Analysis of Apache Web Server Using Self-Signed CA in Webmin

Fauzan Nugroho

Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta

Depok, Jawa Barat

fauzan.nugroho.tik18@mhs.wpnj.ac.id

Abstract - Data communication via the HTTP protocol is vulnerable to eavesdropping attacks, while using certificates from a public Certificate Authority (CA) is often impractical for local development environments. This research analyzes the effectiveness of implementing a self-signed certificate on an Apache Web Server managed via Webmin as a security solution. The research method used is an experiment in an isolated virtual environment comprising a server (Ubuntu), a client (Windows), and an attacker (Kali Linux). System resilience was tested through a Man-in-the-Middle (MITM) attack simulation to compare the security of the connection before (HTTP) and after (HTTPS) certificate implementation. The test results show that the HTTPS connection secured with the self-signed certificate successfully encrypted all data traffic. In contrast to the HTTP connection, which allowed data to be intercepted in plaintext, the encrypted connection ensured that data was only readable as ciphertext by the attacker, thus preserving its confidentiality and integrity. It is concluded that the use of a self-signed certificate is a viable security solution to protect internal development or testing environments from data eavesdropping threats using the MITM method, although it is not recommended for publicly accessed production servers.

Keywords: Apache, HTTPS, Man-in-the-Middle, Self-Signed CA, 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: Apache, HTTPS, Man-in-the-Middle, Self-signed CA, Webmin

I. PENDAHULUAN

Perkembangan teknologi jaringan memicu peningkatan ketergantungan pada layanan berbasis web, namun diiringi dengan potensi celah keamanan (security hole) yang dapat dieksploitasi untuk kejahatan siber [1]. Web server, sebagai komponen krusial, sering menjadi target utama serangan yang dapat berakibat fatal. Oleh karena itu, keamanan server merupakan prioritas utama bagi administrator sistem untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi [2]. Salah satu pilar utama dalam keamanan web modern adalah enkripsi komunikasi menggunakan protokol SSL/TLS, yang

mengubah koneksi dari HTTP menjadi HTTPS. HTTPS memastikan data yang ditransmisikan dienkripsi dan terlindungi dari penyadapan. Untuk mengaktifkan HTTPS, sebuah sertifikat digital diperlukan [3]. Namun, dalam lingkungan pengembangan atau pengujian lokal, memperoleh sertifikat dari Otoritas Sertifikat (CA) publik seringkali tidak praktis karena memerlukan validasi domain yang dapat diakses publik. Sebagai solusi, sertifikat yang ditandatangani sendiri (self-signed certificate) dapat digunakan untuk mensimulasikan lingkungan HTTPS secara penuh di jaringan internal yang terisolasi [4][5][6][7]. Penelitian sebelumnya telah berfokus pada pengamanan web server di

lapisan lain. Liu & Cheng (2024) berfokus pada pengamanan menggunakan Web Application Firewall (WAF) untuk mencegah serangan seperti SQL injection dan XSS [5][8]. Sementara itu, Arman & Rachmat (2020) mengimplementasikan sistem keamanan jaringan menggunakan pfSense dan Snort untuk mendeteksi dan memblokir serangan pada lapisan jaringan [9][10][11]. Terdapat kesenjangan penelitian (research gap) dalam analisis keamanan yang berfokus pada lapisan transportasi data di lingkungan pengembangan lokal [12][13]. Penelitian ini mengisi kesenjangan tersebut dengan menganalisis efektivitas dan cara kerja sertifikat self-signed yang dikelola melalui antarmuka grafis Webmin untuk melindungi Apache Web Server dari serangan penyadapan seperti Man-in-the-Middle (MITM) [14][15][16]. Tujuan dari penelitian ini adalah: (1) Mengimplementasikan sertifikat self-signed CA pada Apache Web Server melalui Webmin untuk mengaktifkan komunikasi HTTPS terenkripsi [17][18][19][20]; (2) Menganalisis perbandingan tingkat keamanan antara koneksi HTTP dan HTTPS ; dan (3) Mengevaluasi efektivitas implementasi SSL/TLS dengan sertifikat self-signed dalam memitigasi serangan MITM di lingkungan pengujian yang terisolasi.

II. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode eksperimen dalam lingkungan laboratorium virtual yang terisolasi untuk menganalisis sistem keamanan secara realistis. Tahapan penelitian dirancang secara sistematis, meliputi persiapan lingkungan, implementasi sistem keamanan, dan pengujian. Lingkungan pengujian dibangun menggunakan VirtualBox untuk menciptakan tiga mesin virtual (VM) dengan peran spesifik. Arsitektur ini terdiri dari:

1. Server: Menggunakan OS Ubuntu Server 24.04 yang diinstal dengan Apache HTTP Server sebagai web server target dan Webmin sebagai panel kontrol untuk manajemen dan konfigurasi SSL/TLS.
2. Client: Menggunakan OS Windows 10 untuk mensimulasikan akses pengguna akhir ke web server.
3. Attacker: Menggunakan OS Kali Linux yang dilengkapi dengan tools untuk audit keamanan seperti Ettercap, Wireshark, dan Network Miner.

Konfigurasi jaringan untuk ketiga mesin virtual tersebut dapat dilihat pada Tabel I, yang

menciptakan sebuah jaringan internal terisolasi untuk pengujian.

Tabel I

Mesin Virtual	Alamat IP	Subnet Mask	Gateway
Client	192.168.57.10	255.255.255.0	192.168.57.2
Server	192.168.57.2	255.255.255.0	192.168.57.1
Attacker	192.168.57.5	255.255.255.0	192.168.57.1

Prosedur penelitian dimulai dengan instalasi dan konfigurasi prasyarat pada server, termasuk DNS lokal, database, dan virtual host Apache untuk domain zeins.local. Selanjutnya, dilakukan implementasi SSL/TLS dengan membuat self-signed certificate menggunakan OpenSSL dan mengonfigurasikannya pada Apache melalui Webmin. Tahap pengujian dilakukan dengan pendekatan komparatif. Pertama, keamanan dasar koneksi diuji dengan mengakses web server melalui HTTP dan HTTPS untuk mengamati perubahan pada indikator keamanan peramban. Kedua, dilakukan simulasi serangan Man-in-the-Middle (MITM) menggunakan Ettercap dari mesin attacker. Tujuannya adalah untuk menyadap lalu lintas data antara client dan server pada kedua kondisi (HTTP dan HTTPS) dan menganalisis paket data yang tertangkap menggunakan Wireshark dan Network Miner untuk memverifikasi apakah data terenkripsi atau terbaca sebagai plaintext.

III. HASIL DAN PEMBAHASAN

Pengujian sistem menghasilkan data empiris yang menunjukkan peningkatan keamanan secara signifikan setelah implementasi sertifikat self-signed.

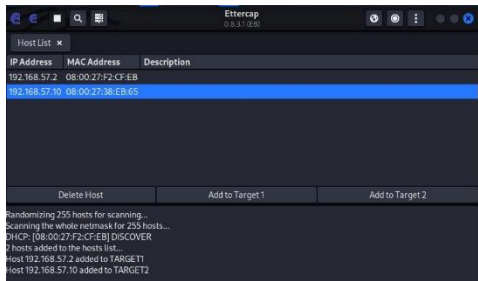
A. Hasil Pengujian Keamanan Dasar

Sebelum implementasi SSL/TLS, akses ke web server melalui protokol HTTP (<http://zeins.local>) menampilkan indikator "Not Secure" pada peramban web. Analisis lalu lintas jaringan menggunakan Network Miner mengonfirmasi bahwa komunikasi berjalan pada port 80 (HTTP) dan data yang ditransmisikan tidak terenkripsi. Setelah sertifikat self-signed diimplementasikan, akses ke web server berhasil dialihkan dan dilakukan melalui HTTPS (<https://zeins.local>). Meskipun peramban menampilkan peringatan keamanan (misalnya, ikon gembok merah) karena sertifikat tidak diterbitkan

oleh CA publik yang tepercaya, analisis lalu lintas jaringan mengonfirmasi bahwa koneksi kini menggunakan port 443 (SSL), menandakan bahwa jalur komunikasi telah terenkripsi.

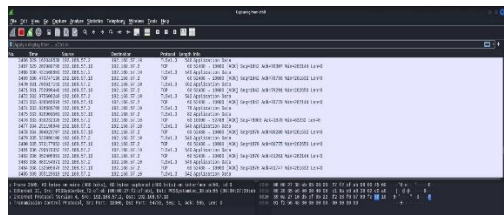
B. Hasil Simulasi Serangan Man-in-the-Middle (MITM)

Simulasi serangan MITM menunjukkan perbedaan drastis antara keamanan koneksi HTTP dan HTTPS. Pada koneksi HTTP, penyerang yang menggunakan Ettercap berhasil menyadap komunikasi antara client dan server. Seluruh data, termasuk kredensial login (username dan password), berhasil ditangkap dan terbaca dalam bentuk plaintext (teks biasa), seperti yang ditunjukkan pada Gambar 1. Hal ini membuktikan kerentanan inheren dari protokol HTTP terhadap serangan penyadapan.



Gambar 1. Hasil Penyadapan Kredensial pada Koneksi HTTP Menggunakan Ettercap

Sebaliknya, pada koneksi HTTPS yang telah diamankan dengan sertifikat self-signed, penyerang tetap dapat menyadap paket data, namun isinya tidak dapat dibaca. Analisis menggunakan Wireshark menunjukkan bahwa data yang ditangkap hanyalah ciphertext (teks tersandi) dari protokol TLSv1.3, seperti terlihat pada Gambar 2. Kredensial dan data sensitif lainnya tetap aman dan tidak terekspos dalam bentuk plaintext.



Gambar 2. Tampilan Lalu Lintas Data yang Terenkripsi (Ciphertext) pada Wireshark

C. Pembahasan

Hasil pengujian secara komprehensif membuktikan bahwa implementasi sertifikat self-signed melalui Webmin berhasil meningkatkan postur keamanan Apache Web Server secara signifikan dalam lingkungan lokal. Meskipun

peramban menampilkan peringatan karena rantai kepercayaan sertifikat tidak dikenali secara publik, fungsionalitas enkripsi pada lapisan transportasi tetap berjalan efektif.

Perubahan fundamental dari HTTP ke HTTPS adalah mitigasi yang efektif terhadap serangan penyadapan seperti MITM. Kegagalan penyerang untuk membaca data pada koneksi HTTPS menegaskan bahwa enkripsi berhasil melindungi kerahasiaan dan integritas data. Ini menjawab perumusan masalah mengenai cara kerja dan efektivitas SSL/TLS dalam mengamankan komunikasi web server.

Kelebihan utama dari pendekatan ini adalah kemampuannya untuk mengaktifkan enkripsi HTTPS secara cepat, tanpa biaya, dan tanpa bergantung pada validasi domain publik, sehingga sangat ideal untuk lingkungan pengembangan dan pengujian yang terisolasi. Namun, keterbatasannya adalah peringatan keamanan di peramban, yang mengharuskan impor manual sertifikat CA lokal ke dalam trust store mesin client untuk menghilangkan peringatan tersebut. Penggunaan Webmin terbukti menyederhanakan proses konfigurasi yang kompleks, menjadikannya alat yang efisien bagi administrator.

IV. KESIMPULAN DAN SARAN

Berdasarkan analisis dan pengujian, disimpulkan bahwa implementasi sertifikat self-signed pada Apache Web Server yang dikelola melalui Webmin merupakan solusi yang efektif untuk mengamankan lingkungan pengembangan lokal. Metode ini berhasil mengubah protokol komunikasi menjadi HTTPS, yang terbukti secara empiris mampu mengenkripsi lalu lintas data dan secara efektif memitigasi risiko penyadapan melalui serangan

Man-in-the-Middle. Kelebihan utamanya adalah kemudahan implementasi tanpa biaya di lingkungan terisolasi, meskipun memiliki keterbatasan berupa tidak adanya kepercayaan otomatis dari peramban publik.

Untuk pengembangan di masa depan, disarankan melakukan studi komparatif dengan web server lain seperti Nginx atau dengan metode implementasi sertifikat lainnya untuk menganalisis performa dan skalabilitas. Selain itu, pengujian penetrasi yang lebih mendalam serta implementasi sistem pemantauan log keamanan secara proaktif dapat dilakukan untuk mengidentifikasi celah keamanan lain di luar lapisan transportasi data.

V. REFERENSI

- [1] M. M. Momin and O. Ali, "Comprehensive Review of the Impact of Advanced Technology Adoption on Work and Continuous Improvement," *HighTech and Innovation Journal*, vol. 4, no. 3, pp. 667–680, Sep. 2023, doi: 10.28991/HIJ-2023-04-03-014.
- [2] M. Mundt and H. Baier, "Threat-Based Simulation of Data Exfiltration Toward Mitigating Multiple Ransomware Extortions," *Digital Threats: Research and Practice*, vol. 4, no. 4, Oct. 2023, doi: 10.1145/3568993.
- [3] M. Arman and N. Rachmat, "Implementasi sistem keamanan web server menggunakan pfsense," *Jusikom: Jurnal Sistem Komputer Musirawas*, vol. 5, no. 1, pp. 13–23, 2020.
- [4] J. Westfall, "Basic Linux Administration via GUI (Webmin)," pp. 77–110, 2021, doi: 10.1007/978-1-4842-6966-4_4.
- [5] J. Liu and W. Cheng, "Design and Implementation of a Web Application Firewall System based on OpenResty," *2024 9th International Symposium on Computer and Information Processing Technology (ISCIPIT)*, pp. 6–9, 2024, doi: 10.1109/ISCIPIT61983.2024.10673202.
- [6] F. R. Nugroho, F. N. Afiana, and A. P. Kuncoro, "NIST Cyber Security Framework Development for Website Information Collection," *Jurnal Teknologi Sistem Informasi dan Aplikasi*, vol. 7, no. 3, pp. 1335–1342, Jul. 2024, doi: 10.32493/jtsi.v7i3.41541.
- [7] J. Koch and W. Hao, "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)*, pp. 673–680, 2021, doi: 10.1109/iemcon53756.2021.9623230.
- [8] M. F. Alby, I. F. Ruslan, and M. L. Muharman, "Information Security Test on Websites and Social Media Using Footprinting Method," *Proceedings of the 8th International Conference on Industrial and Business Engineering*, p., 2022, doi: 10.1145/3568834.3568868.
- [9] E. Nurlailah and K. R. Nova Wardani, "PERANCANGAN WEBSITE SEBAGAI MEDIA INFORMASI DAN PROMOSI OLEH-OLEH KHAS KOTA PAGARALAM," *JUPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 8, no. 4, pp. 1175–1185, Nov. 2023, doi: 10.29100/jupi.v8i4.4006.
- [10] S. S. Tripathy, "A comprehensive survey of cybercrimes in India over the last decade," *International Journal of Science and Research Archive*, p., 2024, doi: 10.30574/ijrsra.2024.13.1.1919.
- [11] Q. Hu, M. Asghar, and N. Brownlee, "A large-scale analysis of HTTPS deployments: Challenges, solutions, and recommendations," *J. Comput. Secur.*, vol. 29, pp. 25–50, 2021, doi: 10.3233/jcs-200070.
- [12] H. Fattah, "Hypertext Transfer Protocol (HTTP)," *LTETM Cellular Narrowband Internet of Things (NB-IoT)*, p., 2021, doi: 10.1201/9781003120018-15.
- [13] N. Khan, A. Khan, H. Kar, Z. Ahmad, S. Tarmizi, and A. Julaihi, "Employing Public Key Infrastructure to Encapsulate Messages During Transport Layer Security Handshake Procedure," *2022 Applied Informatics International Conference (AiIC)*, pp. 126–130, 2022, doi: 10.1109/AiIC54368.2022.9914605.
- [14] A. Mai, O. Schedler, E. Weippl, and K. Krombholz, "Are HTTPS Configurations Still a Challenge?: Validating Theories of Administrators' Difficulties with TLS Configurations," pp. 173–193, 2022, doi: 10.1007/978-3-031-05563-8_12.
- [15] C. Chen, C. Tian, Z. Duan, and L. Zhao, "RFC-Directed Differential Testing of Certificate Validation in SSL/TLS Implementations," *2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE)*, pp. 859–870, 2018, doi: 10.1145/3180155.3180226.
- [16] K. Bhargavan *et al.*, "An In-Depth Symbolic Security Analysis of the ACME Standard," *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, p., 2021, doi: 10.1145/3460120.3484588.
- [17] A. Aayush, Y. Aryan, and B. Muniyal, "Understanding SSL Protocol and Its

- Cryptographic Weaknesses,” in *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, 2022, pp. 825–832, doi: 10.1109/ICIEM54221.2022.9853153.
- [18] A. Mallik, “MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS,” *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, p., 2019, doi: 10.22373/cj.v2i2.3453.
- [19] J. Kponyo, J. Agyemang, and G. Klogo, “Detecting End-Point (EP) Man-In-The-Middle (MITM) Attack based on ARP Analysis: A Machine Learning Approach,” *Int. J. Commun. Networks Inf. Secur.*, vol. 12, p., 2020, doi: 10.22541/au.158938565.57807215.
- [20] M. Al-Shareeda, M. Anbar, S. Manickam, and I. Hasbullah, “Review of Prevention Schemes for Man-In-The-Middle (MITM) Attack in Vehicular Ad hoc Networks,” *International Journal of Engineering and Management Research*, p., 2020, doi: 10.31033/ijemr.10.3.23.