Journal of Internet and Software Engineering Vol: 1, No 4, 2024, Page: 1-9

Meningkatkan Keamanan Sertifikat Digital dengan Pengaktifan HTTPS

Aep Setiawan*, Muchammad Alifandino Satrio, Itqon Madani, Ramma Dwi Rachmat, Stivan Hari Sukma

Teknologi Rekayasa Komputer, Sekolah Vokasi, Institut Pertanian Bogor

Abstrak: Era digital saat ini, keamanan informasi menjadi isu yang sangat penting bagi organisasi maupun individu. Salah satu aspek krusial dalam keamanan digital adalah keamanan sertifikat digital. Sertifikat digital berperan vital dalam mengautentikasi identitas digital dan melindungi komunikasi serta pertukaran data sensitif secara online. Namun, sertifikat digital seringkali rentan terhadap ancaman keamanan, seperti serangan *man-in-the-middle*, pemalsuan sertifikat, dan kebocoran informasi. Untuk mengatasi permasalahan ini, pengaktifan protokol HTTPS (*Hypertext Transfer Protocol Secure*) menjadi solusi yang efektif. HTTPS merupakan protokol komunikasi yang mengenkripsi data yang dikirimkan antara klien dan server, sehingga memperkuat keamanan sertifikat digital dan melindungi komunikasi online. Dengan HTTPS, sertifikat digital dapat terverifikasi dengan lebih baik, meminimalisir risiko peretasan, dan membangun kepercayaan pengguna.

Kata Kunci: *Digital Certificates, Encryption, HTTPS, Information Security, Online Communication*

DOI: https://doi.org/10.47134/pjise.v1i4.3170
*Correspondence: Aep Setiawan
Email: aepsetiawan@apps.ipb.ac.id

Received: 29-08-2024
Accepted: 15-09-2024
Published: 31-10-2024

Abstract: *Digital era, information security has become a crucial issue for organizations and individuals. One crucial aspect of digital security is the security of digital certificates. Digital certificates play a vital role in authenticating digital identities and protecting sensitive data communication and exchange online. However, digital certificates are often vulnerable to security threats, such as man-in-the-middle attacks, certificate forgery, and information leaks. To address this problem, the activation of the HTTPS (Hypertext Transfer Protocol Secure) protocol has become an effective solution. HTTPS is a communication protocol that encrypts data transmitted between clients and servers, thereby strengthening the security of digital certificates and protecting online communication. With HTTPS, digital certificates can be better verified, risks of hacking minimized, and user trust built.*

Keywords: *Digital Certificates, Encryption, HTTPS, Information Security, Online Communication*

Pendahuluan

Era digital saat ini, keamanan informasi menjadi isu yang sangat penting bagi organisasi maupun individu. Salah satu aspek krusial dalam keamanan digital adalah keamanan sertifikat digital. Sertifikat digital berperan vital dalam mengautentikasi identitas digital dan melindungi komunikasi serta pertukaran data sensitif secara online (Hughes, 2022; Ishida, 2023). Namun, sertifikat digital seringkali rentan terhadap ancaman keamanan, seperti serangan *man-in-the-middle*, pemalsuan sertifikat, dan kebocoran informasi (Gergely, 2022; Wang, 2022). Hal ini dapat membahayakan kepercayaan pengguna dan mengundang risiko-risiko keamanan siber yang serius (Hu, 2021). Bila tidak ditangani dengan baik, kerentanan sertifikat digital dapat menimbulkan konsekuensi yang fatal bagi organisasi maupun individu, seperti kebocoran data rahasia, penyalahgunaan identitas, dan hilangnya kepercayaan publik. Untuk mengatasi permasalahan ini, pengaktifan protokol HTTPS (*Hypertext Transfer Protocol Secure*) menjadi solusi yang efektif. HTTPS merupakan protokol komunikasi yang mengenkripsi data yang dikirimkan antara klien dan server, sehingga memperkuat keamanan sertifikat digital dan melindungi komunikasi online. Dengan HTTPS, sertifikat digital dapat terverifikasi dengan lebih baik, meminimalisir risiko peretasan, dan membangun kepercayaan pengguna.

Pelatihan tentang pengenalan dan instalasi Kali Linux penting karena permintaan akan tenaga ahli keamanan digital semakin meningkat. Kali Linux adalah alat penting dalam pengujian penetrasi dan pengelolaan keamanan siber. Dengan pelatihan ini, para profesional dapat memperoleh keterampilan yang diperlukan untuk melindungi sistem dan jaringan dari serangan siber. Ini membantu meningkatkan keamanan secara keseluruhan di dunia digital yang terus berkembang (Jurnal Publikasi et al., 2022).

Cybersecurity berasal dari dua kata yaitu "*cyber*" dan "*security*". *Cyber* berarti dunia maya atau dunia internet dan *security* berarti keamanan. Dengan demikian, pengertian sederhana dari *cybersecurity* adalah keamanan siber. *Cybersecurity* atau keamanan siber mempunyai fungsi atau peran untuk menemukan, memperbaiki, ataupun mengurangi tingkat risiko terjadinya ancaman siber (*cyber threat*) dan serangan siber (*cyber attack*). Hal ini mencakup semua aktivitas yang berpotensi mengancam keamanan seluruh komponen sistem siber itu sendiri, yang meliputi perangkat keras (*hardware*), perangkat lunak (*software*), data/informasi, serta infrastruktur (Ramadhani & Raf'ie Pratama, n.d.). Menurut Arianto melalui konsep Geometripolitika, keamanan informasi adalah bagian dari keamanan siber. Hal ini disebabkan karena metode dan cara-cara mengamankan informasi merupakan bagian integral dari keamanan siber, yang berinduk pada kajian keamanan internasional (Arianto & Anggraini, n.d.-b).

Keamanan siber merupakan rangkaian aktivitas yang diarahkan untuk melindungi jaringan komputer (baik perangkat keras maupun perangkat lunak) dari ancaman, gangguan, dan serangan yang terkait dengan informasi di dalamnya, serta elemen-elemen ruang siber lainnya. Keamanan siber juga dapat digunakan sebagai sarana untuk melindungi terhadap pengawasan yang tidak diinginkan, seperti kegiatan intelijen (Aji, 2023). Segala hal dapat dilakukan melalui dunia internet atau yang sering disebut juga

cyberspace. Banyak sisi positif yang ditawarkan oleh *cyberspace*, seperti meningkatkan kemudahan akses informasi, mendorong kreativitas manusia, dan memberikan berbagai kemudahan serta keuntungan lainnya. Namun, perlu disadari bahwa setiap hal pasti memiliki dua sisi, yaitu sisi positif dan sisi negatif. Sisi negatif yang turut berkembang pesat seiring dengan perkembangan internet adalah munculnya tindakan-tindakan anti-sosial dan berbagai kejahatan melalui jaringan internet yang marak disebut sebagai *cyber crime* (Jurnal Publikasi et al., 2022).

Hypertext Transfer Protocol Secure (HTTPS) merupakan protokol komunikasi yang dikembangkan untuk meningkatkan keamanan dan privasi dalam pertukaran data di internet. HTTPS menggunakan protokol SSL (*Secure Sockets Layer*) atau TLS (*Transport Layer Security*) untuk mengenkripsi komunikasi antara klien (seperti *web browser*) dan server, sehingga mencegah pihak ketiga untuk mengakses atau memanipulasi data yang dikirimkan.

Sertifikat digital adalah sertifikat elektronik yang digunakan untuk mengautentikasi identitas digital suatu entitas, seperti website, server, atau individu. Sertifikat digital diterbitkan oleh *Certification Authority* (CA) yang terpercaya dan berisi informasi penting seperti identitas pemilik, masa berlaku, dan kunci publik yang digunakan untuk verifikasi. Kombinasi penggunaan HTTPS dan sertifikat digital yang valid sangat penting untuk memastikan keamanan komunikasi dan pertukaran data sensitif secara online. HTTPS memastikan komunikasi terenkripsi, sedangkan sertifikat digital memverifikasi identitas digital sehingga pengguna dapat yakin berinteraksi dengan entitas yang benar.

Metode

Penelitian ini dilakukan melalui studi literatur, yang melibatkan pencarian dan analisis terhadap penelitian, artikel, dan publikasi jurnal yang relevan dengan keamanan siber, sertifikat digital, dan implementasi HTTPS. Sumber-sumber yang digunakan mencakup basis data *online*, jurnal akademik, dan situs web terpercaya. Tinjauan literatur berfokus pada topik-topik kunci berikut:

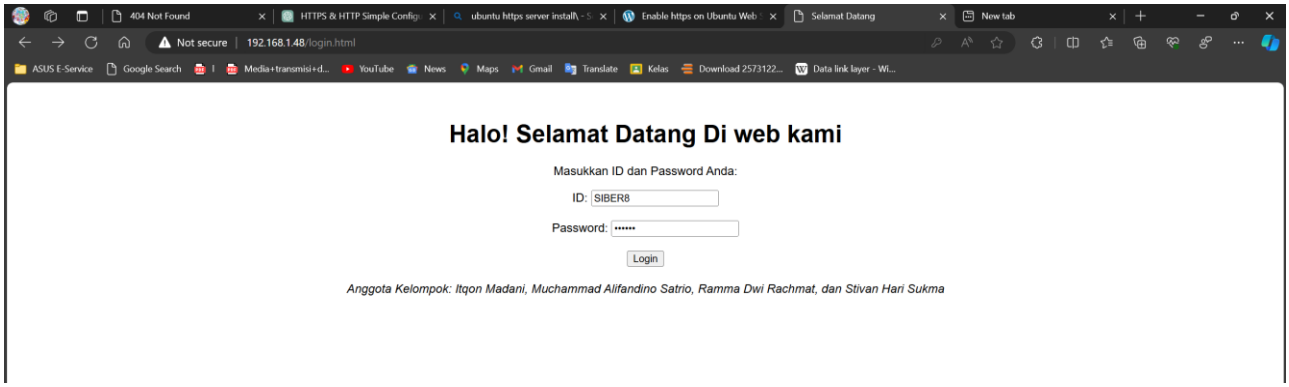
- Konsep dan prinsip keamanan siber
- Peran sertifikat digital dalam komunikasi *online*
- Kerentanan dan ancaman yang terkait dengan sertifikat digital
- Protokol HTTPS dan implementasinya untuk meningkatkan keamanan sertifikat digital
- Praktik terbaik serta studi kasus tentang penerapan HTTPS dan dampaknya

Hasil dan Pembahasan

Implementasi HTTPS pada server web bertujuan untuk meningkatkan keamanan sertifikat digital dan melibatkan beberapa langkah penting. Langkah-langkah tersebut meliputi instalasi dan konfigurasi server web, penerapan HTTPS, serta pemantauan dan validasi enkripsi yang dihasilkan. Pendekatan ini diharapkan dapat memastikan keamanan data dan komunikasi yang dikirimkan melalui server web.

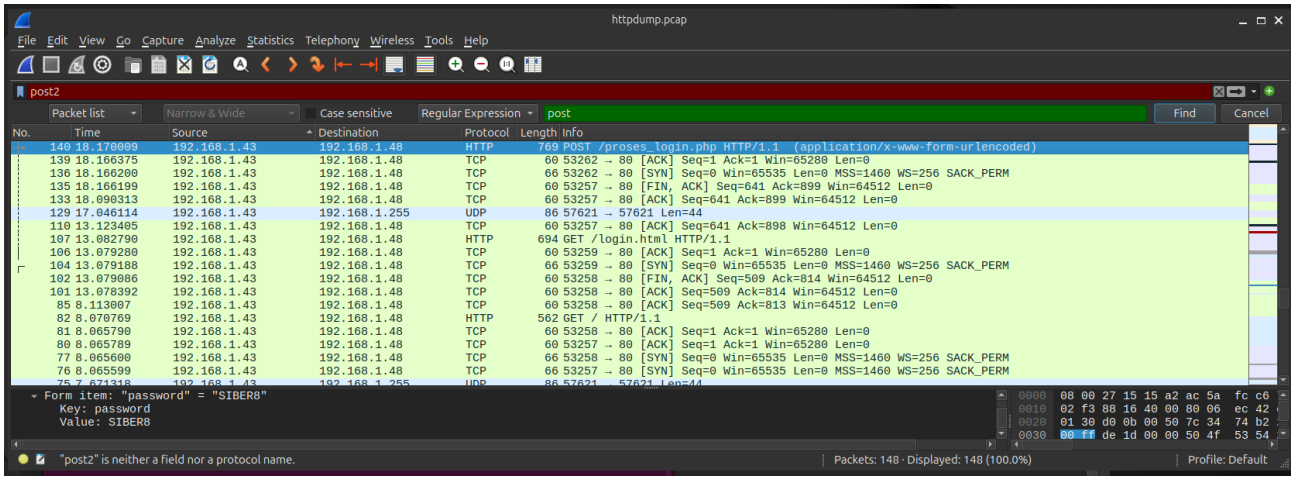
Langkah pertama adalah melakukan instalasi server. Dalam penelitian ini, digunakan sistem operasi Ubuntu versi 22.04 sebagai platform server. Setelah instalasi Ubuntu 22.04,

server web Apache2 dipasang dan dikonfigurasi. Setelah Apache2 terinstal, alamat IP yang dimiliki Ubuntu dapat diakses melalui peramban web. *Website* yang diakses melalui HTTP (*HyperText Transfer Protocol*) akan menampilkan status "*Not Secure*", yang menandakan bahwa tidak ada enkripsi data, sehingga membuatnya rentan terhadap serangan. Setelah pembuatan Website *Login* Sederhana menggunakan PHP, langkah selanjutnya adalah melakukan uji login menggunakan HTTP biasa.



Gambar 1. Tampilan *Login*

Gambar di bawah menunjukkan tampilan antarmuka perangkat lunak Wireshark yang sedang menganalisis lalu lintas jaringan dari sebuah file pcap bernama "httpdump.pcap". Pada bagian atas, ada daftar paket yang ditangkap, di mana paket-paket yang dikirim dan diterima antara alamat IP 192.168.1.43 dan 192.168.1.48 sedang dipantau. Paket nomor 140 terlihat mengandung permintaan HTTP POST menuju halaman "login.php" dengan data "password=SIEBER8" dalam bentuk teks biasa (*unencrypted*). Di bagian bawah, terdapat rincian paket yang diuraikan, termasuk informasi tentang *form item* "*password*" dengan nilai "SIEBER8", yang menunjukkan bahwa kata sandi tersebut dikirim tanpa enkripsi melalui jaringan.

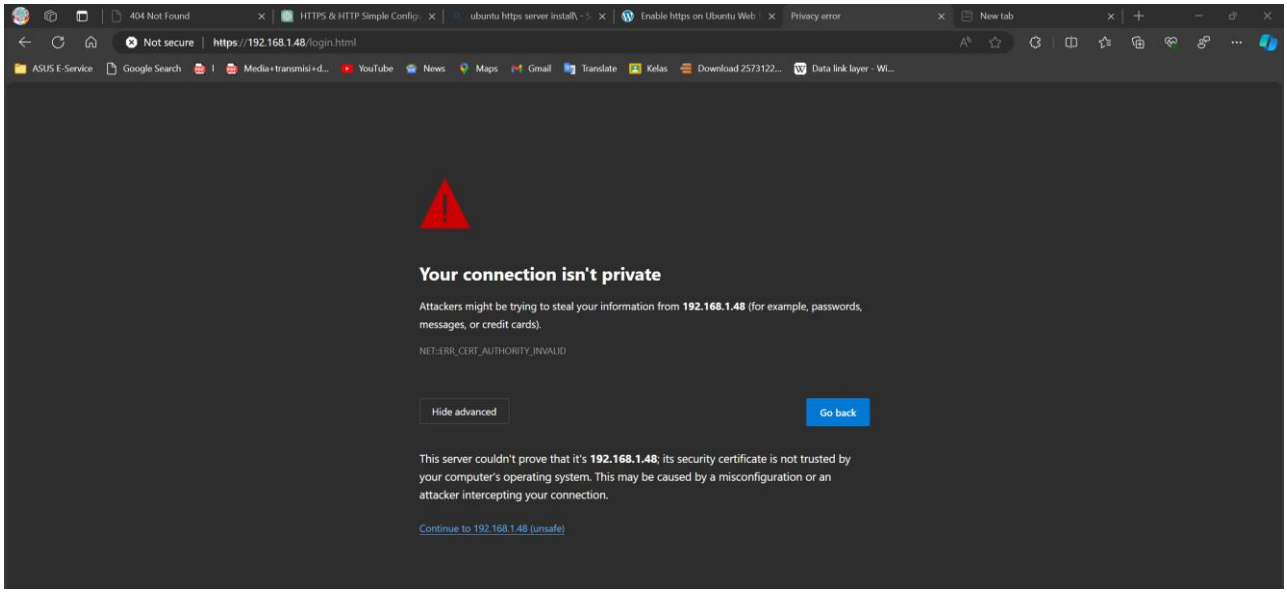


Gambar 2. Tampilan httpdump

Karena hanya menggunakan HTTP, *form item* menampilkan *username* dan *password* secara jelas. Hal ini disebabkan oleh tidak adanya enkripsi pada *form item* tersebut, sehingga akses ini tidak aman dan rentan terhadap peretasan. Untuk mengamankan transmisi data,

HTTPS (*HyperText Transfer Protocol Secure*) harus diterapkan dengan membuat sertifikat TLS menggunakan perintah `**openssl**`. Pertama, buatlah sertifikat TLS untuk proses handshake dengan mengaktifkan SSL pada layanan Apache2 menggunakan perintah `**a2enmod ssl**`.

Buat sertifikat menggunakan perintah `**openssl**`, yang memerlukan pengisian informasi seperti nama negara, organisasi, dan alamat email. Konfigurasikan file `IP.conf` pada situs Apache2 agar mendengarkan pada port 443 (port standar untuk HTTPS). Aktifkan layanan HTTPS pada Apache2. Setelah konfigurasi selesai dan syntax dinyatakan benar, lakukan pengujian dengan mengakses situs web melalui HTTPS di browser dengan alamat https://(alamat IP).



Gambar 3. Akses alamat IP pada *browser*

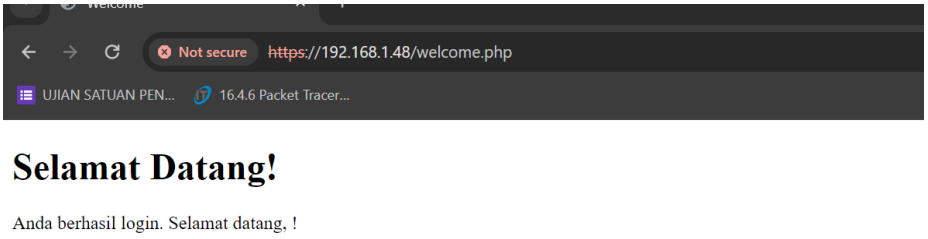
Terlihat bahwa situs web dapat diakses, namun browser masih menandai situs tersebut sebagai *'Not Secure'* karena sertifikat yang digunakan bersifat *self-signed*. Meskipun demikian, data transmisi antara klien dan server saat ini telah terenkripsi.

Gambar 4. Akses Web

Lakukan analisis menggunakan TCPDUMP setelah berhasil mengakses *username* dan *password* melalui HTTPS. Dengan TCPDUMP, aktivitas jaringan dapat dipantau untuk memastikan bahwa data login telah terenkripsi dan tidak dapat dibaca secara langsung, termasuk aktivitas yang terkait dengan HTTPS.

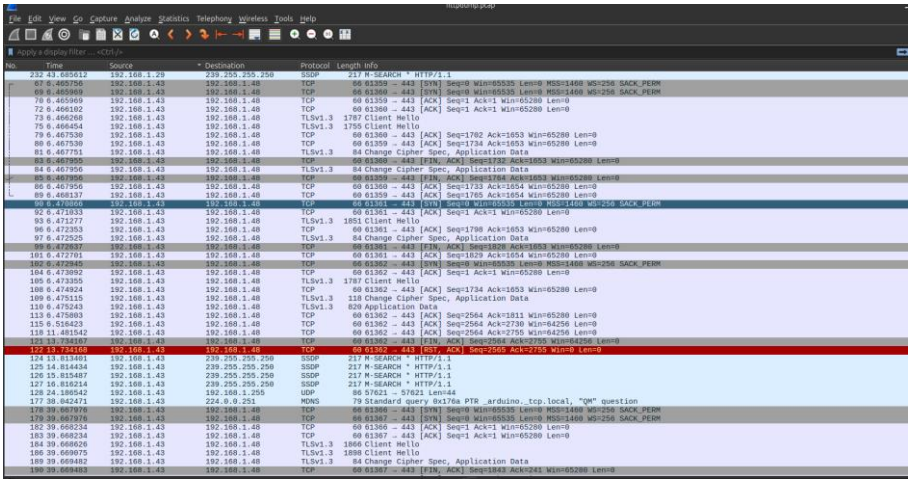
Gambar 5. *Login* setelah penerapan TCPDUMP

Jika sudah selesai *login* seperti ini, hentikan layanan TCPDUMP.



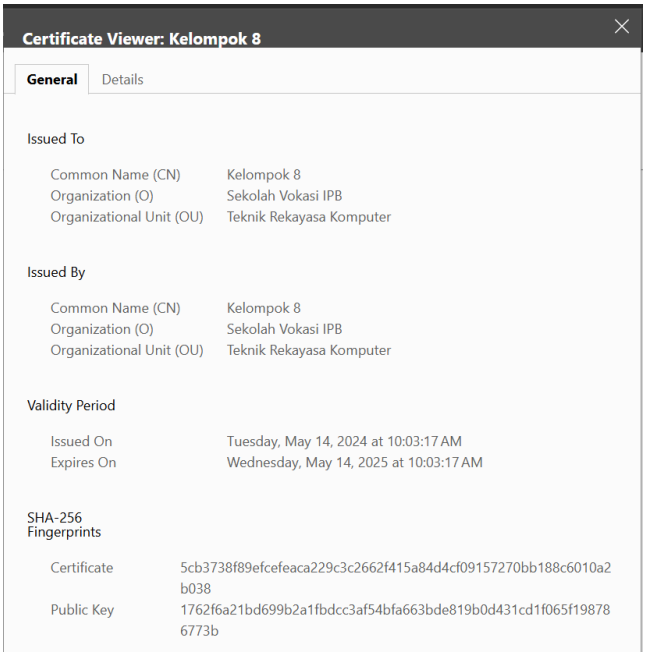
Gambar 6. Tampilan saat berhasil *login*

Selanjutnya, setelah memeriksa aktivitas dari sumber 192.168.1.43 (*Windows Host*) pada TCPDUMP, tidak ditemukan adanya HTTP POST. Hal ini mengindikasikan bahwa transmisi antara file index dan skrip login PHP telah terenkripsi, sehingga menunjukkan bahwa transmisi tersebut dilakukan dengan aman.



Gambar 7. Pengecekan aktivitas

Untuk memeriksa sertifikat, tampilkan sertifikat HTTPS seperti yang ditunjukkan di bawah ini saat diperiksa melalui browser pada Windows Host.



Gambar 8. Pengecekan sertifikat

Sertifikat yang diterbitkan oleh Ubuntu Linux dapat diterima oleh browser karena validitas sertifikat tersebut terjamin. Namun, browser Chrome masih menandai sertifikat tersebut sebagai *'Not Safe'* karena belum sepenuhnya terpercaya. Sertifikat ini penting untuk proses enkripsi, karena enkripsi HTTPS memerlukan sertifikat untuk melakukan *handshake* yang memungkinkan deskripsi data secara aman.

Berdasarkan penelitian yang telah dilakukan, risiko keamanan terkait dengan proses *login* dan *logout* akun melalui HTTP sangat signifikan. Akses akun melalui HTTP memungkinkan *username* dan *password* dengan mudah diakses oleh pihak yang tidak berwenang. Oleh karena itu, HTTPS sangat penting karena mengaktifkan enkripsi data yang ditransmisikan, sehingga meningkatkan keamanan. Sertifikat memainkan peran krusial dalam HTTPS karena sertifikat TLS (*Transport Layer Security*) digunakan untuk melakukan *handshake*, yaitu proses awal yang memastikan komunikasi yang aman antara klien dan server.

Simpulan

Implementasi HTTPS pada server web sangat penting untuk memastikan keamanan data yang ditransmisikan antara klien dan server. Dengan menggunakan sertifikat TLS, transmisi data dapat dienkripsi, sehingga melindungi informasi sensitif dari potensi peretasan. Meskipun sertifikat *self-signed* memberikan tingkat enkripsi yang memadai, untuk menghilangkan status ***'Not Secure'*** pada *browser*, sangat dianjurkan untuk menggunakan sertifikat yang diterbitkan oleh otoritas sertifikasi terpercaya. Proses ini menegaskan bahwa pengamanan server web dengan HTTPS adalah langkah krusial dalam menjaga integritas dan kerahasiaan data pengguna.

Daftar Pustaka

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 13(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Arianto, A. R., & Anggraini, D. G. (n.d.-a). Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team On Internet Infrastructure (Id-Sirtii) Building Indonesia's National Cyber Defense And Security To Face The Global Cyber Threats Through Indonesia Security Incident Response Team On Internet Infrastructure (Id-Sirtii). http://kominfo.go.id/index.

AlFardan, N. J., & Paterson, K. G. (2012). "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols." Proceedings of the 2013 IEEE Symposium on Security and Privacy.

A., Wahib, P., Tunggal Narotama, A., Muhamad Rijki, N., Permana, F., Sagara, D., Ibrahim Azkhal, D., Anwar, M., & Rifqi Juniawan, M. (2022). SOSIALISASI CYBER SECURITY UNTUK MENINGKATKAN LITERASI DIGITAL. 1(2). https://jurnal.portalpublikasi.id/index.php/AJP/index

Bhargavan, K., et al. (2016). "Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS." IEEE Symposium on Security and Privacy.

Bodo, J., & Green, M. (2018). "A Study of Forward Secrecy Deployment in HTTPS." Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems.

Buchegger, S., & Le Boudec, J. Y. (2006). "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes—Fairness In Dynamic Ad-hoc NeTworks)." Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing.

Cremers, C. J., et al. (2017). "The Security Impact of a New Cryptographic Library." Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

Dukhovni, V., et al. (2019). "Extended Validation Certificates Are Dead." Proceedings of the Internet Society Network and Distributed System Security Symposium.

Felt, A. P., et al. (2017). "Measuring HTTPS Adoption on the Web." Proceedings of the Internet Measurement Conference.

Garg, D., et al. (2018). "Understanding and mitigating the impact of layout shifts for developers." Proceedings of the 2018 World Wide Web Conference.

Gergely, A. M. (2022). BlockCACert – A Blockchain-Based Novel Concept for Automatic Deployment of X.509 Digital Certificates. *Lecture Notes in Networks and Systems*, *386*, 820–832. https://doi.org/10.1007/978-3-030-93817-8_73

Horvat, M., et al. (2019). "An Empirical Study of Web Transport Security in Practice." Proceedings of the 2019 ACM Internet Measurement Conference.

Hu, Q. (2021). A large-scale analysis of HTTPS deployments: Challenges, solutions, and recommendations. *Journal of Computer Security*, *29*(1), 25–50.

https://doi.org/10.3233/JCS-200070

Hughes, L. E. (2022). Pro Active Directory Certificate Services: Creating and Managing Digital Certificates for Use in Microsoft Networks. *Pro Active Directory Certificate Services: Creating and Managing Digital Certificates for Use in Microsoft Networks*, 1–459. https://doi.org/10.1007/978-1-4842-7486-6

Ishida, Y. (2023). Analysis of DNS Graph of Phishing Websites Using Digital Certificates. *International Conference on Advanced Communication Technology, ICACT*, *2023*, 174–179. https://doi.org/10.23919/ICACT56868.2023.10079566

Mavrogiannopoulos, N. (2017). "The dangers of key reuse: Practical attacks on IPsec IKE." Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

Mori, Y., et al. (2018). "Detection of SSL/TLS Vulnerabilities using Machine Learning." 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA).

Rescorla, E. (2018). "The Transport Layer Security (TLS) Protocol Version 1.3." RFC 8446. Internet Engineering Task Force (IETF).

Ristic, I. (2015). "Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications." IT Governance Ltd.

Wang, X. (2022). Research on technical scheme for multi type load resource information access. *Journal of Physics: Conference Series*, *2189*(1). https://doi.org/10.1088/1742-6596/2189/1/012030