KEAMANAN DATA PADA SITUS WEB MENGGUNAKAN PROTOKOL HTTP/HTTPS DENGAN SSL

Pingkan Putri Nazarina[1], Silvia Mairiani Rosdilillah[2], Acep Saepuloh Fatah[3]
nazarinakan@gmail.com[1], selfiapriliya23@gmail.com[2], cepstikiara@gmail.com[3]
Universitas Teknologi Yogyakarta

ABSTRAK

Era digital membuat keamanan web menjadi krusial karena peran yang sangat penting dari internet dalam kehidupan kita sehari-hari. Protokol HTTP, yang digunakan untuk komunikasi antara browser web dan server, rentan terhadap serangan karena data yang dikirim tidak dienkripsi. Artikel ini membahas pentingnya keamanan web dan menganalisis penggunaan protokol HTTPS, yang menggabungkan HTTP dengan SSL untuk meningkatkan keamanan komunikasi web. SSL (Secure Socket Layer) adalah protokol untuk mengamankan komunikasi internet dengan melakukan enkripsi data antara client dan server. Dengan implementasi SSL, komunikasi web menjadi lebih aman dan terjamin. Pembahasan meliputi perancangan konsep SSL, implementasi HTTPS, dan pentingnya penggunaan sertifikat SSL/TLS untuk validasi identitas dan enkripsi data. Kesimpulan menegaskan bahwa HTTPS menjadi solusi yang efektif untuk meningkatkan keamanan web, meskipun perlu dilakukan langkah-langkah tambahan seperti pembaruan server secara berkala dan penerapan otentikasi yang kuat untuk melindungi data dari akses yang tidak sah.

Kata Kunci: HTTP, HTTPS, Web Server, SSL.

PENDAHULUAN

Di zaman digital sekarang, menjaga keamanan web jadi amat penting karena internet memegang peran besar dalam kehidupan kita. Protokol HTTP, yang dipakai untuk komunikasi antara browser web dan server, adalah hal pokok dalam ini. Protokol ini digunakan untuk mengambil halaman web, gambar, video, dan lainnya dari server. Namun, HTTP tidak aman karena data yang dikirim antara klien dan server tidak dienkripsi, membuatnya rentan terhadap serangan seperti Man-in-the-Middle (MITM) dan perekaman data (sniffing). Kami akan membahas tentang HTTPS, yang membuat komunikasi web menjadi lebih aman dengan menggabungkan HTTP dengan SSL. Dengan HTTPS, data yang dikirim antara pengguna dan server akan diacak sehingga lebih sulit untuk disadap. Kami juga akan melihat bagaimana kita bisa menerapkan HTTPS untuk membuat website kita lebih aman. Jadi, dengan menggunakan HTTPS, kita bisa membuat website kita terlindungi lebih baik, meskipun tetap penting untuk melakukan langkah-langkah tambahan untuk melindungi data dari serangan yang tidak sah.

METODE PENELITIAN

Metode penelitian ini melibatkan beberapa tahap untuk mengimplementasikan dan menguji protokol HTTPS pada website yang sebelumnya hanya menggunakan HTTP.

HASIL DAN PEMBAHASAN

Perancangan dan Penerapan Konsep Protokol SSL

Dalam perancangan konsep SSL ini terdapat beberapa kriteria (parameter) atau sertifikasi yang ditetapkan dalam penggunaanya, seperti :

1. Public Key Algorithm (RSA/Rivest-Shamir-Adleman)
2. Key Length (2048 bit)
3. Signature Algorithm (SHA-256)

4. Domain Name (example.com/.co.id/.co)
5. Key Purposes (Digital Signature)
6. Extended (Server and Client Authentication)
7. Authority Method (OCSP/Online Certificate Status Protocol)
8. Certificate Policies (Domain Validation)
9. Authority Info (Letsencrypt.org)

Untuk kesembilan kriteria (parameter) diatas merupakan bentuk minimal dan wajib disediakan dalam meminta konfirmasi terhadap Certificate Authority (CA). Jika kriteria ini dikonfirmasi, lalu ketika proses akses ke domain dilakukan pesan untuk pengkonfirmasian ke email dan persetujuan untuk Term of Service. Untuk contoh verifikasi dari Certificate Authority seperti pada gambar dibawah ini.

Gambar 1. Certificate Authority Verification

Gambar tersebut menunjukan proses dalam memastikan bahwa situs web dapat diakses tanpa hambatan dan melakukan otentikasi untuk mendapatkan sertifikat enkripsi. Dimana selanjutnya pengguna harus menggunakan HTTPS bukan HTTP, karena sudah memvalidasi sertifikat SSL.

Untuk mengimplementasikannya perlu dilakukan perubahan atau penambahan sebuah file(.htaccess), yang dimana file ini akan mengarahkan setiap akses pengunjung web agar tetap dalam penggunaan protokol HTTPS. Ini sangat penting dalam komunikasi antara pengguna dan situs web supaya tetap terenkripsi dan aman.

Implementasi SSL

Penerapan protokol ini akan menggunakan salah satu website komunikasi yang belum terindikasi HTTPS, yaitu pada web p3m.pnp.ac.id. Platform perangkat lunak yang didapatkan dari web informasi ini sebagai berikut:

1. Sistem operasi : CentOS 7.8.2003
2. Apache webserver : versi 2.4.6
3. MySQL Version : 5.5.65
4. PHP : Version 5.6.25
5. Virtual share hosting server

Sebelum menerapkan protokol HTTPS, dilakukan pengujian terlebih dahulu. Pertama, informasi dari browser yang digunakan untuk mengakses website p3m.pnp.ac.id dimanfaatkan. Dari gambar 2, terlihat bahwa website p3m.pnp.ac.id belum menerapkan protokol HTTPS, ditandai dengan ikon gembok yang disilang merah. Saat ikon gembok tersebut diklik, muncul informasi bahwa koneksi ke website p3m.pnp.ac.id tidak aman. Informasi teknis menunjukkan bahwa koneksi internet ke website p3m.pnp.ac.id tidak dienkripsi, meningkatkan risiko data dapat dilihat oleh pihak lain.

Gambar 2. Koneksi ke Website Tidak Aman

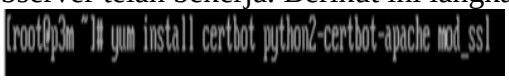
Untuk memperoleh informasi yang lebih akurat, data mengenai website p3m.pnp.ac.id juga dicari melalui website penyedia informasi keamanan website, salah satunya adalah ssllabs.com. Dimana pada website ini dapat memberikan informasi bahwa web p3m.pnp.ac.id memang benar belum menerapakan protokol keamanan dan belum memiliki sertifikasi SSL dalam komunikasi data nya.

Pemahaman Penerapan Dalam Penggunaannya

Pada platform webserver yang digunakan untuk website p3m.pnp.ac.id, yaitu Apache dengan database MySQL, standar enkripsi diterapkan dengan langkah-langkah berikut: Langkah awal melibatkan pembuatan private key (server.key), yang digunakan untuk permintaan penandatanganan sertifikat (CSR). CSR ini berisi informasi domain atau website yang diajukan, dalam hal ini adalah p3m.pnp.ac.id. Setelah private key dan CSR dibuat, langkah selanjutnya adalah mengajukan CSR ke Certificate Authority (CA), seperti Symantec, VeriSign, GoDaddy, atau LetsEncrypt. CA adalah organisasi yang berwenang untuk memvalidasi dan mengeluarkan sertifikat enkripsi domain atau website. Setelah proses validasi selesai dan disetujui oleh CA, mereka akan mengirimkan dua file dengan ekstensi *.pem dan *.crt, bersama dengan server.key yang telah dikirimkan sebelumnya. File *.pem dan *.crt tersebut, juga dikenal sebagai Sertifikat Secure Socket Layer (SSL), harus ditempatkan di web server p3m.pnp.ac.id setelah diterima. Tindakan ini sangat penting untuk menjamin keamanan dan keabsahan komunikasi antara pengguna dan website, serta melindungi data sensitif yang ditransmisikan melalui jaringan.

Pemilihan Protokol SSL yang Akan Digunakan

Sebelum implementasi protokol keamanan komunikasi seperti penerapan sertifikat SSL, pastikan layanan webserver telah bekerja. Berikut ini langkah penerapan protokol:



Gambar 3. Penginstalan mod_ssl

Langkah selanjutnya adalah dengan menetapkan domain yang akan menggunakan sertifikat SSL tersebut, domain yang dipilih adalah domain p3m.pnp.ac.id.

Gambar 4. Penetapan Domain SSL

Perancangan Keamanan SSL

Dalam upaya meningkatkan keamanan komunikasi antara pengunjung dan website p3m.pnp.ac.id, beberapa kriteria atau parameter telah ditetapkan untuk sertifikat SSL. Ini mencakup algoritma kunci publik, panjang kunci, algoritma tanda tangan, nama domain, tujuan kunci, keperluan ekstensi, metode otoritas, kebijakan sertifikat, dan informasi otoritas. Proses otentikasi terhadap keberadaan website menjadi hal mutlak dalam

mengusulkan sertifikat untuk enkripsi website. Oleh karena itu, yang paling penting adalah memastikan bahwa website yang diajukan dapat diakses tanpa hambatan. Langkah berikutnya adalah menetapkan apakah pengunjung atau klien dapat mengakses website p3m.pnp.ac.id menggunakan protokol HTTP tanpa sertifikat SSL atau apakah sudah wajib menggunakan protokol HTTPS. Selain itu, skrip perlu disiapkan untuk meneruskan setiap akses pengunjung ke website p3m.pnp.ac.id sesuai dengan konfigurasi yang ditetapkan.

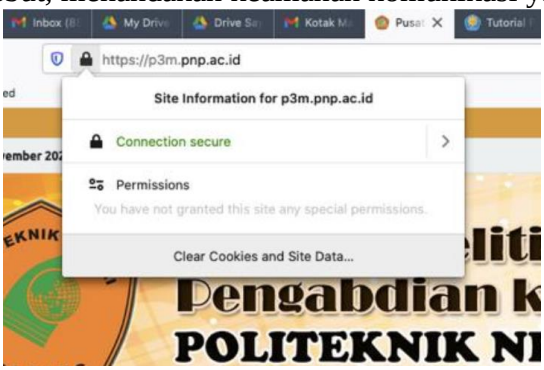
```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Gambar 5. Script .htaccess

Script ini ditempatkan pada webserver p3m.pnp.ac.id, sehingga setiap permintaan koneksi ke website tersebut akan diteruskan ke protokol https, meskipun pengunjung tidak menuliskan nama protokolnya di alamat yang dituju pada web browser.

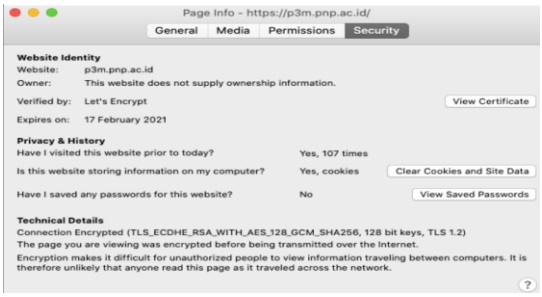
Pembahasan Hasil

Setelah serangkaian tahapan SSL dilakukan, menunjukkan bahwa protokol HTTPS telah berhasil diterapkan pada website p3m.pnp.ac.id setelah melalui tahapan yang telah ditentukan. Pengunjung dapat melihat tanda gembok hijau di alamat URL ketika mengakses website tersebut, menandakan keamanan komunikasi yang lebih baik.



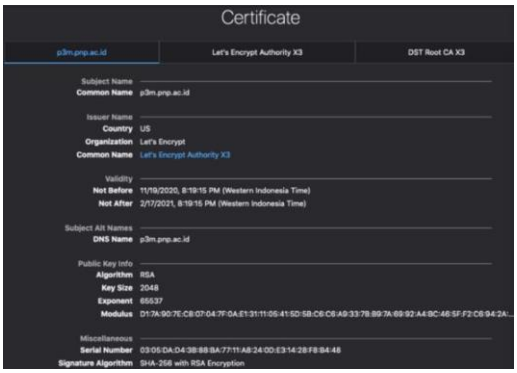
Gambar 6. Protokol https

Jika digali lebih jauh, informasi teknis yang ditampilkan mengenai website p3m.pnp.ac.id dinyatakan bahwa website sudah mendukung enkripsi data, sehingga data yang dikirimkan melalui internet akan menyulitkan bagi orang yang tidak berhak untuk melihat.



Gambar 7. Informasi Teknis Website

Memberikan informasi berupa alamat website yang diakses, kepemilikan, verifikasi untuk keamanan dan tanggal kadaluarsa. Agar informasi yang didapatkan dalam penelitian ini lebih akurat, dengan menggunakan browser firefox, dapat dilihat bahwa parameter yang dipilih untuk sertifikat SSL sudah sesuai dengan yang diharapkan.



Gambar 8. Sertifikat SSL Website p3m

Dari penelitian yang dilakukan, sekarang website p3m.pnp.ac.id telah menggunakan sertifikat SSL untuk melindungi komunikasi data antara pengunjung dan website. Data terenkripsi saat pengunjung berkomunikasi dengan website, dan kunci publik serta algoritma RSA membuat sulit bagi pihak yang tidak berhak untuk mengakses data yang ditangkap selama komunikasi.

Namun, masih ada beberapa kriteria yang tidak memenuhi uji keamanan website berdasarkan observasi Mozilla Observatory yang memeriksa header dan konten sebuah website. Ada empat kriteria yang tidak lulus uji, termasuk kebijakan keamanan konten, pilihan jenis konten, perlindungan XSS, dan opsi frame. Kriteria-kriteria ini penting untuk memastikan keamanan minimal dalam pengaturan website.

KESIMPULAN

Secara kesimpulan, protokol HTTP tidak bisa dikatakan aman terkecuali sudah melakukan enkirpsi penggabungan antara HTTP dan SSL yang menjadi versi terbaru dari HTTP dengan lapisan keamanan, enkripsi data dan validasi identitas dengan sertifikasi SSL/TLS yaitu protokol HTTPS.

Dimana protokol HTTPS ini mengenkripsi data yang membuat informasi sulit dan susah dimanipulasi oleh pihak tidak berwenang. Meskipun HTTPS memberikan tingkat keamanan yang tinggi, tetap penting untuk selalu memperhatikan praktik keamanan yang baik dan memperbarui sistem secara teratur.

Dengan demikian, langkah penting dalam meningkatkan keamanan komunikasi web, dimana bahwa keamanan data web akan selalu melibatkan berbagai aspek dan perlunya perhatian yang berkelanjutan.

DAFTAR PUSTAKA

Utomo, I. C., & Rokhmah, S. (2012). Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta. Jurnal Rekayasa Teknologi Informasi (JURTI), 6(2), 143. ISSN: 2579-8790.

Azwan, M., Adriansyah, A. F., & Al Fauzan, M. R. (2022). Protokol Secure Socket Layer untuk Keamanan Berbasis Web. Jurnal TripleA, 81. ISSN 2962-5688. Diakses dari jurnal.umj.ac.id/index.php/TripleA, pada tanggal 7 Mei 2024.

Prayama, D., Yuhefizar, & Yolanda, A. (2021). Protokol HTTPS, Apakah Benar-benar Aman?. Journal of Applied Computer Science and Technology (JACOST), Vol. 2 No. 1, Hal. 7-11. ISSN 2723-1453. Diakses dari http://journal.isas.or.id/index.php/JACOST, pada tanggal 7 Mei 2024.

Dharmawan, N., Indriyanta, G., & Senapartha, I.K.D. (2022). Analisis Keamanan Jaringan Universitas Kristen Duta Wacana dengan Serangan SSL/TLS. Jurnal Teknologi Informasi dan Ilmu Komputer (JUTEI), 6(2), Halaman 214. DOI: 10.21460/jutei.2022.62.214