

RESUME HTTP, HTTPS, DNS, SERVER

HTTP, atau Hypertext Transfer Protocol, adalah dasar komunikasi web, memungkinkan klien seperti browser untuk meminta dan menerima data dari server. Ini mengikuti model permintaan-respons, dengan klien menggunakan metode seperti GET, POST, atau DELETE untuk meminta sumber daya dan server merespons dengan data. HTTP tidak memiliki kewarganegaraan, tetapi cookie menyimpan informasi sesi, dan HTTPS menambahkan enkripsi untuk keamanan. Versi seperti HTTP/1.1, HTTP/2, dan HTTP/3 (QUIC) meningkatkan efisiensi. Prinsip REST memandu layanan web, sementara WebSockets mendukung interaksi waktu nyata. Tantangan keamanan mencakup XSS dan CSRF, yang diatasi dengan metode autentikasi. Tipe konten mencakup HTML, JSON, dan gambar, dengan kompresi yang mengurangi ukuran payload. CDN dan penyeimbangan beban meningkatkan kinerja, dan taktik pengoptimalan web meningkatkan kecepatan pemuat. Keberadaan HTTP di mana-mana membentuk internet, mendasari pengalaman web modern.

HTTPS, kependekan dari Hypertext Transfer Protocol Secure, adalah protokol internet penting yang memastikan pertukaran data yang aman antara klien (misalnya, browser web) dan server. Dibangun di atas HTTP, ia menambahkan enkripsi SSL/TLS untuk keamanan, melindungi data dari penyadapan dan gangguan selama transit. Diakui dengan awalan "https://" dan port 443, HTTPS mengandalkan sertifikat SSL/TLS yang dikeluarkan oleh Otoritas Sertifikat (CA) tepercaya untuk memvalidasi keaslian situs web, meyakinkan pengguna tentang koneksi server. HTTPS sangat penting untuk melindungi data sensitif seperti kredensial login dan informasi pembayaran, sehingga sangat diperlukan untuk e-commerce dan perbankan online. Mesin pencari memprioritaskan situs HTTPS, sementara situs web non-HTTPS mungkin diberi label tidak aman di browser, sehingga mendorong adopsi secara luas. Transisi ke HTTPS adalah praktik terbaik keamanan siber, yang memastikan penjelajahan web aman dan perlindungan data.

DNS

DNS (Sistem Nama Domain) adalah infrastruktur internet penting yang menerjemahkan nama domain yang dapat dibaca manusia (seperti example.com) menjadi alamat IP numerik (seperti 192.0.2.1) yang digunakan komputer untuk menemukan situs web dan layanan. Ini bertindak sebagai buku alamat internet, memungkinkan pengguna mengakses situs web dengan mengetikkan nama yang dikenal, bukan alamat IP yang rumit. DNS beroperasi melalui hierarki server terdistribusi, termasuk penyelesai rekursif, server root, server domain tingkat atas (TLD), dan server nama otoritatif. Saat Anda memasukkan URL di browser Anda, pemecah DNS lokal Anda menanyakan serangkaian server untuk menemukan alamat IP yang sesuai. Cache di berbagai tingkatan membantu mempercepat proses ini. DNS juga mendukung fitur-fitur penting seperti pendaftaran domain, pengelolaan data sumber daya (misalnya data A, CNAME, MX), dan DNSSEC (Ekstensi Keamanan DNS) untuk melindungi terhadap spoofing DNS dan gangguan data. Meskipun DNS sangat penting untuk fungsionalitas internet, DNS juga rentan terhadap serangan seperti keracunan cache DNS dan serangan Distributed Denial of Service (DDoS), yang menekankan pentingnya langkah-langkah keamanan yang kuat dan praktik terbaik dalam administrasinya.

RESUME HTTP, HTTPS, DNS, SERVER

SERVER

Komputer khusus yang dirancang untuk menyediakan layanan, sumber daya, atau data ke komputer lain, yang dikenal sebagai klien, melalui jaringan. Mereka memainkan peran penting dalam komputasi modern, melayani berbagai fungsi seperti hosting web, manajemen email, penyimpanan file, dan banyak lagi. Server biasanya dilengkapi perangkat keras yang kuat, redundansi untuk keandalan, dan perangkat lunak khusus untuk tugas tertentu. Jenis server yang umum mencakup server web (misalnya Apache, Nginx), server email (misalnya Exchange, Postfix), server file (misalnya FTP, NAS), dan server database (misalnya MySQL, PostgreSQL). Server dapat berupa mesin fisik atau mesin virtual di cloud. Mereka berkomunikasi dengan klien menggunakan protokol standar seperti HTTP, FTP, atau SMTP. Keamanan adalah yang terpenting, dan server menggunakan firewall, enkripsi, dan kontrol akses untuk melindungi data. Skalabilitas server, kinerja, dan waktu aktif merupakan pertimbangan penting dalam manajemen server. Selain itu, pemantauan dan pemeliharaan server memastikan fungsionalitas dan keamanan yang optimal, menjadikan server sebagai bagian integral dari infrastruktur digital organisasi dan internet secara keseluruhan.