TECHNOVATAR Jurnal Teknologi, Industri dan Informasi
Vol. 4, No. 3, Juli 2026, pp. 1 – 17
Open Access:
https://journal.awatarapublisher.com/index.php/technovatar
ISSN: 3031-8874, **DOI**: 10.61434/technovatar.v4i3.410

KEPATUHAN KONFIGURASI TLS DAN HEADER KEAMANAN WEBSITE PTN DAN PTS DI WILAYAH LLDIKTI IV

Mohamad Firdaus[1*]
[1] Program Studi Informatika, Fakultas Teknik, Institut Teknologi dan Kesehatan Mahardika, Cirebon, Indonesia
Email: firdaus@itekesmahardika.ac.id

INFO ARTIKEL
Sejarah Artikel:
Diterima, 15 Mei 2026
Direvisi, 22 Mei 2026
Disetujui, 2 Juli 2026

KEYWORDS
TLS
HTTP security headers
Higher education
Configuration assessment
LLDIKTI IV

ABSTRACT
This cross-sectional study assesses TLS and security response headers on 16 purposively selected institutional websites: four public and twelve private universities in the LLDIKTI IV service area. Verified TLS connections and limited homepage requests supported a criterion-based configuration assessment. Twelve HTTPS HTML homepages were eligible for header analysis, whereas three returned application-layer blocking responses (HTTP 403) post-handshake and one showed client-dependent certificate verification. Fifteen successful handshakes negotiated TLS 1.3. HSTS appeared on 8/12 homepages, nosniff on 7/12, and active CSP on 5/12. Five met the framing profile and one met the selected Referrer-Policy profile. No observed CSP met the selected script, object, and base-URI profile. Independent checks confirmed assessed header values on three homepages. Findings support targeted configuration ownership, staged policy deployment, and repeatable monitoring. The nonprobability sample and uneven coverage restrict population-level conclusions.

This work is licensed under a Creative Commons Attribution 4.0 International License.

KATA KUNCI
TLS
Header keamanan HTTP
Perguruan tinggi
Audit konfigurasi
LLDIKTI IV

CORRESPONDING AUTHOR
Mohamad Firdaus
Program Studi Informatika, Fakultas Teknik, Institut Teknologi dan Kesehatan Mahardika
Jl. Taman Pemuda No. 2, Cirebon 45153, Jawa Barat, Indonesia
Email: firdaus@itekesmahardika.ac.id

ABSTRAK
Studi potong lintang ini mengevaluasi TLS dan header keamanan pada 16 website institusi yang dipilih secara purposif: empat PTN dan dua belas PTS dalam wilayah layanan LLDIKTI IV. Koneksi TLS terverifikasi dan permintaan homepage terbatas digunakan untuk penilaian konfigurasi berbasis kriteria. Dua belas homepage HTML HTTPS memenuhi syarat analisis header, sedangkan tiga memberikan respons blokir lapis aplikasi (HTTP 403) pasca-handshake dan satu menunjukkan perbedaan verifikasi sertifikat antar-klien. Kelima belas handshake yang berhasil menegosiasikan TLS 1.3. HSTS hadir pada 8/12 homepage, nosniff pada 7/12, dan CSP aktif pada 5/12. Lima memenuhi profil framing dan satu memenuhi profil Referrer-Policy terpilih. Tidak ada CSP yang memenuhi profil pembatasan script, object, dan base URI. Pemeriksaan independen mengonfirmasi nilai header pada tiga homepage. Temuan mendukung kepemilikan konfigurasi yang jelas, penerapan kebijakan bertahap, serta pemantauan berulang. Sampel nonprobabilitas dan cakupan tidak seimbang membatasi kesimpulan pada tingkat populasi.

PENDAHULUAN

Website resmi perguruan tinggi menjadi pintu masuk informasi akademik, penerimaan mahasiswa, layanan kelembagaan, dan navigasi menuju aplikasi kampus. Ketergantungan tersebut menjadikan keandalan komunikasi dan konfigurasi browser bagian dari mutu layanan digital. Studi mengenai

keamanan perguruan tinggi memperlihatkan bahwa persoalannya mencakup aset, ancaman, pengelolaan risiko, dan kontrol teknis, bukan satu komponen website saja (Ulven dan Wangen, 2021). Penilaian terukur terhadap komponen publik dapat menyediakan bukti awal bagi pengelola TI, selama cakupan pengamatan dan batas kesimpulan dijelaskan.

TLS dan header respons HTTP menangani fungsi yang berbeda. TLS melindungi komunikasi antara klien dan endpoint serta memungkinkan verifikasi identitas layanan. Header dapat menyampaikan kebijakan kepada browser mengenai penggunaan HTTPS, pemuatan sumber daya, penyematan halaman, interpretasi tipe konten, dan pengiriman referrer. TLS 1.3 didefinisikan oleh Rescorla (2018), sementara rekomendasi penggunaan TLS diberikan oleh Sheffer et al. (2022). Keberhasilan handshake TLS pada lapis transportasi tidak otomatis membuktikan bahwa kebijakan pertahanan browser terhadap risiko injeksi skrip (XSS) atau penyematan halaman (clickjacking) telah disiapkan, sebagaimana keberadaan CSP tidak membuktikan bahwa semua jalur aplikasi terlindungi penuh.

Penelitian terdahulu menyediakan pendekatan yang beragam. Eshetu et al. (2024) mengkaji 16 website universitas Ethiopia menggunakan survei kesadaran dan penilaian kerentanan. Macakoğlu et al. (2023) menilai aksesibilitas, kegunaan, dan keamanan halaman calon mahasiswa pada universitas lintas kawasan. Di Indonesia, Saputra et al. (2025) menggunakan ISSAF pada satu website kampus. Pendekatan tersebut penting sebagai konteks, tetapi unit observasi dan kedalaman pengujiannya berbeda dengan audit respons homepage yang dibatasi pada konfigurasi publik.

Kajian yang langsung berhubungan dengan header dilakukan Mileva et al. (2025) pada 756 website dalam beragam kategori di Makedonia. Penelitian tersebut memperlihatkan bahwa implementasi dan konfigurasi header merupakan objek pengukuran tersendiri. Namun, skor suatu alat maupun proporsi pada negara lain tidak dapat dipindahkan menjadi ukuran keamanan kampus dalam wilayah penelitian ini. Safaei Pour et al. (2023) juga menekankan tantangan ketepatan dan kelengkapan pengukuran Internet. Karena itu, asal domain, respons yang layak dianalisis, perilaku klien, serta data yang tidak terukur harus dipertahankan dalam jejak audit.

Kebutuhan penelitian ini adalah pemetaan terbatas yang menghubungkan konfigurasi transportasi dengan kebijakan browser pada PTN dan PTS dalam wilayah layanan LLDIKTI IV. Istilah wilayah layanan dipakai untuk mencakup perguruan tinggi Jawa Barat dan Banten yang menjadi konteks koordinasi regional, tanpa menyamakan kedudukan administratif PTN dengan pembinaan PTS. Sumber resmi kegiatan koordinasi LLDIKTI IV menunjukkan keterlibatan PTN dan PTS (LLDIKTI IV, 2023). Penelitian tidak mengeklaim sebagai sensus atau sebagai studi pertama pada wilayah tersebut.

Rumusan masalahnya ialah: bagaimana hasil verifikasi transportasi pada website sampel; header apa yang hadir dan konfigurasi apa yang belum memenuhi profil penelitian; serta bagaimana hasil deskriptif tersebut dapat diterjemahkan menjadi tindakan pengelolaan TI. Tujuannya adalah menghasilkan dataset respons yang dapat ditelusuri, klasifikasi dengan aturan eksplisit, dan rekomendasi yang sebanding dengan bukti. Kontribusi utama terletak pada pemisahan antara header yang tidak hadir, konfigurasi parsial, hasil ambigu, dan kegagalan pengukuran, sehingga kekurangan bukti tidak disamakan dengan ketidakpatuhan.

METODE PENELITIAN

Desain, cakupan, dan pemilihan institusi

Penelitian menggunakan desain observasional potong lintang dengan evaluasi konfigurasi berbasis kriteria. Sampel dibatasi pada 16 institusi: 4 PTN dan 12 PTS. Pemilihan bersifat purposif dengan kuota status penyelenggara dan keterwakilan dua provinsi. Kelompok PTN meliputi tiga institusi Jawa Barat dan satu Banten; kelompok PTS meliputi delapan institusi Jawa Barat dan empat Banten. Kuota tidak diturunkan dari proporsi populasi. Ukuran dan komposisi kuota lintas provinsi tersebut dipilih secara terukur untuk menjaga kedalaman audit, memungkinkan verifikasi normalisasi domain resmi, pelaksanaan uji pilot, serta pemeriksaan kasus konfigurasi secara terperinci.

PDDikti digunakan sebagai sumber utama yang dituju untuk identitas institusi. Rekaman individual berhasil dibaca untuk Unsika, UPI, IPB, dan Universitas Pakuan. Untuk sebelas PTS lainnya, identitas dan alamat website diperiksa melalui direktori resmi LLDIKTI IV. Identitas Untirta dan status PTN didukung profil resmi institusi. Jalur verifikasi berbeda tersebut dicatat pada dataset; tidak dinyatakan bahwa semua status aktif sudah dicocokkan secara individual ke PDDikti. Domain yang tampil dengan awalan protokol ganda dinormalisasi, sementara alias www Universitas Pamulang yang tidak dapat diresolusikan diganti dengan hostname institusional yang dikonfirmasi pada homepage resminya.

Tabel 1 menyajikan seluruh unit penelitian, sehingga batas sampel dapat diperiksa tanpa mengandalkan angka agregat peserta rapat atau direktori. PTLN, perguruan tinggi keagamaan di luar lingkup layanan yang dituju, institusi kedinasan, aplikasi login, dan website fakultas tidak dimasukkan. Daftar tersebut ditetapkan sebelum pengukuran utama. Unit metadata ialah institusi; unit teknis ialah hostname homepage resmi. Seluruh 16 hostname awal berbeda, sehingga tidak ada duplikasi unit teknis pada kerangka sampel.

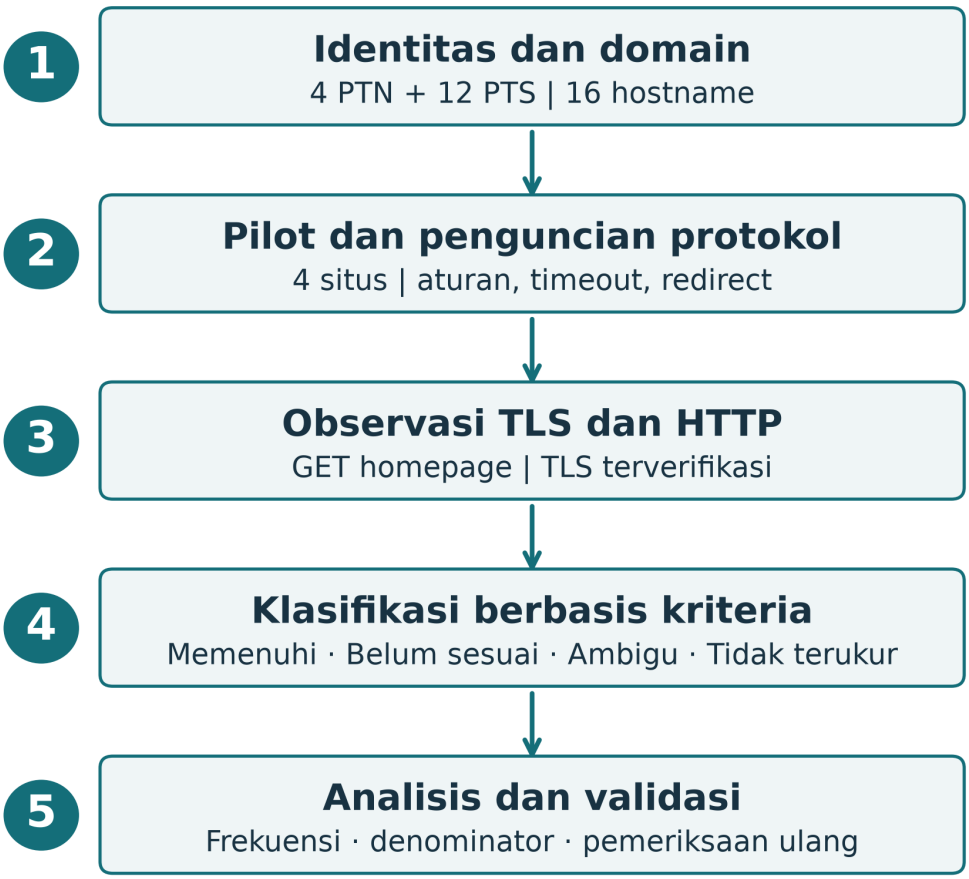
Tabel 1. Sampel institusi dan hostname yang diperiksa

ID	Institusi	Status / provinsi	Hostname
S01	Universitas Singaperbangsa Karawang	PTN / Jabar	www.unsika.ac.id
S02	Universitas Pendidikan Indonesia	PTN / Jabar	www.upi.edu
S03	Institut Pertanian Bogor	PTN / Jabar	www.ipb.ac.id
S04	Universitas Sultan Ageng Tirtayasa	PTN / Banten	untirta.ac.id
S05	Universitas Ibn Khaldun Bogor	PTS / Jabar	www.uika-bogor.ac.id
S06	Universitas Islam Bandung	PTS / Jabar	www.unisba.ac.id
S07	Universitas Islam Nusantara	PTS / Jabar	www.uninus.ac.id
S08	Universitas Pakuan	PTS / Jabar	www.unpak.ac.id
S09	Universitas Katolik Parahyangan	PTS / Jabar	www.unpar.ac.id
S10	Universitas Pasundan	PTS / Jabar	www.unpas.ac.id
S11	Universitas Kristen Maranatha	PTS / Jabar	www.maranatha.edu
S12	Universitas Telkom	PTS / Jabar	www.telkomuniversity.ac.id
S13	Universitas Islam Syekh Yusuf	PTS / Banten	www.unis.ac.id
S14	Universitas Pamulang	PTS / Banten	unpam.ac.id
S15	Universitas Muhammadiyah Tangerang	PTS / Banten	umt.ac.id
S16	Universitas Pembangunan Jaya	PTS / Banten	www.upj.ac.id

Sumber domain dan jalur verifikasi individual tersedia dalam sample16.csv. ID merupakan identitas penelitian, bukan kode administratif nasional.

Pilot dan prosedur pengumpulan

Gambar 1 menunjukkan alur dari verifikasi sampai validasi. Pilot pada empat situs menguji akses DNS, rantai redirect, respons blokir, dan penyimpanan header berulang. Pilot pertama berhenti akibat kesalahan penanganan DNS pada alat; rekaman yang telah tersimpan dipertahankan. Setelah penanganan kesalahan diperbaiki, pilot kedua menyelesaikan empat rekaman. Parameter dan daftar sampel kemudian dikunci. Data pilot tidak digabungkan ke denominator hasil utama.



Gambar 1. Alur studi observasional dan audit konfigurasi. Data pilot dipisahkan dari hasil utama.

Pengumpulan utama memakai permintaan GET tanpa autentikasi pada homepage HTTP dan HTTPS, konkurensi satu, jeda dua detik, timeout 20 detik per operasi, dan maksimum lima redirect. Hanya port layanan normal 80/443 yang digunakan. Redirect boleh diikuti dalam hostname institusional yang telah disahkan, dengan root sebagai jalur awal. Jalur bahasa homepage UPI /id diizinkan secara eksplisit setelah verifikasi; jalur lain tidak ditelusuri otomatis. Tidak dilakukan eksploitasi, pengiriman payload, fuzzing, pemindaian port, pencarian direktori, maupun pengambilan halaman aplikasi internal.

Koneksi TLS memakai verifikasi sertifikat bawaan klien, SNI sesuai hostname, batas minimum klien TLS 1.2, dan negosiasi HTTP/1.1. Bukti TLS menyimpan versi, cipher, SAN, issuer, masa berlaku, serta status kesalahan. Timestamp asli, parameter, versi Python/OpenSSL, dan lokasi trust store dipertahankan dalam data mentah. Header disimpan sebagai daftar pasangan nama–nilai untuk mempertahankan urutan serta duplikasi. Badan halaman tidak dibaca oleh pengumpul utama. Semantik respons dan penggabungan field merujuk Fielding et al. (2022).

Homepage layak analisis header apabila koneksi HTTPS terverifikasi menghasilkan status 2xx dengan tipe HTML/XHTML. Respons blokir 403 yang umumnya dipicu oleh kebijakan proteksi bot pada Web Application Firewall (WAF) atau CDN, kegagalan koneksi, serta rantai yang belum selesai tidak digunakan untuk menilai header homepage. Endpoint HTTPS final dari rantai awal HTTPS dipilih terlebih dahulu; apabila tidak eligible, endpoint HTTPS eligible yang dicapai melalui

rantai HTTP digunakan. TLS tetap dapat terukur ketika homepage diblokir. Oleh karena itu, denominator transportasi dan header tidak selalu sama.

Operasionalisasi kepatuhan

Kepatuhan berarti kesesuaian terhadap profil konfigurasi penelitian, bukan sertifikasi keamanan, kepatuhan hukum, atau bukti bebas kerentanan. Tabel 2 menjelaskan kriteria dan batasnya. Empat status digunakan: M memenuhi profil, F belum sesuai profil, A ambigu, dan U tidak terukur. Keberadaan header dilaporkan terpisah dari penilaian profil. Hasil secara sengaja tidak diringkas menjadi skor komposit tunggal (seperti nilai huruf A–F) agar tidak menyamarkan celah konfigurasi spesifik, mengingat fungsi teknis serta konteks mitigasi tiap indikator sangat berbeda.

Tabel 2. Kriteria operasional dan batas interpretasi

Indikator	Memenuhi profil	Batas penilaian / dasar
HTTP → HTTPS	Rantai teramati mencapai HTTPS tanpa downgrade	Kegagalan rantai: U. RFC 9325; RFC 9110.
Sertifikat	Verifikasi hostname, periode dan chain diterima klien	Hasil berbeda antar-klien: A. RFC 9525.
TLS ternegosiasi	Versi hasil handshake TLS 1.2/1.3	Tidak menguji semua versi server. RFC 8446; RFC 8996.
HSTS	max-age valid dan positif pada HTTPS	includeSubDomains/preload opsional. RFC 6797.
nosniff	Nilai nosniff menurut pemrosesan field	Tidak menguji MIME semua sumber daya. Fetch 2025.
CSP sumber daya	Pembatasan script/default; object none; base URI self/none	Profil penelitian, bukan kewajiban universal. W3C 2021.
Framing	XFO DENY/SAMEORIGIN atau frame-ancestors terbatas	Konteks embedding tidak diuji. RFC 7034; W3C 2021.
Referrer	Token efektif sesuai profil privasi terpilih	Absence tidak membuktikan default browser tidak aman. W3C 2017.
Permissions-Policy	Keberadaan dicatat sebagai indikator tambahan	Tidak diberi status kepatuhan wajib. W3C 2025.

M/F/A/U diterapkan pada delapan indikator inti. Tiga kondisi profil CSP dijelaskan dalam teks metode; bukan validasi browser penuh.

Profil CSP sumber daya menetapkan tiga kondisi teramati: script-src atau default-src yang membatasi sumber tanpa wildcard global, skema luas, unsafe-inline, atau unsafe-eval; object-src 'none'; serta base-uri 'self' atau 'none'. Profil ini adalah aturan operasional penelitian untuk mengidentifikasi kebutuhan peninjauan, bukan persyaratan universal W3C. CSP yang hanya mengatur framing atau upgrade-insecure-requests tetap dihitung hadir dan aktif, tetapi tidak memenuhi profil sumber daya. Parser membantu ekstraksi direktif; kebijakan yang ditemukan dibaca ulang. Efektivitas di browser dan seluruh aplikasi tidak diuji.

Untuk framing, X-Frame-Options DENY/SAMEORIGIN atau CSP aktif frame-ancestors dengan pembatasan yang valid diterima. Allowlist origin HTTPS eksplisit dicatat, tanpa menyimpulkan bahwa kebutuhan bisnis tiap origin sudah diaudit. Bila frame-ancestors aktif ditemukan, penilaiannya mempertimbangkan kebijakan tersebut. CSP Report-Only dipisahkan karena bukan kebijakan penegakan. Aturan framing merujuk Ross dan Gondrom (2013) serta W3C (2021).

Profil Referrer-Policy terpilih mencakup no-referrer, same-origin, strict-origin, dan strict-origin-when-cross-origin. Token valid lain tetap dicatat, tetapi belum memenuhi profil privasi ini. Pada field berulang, token terakhir yang dikenal dipakai menurut aturan pemrosesan kebijakan. Header yang tidak hadir tidak membuktikan bahwa browser mengirim referrer tanpa pembatasan; meta,

atribut elemen, dan default browser berada di luar pengukuran (W3C, 2017). Permissions-Policy hanya dilaporkan keberadaannya, tanpa klasifikasi wajib, karena kebutuhan fitur tidak diuji (W3C, 2025).

Analisis dan validasi

Analisis menggunakan frekuensi serta persentase deskriptif. Untuk indikator j, N_j adalah jumlah M ditambah F, dan proporsi memenuhi dihitung M_j/N_j × 100%. A dan U selalu ditampilkan terpisah. Untuk keberadaan header, denominator adalah seluruh homepage eligible, termasuk yang tidak memuat header. Grafik status menggunakan kerangka awal n = 16 agar kehilangan cakupan tetap terlihat. Tidak digunakan imputasi untuk kegagalan akses, uji signifikansi antarstatus institusi, atau interval kepercayaan yang menyiratkan sampel probabilitas.

Validasi mencakup pembacaan ulang nilai mentah serta pengambilan ulang empat kasus dengan curl sebagai klien independen tanpa opsi melewati verifikasi TLS. Tiga kasus merupakan homepage eligible; satu dipilih karena kegagalan issuer pada klien utama. Peninjauan memeriksa lima indikator header per homepage eligible, dengan total 15 sel penilaian. Ini pemeriksaan konsistensi alat dan pembacaan ulang, bukan studi kesepakatan antar-reviewer. Perbedaan klien tidak disembunyikan dan digunakan dalam adjudikasi status ambigu.

HASIL

Cakupan pengukuran

Seluruh 16 situs menghasilkan rekaman percobaan pengukuran. Dua belas homepage eligible, terdiri atas dua PTN dan sepuluh PTS. Tiga homepage memberikan respons 403, yaitu S02, S04, dan S06. S05 gagal verifikasi issuer pada klien utama. Respons blokir tetap disimpan sebagai bukti akses, tetapi header halaman tersebut dikeluarkan dari analisis homepage. Tabel 3 memperlihatkan denominator menurut status institusi.

Tabel 3. Cakupan analisis menurut status penyelenggara

Kelompok	Kerangka	Header eligible	Blokir 403	Kendala TLS klien utama
PTN	4	2	2	0
PTS	12	10	1	1
Total	16	12	3	1

Seluruh unit memiliki rekaman percobaan. Kendala TLS S05 diputuskan ambigu setelah validasi antar-klien; header klien kedua tidak dipool ke dataset utama.

Cakupan header sebesar 12/16 atau 75,0% penting untuk interpretasi. Penghilangan empat situs dari analisis tidak terjadi secara acak, dan proporsi yang terukur berbeda antara PTN dan PTS. Karena itu, hasil 12 homepage tidak boleh dilaporkan sebagai prevalensi seluruh wilayah. Perbedaan denominator juga menjelaskan mengapa statistik TLS dapat tersedia pada situs yang tidak mempunyai statistik header homepage.

Transportasi dan sertifikat

Empat belas rantai HTTP dapat diklasifikasikan dan seluruhnya mencapai endpoint HTTPS yang teramati. Dua rantai tidak cukup untuk memastikan hasil redirect. Tidak ditemukan downgrade pada rantai yang berhasil diamati. Kelima belas handshake utama yang berhasil menegosiasikan TLS 1.3. Karena klien menetapkan minimum TLS 1.2, pengamatan ini tidak menguji apakah server juga menerima TLS 1.0/1.1. Dengan demikian, hasil tidak ditafsirkan sebagai bukti bahwa protokol lama sudah dinonaktifkan pada seluruh server.

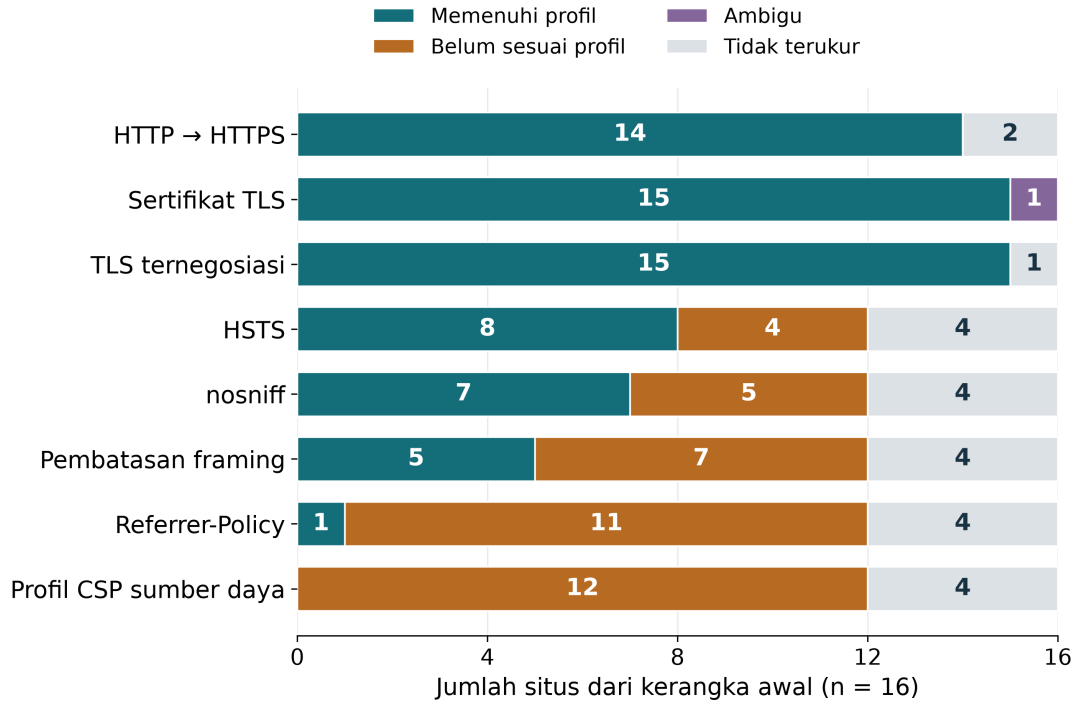
Lima belas hostname diterima oleh verifikasi sertifikat klien utama. Pada S05, klien utama melaporkan verify_code 20, yaitu issuer tidak dapat diverifikasi oleh trust store yang digunakan. Pengambilan ulang dengan curl menerima koneksi HTTPS terverifikasi dan mendapatkan header

respons 200; transfer badan kemudian mengalami timeout. Perbedaan perilaku validasi akibat kelengkapan pengiriman rantai sertifikat perantara (intermediate CA chain) dan mekanisme pengambilan sertifikat antar-klien tersebut tidak cukup untuk menyatakan sertifikat server tidak valid secara universal. Setelah adjudikasi, S05 diberi A pada indikator sertifikat dan U pada versi TLS serta header dalam dataset utama. Tabel 4 dan Gambar 2 mempertahankan kategori tersebut.

Tabel 4. Distribusi kesesuaian indikator dengan denominator eksplisit

Indikator	M	F	A	U	N_j	M/N_j
HTTP → HTTPS	14	0	0	2	14	100,0%
Sertifikat	15	0	1	0	15	100,0%
TLS ternegosiasi	15	0	0	1	15	100,0%
HSTS	8	4	0	4	12	66,7%
nosniff	7	5	0	4	12	58,3%
Profil CSP	0	12	0	4	12	0,0%
Framing	5	7	0	4	12	41,7%
Referrer-Policy	1	11	0	4	12	8,3%

N_j = M + F. A dan U tidak diimputasi. Keberhasilan negosiasi TLS tidak membuktikan penolakan protokol lama. S05 ambigu pada sertifikat setelah pemeriksaan independen.



Gambar 2. Status indikator terhadap kerangka awal 16 situs. Kategori ambigu dan tidak terukur ditampilkan terpisah; persentase memenuhi memakai denominator terklasifikasi pada Tabel 4.

Keberadaan dan konfigurasi header

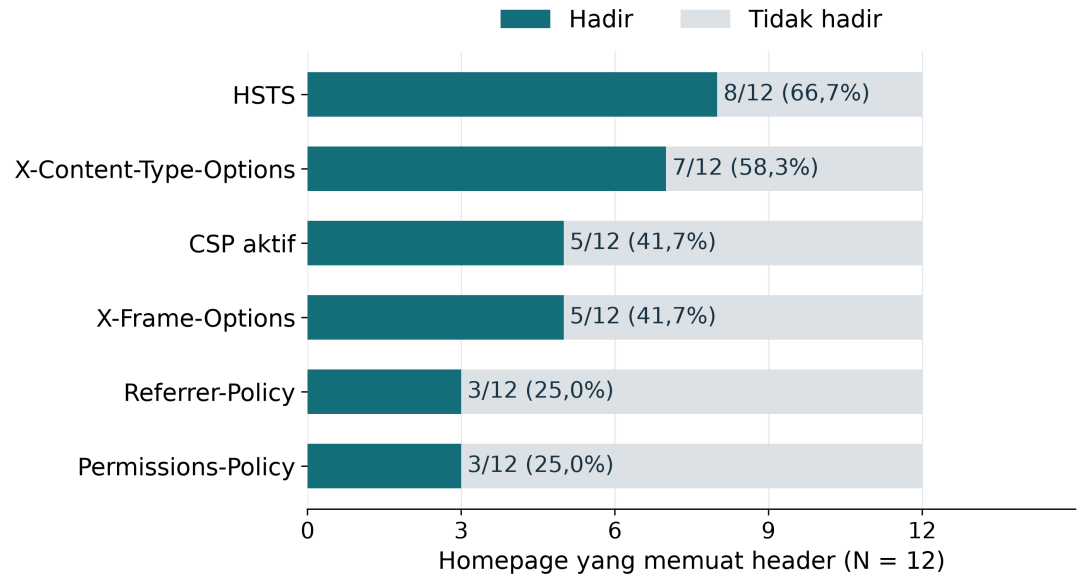
Tabel 5 dan Gambar 3 menunjukkan bahwa keberadaan header bervariasi. HSTS ditemukan pada 8/12 homepage (66,7%) dan seluruh delapan nilai mempunyai max-age positif. Empat homepage tidak memuat HSTS. nosniff ditemukan dan memenuhi aturan nilai pada 7/12 homepage (58,3%);

lima tidak memuatnya. Temuan ini berhubungan dengan kebijakan yang disampaikan respons homepage, bukan dengan keseluruhan konfigurasi server atau isi MIME semua berkas.

Tabel 5. Keberadaan header pada respons homepage eligible

Header	Hadir	Tidak hadir	Hadir / N = 12
HSTS	8	4	66,7%
nosniff	7	5	58,3%
CSP aktif	5	7	41,7%
X-Frame-Options	5	7	41,7%
Referrer-Policy	3	9	25,0%
Permissions-Policy	3	9	25,0%
CSP Report-Only	0	12	0,0%

Keberadaan dan kesesuaian merupakan keluaran berbeda. Tidak adanya Permissions-Policy atau Report-Only tidak dinilai sebagai pelanggaran universal.



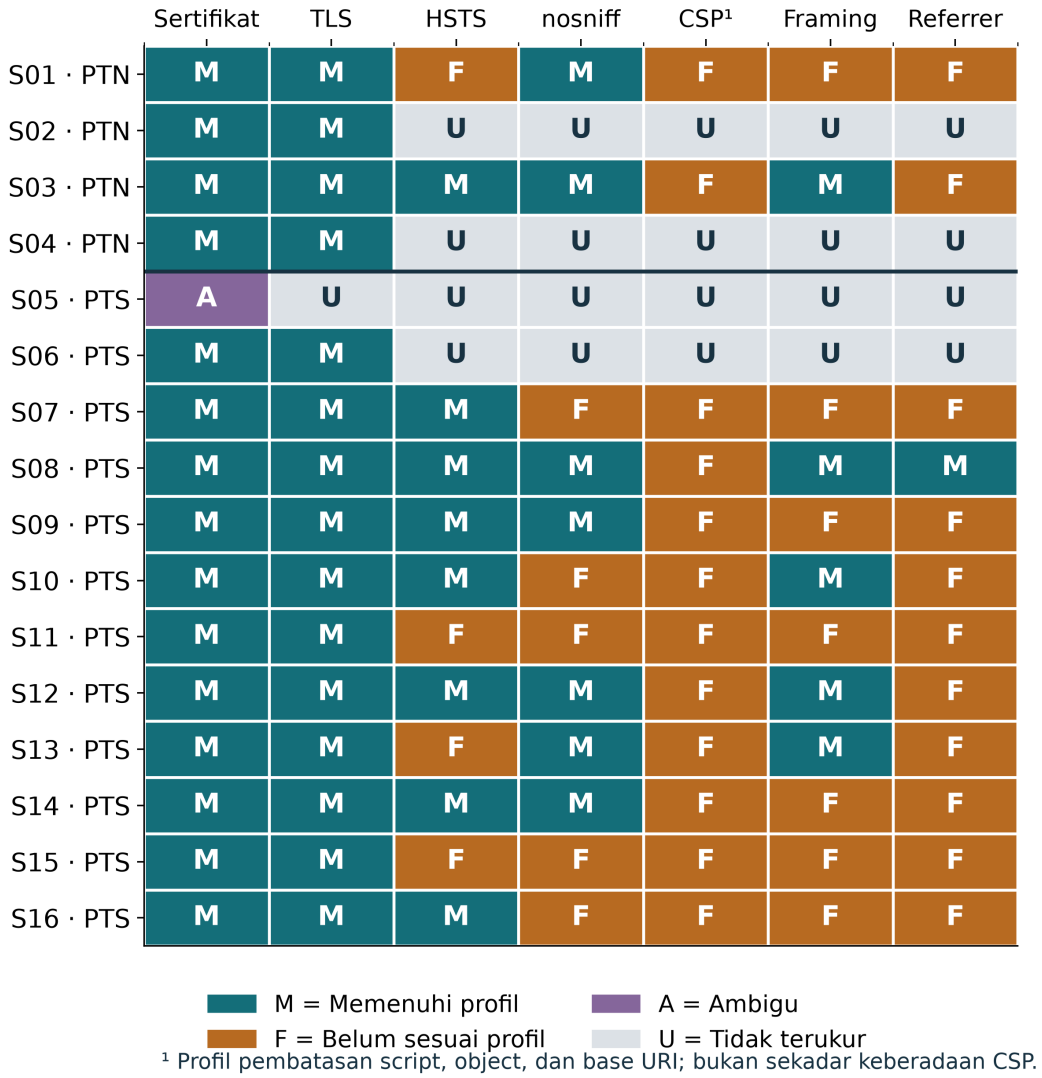
Gambar 3. Keberadaan header pada 12 homepage eligible. Kehadiran tidak menyatakan efektivitas perlindungan.

CSP aktif hadir pada 5/12 homepage (41,7%), sementara tujuh tidak memuatnya. Kelima kebijakan yang hadir menyediakan kontrol parsial: upgrade-insecure-requests, pembatasan frame-ancestors, atau kombinasi keduanya; satu juga memuat block-all-mixed-content. Tidak ditemukan CSP Report-Only pada 12 respons eligible. Tidak satu pun dari lima konfigurasi memenuhi seluruh profil sumber daya yang ditetapkan. Oleh sebab itu, angka 0/12 pada indikator profil CSP harus dibaca bersama angka kehadiran 5/12, di mana ketergantungan sistem manajemen konten (CMS) kampus terhadap inline script sering menjadi kendala penerapan pembatasan ketat tanpa mekanisme nonce atau hash.

X-Frame-Options ditemukan pada lima homepage. Setelah mempertimbangkan alternatif CSP frame-ancestors, lima homepage memenuhi profil pembatasan framing dan tujuh belum memenuhi. Referrer-Policy hadir pada tiga homepage: dua menggunakan no-referrer-when-downgrade, sedangkan satu mempunyai dua field dengan token akhir strict-origin-when-cross-origin. Semua token tersebut dikenal, tetapi hanya kasus terakhir memenuhi profil privasi terpilih. Sembilan

homepage tidak memuat Referrer-Policy. Permissions-Policy hadir pada tiga homepage dan tidak diberi skor kepatuhan.

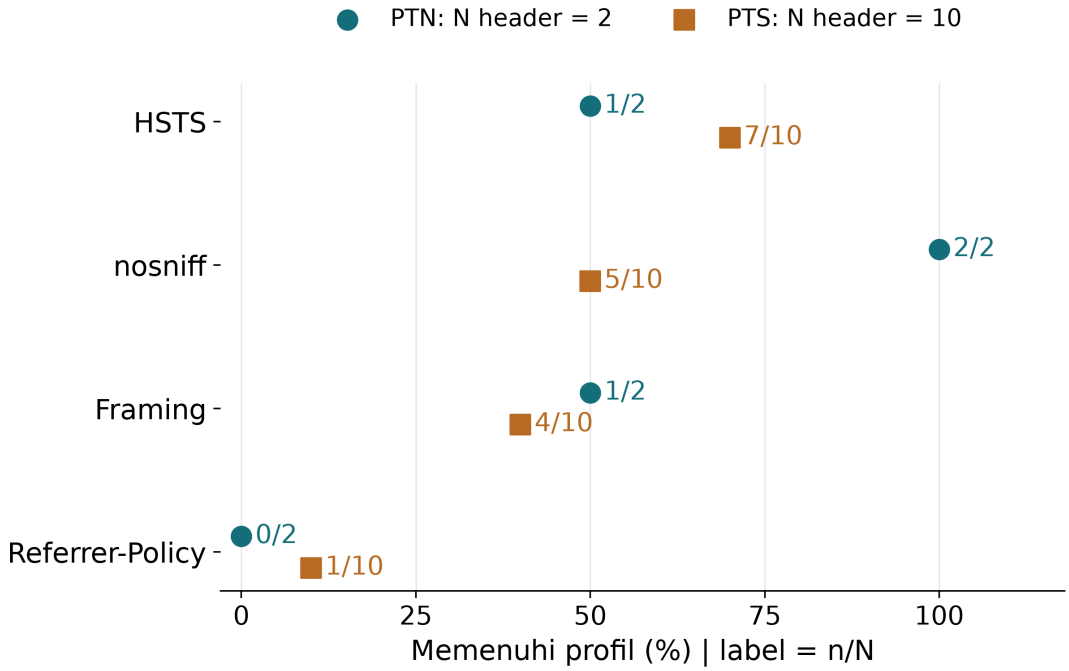
Matriks Gambar 4 menunjukkan konfigurasi per situs tanpa membuat peringkat keamanan. Satu situs dapat memenuhi TLS tetapi tidak mempunyai beberapa header yang dinilai. Kategori U pada situs yang diblokir tetap terlihat, sehingga kekurangan pengukuran tidak tampak sebagai kegagalan konfigurasi. Pemetaan ID ke institusi tersedia pada Tabel 1 dan dataset.



Gambar 4. Matriks hasil per situs. M: memenuhi; F: belum sesuai profil; A: ambigu; U: tidak terukur. CSP merujuk profil sumber daya terpilih, bukan sekadar kehadiran.

Perbandingan deskriptif dan pemeriksaan ulang

Pada dua homepage PTN eligible, HSTS memenuhi profil pada 1/2, nosniff pada 2/2, framing pada 1/2, dan Referrer-Policy pada 0/2. Pada sepuluh homepage PTS eligible, hasilnya masing-masing 7/10, 5/10, 4/10, dan 1/10. Gambar 5 mencantumkan pembilang serta penyebut setiap titik. Ukuran PTN yang sangat kecil dan dua homepage PTN yang diblokir tidak mendukung kesimpulan bahwa salah satu status penyelenggara lebih aman.



Gambar 5. Perbandingan deskriptif pada dua homepage PTN dan sepuluh PTS eligible. Label titik menyatakan n/N; tidak dilakukan inferensi perbedaan populasi.

Pemeriksaan ulang pada S01, S03, dan S08 mengonfirmasi 15/15 sel penilaian header yang diperiksa. S03 memuat dua field CSP aktif yang dipertahankan terpisah, sementara S08 memuat dua field Referrer-Policy dengan urutan yang sama pada klien independen. Pada S05, terdapat perbedaan penerimaan TLS antar-klien sehingga kesimpulan dibatasi. Tabel 6 merangkum keputusan validasi, termasuk timeout setelah header diterima.

Tabel 6. Pemeriksaan ulang dan keputusan klasifikasi

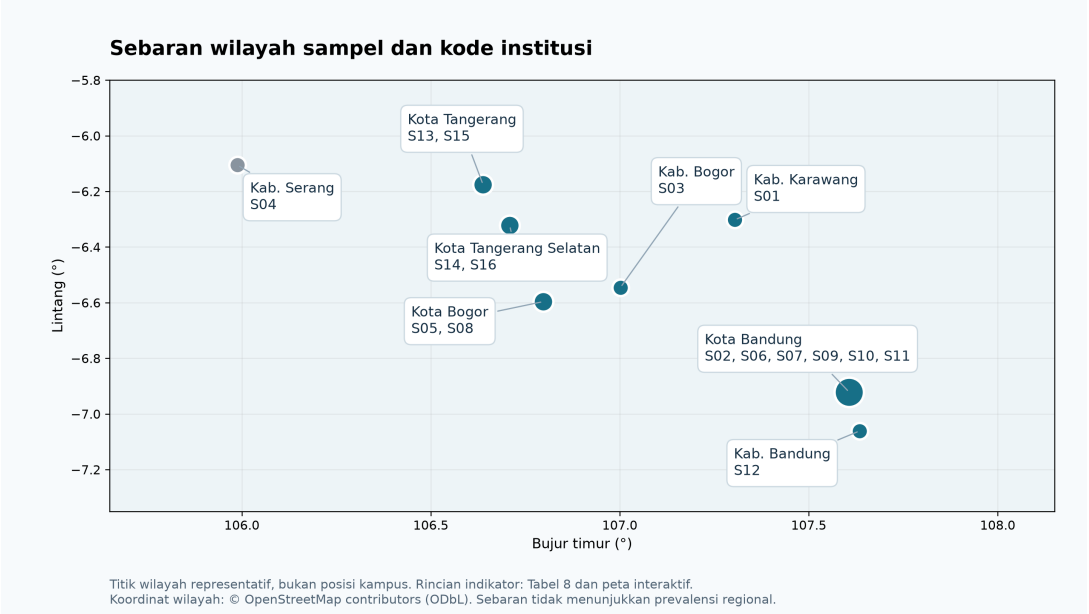
Kasus	Observasi utama	Pemeriksaan independen	Keputusan
S01	nosniff; header lain yang dinilai tidak hadir	Nilai sama pada respons 200	Lima sel header konsisten
S03	Dua field CSP; referrer no-referrer-when-downgrade	Dua CSP dan token referrer tetap sama	Lima sel header konsisten
S08	Framing CSP; dua field Referrer-Policy	Urutan token referrer sama	Lima sel header konsisten
S05	TLS issuer gagal, verify_code 20	TLS diterima; header HTTPS 200; body timeout	Sertifikat A; header utama U

Pemeriksaan ulang tanpa bypass TLS. Sebanyak 15/15 sel header yang diperiksa konsisten; ini bukan kesepakatan antar-reviewer atau bukti kestabilan seluruh sampel.

Pemetaan wilayah dan kode institusi

Pemetaan menghubungkan identitas penelitian S01–S16 dengan kota/kabupaten dan indikator konfigurasi pada Tabel 8. Delapan wilayah representatif mencakup Kabupaten Karawang, Kota Bandung, Kabupaten Bogor, Kabupaten Serang, Kota Bogor, Kabupaten Bandung, Kota Tangerang, dan Kota Tangerang Selatan. Untuk institusi multikampus, wilayah dipilih berdasarkan alamat institusi atau kampus utama yang dirujuk; pemetaan tidak mencakup seluruh cabang. Penanda berbasis koordinat administratif OpenStreetMap, bukan pengukuran koordinat kampus. Kabupaten

Serang merujuk kampus utama Sindangsari; Kabupaten Bandung merujuk lokasi Dayeuhkolot. Penempatan geografis merupakan pelengkap deskriptif dan tidak menambah unit observasi keamanan.



Gambar 7. Sebaran delapan wilayah representatif dan kode institusi. Penanda bukan koordinat kampus; rincian indikator terdapat pada Tabel 8. Koordinat wilayah © OpenStreetMap contributors (ODbL).

Tabel 8. Pemetaan kode institusi, wilayah dan indikator belum sesuai

ID	Kota/kabupaten	Belum sesuai profil	Status observasi
S01	Kab. Karawang	HSTS; Profil CSP (absen); Framing; Referrer-Policy	Header terukur
S02	Kota Bandung	Tidak dinilai	Header tidak terukur (403)
S03	Kab. Bogor	Profil CSP (parsial); Referrer-Policy	Header terukur
S04	Kab. Serang	Tidak dinilai	Header tidak terukur (403)
S05	Kota Bogor	Tidak dinilai	Header tidak terukur; sertifikat ambigu
S06	Kota Bandung	Tidak dinilai	Header tidak terukur (403)
S07	Kota Bandung	nosniff; Profil CSP (absen); Framing; Referrer-Policy	Header terukur
S08	Kota Bogor	Profil CSP (parsial)	Header terukur
S09	Kota Bandung	Profil CSP (absen); Framing; Referrer-Policy	Header terukur
S10	Kota Bandung	nosniff; Profil CSP (parsial); Referrer-Policy	Header terukur
S11	Kota Bandung	HSTS; nosniff; Profil CSP (absen); Framing; Referrer-Policy	Header terukur
S12	Kab. Bandung	Profil CSP (parsial); Referrer-Policy	Header terukur
S13	Kota Tangerang	HSTS; Profil CSP (parsial); Referrer-Policy	Header terukur
S14	Kota Tangerang Selatan	Profil CSP (absen); Framing; Referrer-Policy	Header terukur

ID	Kota/kabupaten	Belum sesuai profil	Status observasi
S15	Kota Tangerang	HSTS; nosniff; Profil CSP (absen); Framing; Referrer-Policy	Header terukur
S16	Kota Tangerang Selatan	nosniff; Profil CSP (absen); Framing; Referrer-Policy	Header terukur

CSP absen/parsial mengacu profil penelitian. Header tidak terukur tidak diberi status gagal. Wilayah institusi multikampus dipilih sebagai lokasi representatif. Tautan pencarian Google Maps tersedia pada peta interaktif pendamping.

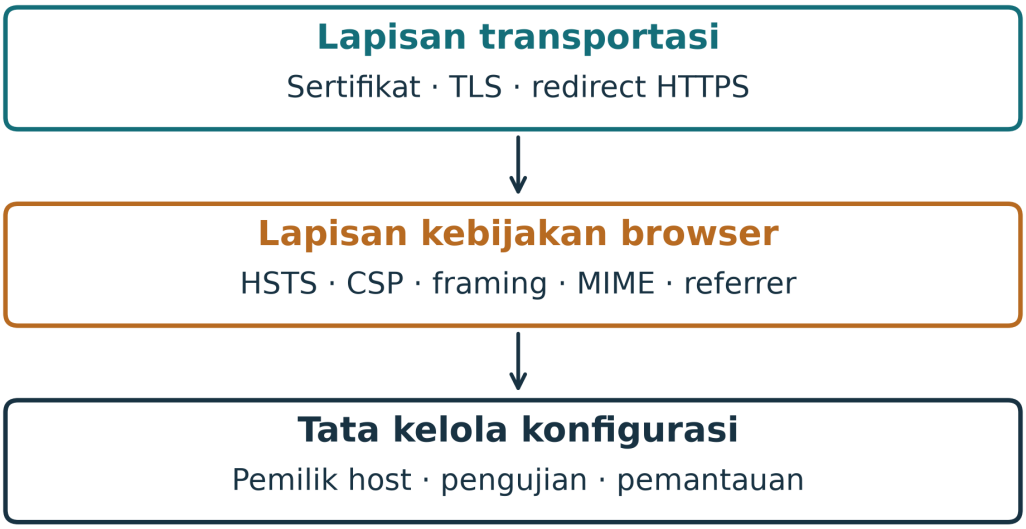
Peta interaktif pendamping menyediakan filter PTN/PTS dan indikator, rincian kode institusi, serta tautan pencarian Google Maps. Pencarian Google Maps tidak diperlakukan sebagai bukti koordinat kampus. S01, misalnya, belum memenuhi profil HSTS, CSP, framing, dan Referrer-Policy, sedangkan nosniff memenuhi. S08 memenuhi framing dan Referrer-Policy, tetapi CSP-nya masih parsial terhadap profil sumber daya yang dipilih. S02, S04, dan S06 tidak diberikan daftar kekurangan header karena respons 403 tidak eligible; S05 dipisahkan karena kendala klien utama dan ambiguitas sertifikat. Dengan demikian, pengelola dapat menelusuri jenis tindak lanjut tanpa menyamakan ketidaktersediaan data dengan ketidakpatuhan.

Sebaran kode geografis ini murni mencerminkan pemilihan sampel purposif dalam wilayah koordinasi LLDIKTI IV; pengelompokan sejumlah institusi di satu kota sama sekali tidak membuktikan bahwa wilayah tersebut secara spasial lebih rentan. Penelitian tidak menghitung proporsi kepatuhan per wilayah karena ukuran dan cakupan sampel wilayah tidak mewakili populasi.

DISKUSI DAN PEMBAHASAN

Kesenjangan transportasi dan kebijakan browser

Temuan utama adalah ketimpangan antara transportasi yang berhasil dinegosiasikan dan kelengkapan kebijakan browser pada homepage. Semua handshake yang berhasil memakai TLS 1.3, tetapi empat homepage tidak memuat HSTS, lima tidak memuat nosniff, dan tujuh belum mempunyai pembatasan framing yang memenuhi profil. Dua lapisan tersebut perlu dikelola bersama sebagaimana digambarkan dalam Gambar 6. Hasil tidak membuktikan bahwa salah satunya dapat menggantikan fungsi yang lain.



Gambar 6. Lapisan pemeriksaan dan tindak lanjut pengelolaan konfigurasi. Diagram konseptual, bukan arsitektur jaringan institusi.

Secara operasional, sertifikat yang diterima belum menjamin bahwa pengunjung yang memulai dari HTTP memperoleh kebijakan transportasi tersimpan pada browser. Demikian pula, HTTPS tidak menetapkan sumber script, asal embedding, atau kebijakan referrer. Konfigurasi TLS perlu diuji menurut identitas layanan (Saint-Andre dan Salz, 2023), sedangkan rekomendasi versi protokol tetap merujuk Moriarty dan Farrell (2021) serta Sheffer et al. (2022). Penelitian ini tidak memperluas pengukuran menjadi enumerasi protokol atau cipher yang didukung server.

Makna konfigurasi parsial

Pemisahan keberadaan dan kualitas konfigurasi menghasilkan temuan yang lebih informatif daripada daftar header ada/tidak ada. Lima CSP aktif yang ditemukan menunjukkan bahwa sebagian pengelola telah mengirim kebijakan tertentu. Namun, kebijakan upgrade transportasi atau framing memiliki fungsi berbeda dari pembatasan script, object, dan base URI. Tidak terpenuhinya profil penelitian memberi alasan untuk meninjau konfigurasi, tanpa menyatakan bahwa kebijakan parsial itu tidak bermanfaat atau bahwa kelemahan tertentu dapat dieksploitasi.

Hasil Referrer-Policy juga memerlukan pembedaan serupa. Dua homepage mengirim token yang sah tetapi belum memenuhi profil privasi terpilih. Dengan demikian, masalah yang diamati tidak hanya ketidakhadiran pada sembilan homepage, tetapi juga pilihan kebijakan pada dua kasus lainnya. Untuk framing, penerimaan allowlist origin HTTPS adalah penilaian struktur kebijakan; pengelola tetap perlu memastikan bahwa setiap origin mempunyai alasan operasional. Penelitian tidak menilai integrasi mitra atau kebutuhan embedding institusi.

Hubungan dengan penelitian terdahulu

Temuan konfigurasi yang tidak merata sejalan secara tematik dengan kajian header Mileva et al. (2025), tetapi persentase kedua penelitian tidak dibandingkan sebagai ukuran yang setara. Penelitian tersebut memakai Mozilla Observatory, kategori website yang lebih luas, dan skor alat; penelitian ini memakai profil eksplisit tanpa skor gabungan. Perbedaan metode, populasi, dan penanganan respons blokir dapat mengubah denominator maupun klasifikasi.

Eshetu et al. (2024) dan Saputra et al. (2025) melakukan pengujian dengan ruang lingkup lebih luas. Data homepage dalam studi ini tidak dapat mengonfirmasi jumlah kerentanan, tingkat

eksploitabilitas, atau efektivitas remediasi seperti yang mungkin dinilai oleh metode tersebut. Model evaluasi Haque et al. (2023) juga mengarah pada risiko operasional perguruan tinggi yang lebih menyeluruh. Kontribusi studi ini lebih sempit: menyediakan bukti konfigurasi yang dapat diulang dan aturan interpretasi yang menjaga batas antara observasi dan inferensi.

Implikasi pengelolaan TI

Rekomendasi pada Tabel 7 diturunkan dari kondisi teramati, bukan dari asumsi kapasitas atau anggaran institusi. Perbaikan yang dapat ditinjau meliputi konsistensi pengiriman nosniff, kebijakan HSTS setelah kesiapan HTTPS diperiksa, serta Referrer-Policy sesuai kebutuhan privasi. CSP memerlukan inventaris sumber daya dan pengujian kompatibilitas. Penerapan bertahap melalui direktif Content-Security-Policy-Report-Only sangat direkomendasikan bagi pengelola TI kampus untuk menginventarisasi pemuatan skrip dan mencegah gangguan fungsi halaman (breaking changes) sebelum penegakan penuh, meskipun mode tersebut tidak dinilai sebagai perlindungan aktif dalam penelitian ini.

Tabel 7. Tindak lanjut yang diturunkan dari observasi

Temuan	Cakupan utama	Tindak lanjut	Batas interpretasi
HSTS tidak hadir	4/12 homepage	Tinjau kesiapan HTTPS, lalu kebijakan max-age	Jangan mengaktifkan cakupan subdomain tanpa inventaris
nosniff tidak hadir	5/12 homepage	Tinjau pengiriman konsisten dan MIME yang benar	Belum membuktikan serangan MIME
CSP absent / parsial	7 absent; 5 parsial	Inventaris sumber; uji Report-Only; penegakan bertahap	Profil penelitian tidak wajib universal
Framing belum memenuhi	7/12 homepage	Tentukan kebutuhan embedding dan allowlist	Tidak membuktikan clickjacking berhasil
Referrer absent / di luar profil	9 absent; 2 token di luar profil	Pilih kebijakan privasi sesuai alur layanan	Default browser/meta tidak diukur
Sertifikat berbeda antar-klien	1/16 situs	Periksa chain, trust store, dan klien pembanding	Bukan bukti invaliditas server universal

Rekomendasi merupakan tindakan peninjauan konfigurasi; tidak berasal dari pengujian eksploitasi atau audit kebutuhan bisnis institusi.

Penerapan kebijakan sebaiknya mempunyai pemilik konfigurasi yang jelas pada web server, reverse proxy, atau CDN, serta pemeriksaan setelah perubahan. HSTS includeSubDomains maupun preload memerlukan pertimbangan cakupan subdomain; penelitian ini tidak menjadikannya kewajiban universal (Hodges et al., 2012). Pendekatan tata kelola tersebut berhubungan dengan perhatian Cheng dan Wang (2022) pada strategi institusional, walaupun dataset ini tidak mengukur proses organisasi, kompetensi SDM, atau kematangan keamanan kampus.

Keterbatasan dan arah penelitian

Sampel purposif 16 institusi dan 12 homepage eligible membatasi validitas eksternal. Pemilihan institusi yang domainnya dapat diverifikasi tidak menjamin representasi semua ukuran, bentuk, maupun kapasitas TI perguruan tinggi. Kelompok PTN dan PTS mempunyai ukuran serta kehilangan cakupan berbeda. Perbandingan angka kecil hanya menggambarkan observasi yang diperoleh dan tidak menunjukkan pengaruh status penyelenggara.

Pengukuran dibatasi pada satu jendela observasi, satu klien utama, HTTP/1.1, dan homepage. CDN, kebijakan antiotomasi, perubahan edge, serta trust store dapat memengaruhi hasil. Kasus S05 menunjukkan bahwa masalah verifikasi pada satu klien perlu ditinjau sebelum diatribusikan kepada server. Pemeriksaan ulang tiga homepage tidak membuktikan stabilitas seluruh sampel atau seluruh

indikator. Kedudukan institusi dan domain juga harus dipelihara sebagai metadata yang dapat berubah.

Penelitian tidak merender aplikasi dalam browser, tidak menilai kebijakan melalui meta/atribut elemen, tidak menelusuri semua subdomain, dan tidak menguji serangan. Karena itu, efektivitas end-to-end, dukungan seluruh versi TLS, kebutuhan Permissions-Policy, dan keamanan sistem akademik tidak dapat disimpulkan. Pengembangan berikutnya dapat menggunakan kerangka institusi yang lebih lengkap, pengukuran berulang, beberapa klien, serta validasi browser yang mendapat otorisasi dan tetap menjaga batas akses.

KESIMPULAN

Studi pada 16 PTN/PTS menghasilkan 12 homepage eligible untuk analisis header dan 15 handshake utama yang berhasil, seluruhnya menegosiasikan TLS 1.3. Kesesuaian header belum merata: HSTS memenuhi profil pada 8/12 homepage, nosniff pada 7/12, pembatasan framing pada 5/12, serta Referrer-Policy pada 1/12. Lima CSP aktif yang teramati memberikan kontrol parsial, tetapi tidak memenuhi profil sumber daya terpilih. Satu kasus sertifikat diklasifikasikan ambigu setelah hasil klien independen berbeda dengan klien utama.

Hasil menjawab kebutuhan pemetaan konfigurasi pada sampel terbatas dan menunjukkan pentingnya memisahkan transportasi, keberadaan header, dan kualitas kebijakan. Rekomendasi berpusat pada kepemilikan konfigurasi, peninjauan kebijakan sesuai kebutuhan aplikasi, penerapan bertahap, serta pemantauan yang dapat diulang. Kesimpulan tidak berlaku sebagai prevalensi seluruh LLDIKTI IV, peringkat keamanan kampus, atau bukti kerentanan yang dapat dieksploitasi.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih yang sebesar-besarnya kepada Program Studi Informatika, Fakultas Teknik, Institut Teknologi dan Kesehatan Mahardika Cirebon atas penyediaan fasilitas komputasi jaringan dan dukungan kelembagaan selama pelaksanaan penelitian ini.

KONTRIBUSI PENULIS

Mohamad Firdaus: Conceptualization, Methodology, Investigation, Data Curation, Formal Analysis, Visualization, Writing – Original Draft, serta Writing – Review and Editing. Penulis telah memeriksa dan menyetujui versi akhir naskah.

PERNYATAAN KETERSEDIAAN DATA

Data mentah respons dan TLS, daftar sampel beserta sumber domain, hasil klasifikasi, keputusan validasi, kamus variabel, serta skrip pengumpulan dan analisis disertakan dalam paket pendukung naskah. Dataset utama dan pilot dipisahkan. Paket artefak lengkap yang mencakup berkas sample16.csv, rekaman mentah jabat tangan TLS dan pasangan header HTTP, matriks klasifikasi, serta skrip analisis Python tersedia dari penulis atas permintaan yang wajar guna mendukung auditabilitas dan replikasi ilmiah.

PERNYATAAN BEBAS KONFLIK KEPENTINGAN

Para penulis menyatakan bahwa tidak terdapat konflik kepentingan finansial maupun hubungan pribadi yang dapat memengaruhi hasil penelitian yang dilaporkan dalam naskah ini.

PERNYATAAN ETIKA PENELITIAN DAN PUBLIKASI

Pengumpulan dibatasi pada konfigurasi layanan dan respons homepage yang dapat diakses publik, tanpa autentikasi, eksploitasi, ataupun pengujian aplikasi internal. Respons blokir tidak dilewati. Tidak ada nomor persetujuan etik yang diklaim dalam naskah ini. Para penulis bertanggung jawab memastikan kepatuhan terhadap kebijakan institusi dan prinsip etika penelitian serta publikasi, termasuk kejujuran pelaporan dan penggunaan sumber.

PERNYATAAN PEMANFAATAN TEKNOLOGI ASISTIF

AI generatif digunakan untuk membantu perancangan skrip pengumpulan dan analisis, penyusunan serta penyuntingan draf, dan penataan visual. Angka hasil berasal dari observasi yang disimpan dalam data mentah dan analisis yang dijalankan, bukan angka hasil generasi. Penulis bertanggung jawab melakukan penelaahan akhir terhadap metode, sumber, interpretasi, dan naskah sebelum pengajuan.

REFERENSI

Cheng, E. C. K., dan Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Information, 13(4), 192. https://doi.org/10.3390/info13040192

Eshetu, A. Y., Mohammed, E. A., dan Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. Journal of Big Data, 11(1), Artikel 118. https://doi.org/10.1186/s40537-024-00980-z

Fielding, R., Nottingham, M., dan Reschke, J. (2022). HTTP semantics (RFC 9110). RFC Editor. https://www.rfc-editor.org/rfc/rfc9110.html

Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., dan Nazeer, J. (2023). Cybersecurity in Universities: An Evaluation Model. SN Computer Science, 4(5), Artikel 569. https://doi.org/10.1007/s42979-023-01984-x

Hodges, J., Jackson, C., dan Barth, A. (2012). HTTP Strict Transport Security (HSTS) (RFC 6797). RFC Editor. https://www.rfc-editor.org/rfc/rfc6797

Kementerian Pendidikan Tinggi, Sains, dan Teknologi. (n.d.). Pangkalan Data Pendidikan Tinggi: Detail perguruan tinggi. https://pddikti.kemdiktisaintek.go.id/perguruan-tinggi

Lembaga Layanan Pendidikan Tinggi Wilayah IV. (2023). LLDIKTI Wilayah IV kembali selenggarakan rapat koordinasi dan anugerah LLDIKTI4. https://lldikti4.kemdiktisaintek.go.id/2023/02/lldikti-wilayah-iv-kembali-selenggarakan-rapat-koordinasi-dan-anugerah-lldikti4/

Lembaga Layanan Pendidikan Tinggi Wilayah IV. (n.d.). Direktori perguruan tinggi. https://direktori.lldikti4.id/perguruantinggi/

Macakoğlu, Ş. S., Peker, S., dan Medeni, İ. T. (2023). Accessibility, usability, and security evaluation of universities' prospective student web pages: a comparative study of Europe, North America, and Oceania. Universal Access in the Information Society, 22(2), 671-683. https://doi.org/10.1007/s10209-022-00869-9

Mileva, A., Bikov, D., Tasheva, B., dan Brashnarova, A. (2025). HTTP Security Headers Analysis of Several Macedonian Website Categories. Computer Science Journal of Moldova, 33(1(97)), 3-29. https://doi.org/10.56415/csjm.v33.01

Moriarty, K., dan Farrell, S. (2021). Deprecating TLS 1.0 and TLS 1.1 (RFC 8996). RFC Editor. https://www.rfc-editor.org/rfc/rfc8996.html

Rescorla, E. (2018). The Transport Layer Security (TLS) protocol version 1.3 (RFC 8446). RFC Editor. https://www.rfc-editor.org/rfc/rfc8446

Ross, D., dan Gondrom, T. (2013). HTTP header field X-Frame-Options (RFC 7034). RFC Editor. https://www.rfc-editor.org/rfc/rfc7034

Safaei Pour, M., Nader, C., Friday, K., dan Bou-Harb, E. (2023). A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security. Computers & Security, 128, 103123. https://doi.org/10.1016/j.cose.2023.103123

Saint-Andre, P., dan Salz, R. (2023). Service identity in TLS (RFC 9525). RFC Editor. https://www.rfc-editor.org/rfc/rfc9525.html

Saputra, D. W., Pradini, R. S., dan Anshori, M. (2025). Analisis dan Rekomendasi Keamanan Website Kampus X Menggunakan ISSAF. Jurnal Indonesia : Manajemen Informatika dan Komunikasi, 6(1), 830-843. https://doi.org/10.35870/jimik.v6i1.1306

Sheffer, Y., Saint-Andre, P., dan Fossati, T. (2022). Recommendations for secure use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) (RFC 9325). RFC Editor. https://www.rfc-editor.org/rfc/rfc9325

Ulven, J. B., dan Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 13(2), 39. https://doi.org/10.3390/fi13020039

Web Hypertext Application Technology Working Group. (2025). Fetch standard (snapshot commit 4775fcb, 29 September 2025). https://github.com/whatwg/fetch/blob/4775fcb48042c8411df497c0b7cf167b4240004f/fetch.bs

World Wide Web Consortium. (2017). Referrer Policy (Candidate Recommendation, 26 January 2017). https://www.w3.org/TR/2017/CR-referrer-policy-20170126/

World Wide Web Consortium. (2021). Content Security Policy Level 3 (Working Draft, 29 June 2021). https://www.w3.org/TR/2021/WD-CSP3-20210629/

World Wide Web Consortium. (2025). Permissions Policy (Editor's Draft, snapshot commit 20ab675, 18 July 2025). https://github.com/w3c/webappsec-permissions-policy/blob/20ab675cf4dcab2c198c2cf4c2584e0483dfc204/index.bs