Nama : Rifko Satrio Rahmadani
Email : ikosatriorahmadani@gmail.com
Pekerjaan : Mahasiswa
Nama Instansi/Sekolah : Politeknik Negeri Bandung

Final Assignment

I. PENDAHULUAN

Pada final assignment ini saya memilih untuk menganalisa kerentanan pada website akademik.polban.ac.id, yaitu portal akademik utama yang dipakai oleh seluruh mahasiswa Politeknik Negeri Bandung. Hampir semua urusan akademik ada di sini, mulai dari cek status pembayaran UKT, melihat absensi, mengisi kuesioner, membuka KRS, sampai mengunduh berbagai dokumen akademik. Karena setiap hari kami mengakses website ini, fungsinya memang cukup penting untuk menunjang kegiatan perkuliahan.

Saya mengambil topik ini supaya bisa tahu apa saja yang mungkin berisiko di dalam website tersebut. Tujuannya bukan untuk mencari celah yang berbahaya, tapi lebih ke melihat sisi mana yang perlu diperhatikan dan diperbaiki sejak awal, supaya tidak ada potensi disalahgunakan oleh orang yang tidak bertanggung jawab. Dengan begitu, keamanan dan kenyamanan pengguna baik mahasiswa maupun dosen bisa tetap terjaga

II. METODOLOGI

Analisa dilakukan secara pasif menggunakan beberapa tools yang hanya membaca informasi yang sudah disediakan oleh server, tanpa melakukan aktivitas yang mengganggu sistem. Tools yang digunakan:

1. Browser Certificate Viewer (Brave)
   Untuk melihat detail sertifikat SSL, CA, masa berlaku, dan algoritma keamanan.
2. SecurityHeaders.com
   Untuk memeriksa konfigurasi header keamanan yang dikirim server, seperti CSP, X-Frame-Options, HSTS, dan lainnya.
3. SSL Labs – SSL Server Test
   Untuk mengetahui kekuatan konfigurasi TLS, cipher suite, dan rating keamanan SSL.

4. Chrome DevTools → Application → Cookies

   Untuk melihat pengaturan cookie seperti Secure dan HttpOnly.

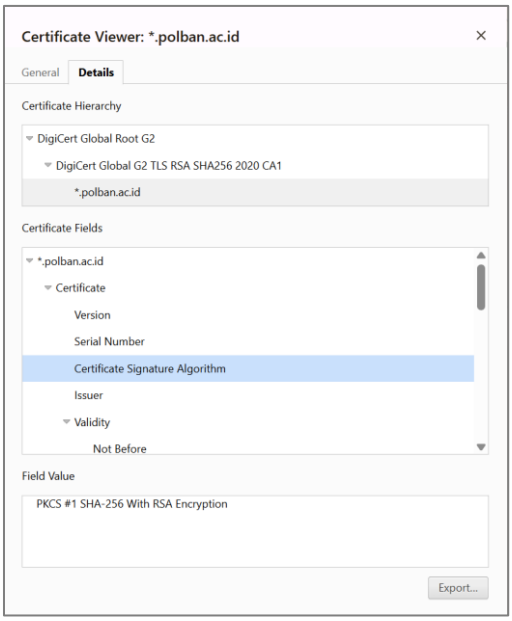
5. Observasi Halaman Login

   Untuk mengevaluasi aspek keamanan dasar seperti penggunaan HTTPS, absennya CAPTCHA, dan alur login secara umum.

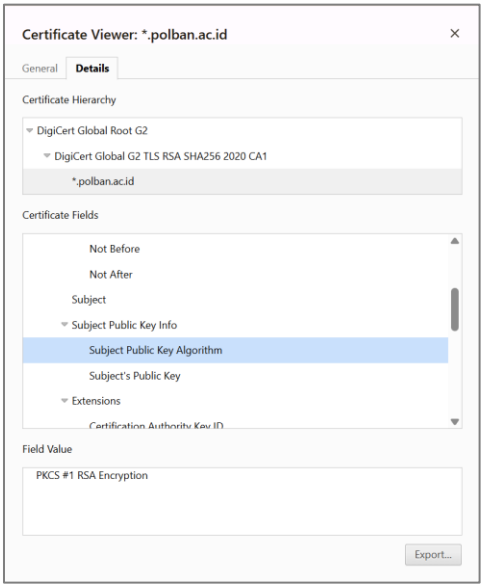
III. HASIL ANALISA

1. Analisa Sertifikat SSL/TLS

Dari halaman General, sertifikat *.polban.ac.id terlihat valid, dikeluarkan untuk Politeknik Negeri Bandung oleh DigiCert, yang memang CA tepercaya. Masa berlakunya masih aktif (2025–2026), jadi situsnya aman dipakai dan tidak ada risiko “sertifikat kadaluarsa”. Fingerprint SHA-256 juga muncul normal, artinya sertifikatnya asli dan tidak ada indikasi man-in-the-middle.

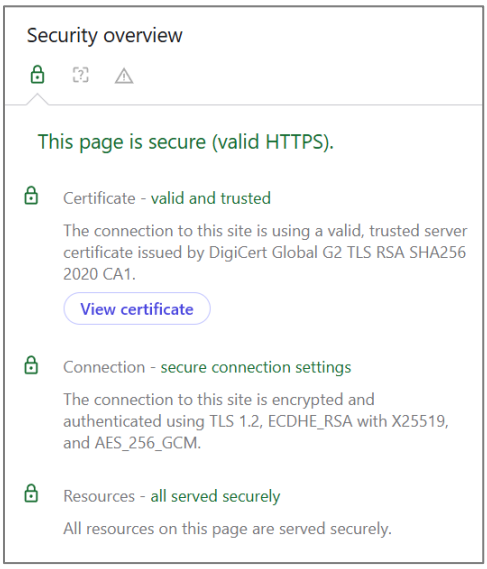


Di bagian ini tertulis “SHA-256 with RSA Encryption”. Intinya, sertifikat web Polban ditandatangani pakai kombinasi RSA dan SHA-256, yang memang standar umum buat website sekarang. Algoritma ini masih aman dan susah dipalsukan, jadi dari sisi tanda tangan digitalnya sudah oke dan nggak ada masalah berarti.



Di bagian *Public Key Algorithm*, tertulis PKCS #1 RSA Encryption. Intinya, website akademik pakai RSA buat kunci publiknya. RSA ini standar umum buat ngamanin komunikasi antara browser dan server. Selama ukuran kuncinya besar, ini masih aman dipakai. Jadi pas kita

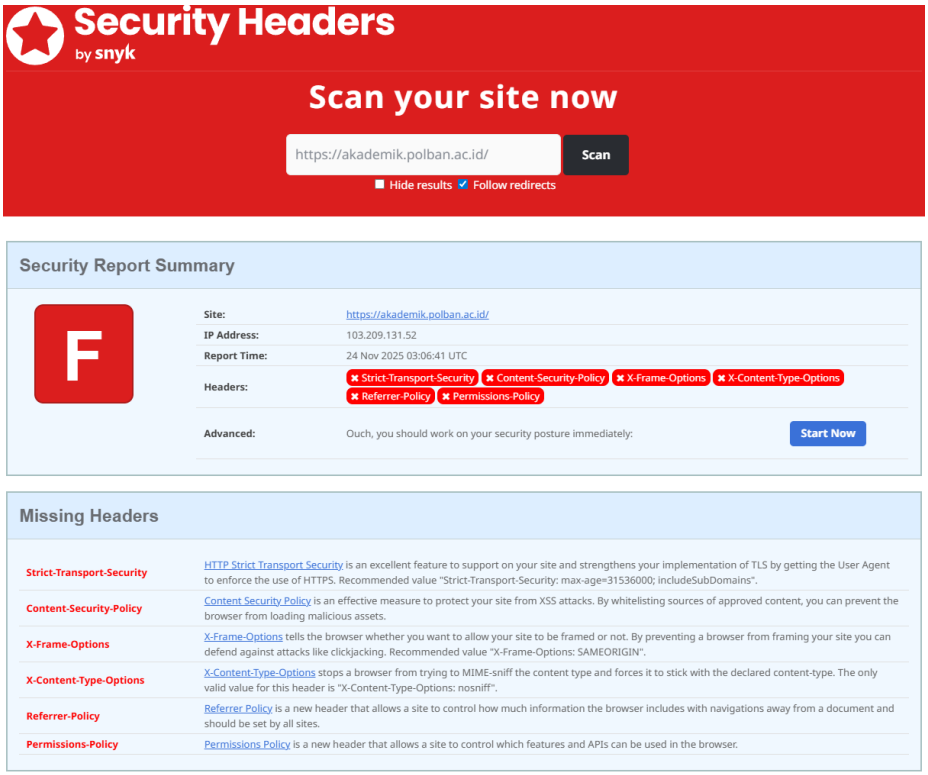
akses website, data awal yang dikirim bakal dienkripsi dulu pakai kunci publik RSA, biar nggak bisa disadap orang.



Berdasarkan informasi pada DevTools, website *polban.ac.id* menggunakan koneksi yang terenkripsi dengan TLS 1.2, ditambah mekanisme ECDHE_RSA dengan X25519 dan cipher AES-256-GCM. Kombinasi ini termasuk standar keamanan yang kuat dan masih banyak digunakan pada layanan besar.

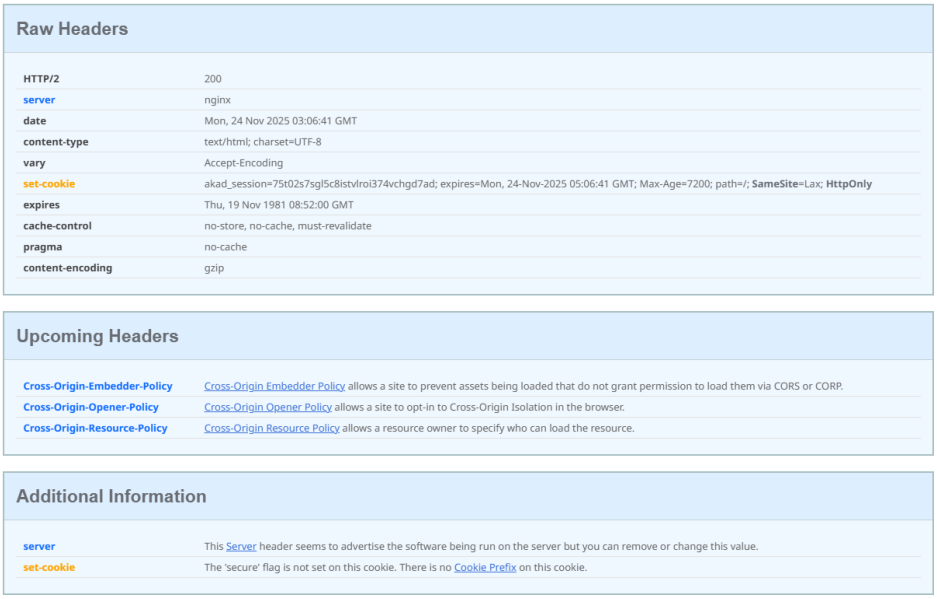
Penggunaan ECDHE menunjukkan bahwa website mendukung Perfect Forward Secrecy, sehingga session key tidak bisa dibuka meskipun suatu saat private key server bocor. Cipher AES-256-GCM juga memberikan proteksi yang baik terhadap manipulasi data. Secara keseluruhan, konfigurasi TLS yang digunakan sudah aman dan tidak ada indikator kelemahan pada sisi enkripsi koneksi.

2. Analisa Security Headers



Berdasarkan hasil pengecekan di SecurityHeaders.io, website akademik.polban.ac.id mendapatkan nilai F. Artinya, beberapa header keamanan penting belum diterapkan. Dari laporan terlihat bahwa header seperti Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, dan Permissions-Policy masih belum ada.

Ketiadaan header-header ini bisa membuka peluang risiko keamanan, misalnya: konten bisa di-frame oleh website lain (rawan clickjacking), browser bisa salah membaca tipe file, hingga minimnya kontrol terkait referer dan izin fitur browser. Walaupun situs sudah berjalan di HTTPS dan servernya responsif, dari sisi konfigurasi header masih perlu ditingkatkan supaya lebih aman dan sesuai standar praktik keamanan web.



Raw Headers

HTTP/2	200
server	nginx
date	Mon, 24 Nov 2025 03:06:41 GMT
content-type	text/html; charset=UTF-8
vary	Accept-Encoding
set-cookie	akad_session=75t02s7sgl5c8istvlroi374vchgd7ad; expires=Mon, 24-Nov-2025 05:06:41 GMT; Max-Age=7200; path=/; **SameSite**=Lax; **HttpOnly**
expires	Thu, 19 Nov 1981 08:52:00 GMT
cache-control	no-store, no-cache, must-revalidate
pragma	no-cache
content-encoding	gzip

Upcoming Headers

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Additional Information

server	This Server header seems to advertise the software being run on the server but you can remove or change this value.
set-cookie	The 'secure' flag is not set on this cookie. There is no Cookie Prefix on this cookie.

Dari hasil *Raw Headers*, server akademik.polban.ac.id pakai nginx dan sudah jalan di HTTP/2. Secara performa oke, tapi dari sisi keamanan masih ada beberapa kekurangan yang cukup penting.

Cookie sesi ada HttpOnly dan SameSite=Lax, tapi flag Secure belum ada, jadi cookie berisiko bocor kalau ada request non-HTTPS.

Lalu, header perlindungan MIME-sniffing seperti X-Content-Type-Options: nosniff tidak muncul, jadi browser bisa saja salah menafsirkan tipe konten, ini bisa jadi celah kalau ada file berbahaya yang tersisip.

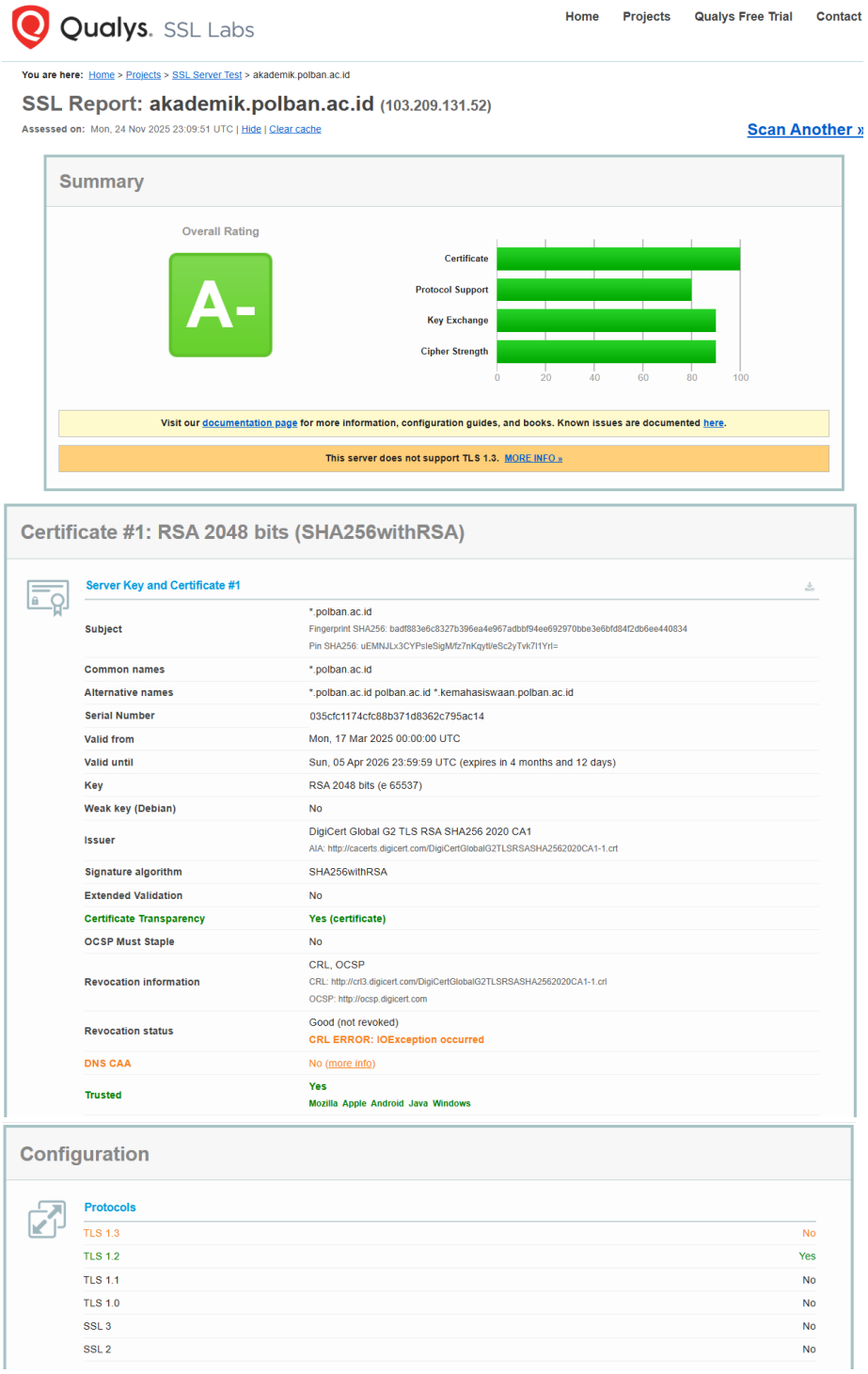
Header *cross-origin* seperti COEP, COOP, dan CORP juga belum dipasang. Memang sifatnya tambahan, tapi sekarang cukup penting untuk mencegah data dari domain dieksekusi sembarangan.

Terakhir, header server menampilkan langsung “nginx”. Info ini kelihatan sepele, tapi sebenarnya bisa dimanfaatkan attacker untuk menyesuaikan jenis serangannya.

3. SSL Labs – SSL Server Test

   Berdasarkan hasil uji di SSL Labs, domain akademik.polban.ac.id mendapatkan nilai A–, yang menunjukkan konfigurasi SSL-nya sudah cukup baik. Sertifikatnya valid, diterbitkan oleh DigiCert, dan memakai RSA 2048 bit dengan SHA256. Untuk protokol, server hanya mendukung TLS 1.2, sedangkan TLS 1.3 belum aktif. Selain itu, masih terlihat beberapa cipher yang dikategorikan “weak”. Secara umum sudah aman dipakai, tapi akan lebih bagus jika TLS 1.3 diaktifkan dan

cipher lemah dinonaktifkan untuk meningkatkan keamanan ke depannya.



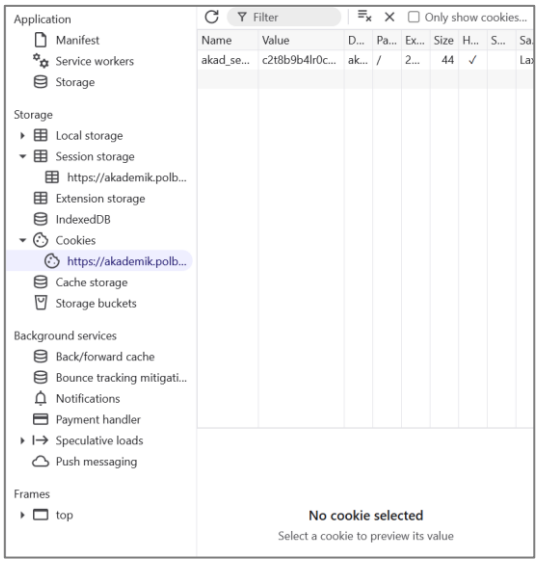
Cipher Suites

# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1) **WEAK**	256
TLS_RSA_WITH_AES_256_CCM (0xc09d) **WEAK**	256
TLS_RSA_WITH_ARIA_256_GCM_SHA384 (0xc051) **WEAK**	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0) **WEAK**	128
TLS_RSA_WITH_AES_128_CCM (0xc09c) **WEAK**	128
TLS_RSA_WITH_ARIA_128_GCM_SHA256 (0xc050) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc027
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No

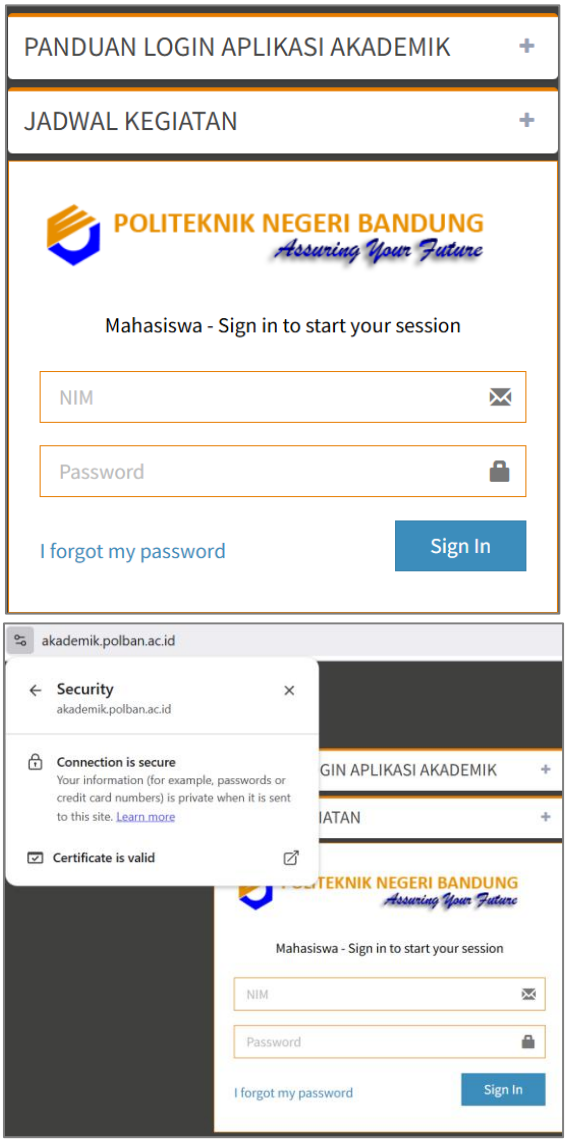
4. Chrome DevTools → Application → Cookies



Dari hasil pengecekan di Chrome DevTools, situs akademik.polban.ac.id ternyata menyimpan satu buah cookie bernama akad_session. Cookie ini berfungsi sebagai session ID untuk menandai pengguna yang sedang login. Beberapa atributnya sudah cukup aman, misalnya HttpOnly, jadi isi cookie tidak bisa dibaca lewat JavaScript. Namun ada juga catatan penting, yaitu cookie ini belum memiliki atribut Secure, sehingga cookie tetap bisa terkirim melalui HTTP biasa kalau terjadi downgraded connection. Idealnya, cookie session sebaiknya memakai Secure dan SameSite=Strict supaya resiko pencurian session lebih kecil.

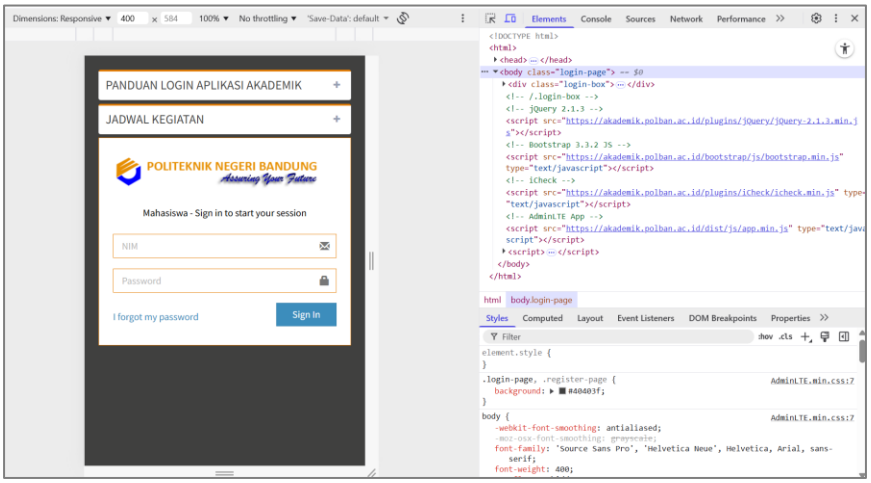
5. Observasi Halaman Login
   - Tampilan Halaman Login

     Pada tahap ini, saya mengakses halaman login akademik POLBAN di https://akademik.polban.ac.id. Halaman login menampilkan dua input utama, yaitu NIM dan Password, serta tombol Sign In and I forget my password.



Halaman sudah berjalan di protokol HTTPS, ditunjukkan oleh ikon gembok pada browser. Artinya proses pengiriman data login sudah terenkripsi dan lebih aman.

- Pemeriksaan Elemen Form Login



Pada halaman login akademik.polban.ac.id, saya mengecek struktur form menggunakan Chrome DevTools. Input untuk password sudah menggunakan tipe password, jadi karakter yang diketik tidak tampil secara langsung. Dari sisi HTML juga tidak ditemukan informasi sensitif yang bocor di bagian front-end. Tampilan login sederhana dan hanya berisi form NIM serta password, tanpa mekanisme tambahan seperti CAPTCHA atau limitasi percobaan login. Secara umum halaman login sudah aman untuk penggunaan dasar, tetapi fitur keamanan tambahan mungkin bisa ditambahkan untuk memperkuat perlindungan terhadap serangan brute-force.

IV. TEMUAN KERENTANAN

1. Website belum menerapkan beberapa security header penting seperti HSTS, CSP, X-Frame-Options, dan Referrer-Policy (hasil Security Headers: grade F).
2. TLS sudah aman, tetapi masih terbatas di TLS 1.2 dan belum mendukung TLS 1.3.
3. Beberapa cipher suite masih dikategorikan “WEAK”.
4. Tidak ada mekanisme tambahan di halaman login (misalnya: CAPTCHA atau limit brute-force).
5. Cookie sesi sudah memakai HttpOnly, tapi belum pakai Secure flag karena login masih dilakukan lewat HTTP/1.1 di beberapa request tertentu.

V. REKOMENDASI PERBAIKAN

1. Menambahkan security header seperti HSTS, X-Content-Type-Options, CSP, dan Permissions-Policy.
2. Mengaktifkan dukungan TLS 1.3 dan menonaktifkan cipher suite yang ditandai “WEAK”.
3. Menambah proteksi brute-force seperti CAPTCHA atau delay setelah gagal login berkali-kali.

4. Mengaktifkan Secure flag pada cookie agar cookie hanya dikirim lewat koneksi HTTPS.
5. Menghindari pemanggilan resource HTTP/1.1 dan memastikan seluruh request berjalan melalui HTTPS.

VI. KESIMPULAN

Dari hasil analisa, website akademik POLBAN sudah memakai sertifikat valid dan TLS yang cukup aman. Namun, masih ada beberapa kekurangan terutama pada security headers dan konfigurasi cipher suite. Hal ini tidak berbahaya untuk penggunaan normal, tetapi tetap perlu diperbaiki untuk mengurangi risiko serangan tertentu. Dengan menerapkan rekomendasi di atas, keamanan website bisa meningkat dan lebih siap menghadapi potensi ancaman.