Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

EVALUASI KEAMANAN DASAR WEBSITE UNIVERSITAS UDAYANA MENGGUNAKAN SSL LABS DAN SECURITYHEADERS.COM

Kadek Aryana Dwi Putra[1], Ni Made Ayu Martiani[2]

[1]Program Studi Perpustakaan dan Sains Informasi, Universitas Udayana
[2]Program Studi Magister Ilmu Manajemen, Universitas Pendidikan Ganesha

[1]Jl. Raya Kampus Unud, Jimbaran, Kuta Selatan, Kabupaten Badung, Bali
[2]Jl. Udayana No. 11, Singaraja, Kec. Buleleng, Kabupaten Buleleng, Bali

[1] aryanadwiputra@unud.ac.id
[2] ayu.martiani@student.undiksha.ac.id

Abstract

University websites play an important role as official digital information channels for academic institutions. These websites are used to publish institutional profiles, academic information, public announcements, student services, and other official content. Therefore, basic website security should be evaluated to ensure that communication between users and servers is properly protected. This study aims to evaluate the basic security of the Universitas Udayana website based on Secure Sockets Layer/Transport Layer Security (SSL/TLS) configuration and Hypertext Transfer Protocol security headers. This research applies a descriptive quantitative method using an automated website security audit approach. The object of this study is the official website of Universitas Udayana, accessed through https://www.unud.ac.id/. Data were collected using SSL Labs SSL Server Test and SecurityHeaders.com. The analyzed indicators include certificate validity, protocol support, cipher strength, vulnerability status, Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy. The results show that the Universitas Udayana website obtained grade B from SSL Labs. The website already uses a valid certificate, supports TLS 1.2 and TLS 1.3, and does not support SSL 2 or SSL 3. However, TLS 1.0 and TLS 1.1 are still enabled, causing the grade to be capped at B. Meanwhile, SecurityHeaders.com gave the website grade C. The website has implemented X-Frame-Options, X-Content-Type-Options, and Referrer-Policy, but has not implemented Strict-Transport-Security, Content-Security-Policy, and Permissions-Policy. Overall, the basic security of the Universitas Udayana website is considered adequate but still requires improvement, particularly in disabling outdated TLS protocols and strengthening browser-side security headers.

Keywords: *website security, SSL/TLS, security headers, SSL Labs, university website*

Abstrak

Website perguruan tinggi berperan penting sebagai media informasi resmi sehingga aspek keamanan perlu diperhatikan untuk melindungi komunikasi antara pengguna dan server. Penelitian ini bertujuan mengevaluasi keamanan dasar website Universitas Udayana berdasarkan konfigurasi SSL/TLS dan HTTP *Security Headers*. Metode yang digunakan adalah deskriptif kuantitatif dengan pendekatan audit keamanan menggunakan SSL Labs dan SecurityHeaders.com. Objek penelitian adalah *website* resmi Universitas Udayana (https://www.unud.ac.id/). Hasil pengujian menunjukkan bahwa *website* memperoleh grade B dari SSL Labs. *Website* telah menggunakan sertifikat yang *valid*, mendukung TLS 1.2 dan TLS 1.3, serta tidak mendukung SSL 2 dan SSL 3. Namun, TLS 1.0 dan TLS 1.1 masih aktif sehingga membatasi nilai keamanan yang diperoleh. Sementara itu, SecurityHeaders.com memberikan grade C. Website telah menerapkan *X-Frame-Options, X-Content-Type-Options,* dan *Referrer-Policy*, tetapi belum

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

menerapkan *Strict-Transport-Security, Content-Security-Policy,* dan *Permissions-Policy*. Secara umum, keamanan dasar *website* Universitas Udayana tergolong cukup baik, namun masih memerlukan perbaikan melalui penonaktifan protokol TLS lama dan penguatan *security headers* untuk meningkatkan perlindungan terhadap berbagai risiko keamanan web.

Kata kunci: *Keamanan Website, SSL/TLS, Security Headers, SSL Labs, Website Universitas*

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong perguruan tinggi untuk memanfaatkan website sebagai media utama dalam menyampaikan informasi resmi kepada masyarakat. Website perguruan tinggi tidak hanya digunakan sebagai sarana publikasi profil institusi, tetapi juga menjadi pusat informasi akademik, pengumuman kegiatan, penerimaan mahasiswa baru, publikasi berita, layanan administrasi, serta komunikasi antara institusi dengan publik. Dengan fungsi tersebut, website universitas memiliki posisi strategis dalam mendukung transformasi digital pendidikan tinggi.

Universitas Udayana sebagai salah satu perguruan tinggi negeri di Indonesia memiliki *website* resmi yang dapat diakses melalui alamat https://www.unud.ac.id/. *Website* tersebut menjadi salah satu pintu utama bagi mahasiswa, dosen, calon mahasiswa, alumni, mitra, dan masyarakat umum untuk memperoleh informasi kelembagaan. Semakin pentingnya fungsi *website* sebagai media resmi membuat aspek keamanan menjadi hal yang perlu diperhatikan. Risiko keamanan pada website perguruan tinggi tidak hanya berdampak pada gangguan layanan informasi, tetapi juga berpotensi menimbulkan kebocoran data, penyalahgunaan identitas institusi, penyisipan konten berbahaya, hingga serangan *phishing* yang memanfaatkan domain resmi universitas. Selain itu, kelemahan konfigurasi keamanan dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan manipulasi informasi, *defacement website*, maupun penyadapan komunikasi antara pengguna dan *server*. Apabila keamanan dasar *website* tidak dikonfigurasi dengan baik dampaknya dapat menurunkan kepercayaan sivitas akademika dan masyarakat terhadap kredibilitas institusi serta mengganggu penyelenggaraan layanan digital perguruan tinggi [1], [2], [3].

Keamanan *website* mencakup berbagai aspek, mulai dari keamanan aplikasi, keamanan *server*, keamanan jaringan, keamanan basis data, hingga keamanan komunikasi antara pengguna dan *server*. Salah satu aspek dasar yang penting adalah penerapan SSL/TLS. SSL/TLS berfungsi untuk mengenkripsi komunikasi antara *browser* pengguna dan *server* sehingga data yang dikirimkan tidak mudah dibaca atau dimodifikasi oleh pihak yang tidak berwenang [4], [5].

Selain SSL/TLS, keamanan dasar *website* juga dapat diperkuat melalui penerapan HTTP *Security Headers*. *Security headers* adalah instruksi keamanan yang dikirimkan oleh *server* kepada *browser* melalui respons HTTP. Instruksi tersebut digunakan untuk mengatur perilaku keamanan pada sisi *browser*, seperti memaksa penggunaan HTTPS, mencegah *clickjacking*, membatasi sumber konten, mencegah *MIME-sniffing*, mengatur informasi *referrer*, serta membatasi akses terhadap fitur *browser* tertentu [6], [7].

Beberapa HTTP *Security Headers* yang umum digunakan antara lain Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, dan Permissions-Policy. Header Strict-Transport-Security berfungsi untuk memaksa *browser* menggunakan HTTPS. Content-Security-Policy digunakan untuk mengendalikan sumber konten yang boleh dimuat oleh *browser*. X-Frame-Options membantu melindungi halaman dari risiko *clickjacking*. X-Content-Type-Options mencegah *browser* melakukan *MIME-sniffing*. Referrer-Policy mengatur jumlah informasi *referrer* yang dikirimkan saat pengguna berpindah halaman. Permissions-Policy digunakan untuk membatasi akses terhadap fitur *browser* seperti kamera, mikrofon, lokasi, dan sensor [8], [9].

Dalam penelitian ini, evaluasi dilakukan menggunakan dua *tools*, yaitu SSL Labs SSL Server Test dan SecurityHeaders.com. SSL Labs digunakan untuk mengevaluasi konfigurasi SSL/TLS, sedangkan SecurityHeaders.com digunakan untuk mengevaluasi penerapan HTTP *Security Headers*. Penggunaan dua *tools* ini diharapkan dapat memberikan gambaran keamanan dasar *website* Universitas Udayana dari

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

dua sisi utama, yaitu keamanan komunikasi terenkripsi dan keamanan pada sisi *browser*.

Sejumlah penelitian terdahulu telah mengevaluasi keamanan *website* perguruan tinggi di berbagai negara. Alhassan et al. [10] mengevaluasi keamanan *website* universitas federal di Nigeria, sedangkan Sinha dan Karmakar [11] mengevaluasi konfigurasi SSL/TLS dan *security headers* institusi pendidikan di India. Penelitian serupa juga telah dilakukan oleh Chandra et al. [12]terhadap *website* perguruan tinggi di Indonesia menggunakan metode OWASP. Namun, penelitian-penelitian tersebut belum mencakup evaluasi khusus terhadap *website* Universitas Udayana, dan belum ada yang menggabungkan evaluasi SSL/TLS dengan HTTP *Security Headers* secara bersamaan menggunakan SSL Labs dan SecurityHeaders.com pada institusi perguruan tinggi negeri di Bali. Kesenjangan inilah yang menjadi dasar dilakukannya penelitian ini.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengevaluasi keamanan dasar *website* Universitas Udayana, mengidentifikasi kelemahan konfigurasi keamanan yang ditemukan, serta memberikan rekomendasi perbaikan yang dapat digunakan sebagai masukan bagi pengelola *website*. Dengan demikian, hasil penelitian ini diharapkan dapat mendukung peningkatan kualitas keamanan layanan informasi digital perguruan tinggi.

2. TINJAUAN PUSTAKA

Keamanan *website* merupakan bagian penting dalam pengelolaan sistem informasi modern. Menurut OWASP, aplikasi *web* memiliki berbagai potensi risiko keamanan, seperti *broken access control*, kesalahan konfigurasi keamanan, kerentanan injeksi, dan kegagalan identifikasi maupun autentikasi [12].

TLS merupakan protokol keamanan yang digunakan untuk menyediakan kerahasiaan, integritas, dan autentikasi dalam komunikasi jaringan [1]. TLS 1.2 dan TLS 1.3 merupakan protokol yang masih banyak digunakan dalam komunikasi *web* modern. TLS 1.3 dirancang untuk meningkatkan keamanan sekaligus menyederhanakan proses *handshake* dibandingkan versi sebelumnya[4]. Sebaliknya, TLS 1.0 dan TLS 1.1 telah dinyatakan tidak lagi direkomendasikan untuk penggunaan modern karena memiliki kelemahan dan tidak mendukung standar keamanan terbaru [13]. Penelitian terbaru menunjukkan bahwa TLS 1.3 tidak hanya meningkatkan keamanan komunikasi melalui penyederhanaan proses handshake, tetapi juga memberikan efisiensi yang lebih baik dibandingkan versi sebelumnya [14].

Penerapan TLS yang baik tidak hanya bergantung pada versi protokol, tetapi juga pada konfigurasi cipher suite yang digunakan. Cipher suite menentukan kombinasi algoritma enkripsi, pertukaran kunci, dan integritas pesan yang digunakan dalam sesi TLS. Penggunaan cipher suite yang lemah atau usang dapat membuka celah bagi serangan seperti POODLE, BEAST, dan ROBOT meskipun versi protokol yang digunakan sudah tergolong aman [15]. Oleh karena itu, pemilihan cipher suite yang tepat menjadi bagian penting dalam evaluasi konfigurasi SSL/TLS secara menyeluruh.

Sertifikat digital juga menjadi komponen penting dalam SSL/TLS. Sertifikat digunakan untuk membuktikan identitas *server* dan memungkinkan *browser* memverifikasi bahwa koneksi yang dilakukan benar-benar menuju domain yang sah [15]. Sertifikat yang valid, dipercaya oleh *browser*, dan belum kedaluwarsa merupakan salah satu indikator bahwa koneksi HTTPS dapat digunakan dengan baik. Sertifikat yang dikeluarkan oleh Certificate Authority (CA) terpercaya memastikan bahwa identitas server dapat diverifikasi oleh browser pengguna. Kekuatan kunci sertifikat, algoritma tanda tangan, serta periode validitasnya merupakan aspek yang turut dinilai dalam evaluasi keamanan SSL/TLS [15].

Header Strict-Transport-Security atau HSTS memberi instruksi kepada *browser* agar selalu menggunakan koneksi HTTPS selama jangka waktu tertentu [8]. Content-Security-Policy atau CSP merupakan header yang digunakan untuk membatasi sumber daya yang dapat dimuat oleh *browser* [7]. X-Frame-Options merupakan header yang digunakan untuk mencegah halaman *website* dimuat di dalam *frame* oleh situs lain, sehingga mengurangi risiko *clickjacking* [6], [16].

Referrer-Policy digunakan untuk mengatur informasi *referrer* yang dikirimkan oleh *browser* ketika pengguna berpindah dari satu halaman ke halaman lain [9]. Permissions-Policy digunakan untuk membatasi akses *website* terhadap fitur tertentu pada *browser*, seperti kamera, mikrofon, lokasi, *fullscreen*, dan sensor perangkat. Penerapan Permissions-Policy yang tepat membantu mencegah penyalahgunaan fitur perangkat oleh skrip pihak ketiga yang mungkin termuat di dalam halaman website. Kombinasi

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

penerapan seluruh security headers tersebut secara bersama-sama akan membentuk lapisan perlindungan yang komprehensif pada sisi browser, sehingga memperkuat postur keamanan website secara keseluruhan [6], [8], [9].

Penelitian terkini menunjukkan bahwa penerapan *Content-Security-Policy* (CSP), HSTS, dan *Permissions-Policy* menjadi komponen penting dalam strategi pertahanan berlapis *(defense in depth)* pada aplikasi web modern. Ketiga mekanisme tersebut mampu mengurangi risiko eksploitasi berbasis *browser*, termasuk *cross-site scripting, clickjacking,* dan penyalahgunaan fitur perangkat oleh skrip pihak ketiga[17] .

SSL Labs SSL Server Test merupakan *tools* yang dapat menilai konfigurasi SSL/TLS, termasuk validitas sertifikat, dukungan protokol, kekuatan *cipher*, *forward secrecy*, serta potensi kerentanan [10]. SecurityHeaders.com merupakan *tools* yang digunakan untuk memeriksa keberadaan HTTP *Security Headers* dan memberikan grade berdasarkan konfigurasi yang ditemukan [11].

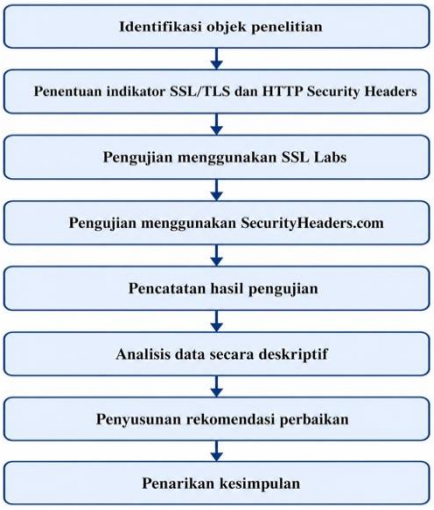
Beberapa penelitian terdahulu telah mengkaji keamanan *website* perguruan tinggi dari berbagai sudut pandang. Alhassan et al. [10] berfokus pada evaluasi keamanan SSL/TLS *website* universitas federal di Nigeria, namun tidak mencakup aspek HTTP *Security Headers*. Sinha dan Karmakar [11] mengevaluasi kedua aspek tersebut pada institusi pendidikan di India, tetapi tidak mencakup konteks perguruan tinggi di Indonesia. Chandra et al. [12] melakukan evaluasi keamanan *website* perguruan tinggi di Indonesia dengan pendekatan OWASP, namun tidak menggunakan pendekatan berbasis SSL Labs dan SecurityHeaders.com yang memungkinkan penilaian otomatis dan terstandar. Dengan demikian, terdapat kesenjangan penelitian berupa belum adanya evaluasi keamanan dasar *website* Universitas Udayana yang mengintegrasikan evaluasi SSL/TLS dan HTTP *Security Headers* secara bersamaan menggunakan kombinasi SSL Labs dan SecurityHeaders.com [1], [18].

3. METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Penelitian ini menggunakan metode deskriptif kuantitatif dengan pendekatan audit keamanan *website* berbasis *tools* otomatis. Metode deskriptif digunakan untuk menggambarkan kondisi keamanan dasar *website* berdasarkan hasil pengujian. Pendekatan kuantitatif digunakan karena hasil pengujian menghasilkan data berupa grade, status, dan indikator teknis yang dapat disajikan dalam bentuk tabel.

Tahapan penelitian disusun untuk menggambarkan urutan pelaksanaan penelitian secara sistematis, dimulai dari identifikasi objek penelitian, penentuan indikator keamanan, pengumpulan data menggunakan tools, pencatatan hasil pengujian, analisis hasil, penyusunan rekomendasi, hingga penarikan kesimpulan. Pendekatan ini dipilih karena setiap tahapan saling berkaitan dan memerlukan urutan yang terstruktur agar hasil evaluasi dapat dipertanggungjawabkan secara ilmiah. Identifikasi objek penelitian dilakukan untuk memastikan bahwa website yang dievaluasi merupakan website resmi yang aktif digunakan sebagai media layanan publik institusi. Penentuan indikator keamanan dilakukan berdasarkan standar dan referensi yang diakui, yaitu SSL Labs Rating Guide (Sinha & Karmakar, 2021) untuk aspek SSL/TLS dan SecurityHeaders.com [6]untuk aspek HTTP Security Headers.



Gambar 1. Tahapan Penelitian

Objek penelitian adalah *website* resmi Universitas Udayana yang diakses melalui alamat https://www.unud.ac.id/. Pemilihan objek dilakukan karena *website* tersebut merupakan media informasi resmi institusi dan digunakan oleh berbagai pihak, seperti mahasiswa, dosen, calon mahasiswa, alumni, mitra, dan masyarakat umum. Universitas Udayana merupakan salah satu perguruan tinggi negeri terbesar di Bali dan kawasan Indonesia Timur, sehingga keamanan website-nya memiliki implikasi yang luas terhadap kepercayaan publik. Pengujian dilakukan secara daring tanpa interaksi langsung terhadap sistem server, sehingga tidak

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

mengganggu operasional website yang sedang berjalan.

3.2 Pengumpulan Data

Data dalam penelitian ini diperoleh melalui observasi non-partisipatif dan dokumentasi hasil pengujian menggunakan *tools* otomatis. Dua *tools* yang digunakan adalah SSL Labs SSL Server Test dan SecurityHeaders.com. SSL Labs digunakan untuk menguji aspek SSL/TLS, sedangkan SecurityHeaders.com digunakan untuk menguji penerapan HTTP *Security Headers*.

SSL Labs SSL Server Test dikembangkan oleh Qualys dan telah digunakan secara luas oleh para peneliti dan praktisi keamanan sebagai standar de facto dalam mengevaluasi konfigurasi SSL/TLS sebuah server. Tools ini bekerja dengan mengirimkan serangkaian permintaan koneksi ke server target dan menganalisis respons yang diterima, mencakup versi protokol yang didukung, cipher suite yang tersedia, validitas sertifikat, serta ketahanan terhadap berbagai kerentanan yang diketahui [19]. SecurityHeaders.com dikembangkan oleh Scott Helme dan berfungsi menganalisis header HTTP yang dikembalikan oleh server ketika menerima permintaan dari browser. Tools ini memberikan grade berdasarkan keberadaan dan konfigurasi security headers yang dianggap penting untuk keamanan sisi browser [6]. Penggunaan kedua tools ini bersifat pasif dan tidak mengubah konfigurasi server yang diuji, sehingga dapat digunakan secara etis tanpa memerlukan izin khusus dari pengelola server.

Tabel 1. Tools Penelitian

No	Tools	Fungsi	Data yang Diperoleh
1	SSL Labs SSL Server Test	Mengevaluasi konfigurasi SSL/TLS	Grade SSL, sertifikat, protokol TLS, cipher, HSTS, kerentanan
2	SecurityHeaders .com	Mengevaluasi HTTP Security Headers	Grade header, header tersedia, header yang hilang

3.3 Analisa Data

Analisis data dilakukan dengan pendekatan deskriptif. Data dari SSL Labs dianalisis berdasarkan overall rating, validitas sertifikat, penerbit sertifikat, masa berlaku sertifikat, dukungan protokol TLS, kekuatan cipher, status kerentanan, HSTS, dan OCSP Stapling. Data dari SecurityHeaders.com dianalisis berdasarkan grade keamanan dan status keberadaan masing-masing HTTP Security Headers.

Tabel 2. Analisis 5W1H Penelitian

Unsur	Keterangan
What	Evaluasi keamanan dasar website Universitas Udayana
Why	Untuk mengetahui kekuatan dan kelemahan konfigurasi keamanan dasar website
Who	Objek yang dianalisis adalah website resmi Universitas Udayana
Where	Pengujian dilakukan secara daring menggunakan SSL Labs dan SecurityHeaders.com
When	Data hasil pengujian diperoleh pada 3 Mei 2026
How	Pengujian dilakukan dengan memasukkan URL website ke tools, kemudian hasilnya dianalisis secara deskriptif

Tabel 3. Kategori Penilaian

Grade	Kategori
A+ / A	Sangat baik
B	Baik
C	Cukup
D / E	Kurang
F	Buruk

3.4 Indikator Penelitian

Indikator penelitian dibagi menjadi dua kelompok, yaitu indikator SSL/TLS dan indikator HTTP Security Headers.

Tabel 4. Indikator SSL/TLS

No	Indikator	Keterangan
1	Overall Rating	Grade keamanan SSL/TLS
2	Certificate Validity	Status validitas sertifikat
3	Certificate Issuer	Penerbit sertifikat
4	Expiration Date	Masa berlaku sertifikat

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

5	Protocol Support	Dukungan TLS dan SSL
6	Cipher Strength	Kekuatan algoritma enkripsi
7	Vulnerability Status	Status potensi kerentanan
8	HSTS	Penerapan Strict Transport Security
9	OCSP Stapling	Validasi status sertifikat tambahan

Tabel 5. Indikator HTTP Security Headers

No	Header	Fungsi
1	Strict-Transport-Security	Memaksa penggunaan HTTPS
2	Content-Security-Policy	Membatasi sumber konten
3	X-Frame-Options	Mencegah clickjacking
4	X-Content-Type-Options	Mencegah MIME-sniffing
5	Referrer-Policy	Mengatur informasi referrer
6	Permissions-Policy	Membatasi akses fitur browser

4. HASIL DAN PEMBAHASAN

4.1 Hasil Pengujian SSL Labs

Berdasarkan hasil pengujian menggunakan SSL Labs SSL Server Test, *website* Universitas Udayana memperoleh **Overall Rating B**. Hasil ini menunjukkan bahwa konfigurasi SSL/TLS sudah berjalan dengan baik, tetapi belum mencapai kategori sangat baik. Laporan SSL Labs menyatakan bahwa *server* mendukung TLS 1.0 dan TLS 1.1 sehingga grade dibatasi pada B. Pada saat yang sama, laporan juga menunjukkan bahwa *server* telah mendukung TLS 1.2 dan TLS 1.3, serta tidak mendukung SSL 2 dan SSL 3.

Gambar 2. Hasil Pengujian SSL Labs - Overall Rating B

Tabel 6. Ringkasan Hasil SSL Labs

Indikator	Hasil Pengujian	Kategori
Overall Rating	B	Baik
Domain	www.unud.ac.id	-
IP Address	103.69.197.89	-
Sertifikat	*.unud.ac.id	Valid
Key	RSA 2048 bits	Cukup baik
Signature Algorithm	SHA256withRSA	Baik
Issuer	Sectigo Public Server Authentication CA DV R36	Baik
Valid Until	4 Oktober 2026	Valid
TLS 1.3	Didukung	Baik
TLS 1.2	Didukung	Baik
TLS 1.1	Didukung	Perlu dinonaktifkan
TLS 1.0	Didukung	Perlu dinonaktifkan
SSL 3	Tidak didukung	Baik
SSL 2	Tidak didukung	Baik
HSTS	Tidak diterapkan	Perlu perbaikan
OCSP Stapling	Tidak aktif	Perlu perbaikan
Forward Secrecy	Ya, dengan sebagian besar browser	Baik

Dari sisi dukungan protokol, *website* telah mendukung TLS 1.2 dan TLS 1.3. TLS 1.3 memiliki keunggulan karena proses *handshake* lebih sederhana dan dirancang dengan keamanan yang lebih baik dibandingkan versi sebelumnya [4]. Namun, dukungan terhadap TLS 1.0 dan TLS 1.1 menjadi kelemahan utama karena protokol tersebut sudah tidak direkomendasikan [13]. Masih aktifnya TLS 1.0 dan TLS 1.1 menyebabkan grade SSL Labs dibatasi pada B. Kondisi ini konsisten dengan temuan Kotzias et al. [4] yang menunjukkan bahwa meskipun ekosistem TLS terus berkembang, banyak server masih mempertahankan dukungan terhadap protokol lama sebagai bentuk kompatibilitas mundur. Namun dari sudut pandang keamanan, keberadaan protokol lama tersebut membuka

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

potensi serangan downgrade yang memaksa koneksi menggunakan protokol yang lebih rentan. Penghapusan dukungan TLS 1.0 dan TLS 1.1 merupakan langkah yang diprioritaskan oleh NIST [15] sebagai bagian dari panduan implementasi TLS yang aman. Temuan ini menunjukkan bahwa konfigurasi keamanan website Universitas Udayana masih menempatkan kompatibilitas sistem lama sebagai pertimbangan dibandingkan penerapan standar keamanan terkini. Meskipun pendekatan tersebut dapat mempertahankan aksesibilitas bagi pengguna dengan perangkat lama, keberadaan TLS 1.0 dan TLS 1.1 meningkatkan permukaan serangan dan tidak lagi sejalan dengan rekomendasi keamanan modern. Dengan demikian, terdapat *trade-off* antara kompatibilitas dan keamanan yang perlu dipertimbangkan oleh pengelola *website*.

Hasil pengujian juga menunjukkan bahwa HSTS belum diterapkan. HSTS penting karena memberi instruksi kepada *browser* agar selalu menggunakan HTTPS ketika mengakses domain tertentu. Tanpa HSTS, pengguna masih berpotensi mengakses *website* melalui HTTP. Selain itu, OCSP Stapling juga belum aktif. OCSP Stapling digunakan untuk membantu *browser* memverifikasi status pencabutan sertifikat secara lebih efisien [19]. Tanpa OCSP Stapling, browser harus menghubungi server CA secara terpisah untuk memverifikasi status sertifikat, yang dapat menambah latensi dan berpotensi gagal apabila server CA tidak dapat dijangkau. Ketiadaan HSTS dan OCSP Stapling secara bersamaan menunjukkan bahwa konfigurasi SSL/TLS website Universitas Udayana belum sepenuhnya mengikuti praktik terbaik keamanan modern, meskipun aspek-aspek dasar seperti penggunaan sertifikat yang valid dan dukungan TLS terkini sudah terpenuhi.

Dari sisi kerentanan, hasil SSL Labs menunjukkan bahwa *website* tidak rentan terhadap beberapa kerentanan umum seperti *Heartbleed, POODLE SSLv3, ROBOT, OpenSSL CCS vulnerability, Ticketbleed,* dan beberapa kerentanan lain yang diuji oleh SSL Labs [19]. Hal ini merupakan temuan positif karena tidak ditemukan indikasi kerentanan besar pada konfigurasi SSL/TLS berdasarkan indikator yang diuji.

4.2 Hasil Pengujian SecurityHeaders.com

Berdasarkan hasil pengujian menggunakan SecurityHeaders.com, *website* Universitas Udayana memperoleh **grade C**. Hasil ini menunjukkan bahwa *website* telah menerapkan sebagian HTTP *Security Headers*, tetapi belum menerapkan beberapa header penting lainnya. Header yang telah diterapkan *adalah X-Frame-Options, X-Content-Type-Options,* dan *Referrer-Policy.* Sementara itu, header yang belum diterapkan adalah Strict-Transport-Security, Content-Security-Policy, dan Permissions-Policy [6].

Gambar 3. Hasil Pengujian SecurityHeaders.com

Tabel 7. Ringkasan Hasil Security Headers

Security Header	Status	Nilai/Keterangan
X-Frame-Options	Ada	SAMEORIGIN
X-Content-Type-Options	Ada	nosniff
Referrer-Policy	Ada	strict-origin-when-cross-origin
Strict-Transport-Security	Tidak ada	Perlu diterapkan
Content-Security-Policy	Tidak ada	Perlu diterapkan
Permissions-Policy	Tidak ada	Perlu diterapkan
Grade	C	Cukup

X-Frame-Options dengan nilai SAMEORIGIN berarti halaman hanya dapat dimuat di dalam *frame* oleh halaman dari *origin* yang sama, sehingga membantu mengurangi risiko *clickjacking*. *X-Content-Type-Options* dengan nilai *nosniff* mencegah *browser* menebak jenis konten secara otomatis. *Referrer-Policy* dengan nilai *strict-origin-when-cross-origin* membantu membatasi informasi URL yang dikirim ke domain berbeda [6].

Namun, *Strict-Transport-Security* belum diterapkan. HSTS memungkinkan *browser* mengingat bahwa domain tertentu hanya boleh diakses melalui HTTPS selama periode waktu yang ditentukan. Tanpa HSTS, perlindungan HTTPS belum sepenuhnya diperkuat pada sisi *browser*. *Content-Security-Policy* juga belum

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

diterapkan, sehingga *website* belum memiliki kebijakan eksplisit untuk mengendalikan sumber konten. *Permissions-Policy* juga belum ditemukan dalam hasil pengujian [6]. Ketiadaan ketiga header tersebut menunjukkan adanya kesenjangan dalam penerapan keamanan sisi *browser* yang cukup signifikan. Buchanan et al. [6] dalam studinya terhadap satu juta *website* terpopuler menemukan bahwa HSTS dan CSP merupakan dua *header* yang paling jarang diterapkan, padahal keduanya memberikan perlindungan paling substansial terhadap serangan yang memanfaatkan celah pada lapisan komunikasi *browser*. Temuan pada website Universitas Udayana sejalan dengan pola umum tersebut, di mana implementasi header yang mudah diterapkan *seperti X-Frame-Options dan X-Content-Type-Options* sudah ada, namun *header* yang memerlukan konfigurasi lebih kompleks seperti CSP dan HSTS belum diterapkan. Kondisi ini juga konsisten dengan hasil evaluasi yang dilakukan oleh Sinha dan Karmakar [11] pada institusi pendidikan di India, yang menemukan pola serupa di mana sebagian besar institusi baru menerapkan header-header dasar namun belum mengimplementasikan HSTS dan CSP secara penuh.

4.3 Perbandingan Hasil SSL Labs dan SecurityHeaders.com

Tabel 8. Perbandingan Hasil Pengujian

Aspek	Tools	Hasil	Interpretasi
SSL/TLS	SSL Labs	B	Baik, tetapi masih ada protokol lama
HTTP Security Headers	SecurityHeaders.com	C	Cukup, beberapa header penting belum diterapkan

Hasil dari kedua *tools* menunjukkan bahwa keamanan dasar *website* Universitas Udayana sudah berjalan, tetapi belum optimal. SSL Labs memberikan grade B, sedangkan SecurityHeaders.com memberikan grade C. Perbedaan grade ini terjadi karena kedua *tools* mengukur aspek yang berbeda. Temuan yang saling menguatkan dari kedua *tools* adalah ketiadaan HSTS, yang merupakan salah satu aspek perbaikan yang paling jelas. Jika dibandingkan dengan hasil penelitian serupa, grade B dari SSL Labs yang diperoleh website Universitas Udayana berada pada level yang umum ditemukan pada website institusi pendidikan di negara berkembang. Alhassan et al. [10] melaporkan bahwa sebagian besar website universitas federal di Nigeria juga memperoleh grade B atau lebih rendah, dengan dukungan protokol lama sebagai penyebab utama. Sementara itu, grade C dari SecurityHeaders.com menunjukkan posisi yang lebih rendah dibandingkan rata-rata yang ditemukan oleh Sinha dan Karmakar [11] pada institusi di India, di mana beberapa institusi sudah mulai menerapkan HSTS. Secara keseluruhan, hasil evaluasi ini memberikan gambaran yang komprehensif tentang posisi keamanan dasar website Universitas Udayana dalam konteks global dan nasional, serta menjadi dasar yang kuat untuk menyusun langkah-langkah perbaikan yang terstruktur.

4.4 Rekomendasi Perbaikan

Tabel 9. Rekomendasi Perbaikan

No	Temuan	Rekomendasi
1	TLS 1.0 dan TLS 1.1 masih aktif	Nonaktifkan TLS 1.0 dan TLS 1.1, gunakan TLS 1.2 dan TLS 1.3
2	HSTS belum diterapkan	Tambahkan header Strict-Transport-Security
3	Content-Security-Policy belum diterapkan	Terapkan CSP secara bertahap melalui mode report-only
4	Permissions-Policy belum diterapkan	Batasi fitur browser yang tidak diperlukan
5	OCSP Stapling belum aktif	Aktifkan OCSP Stapling
6	Masih ada cipher suite lemah	Nonaktifkan cipher suite lama atau lemah
7	Informasi server terlihat	Kurangi detail informasi pada header server

Contoh konfigurasi HSTS yang dapat dipertimbangkan: *Strict-Transport-Security: max-age=31536000; includeSubDomains*. Nilai *max-age=31536000* berarti browser akan mengingat bahwa domain tersebut harus diakses melalui HTTPS selama satu tahun ke depan. Penambahan direktif includeSubDomains juga disarankan agar subdomain yang dimiliki universitas turut terlindungi. Penerapan *Content-Security-Policy* sebaiknya dimulai dengan mode *report-only* untuk

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

melihat potensi pelanggaran kebijakan tanpa langsung memblokir konten. Mode ini memungkinkan pengelola *website* memantau sumber konten yang dimuat halaman dan menyesuaikan kebijakan secara bertahap sebelum beralih ke mode enforcement. Untuk Permissions-Policy, konfigurasi awal dapat membatasi fitur-fitur yang tidak dibutuhkan oleh website, seperti akses kamera, mikrofon, dan geolokasi, menggunakan *sintaks Permissions-Policy: camera=(), microphone=(), geolocation=().* Pengaktifan OCSP *Stapling* dapat dilakukan melalui konfigurasi web server, misalnya dengan menambahkan ssl_stapling on pada konfigurasi *Nginx* atau *SSLUseStapling on* pada *Apache*. Selain itu, penghapusan informasi detail pada header Server juga disarankan untuk mengurangi informasi yang dapat dimanfaatkan oleh penyerang dalam tahap pengintaian.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil evaluasi menggunakan SSL Labs dan SecurityHeaders.com, keamanan dasar *website* Universitas Udayana tergolong cukup baik, namun belum sepenuhnya memenuhi praktik terbaik keamanan web modern. *Website* memperoleh grade B pada pengujian SSL Labs karena telah menggunakan sertifikat SSL yang valid, mendukung TLS 1.2 dan TLS 1.3, serta tidak lagi mendukung SSL 2 dan SSL 3. Akan tetapi, keberadaan TLS 1.0 dan TLS 1.1 menunjukkan bahwa konfigurasi keamanan masih mempertahankan protokol yang telah usang sehingga berpotensi meningkatkan risiko keamanan dan membatasi nilai keamanan yang diperoleh.

Pada aspek HTTP *Security Headers, website* memperoleh grade C karena baru menerapkan sebagian header keamanan yang direkomendasikan. Ketiadaan *Strict-Transport-Security, Content-Security-Policy,* dan *Permissions-Policy* menunjukkan bahwa perlindungan pada sisi browser masih belum optimal. Temuan ini mengindikasikan bahwa penguatan keamanan *website* tidak cukup hanya melalui penggunaan HTTPS dan sertifikat yang *valid*, tetapi juga memerlukan konfigurasi *security headers* yang komprehensif.

Secara keseluruhan, penelitian ini menunjukkan bahwa tantangan utama keamanan website perguruan tinggi saat ini bukan lagi pada penerapan SSL/TLS, melainkan pada optimalisasi konfigurasi keamanan yang lebih menyeluruh. Hasil penelitian diharapkan dapat menjadi dasar evaluasi dan perbaikan bagi pengelola *website* Universitas Udayana maupun institusi pendidikan lainnya dalam meningkatkan keamanan layanan informasi digital.

5.2 Saran

Saran yang dapat diberikan adalah pengelola *website* perlu menonaktifkan TLS 1.0 dan TLS 1.1, menerapkan HSTS, menambahkan *Content-Security-Policy,* menerapkan *Permissions-Policy*, mengaktifkan OCSP *Stapling*, serta menonaktifkan *cipher suite* yang lemah. Penelitian selanjutnya dapat memperluas objek dengan membandingkan *website* Universitas Udayana dengan *website* fakultas, perpustakaan, atau perguruan tinggi lain. Perluasan objek tersebut akan memungkinkan analisis komparatif yang memberikan gambaran menyeluruh tentang tingkat kematangan keamanan digital di ekosistem perguruan tinggi di Indonesia, khususnya di wilayah Bali. Selain itu, penelitian lanjutan juga dapat mempertimbangkan penggunaan metode pengujian yang lebih mendalam, seperti penetration testing atau vulnerability assessment, untuk melengkapi hasil evaluasi berbasis tools otomatis yang telah dilakukan dalam penelitian ini. Pendekatan longitudinal yang mengevaluasi perkembangan konfigurasi keamanan website secara berkala juga dapat menjadi arah penelitian yang bermanfaat untuk memantau efektivitas perbaikan yang dilakukan oleh pengelola website dari waktu ke waktu.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak yang telah mendukung penyusunan penelitian ini. Ucapan terima kasih juga disampaikan kepada penyedia layanan SSL Labs dan SecurityHeaders.com yang menyediakan *tools* audit keamanan *website* secara terbuka sehingga penelitian ini dapat dilakukan secara objektif dan dapat direplikasi.

DAFTAR PUSTAKA

[1] K. A. D. Putra, I. P. Suhartika, N. P. P. Haryanti, and N. A. S. Pramestisari, “Analisis Pengaruh Kualitas Web Perpustakaan Universitas Udayana Terhadap Kepuasan Pengguna

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 2, Juni 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

Menggunakan Webqual 4.0," *Pustakaloka:Jurnal Kajian Informasi dan Perpustakaan*, vol. 14, no. 2, pp. 148–165, 2022.

[2] A. Syarifuddin Syahab *et al.*, "Analisis Audit Keamanan Informasi Website dari Drown Attack Menggunakan Network Mapper dan Qualys SSL," *Jurnal Manajemen Informatika & Sistem Informasi (MISI)*, vol. 6, no. 1, 2023, doi: 10.36595/misi.v5i2.

[3] A. Yoga Pratama, J. Alfa Razaq, J. Tri Lomba Juang No, K. Semarang Selatan, K. Semarang, and J. Tengah, "Integrasi Sistem Informasi Akademik dan Elearning Moodle Dengan Rest API," *Jurnal Manajemen Informatika & Sistem Informasi (MISI)*, vol. 6, no. 1, 2023, doi: 10.36595/misi.v5i2.

[4] P. Kotzias, A. Razaghpanah, J. Amann, K. G. Paterson, N. Vallina-Rodríguez, and J. Caballero, "Coming of Age," pp. 415–428, 2018, doi: 10.1145/3278532.3278568.

[5] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," Internet Engineering Task Force, 2018. doi: 10.17487/RFC8446.

[6] W. J. Buchanan, S. Helme, and A. Woodward, "Analysis of the adoption of security headers in HTTP," *IET Inf. Secur.*, vol. 12, no. 2, pp. 118–126, 2017, doi: 10.1049/iet-ifs.2016.0621.

[7] S. Calzavara, S. Roth, A. Rabitti, M. Backes, and B. Stock, "A Tale of Two Headers: A Formal Analysis of Inconsistent Click-Jacking Protection on the Web," *Figshare*, pp. 683–697, 2020, doi: 10.22028/d291-47369.

[8] A. Lavrenovs and F. J. R. Melón, "HTTP security headers analysis of top one million websites," pp. 345–370, 2018, doi: 10.23919/cycon.2018.8405025.

[9] A. Syed, M. Alzahrani, and S. Bradley, "A Comparative Analysis of HTTP Security Header Implementation on Popular Websites," *Information*, vol. 11, no. 6, p. 291, 2020, doi: 10.3390/info11060291.

[10] I. Alhassan, I. Abba-Dabo, M. S. Umar, and M. Abdullahi, "Security Evaluation of University Websites: A Case Study of Federal Universities in Nigeria," *Int. J. Comput. Appl.*, vol. 166, no. 9, pp. 1–7, 2017.

[11] R. Sinha and S. Karmakar, "Evaluating Web Security Headers and SSL/TLS Configurations of Indian Educational Institutions," *International Journal of Information Security Science*, vol. 10, no. 4, pp. 112–125, 2021.

[12] D. Chandra, G. Guntoro, and A. Wahyudi, "Analisis Keamanan Website Perguruan Tinggi Menggunakan Metode OWASP," *Jurnal Informatika dan Sistem Informasi*, vol. 8, no. 2, pp. 95–104, 2022.

[13] K. Moriarty and S. Farrell, "Deprecating TLS 1.0 and TLS 1.1," 2021. doi: 10.17487/rfc8996.

[14] M. E. Abdelhafez, S. Ramadass, and M. Abdelwahab, "TLS Guard for TLS 1.3 zero round-trip time (0-RTT) in a distributed environment," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 10, p. 101797, Dec. 2023, doi: 10.1016/j.jksuci.2023.101797.

[15] K. A. McKay and D. A. Cooper, "Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations," Gaithersburg, MD, Aug. 2019. doi: 10.6028/NIST.SP.800-52r2.

[16] S. Kaur and K. Kaur, "Analysis of website usability evaluation methods," in *2016 3rd International Conference on Computing for Sustainable Global Development*, 2016, pp. 1043–1046.

[17] A. Turcan, D. Ciorba, D. Turcanu, and R. Rughinis, "Assessing the Adoption of HTTP Security Headers," in *International Conference on Electronics, Communications and Computing (ECCO 2024)*, 2024. [Online]. Available: https://repository.utm.md/handle/5014/28773

[18] K. A. D. Putra, W. Nashihuddin, and F. Hidayatullah, "Analysis of Interface & Information Content of LIPI Botanical Gardens Website Based on Scanmic Model," *Record and Library Journal*, vol. 7, no. 1, pp. 112–124, 2021, doi: https://doi.org/10.20473/rlj.v7i1.112.

[19] Q. S. S. L. Labs, "SSL Server Rating Guide," Qualys, Inc., 2022. [Online]. Available: https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide