KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI JURAI SIWO LAMPUNG
LEMBAGA PENELITIAN DAN PENGABDIAN MASYARAKAT
Jalan Ki. HajarDewantaraKampus 15A Iringmulyo Metro Timur Kota Metro Lampung 34111
Telepon (0725) 41507; Faksimili (0725) 47296; *Website*: www.lppm.metrouniv.ac.id; *email*: lppm.iain@metrouniv.ac.id

PROTOKOL UJI KEMIRIPAN
SYARAT KHUSUS PERTAMA

Dokumen Verifikasi Kemiripan Karya Ilmiah

A. IDENTITAS KARYA ILMIAH

Nama Pengusul/Penulis	Toto Andri Puspito dan Suyono
Judul Karya Ilmiah	Performance and Security Evaluation of Selected Indonesian Mosque Websites
Nama Jurnal	Journal of Embedded System Security and Intelligent Systems (JESSI), Vol. 7 No. 3 (2026), hlm. 240–257
Tahun Terbit	2026
Indeks/Akreditasi Jurnal	Sinta 2
DOI/URL Karya Ilmiah	https://doi.org/10.59562/jessi.v7i3.14599

B. PROTOKOL UJI KEMIRIPAN

Uji kemiripan dilakukan terhadap karya ilmiah yang diajukan dengan menggunakan perangkat lunak pendeteksi kemiripan yang diakui oleh institusi. Pemeriksaan dilakukan secara objektif dengan memperhatikan sumber-sumber yang dikecualikan sesuai kebijakan institusi dan/atau ketentuan yang berlaku.

No.	Komponen Pemeriksaan	Hasil/Keterangan
1	**Aplikasi/perangkat lunak uji kemiripan**	iThenticate. Pemeriksaan dilakukan melalui submission baru untuk kepentingan verifikasi institusional.
2	**Tanggal pelaksanaan uji kemiripan**	30 Oktober 2026. Submission dilakukan pukul 10:08 WIB (GMT+7).

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI JURAI SIWO LAMPUNG
LEMBAGA PENELITIAN DAN PENGABDIAN MASYARAKAT
Jalan Ki. HajarDewantaraKampus 15A Iringmulyo Metro Timur Kota Metro Lampung 34111
Telepon (0725) 41507; Faksimili (0725) 47296; *Website*: www.lppm.metrouniv.ac.id; *email*: lppm.iain@metrouniv.ac.id

No.	Komponen Pemeriksaan	Hasil/Keterangan
3	**Nilai Similarity Index keseluruhan**	9% Overall Similarity. Nilai tersebut berada di bawah batas maksimal 25% untuk keseluruhan naskah.
4	**Sumber tunggal tertinggi**	1%. Sumber dengan kecocokan tertinggi adalah ioinformatic.org sebesar 1%; sumber lainnya berada di bawah 1%. Nilai ini berada di bawah batas maksimal 3% per sumber.
5	**Pengecualian kutipan (Exclude Quotes / Quoted Text)**	Ya. Quoted Text dikecualikan dari perhitungan kemiripan.
6	**Pengecualian daftar pustaka (Exclude Bibliography)**	Ya. Bibliography/daftar pustaka dikecualikan dari perhitungan kemiripan.
7	**Pengecualian kemiripan kecil (Small Matches)**	Tidak. Small Matches tidak dikecualikan dan tetap dimasukkan dalam perhitungan kemiripan.
8	**Pengecualian Cited Text**	Tidak. Cited Text tidak dikecualikan dan tetap dimasukkan dalam perhitungan kemiripan.
9	**Pengecualian Abstract**	Tidak. Abstract tidak dikecualikan dan tetap dimasukkan dalam perhitungan kemiripan.
10	**Pengecualian sumber tertentu secara manual**	Tidak ada. Tidak dilakukan pengecualian sumber tertentu secara manual dengan tujuan menurunkan nilai kemiripan.
11	**Hasil evaluasi terhadap indikasi kemiripan yang tidak wajar**	Tidak terdapat indikasi manipulasi teks yang mencurigakan. Laporan menunjukkan 0 Integrity Flags.

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI JURAI SIWO LAMPUNG
LEMBAGA PENELITIAN DAN PENGABDIAN MASYARAKAT
Jalan Ki. HajarDewantaraKampus 15A Iringmulyo Metro Timur Kota Metro Lampung 34111
Telepon (0725) 41507; Faksimili (0725) 47296; *Website*: www.lppm.metrouniv.ac.id; *email*: lppm.iain@metrouniv.ac.id

No.	Komponen Pemeriksaan	Hasil/Keterangan
12	**Kesimpulan hasil uji kemiripan**	Hasil uji kemiripan sesuai dengan kaidah penulisan dan tidak ada indikasi kemiripan yang tidak wajar.

C. KESIMPULAN VERIFIKASI

Berdasarkan hasil uji kemiripan dan pemeriksaan konfigurasi laporan, karya ilmiah tersebut dinyatakan:

[X] MEMENUHI ketentuan batas kuantitatif uji kemiripan yang digunakan dalam proses verifikasi.

[ ] MEMERLUKAN PERBAIKAN sebelum dapat dinyatakan memenuhi ketentuan.

[ ] TIDAK MEMENUHI ketentuan uji kemiripan yang berlaku.

Catatan Verifikator:

Hasil uji kemiripan menunjukkan Overall Similarity sebesar 9% dengan kecocokan sumber tertinggi sebesar 1%. Pengecualian hanya diterapkan pada Bibliography dan Quoted Text. Cited Text, Abstract, dan Small Matches tetap dimasukkan dalam perhitungan. Tidak terdapat pengecualian sumber tertentu secara manual dan laporan menunjukkan 0 Integrity Flags. Dengan demikian, hasil pemeriksaan dapat diverifikasi secara transparan sesuai protokol yang digunakan.

E. DOKUMEN PENDUKUNG YANG DILAMPIRKAN

1. Laporan hasil kemiripan
2. Halaman Integrity Overview yang menunjukkan Overall Similarity 9% dan filter: Bibliography serta Quoted Text.
3. Halaman Top Sources yang menunjukkan sumber tertinggi sebesar 1%.
4. Laporan hasil uji kemiripan lengkap atau bagian laporan yang dipersyaratkan pada sistem pengajuan.

Metro, 30 Oktober 2026

Pengusul	Petugas/Verifikator Uji Kemiripan	Mengetahui, Ketua/Kepala LPPM
Toto Andri Puspito	Ahmad Arifin, M.Pd.	Dr. Nurkholis, M.Pd.
NIP.198902192019031007	NIP.198911262023211014	NIP.197807142011011005

12 Dokumen Artikel (submit sister).pdf

Universitas Islam Negeri Jurai Siwo Lampung

Document Details

Submission ID
trn:oid:::3618:156461874

Submission Date
Oct 30, 2026, 10:08 AM GMT+7

Download Date
Oct 30, 2026, 10:15 AM GMT+7

File Name
12 Dokumen Artikel (submit sister).pdf

File Size
596.5 KB

18 Pages

8,239 Words

52,031 Characters

9% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

41 Not Cited or Quoted 7%
Matches with neither in-text citation nor quotation marks

11 Missing Quotations 2%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

8% Internet sources
5% Publications
0% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **41** Not Cited or Quoted 7%
  Matches with neither in-text citation nor quotation marks
- **11** Missing Quotations 2%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

8% Internet sources
5% Publications
0% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	ioinformatic.org 1%
2	Publication	Komal Gupta, Mahender Pratap Singh. "Website performance assessment of acad... <1%
3	Internet	publichealth.jmir.org <1%
4	Internet	journal.unm.ac.id <1%
5	Internet	docs.middleware.io <1%
6	Internet	www.mdpi.com <1%
7	Publication	Zhiguo Zhang, Zhenchao Wang. "Low-light image enhancement with retinex theo... <1%
8	Internet	journal.universitaspahlawan.ac.id <1%
9	Internet	cdn.juris.id <1%
10	Internet	www.achneuro.site <1%

11 Internet

docs.mipro-proceedings.com <1%

12 Internet

www.campaignsyoulove.com <1%

13 Publication

Muhammad Adi Zacky Zahran, Binastya Anggara Sekti. "Design and Development... <1%

14 Internet

www.softguide.com <1%

15 Internet

dspace.znu.edu.ua <1%

16 Internet

www.gestenco.com <1%

17 Internet

juna.nusantarajournal.com <1%

18 Internet

assets-eu.researchsquare.com <1%

19 Internet

cris.vub.be <1%

20 Internet

noise.getoto.net <1%

21 Internet

recipp.ipp.pt <1%

22 Internet

woshub.com <1%

23 Publication

Corrado Fasciano, Filippo Gramegna, Floriano Scioscia, Michele Ruta et al. "NextH... <1%

24 Publication

Max Shestov, Christopher Felix Brewer. "Regulated medication information, acce... <1%

25 Publication

Tegar Fadillah Zanestri, Indra Lukmana Sardi, Kusuma Ayu Laksitowening. "React... <1%

26 Internet

e-journal.metrouniv.ac.id <1%

27 Internet

gulhanemedj.org <1%

28 Internet

repository.ikado.ac.id <1%

29 Internet

rizk.appuwa.com <1%

30 Internet

www.ijltemas.in <1%

31 Publication

Sami Naouali, Semeh Ben Salem, Zied Chtourou. "Uncertainty mode selection in c... <1%

iThenticate Page 6 of 23 - Integrity Submission Submission ID trn:oid:::3618:156461874

Journal of Embedded System Security and Intelligent Systems
E-ISSN: 2722-273X; P-ISSN: 2745-925X
https://journal.unm.ac.id/index.php/JESSI

Performance and Security Evaluation of Selected Indonesian Mosque Websites

Toto Andri Puspito✉
UIN Jurai Siwo Lampung, Indonesia
Suyono
Institut Bakti Nusantara, Indonesia

ARTICLE INFO

Keywords:

Core Web Vitals;
HTTP security headers;
Mosque websites;
Web performance;
Web security

Article History

Received: May 30, 2026
Revised : August 09, 2026
Accepted: August 30, 2026

This is an open access article under the CC BY-SA licenz

ABSTRACT

Purpose – Mosque websites increasingly serve as public digital service platforms for information dissemination, administrative services, donations, and community engagement. However, previous studies have mainly focused on system development, functionality, and usability, while integrated evaluations of technical performance and externally observable security remain limited. This study evaluates the performance and basic security posture of selected Indonesian mosque websites through a multidimensional technical audit framework.

Design/methods/approach – A quantitative non-invasive comparative design was applied to seven purposively selected operational mosque websites. Data were collected through repeated Google Lighthouse measurements, PageSpeed Insights field data, Core Web Vitals analysis, HTTP security-header evaluation, and Transport Layer Security (TLS) assessment. The framework considers performance, user experience indicators, browser-level security controls, and transport security as complementary dimensions.

Findings – Desktop performance was significantly better than mobile performance, particularly in loading-related metrics, while Accessibility, Best Practices, and Search Engine Optimization (SEO) remained relatively consistent across devices. Security evaluation revealed uneven browser-level security implementation, showing that header presence does not always indicate effective configuration. TLS protection was generally stronger than browser-level controls.

Research implications/limitations – The findings demonstrate the importance of multidimensional website assessment. However, the study is limited to seven purposively selected websites concentrated in Java and represents comparative case evidence rather than national assessment.

Originality/value – This study contributes an integrated evaluation framework combining performance, user experience, HTTP security configuration, and TLS assessment for mosque websites.

To cite this article : Puspito, T. A., & Suyono. (2026). Performance and Security Evaluation of Selected Indonesian Mosque Websites. *Journal of Embedded System Security and Intelligent Systems, 7*(3), 240-257. 10.59562/jessi.v7i3.14599

INTRODUCTION

Mosque websites increasingly function as public digital service platforms rather than merely as institutional profiles. Through these platforms, mosque administrators can provide prayer schedules, religious announcements, educational materials, donation information, financial transparency reports, event calendars, and community services. The development of web-based mosque information systems in Indonesia demonstrates that digital platforms contribute to improving information accessibility, administrative efficiency, and communication between mosque organizations and congregations [1], [2], [3]. Unlike conventional organizational websites, mosque websites represent a public-interest digital infrastructure because they support continuous interaction between religious institutions and communities through information dissemination, service delivery, and transparency-related functions. Similar trends have been observed in broader digital transformation initiatives, where organizational websites are

iThenticate Page 6 of 23 - Integrity Submission Submission ID trn:oid:::3618:156461874

increasingly expected to provide not only information delivery but also reliable, accessible, and secure digital services [4], [5]. Therefore, technical website quality has become an essential consideration because the availability of digital functions alone does not guarantee effective service delivery. Slow loading times, poor mobile performance, limited accessibility, and weak security configurations may reduce the reliability and trustworthiness of these digital services [6], [7].

Previous studies on mosque digitalization have primarily emphasized system development, functional requirements, and user-centered evaluation. Herfandi and Hamdani developed a web-based mosque management information system to support administrative activities [3], while Ardli implemented Rapid Application Development to integrate services such as donations, zakat, qurban, financial information, and activity management into a mosque website [1]. Fauzan also proposed a web-based mosque management system to improve structured access to congregation and administrative data [2]. Furthermore, Farizqi and Haryono evaluated a mosque management information system using usability testing and reported user experience results based on the System Usability Scale [8]. These studies demonstrate that websites have become important digital infrastructure for mosque management; however, their primary emphasis remains on system functionality, service features, and user perception rather than objective evaluation of technical performance and externally observable security posture. This limitation reflects a broader challenge in digital service research, where functional availability does not necessarily represent technical reliability, performance quality, or security readiness [4], [5].

Beyond functional evaluation, modern website assessment increasingly requires measurable technical indicators that can identify weaknesses in digital service delivery. Automated auditing approaches have therefore become widely adopted because they provide reproducible measurements of website quality. Google Lighthouse is one of the widely used tools for evaluating website quality through standardized laboratory-based measurements of Performance, Accessibility, Best Practices, and Search Engine Optimization (SEO) [6]. Previous studies have demonstrated that Lighthouse-based evaluation can reveal technical weaknesses in institutional and public-service websites that may not be identified through functional assessment alone [9], [10], [11]. Puspito further showed that combining automated performance evaluation with usability assessment provides a broader understanding of website quality [12]. Automated web-performance analysis is valuable because it enables the identification of technical bottlenecks related to loading behavior, rendering efficiency, and resource delivery that influence user experience [13], [14]. However, mosque website evaluations have rarely incorporated automated performance auditing as part of a comprehensive technical assessment framework.

Website performance assessment also requires consideration of the difference between laboratory measurements and actual user experience. Lighthouse provides controlled laboratory-based diagnostics, whereas PageSpeed Insights incorporates field data from the Chrome User Experience Report (CrUX) when sufficient real-user observations are available [6]. Core Web Vitals provide standardized indicators of user experience through Largest Contentful Paint (LCP) for loading performance, Interaction to Next Paint (INP) for interaction responsiveness, and Cumulative Layout Shift (CLS) for visual stability. Google defines good performance thresholds at the 75th percentile as LCP ≤ 2.5 seconds, INP ≤ 200 milliseconds, and CLS ≤ 0.1 [15]. Recent studies have confirmed that Core Web Vitals can serve as objective indicators for evaluating website responsiveness and user experience across different website categories [16]. Previous usability research has also demonstrated that waiting time, responsiveness, and system feedback influence user satisfaction and acceptance of digital services [17], [18]. Therefore, comprehensive website evaluation should consider multiple performance indicators rather than relying solely on a single overall score.

In addition to performance, security represents another critical dimension of website quality, particularly for public-facing platforms that support information dissemination and community-related services. Websites operated by public-interest institutions require appropriate browser security mechanisms to reduce risks associated with client-side attacks, unauthorized content manipulation, and insecure resource execution. HTTP security headers, including Strict-Transport-Security (HSTS), Content-Security-Policy (CSP), X-Content-Type-Options, frame protection, and Referrer-Policy, provide important browser-level security controls when correctly implemented [19]. Nevertheless, previous studies have shown that many websites continue to demonstrate weaknesses in security-header deployment and configuration. Erden evaluated thousands of domains and identified widespread weaknesses in HTTP security-header implementation, particularly related to missing or incorrectly configured CSP policies [20]. Besmer further demonstrated that the presence of security headers does not necessarily indicate effective protection because insecure configurations may reduce their intended security benefits [21]. Similarly, Waheed and Alazab (2026) identified gaps in baseline security-header adoption among public-sector websites. These findings indicate that security assessment should evaluate not only the existence of security mechanisms but also their configuration quality and effectiveness [22].

Security evaluation approaches also measure different layers of website protection and should therefore be interpreted as complementary rather than interchangeable. HTTP security-header analysis focuses on browser-enforced security controls and their configuration quality [19], [20], whereas SSL/TLS assessment evaluates encrypted transport security, including certificate validity and protocol configuration [23], [24]. Consequently, a website may demonstrate strong TLS implementation while still having insufficient browser-level protection, or may contain security headers that exist but are incorrectly configured. Similar distinctions between application-facing security controls and transport-layer security have been emphasized in cybersecurity assessment frameworks. Therefore, reliable website security evaluation requires multiple assessment perspectives rather than dependence on a single security indicator.

A research gap emerges from the intersection between mosque digitalization studies and broader website-quality assessment research. Existing mosque website studies have mainly investigated information-system development, service functionality, and usability evaluation, whereas general website-quality studies frequently examine performance or security as separate dimensions. Limited empirical evidence exists regarding the integrated evaluation of technical performance and externally observable security posture of operational mosque websites in Indonesia. More specifically, previous studies have rarely combined repeated laboratory performance measurements, field-based Core Web Vitals, HTTP security-header deployment, configuration-sensitive security assessment, and TLS evaluation within a single comparative framework. This limitation is significant because mosque websites increasingly function as public digital services where accessibility, responsiveness, reliability, and security contribute to institutional credibility and user trust.

Accordingly, this study evaluates seven selected Indonesian mosque websites through a multidimensional and non-invasive technical audit framework. The contribution of this research extends beyond the simultaneous use of several assessment tools by establishing a structured evaluation approach that separates and integrates four complementary technical dimensions: laboratory-based web performance, available field-based Core Web Vitals, HTTP security-header implementation and configuration quality, and TLS transport security. This approach enables a more comprehensive understanding of website quality by identifying whether weaknesses originate from performance limitations, user-experience constraints, browser security configuration, or transport-layer protection. Considering that the selected websites represent purposive comparative cases rather than a statistically representative national sample, this study

aims to provide empirical evidence regarding technical characteristics and improvement priorities among selected Indonesian mosquewebsites.This study addresses the following research questions:

1. RQ1: How do selected Indonesian mosque websites perform in terms of Performance, Accessibility, Best Practices, SEO, and key loading metrics?
2. RQ2: How does website performance differ between mobile and desktop environments?
3. RQ3: To what extent do selected mosque websites implement and securely configure basic web security mechanisms?

For RQ2, the null hypothesis (H0) states that there is no significant difference between paired mobile and desktop performance scores, while the alternative hypothesis (H1) states that significant differences exist.

METHOD

This research used a quantitative comparative observational design based entirely on publicly accessible web responses. The study was designed as a non-invasive technical audit and did not involve authentication bypass, exploitation attempts, password testing, vulnerability injection, or intrusive penetration testing. The unit of analysis was the public homepage of each selected mosque website because the homepage represents the primary entry point for information access and public digital interaction.

Data collection was conducted within the same predefined measurement period to minimize temporal variation caused by website updates, server changes, or content modifications. All websites were evaluated using the same assessment procedures, tools, and measurement criteria. Because the selected tools rely on externally operated assessment infrastructures, possible variations caused by remote execution environments, network conditions, server load, third-party resources, and website changes were treated as potential sources of measurement variability.

The overall research workflow is presented in Figure 1.

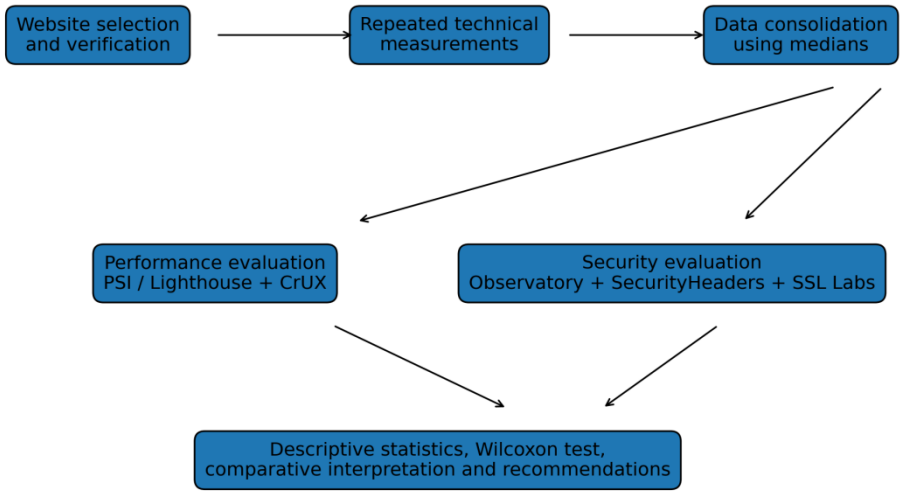


Figure 1. Research workflow

Website Selection

The sample consisted of seven publicly accessible mosque websites selected using a purposive case-selection strategy. The selection approach was adopted because independent official mosque websites are not uniformly available across Indonesian mosque institutions. Candidate websites were identified through publicly available web searches and institutional verification processes.

A website was included when it met the following criteria: (1) represented an identifiable mosque institution in Indonesia; (2) was publicly accessible without authentication requirements; (3) could reasonably be verified as an official website or institutionally affiliated platform; (4) provided an operational homepage during the observation period; and (5) could be evaluated using the selected non-invasive performance and security assessment tools.

Websites were excluded when they were inaccessible during the observation period, consisted only of third-party directory pages or social-media profiles, lacked sufficient institutional identification, or could not produce comparable homepage-level measurements. After applying these criteria, seven websites were retained as comparative technical cases.

The selected websites are geographically concentrated on Java and represent different institutional contexts, including national-scale, urban/community, foundation-based, and university-associated mosques. This concentration is explicitly recognized as a limitation. Therefore, the purpose of the sample is not to estimate national website adoption or security levels but to provide comparative evidence regarding the technical characteristics of selected mosque websites.

Table 1. Selected mosque websites

Code	Mosque	Homepage	Institutional context
M1	Masjid Agung Sunda Kelapa	https://masjid-sundakelapa.id/	Urban/community
M2	Masjid Istiqlal	https://www.istiqlal.or.id/	National
M3	Masjid Cut Meutia	https://masjidcutmeutia.com/	Urban/community
M4	Masjid Tazkia	https://www.masjidtazkia.com/	Institutional/foundation
M5	Masjid Nasional Al Akbar	https://www.masjidalakbar.or.id/	Regional/national-scale
M6	Masjid IPB	https://masjid.ipb.ac.id/	University/campus
M7	Masjid Agung Al Azhar	https://masjidagungalazhar.com/	Foundation/education

Performance and Core Web Vitals Measurement

Performance testing used Google PageSpeed Insights with its Lighthouse laboratory audit framework. Each homepage was tested three times using Mobile mode and three times using Desktop mode, producing 42 laboratory runs in total (7 websites × 2 device modes × 3 repetitions). Repeated measurements were retained rather than selecting the best-performing result because Lighthouse outputs may vary due to remote execution conditions, resource availability, server response variation, and third-party dependencies.

For each website and device category, the median value from the three Lighthouse runs was used as the primary comparative measurement. The median approach was selected to reduce the influence of individual abnormal runs and provide a more stable representation of observed performance. Lighthouse results were interpreted as laboratory measurements, while available PageSpeed Insights field data were interpreted as real-user experience observations. Previous PSI-based research similarly distinguishes between laboratory diagnostics and field measurements, noting that field metrics may be unavailable when Chrome User Experience Report (CrUX) coverage is insufficient [25].

The testing environment relied on the publicly available PageSpeed Insights and Lighthouse infrastructure. The researchers did not modify Lighthouse configuration parameters, network throttling profiles, or execution environments. Therefore, the measurements represent standardized external assessments rather than controlled local benchmarking experiments. Four Lighthouse category scores were recorded: Performance, Accessibility, Best Practices, and SEO. Scores of 0–49 are categorized as poor, 50–89 as needing improvement, and 90–100 as good according to Lighthouse scoring guidance [26]. Five detailed laboratory metrics were also recorded: First Contentful Paint (FCP), Largest Contentful Paint (LCP), Total Blocking Time (TBT), Cumulative Layout Shift (CLS), and Speed Index (SI). Category-level results provide an overall

quality comparison, while detailed metrics identify specific performance characteristics associated with loading, responsiveness, and visual stability.

Field-based Core Web Vitals were analyzed separately from Lighthouse laboratory results. The study used available PSI/CrUX values for LCP, INP, and CLS together with the overall Core Web Vitals assessment. Google defines good performance thresholds at the 75th percentile as LCP ≤ 2.5 seconds, INP ≤ 200 milliseconds, and CLS ≤ 0.1 [15]. When PSI did not provide sufficient field data, the value was coded as N/A rather than zero because unavailable field coverage does not indicate poor performance [25].

Table 2. Core Web Vitals field thresholds used in the study

Metric	Good	Needs improvement	Poor
LCP	<= 2.5 s	> 2.5-4.0 s	> 4.0 s
INP	<= 200 ms	> 200-500 ms	> 500 ms
CLS	<= 0.10	> 0.10-0.25	> 0.25

Security Measurement

First, MDN HTTP Observatory was used as a configuration-sensitive assessment of HTTP security practices. Observatory-based studies have shown that low scores frequently reflect missing or incorrectly configured browser-side security controls, particularly CSP and related HTTP headers [27]. Therefore, this study uses the term "basic web security posture" rather than "complete website security." Second, SecurityHeaders.com was used as a complementary indicator of HTTP security-header deployment. Previous large-scale research has demonstrated substantial variation in the adoption of HSTS, CSP, X-Frame-Options, and other response-header protections [28]. The present study therefore distinguishes between header presence and configuration quality.

Third, Qualys SSL Labs was used to evaluate transport-layer security characteristics, including certificate status and supported TLS protocols. Previous TLS ecosystem studies demonstrate that certificate properties and protocol configuration provide important but separate evidence regarding transport security quality [29]. Because these tools assess different security layers, their outputs were interpreted as complementary indicators rather than interchangeable security scores.

Data Aggregation and Statistical Analysis

For each website-device combination, the median value from three Lighthouse runs was calculated as the primary comparative measurement to reduce the influence of run-to-run variation caused by remote execution conditions, temporary network fluctuations, server response changes, and third-party resource behavior. Descriptive statistics, including mean, standard deviation, median, minimum, and maximum values, were calculated for all performance indicators across the seven evaluated websites. The primary comparison between Mobile and Desktop performance was analyzed using the Wilcoxon signed-rank test because the study involved paired observations from the same websites under two device conditions and the small sample size did not support reliable assumptions of normal distribution for paired differences [30]. The significance level was set at $\alpha = 0.05$. The paired difference between Desktop and Mobile performance scores was calculated as:

$$d_i = Desktop_i - Mobile_i$$

where d_i represents the difference between Desktop and Mobile performance scores for website i.The Wilcoxon signed-rank statistic was determined by comparing the ranked positive and negative differences as follows:

$$W = Min\,(W+, W-) \quad [30]$$

where $W+$ represents the sum of positive ranks and (W^-) represents the sum of negative ranks from the paired differences [30]. In addition to statistical significance, an effect-size estimate was calculated using a non-parametric measure to describe the practical magnitude of the observed Mobile–Desktop differences. The primary inferential analysis focused on Lighthouse Performance scores, while additional comparisons involving First Contentful Paint (FCP), Largest Contentful Paint (LCP), Total Blocking Time (TBT), Cumulative Layout Shift (CLS), and Speed Index were conducted as exploratory analyses to identify specific performance characteristics associated with differences between device environments. Because these comparisons were based on only seven paired websites, the resulting p-values and effect-size estimates were interpreted as comparative evidence for the selected cases rather than population-level conclusions. Security results were analyzed descriptively using tool grades, security scores, TLS characteristics, and the proportion of websites implementing specific HTTP security headers. Since HTTP security-header evaluation and TLS assessment represent different layers of website protection, their results were interpreted as complementary indicators of basic web security posture rather than combined into a single security score.

RESULTS AND DISCUSSION

Lighthouse Category Scores

Table 3 presents the median Lighthouse category scores obtained from three repeated measurements for each website under Mobile and Desktop conditions. The results indicate that device conditions primarily affected the Performance category, while Accessibility, Best Practices, and SEO showed relatively stable patterns across devices. Among the evaluated websites, Masjid Tazkia (M4) demonstrated the strongest laboratory performance profile, achieving median Performance scores of 86 on Mobile and 99 on Desktop. In contrast, Masjid IPB (M6) recorded the lowest Mobile Performance score (31), whereas Masjid Cut Meutia (M3) obtained the lowest Desktop Performance score (45). Most websites remained within the Lighthouse "needs improvement" category for Performance, indicating that loading efficiency represents the main technical limitation among the evaluated mosque websites.

Accessibility scores showed relatively consistent results, ranging from 69 to 86 on Mobile and from 69 to 88 on Desktop. This indicates that accessibility-related implementation was less influenced by device conditions compared with loading performance. Similarly, Best Practices and SEO scores were generally higher across the evaluated websites, although several differences remained. M7 and M3 demonstrated lower Best Practices scores on specific device conditions, while SEO scores remained identical between Mobile and Desktop for all evaluated websites.

Table 3. Median Lighthouse category scores (three runs per device)

Code	Perf M	Perf D	Acc M	Acc D	BP M	BP D	SEO M	SEO D
M1	57	80	82	75	96	100	83	83
M2	56	67	69	69	92	92	92	92
M3	56	45	83	83	100	77	100	100
M4	86	99	84	84	100	100	100	100
M5	52	76	82	88	96	96	100	100
M6	31	57	86	86	96	100	85	85
M7	46	68	83	77	73	73	92	92

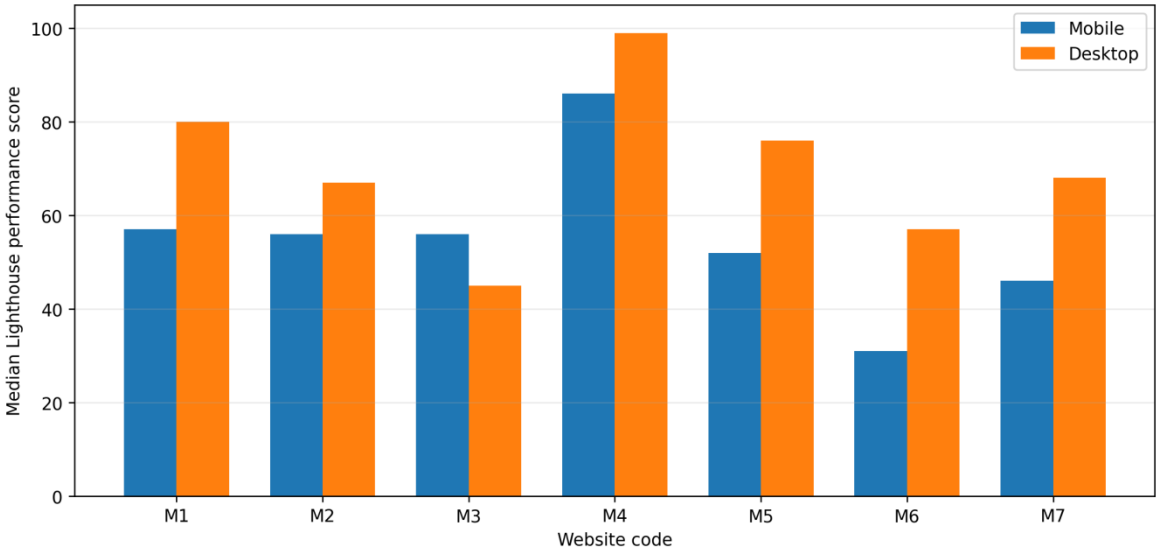


Figure 2. Median Lighthouse Performance scores by device

Across all websites, the mean Mobile Performance score was 54.86 (SD = 16.50), with a median value of 56, whereas the mean Desktop Performance score reached 70.29 (SD = 17.24), with a median value of 68. The Wilcoxon signed-rank test revealed a statistically significant difference between Mobile and Desktop Performance scores (W = 1.5, p = 0.0469). Therefore, the null hypothesis for RQ2 was rejected, indicating that performance differed significantly between the two device environments. Six of the seven evaluated websites achieved higher Performance scores on Desktop than on Mobile. Masjid Cut Meutia (M3) was the only exception, with a Mobile score of 56 and a Desktop score of 45. This result indicates that mobile environments generally represent a more demanding condition for website delivery. However, the finding does not directly demonstrate a specific technical cause because this study did not include source-code inspection or server-side analysis.

The device-related difference was not observed across all Lighthouse categories. Accessibility produced an identical median score of 83 for both Mobile and Desktop, with no statistically significant difference (p = 0.750). Best Practices also showed identical median values of 96 (p = 1.000), while SEO maintained a median score of 92 across both environments (p = 1.000). These results suggest that the primary device-dependent limitation within the observed websites was related to loading performance rather than general technical quality degradation. This finding is consistent with previous Lighthouse-based evaluations showing that websites may achieve relatively strong SEO and best-practice scores while still experiencing performance limitations. Therefore, website quality assessment should consider multiple technical dimensions rather than relying on a single overall score [31], [32], [33].

Detailed Loading Metrics and Mobile-Desktop Differences

The detailed Lighthouse laboratory metrics provide further insight into the factors contributing to the differences in Performance scores. Table 4 summarizes the median values of key performance indicators, including First Contentful Paint (FCP), Largest Contentful Paint (LCP), Total Blocking Time (TBT), Cumulative Layout Shift (CLS), and Speed Index (SI).

Table 4. Median Lighthouse laboratory metrics (FCP, LCP, SI in seconds; TBT in ms)

Code	FCP M	FCP D	LCP M	LCP D	TBT M	TBT D	CLS M	CLS D	SI M	SI D
M1	4.4	0.8	9.7	2	40	50	0.003	0.029	5.8	5.3
M2	4.5	1	60.9	10.2	30	0	0	0.005	16.5	5
M3	8.2	0.8	13.9	2.7	40	240	0	0.995	9.2	2.7

Code	FCP M	FCP D	LCP M	LCP D	TBT M	TBT D	CLS M	CLS D	SI M	SI D
M4	0.9	0.2	4.2	0.8	0	0	0.063	0.009	2.1	0.8
M5	7.3	1	15.4	2.5	220	240	0	0.004	10.4	1.7
M6	4.2	0.6	16	2.8	270	20	0.689	0.353	6.7	3.1
M7	16.3	1	36.9	1.4	330	370	0.081	0	22	5.7

The results demonstrate that loading-related metrics represented the most substantial differences between Mobile and Desktop conditions. Several websites recorded considerably high Mobile LCP values, particularly Masjid Istiqlal (M2) with 60.9 seconds and Masjid Agung Al Azhar (M7) with 36.9 seconds. Masjid IPB (M6) and Masjid Nasional Al Akbar (M5) also showed relatively high Mobile LCP values of 16.0 seconds and 15.4 seconds, respectively. These results indicate that the rendering of the largest visible content element was substantially delayed under mobile emulation conditions. M7 showed the weakest mobile loading profile, with FCP of 16.3 seconds and Speed Index of 22.0 seconds. Conversely, Masjid Tazkia (M4) demonstrated the most consistent performance, achieving Mobile FCP of 0.9 seconds, Mobile LCP of 4.2 seconds, and Desktop LCP of 0.8 seconds. The paired statistical analysis presented in Table 5 further confirms that Mobile–Desktop differences were primarily associated with loading-related indicators.

Table 5. Paired Mobile-Desktop Wilcoxon signed-rank results

Measure	Mobile median	Desktop median	W	p-value	Result
Performance score	56	68	1.5	0.0469	Significant
FCP (s)	4.5	0.8	0.0	0.0156	Significant
LCP (s)	15.4	2.5	0.0	0.0156	Significant
TBT (ms)	40	50	9.0	0.8438	Not significant
CLS	0.003	0.009	13.0	0.9375	Not significant
Speed Index (s)	9.2	3.1	0.0	0.0156	Significant

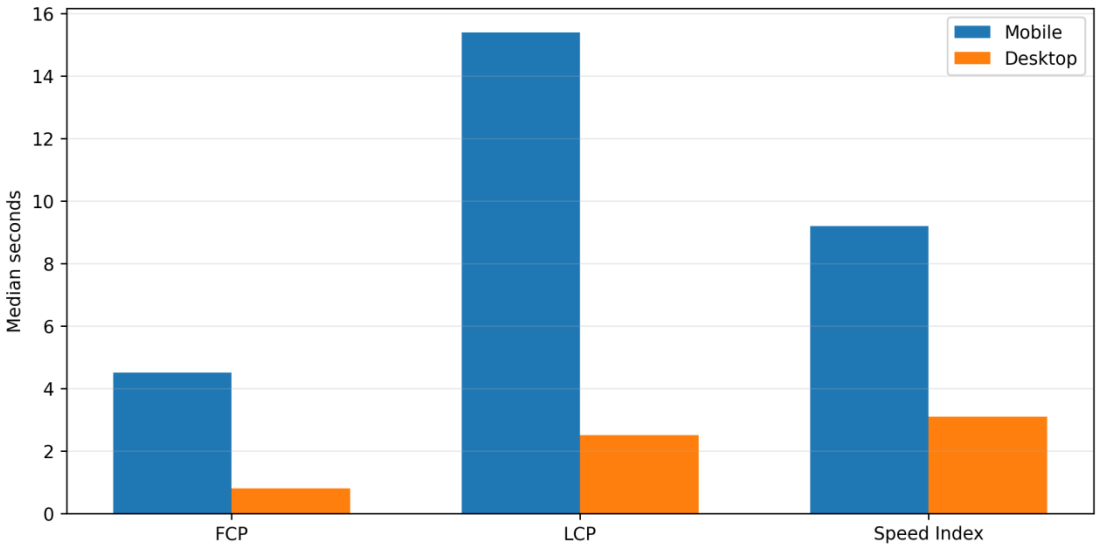


Figure 3. Across-site median FCP, LCP, and Speed Index

The Wilcoxon analysis showed significant differences for FCP, LCP, and Speed Index, with all three metrics demonstrating lower values on Desktop compared with Mobile (W = 0, p = 0.0156). The median LCP decreased from 15.4 seconds on Mobile to 2.5 seconds on Desktop, while the median FCP decreased from 4.5 seconds to 0.8 seconds. In contrast, TBT and CLS did not demonstrate statistically significant differences between the two environments. Nevertheless, several individual websites showed technically important visual stability issues. Masjid Cut Meutia (M3) recorded a very high Desktop CLS value of 0.995, while Masjid IPB (M6) showed high CLS values on both Mobile (0.689) and Desktop (0.353). Although these differences were not statistically significant at the group level, these cases indicate potential layout stability problems that may affect user experience.

The combination of high LCP values and relatively moderate TBT values suggests that delayed loading was not necessarily caused only by JavaScript execution limitations. Other factors, such as large media resources, rendering dependencies, server response conditions, and resource delivery strategies, may contribute to slower content rendering. However, because this study was conducted through external technical auditing without source-code examination, these factors should be interpreted as possible explanations rather than confirmed causes.

Field-Based Core Web Vitals

Field-based Core Web Vitals data were available for only three of the seven evaluated websites, namely M1, M2, and M5. The limited availability of CrUX-based field data indicates that smaller institutional websites may not always have sufficient real-user traffic to generate complete field measurements. Therefore, unavailable values (N/A) were treated as missing observations rather than interpreted as poor performance.

Table 6. Core Web Vitals field results from PageSpeed Insights/CrUX

Code	Device	Assessment	LCP	INP	CLS
M1	Mobile	Failed	4.2 s	110 ms	0.18
M1	Desktop	Passed	1.7 s	65 ms	0.04
M2	Mobile	Failed	5.0 s	247 ms	0.02
M2	Desktop	Failed	2.6 s	66 ms	0.01
M3	Mobile/Desktop	N/A	N/A	N/A	N/A
M4	Mobile/Desktop	N/A	N/A	N/A	N/A
M5	Mobile	Passed	2.5 s	N/A	0.01
M5	Desktop	Passed	2.3 s	61 ms	0.02
M6	Mobile/Desktop	N/A	N/A	N/A	N/A
M7	Mobile/Desktop	N/A	N/A	N/A	N/A

The available field results demonstrate differences between laboratory-based measurements and real-user performance observations. Masjid Agung Sunda Kelapa (M1) failed the Mobile Core Web Vitals assessment but passed the Desktop assessment. Under Mobile conditions, M1 recorded an LCP value of 4.2 seconds and CLS of 0.18, while Desktop measurements showed improved values with LCP of 1.7 seconds and CLS of 0.04. These results indicate that the limitation was mainly associated with loading performance and visual stability rather than interaction responsiveness.

Masjid Istiqlal (M2) demonstrated the weakest field-based performance among the websites with available data. The website failed both Mobile and Desktop assessments. Mobile measurements showed LCP of 5.0 seconds and INP of 247 milliseconds, exceeding the recommended thresholds. Although Desktop INP improved to 66 milliseconds, the overall assessment remained unsuccessful because the loading experience still did not meet the required

criteria. In contrast, Masjid Nasional Al Akbar (M5) achieved passing Core Web Vitals assessments on both devices. The website recorded Mobile LCP of 2.5 seconds and Desktop LCP of 2.3 seconds, accompanied by low CLS values. This indicates relatively stable real-user experience compared with the other websites with available field data.

The differences between Lighthouse laboratory results and Core Web Vitals field measurements should not be interpreted as inconsistencies. Laboratory measurements represent controlled testing conditions designed to diagnose technical performance issues, whereas field measurements represent aggregated experiences from actual users under diverse conditions [25], [34]. Therefore, both measurements provide complementary perspectives for evaluating website quality.

HTTP Security Posture

The HTTP security evaluation revealed a weaker condition compared with transport-layer security. The results indicate that although several websites implemented basic security mechanisms, configuration quality remained inconsistent across the evaluated cases. The MDN HTTP Observatory assessment produced scores ranging from 0 to 70, with a mean score of 29.29 and a median score of 25. Masjid Agung Sunda Kelapa (M1) achieved the highest Observatory score (70, Grade B), followed by Masjid Istiqlal (M2) and Masjid Tazkia (M4), which each obtained Grade C with a score of 50. Masjid IPB (M6) received Grade D- with a score of 25, while M3, M5, and M7 received Grade F.

Table 7. Overall security assessment by tool

Code	Observatory	Obs. grade	SecurityHeaders	SSL Labs	TLS 1.3	TLS 1.0/1.1	Certificate
M1	70	B	A	B	Yes	Yes	Valid
M2	50	C	D	B	Yes	Yes	Valid
M3	0	F	D	A	Yes	No	Valid
M4	50	C	D	A+	Yes	No	Valid
M5	5	F	Fs	A	Yes	No	Valid
M6	25	D-	A	A-	Yes	No	Valid
M7	5	F	D	A+	Yes	No	Valid

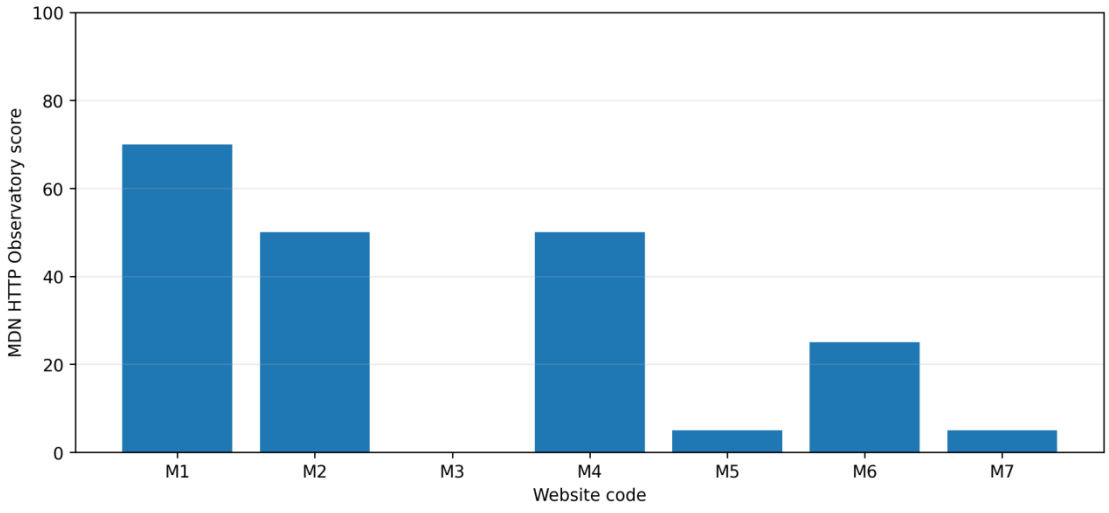


Figure 4. MDN HTTP Observatory scores

Overall, six of the seven websites obtained Observatory grades below Grade B, indicating that browser-level security configuration remains an important area for improvement. This finding is consistent with previous large-scale security studies reporting that many public-facing websites still experience weaknesses in implementing or configuring HTTP security headers [27], [35], [36]. SecurityHeaders.com produced a different evaluation pattern because the tool primarily focuses on detecting the presence of security-related response headers rather than evaluating their effectiveness in preventing security risks. The aggregation of detected headers showed that HSTS was implemented on six of seven websites (85.7%), while X-Content-Type-Options was identified on four websites (57.1%). In contrast, CSP, Referrer-Policy, and frame protection were detected on only two websites each (28.6%), while Permissions-Policy appeared on only one website (14.3%).

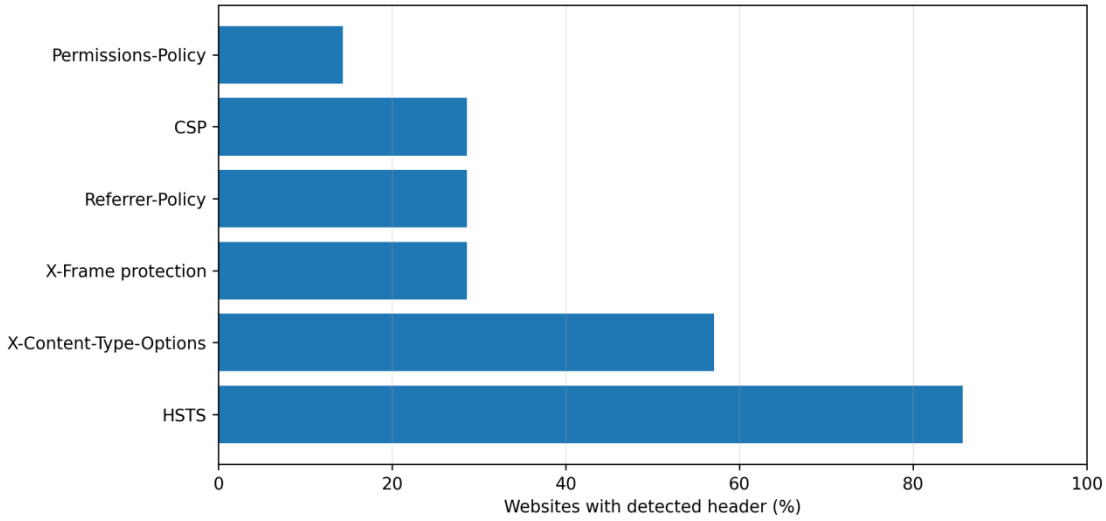


Figure 5. Security-header presence detected by SecurityHeaders.com

The comparison between SecurityHeaders.com and Observatory results highlights an important distinction between security-header deployment and security-header effectiveness. For example, M1 received an A grade from SecurityHeaders.com but obtained only Grade B from Observatory. Although several security controls were detected, Observatory identified weaknesses related to CSP configuration, Referrer-Policy implementation, and the absence of Subresource Integrity (SRI). A similar pattern was observed for M6. Although SecurityHeaders.com assigned Grade A, Observatory provided a lower score of 25 (Grade D-). The Observatory assessment identified problems related to CSP configuration, Referrer-Policy, HSTS recognition, X-Content-Type-Options, frame protection, and the absence of SRI. These differences demonstrate that the presence of a security header does not necessarily indicate effective protection when the configuration is incomplete, overly permissive, or incorrectly implemented.

Therefore, the results for RQ3 indicate that security evaluation should distinguish between header presence and configuration quality. A presence-based assessment is useful for identifying whether security mechanisms have been deployed, whereas configuration-sensitive evaluation provides deeper insight into whether these mechanisms provide meaningful protection. Consequently, security tools should be interpreted as complementary measurements rather than combined into a single security score because each tool evaluates different aspects of website security posture.

SSL/TLS Configuration

Compared with HTTP security-header implementation, transport-layer security demonstrated a stronger overall condition. All seven evaluated websites possessed valid certificates and supported modern TLS protocols, including TLS 1.2 and TLS 1.3. SSL Labs assigned the highest rating (A+) to M4 and M7, followed by A ratings for M3 and M5. M6 obtained

an A- rating, while M1 and M2 received B ratings. Therefore, five of the seven websites achieved A- or higher ratings, indicating relatively strong transport-security implementation. However, M1 and M2 still supported legacy TLS 1.0 and TLS 1.1 protocols. Although modern protocols were also available, continued support for outdated versions represents a remaining security consideration because older protocols may introduce compatibility and security risks [29].

The difference between HTTP security evaluation and TLS evaluation demonstrates that website security consists of multiple independent layers. TLS configuration primarily protects data transmission through encryption and certificate validation, whereas HTTP security headers provide browser-level protection against threats such as content injection, clickjacking, and unauthorized resource execution. The results demonstrate that a website can achieve strong TLS ratings while maintaining weaker browser security configurations. Therefore, HTTPS availability alone should not be considered sufficient evidence of comprehensive website security. For public-interest digital platforms such as mosque websites, security assessment should consider both encrypted communication and effective browser-level protection mechanisms.

Integrated Interpretation and Practical Recommendations

The integrated analysis demonstrates that website performance and security represent two distinct but interconnected dimensions of digital service quality. The results show that strong performance does not automatically correspond to strong security configuration, and conversely, websites with acceptable security indicators may still experience significant performance limitations. Masjid Tazkia (M4) represents the strongest performance case, achieving the highest Lighthouse Performance scores among the evaluated websites (86 on Mobile and 99 on Desktop). However, its security assessment remained moderate, with an Observatory Grade C and a lower SecurityHeaders.com rating. This finding indicates that technical optimization in one dimension does not necessarily reflect maturity in another dimension.

A similar pattern was observed for Masjid IPB (M6). The website recorded the lowest Mobile Performance score (31) and showed high CLS values, indicating performance and visual stability issues. Nevertheless, SecurityHeaders.com assigned a high grade based on detected security headers, while the configuration-sensitive Observatory assessment produced a lower score (Grade D-). This difference demonstrates that security-header presence alone may not represent effective security implementation. These findings support the importance of a multidimensional evaluation framework. Assessing only performance indicators may overlook security weaknesses, while evaluating only security mechanisms may fail to identify user-experience limitations. For public-interest digital platforms such as mosque websites, both responsive access and trustworthy digital delivery are necessary because users increasingly depend on websites for religious information, community services, donation activities, and institutional communication.

From a digital governance perspective, the results indicate that institutional websites should not be evaluated solely based on functional availability. Website maturity also involves the capability to provide reliable, accessible, and secure digital services. Performance optimization contributes to user confidence by reducing access barriers, while appropriate security configurations strengthen institutional accountability and protect users interacting with online services.

Table 8. Site-specific technical priorities derived from the measurements

Code	Primary technical issue	Priority recommendation
M1	Mobile field CWV fails; unsafe CSP/referrer policy; legacy TLS	Reduce mobile LCP/CLS; harden CSP and Referrer-Policy; consider SRI for applicable externally hosted static resources; retire TLS 1.0/1.1.
M2	Very high mobile lab LCP; CWV fails on both devices; legacy TLS	Prioritize media/rendering optimization; improve security-header baseline; retire TLS 1.0/1.1.
M3	Low desktop performance and extreme desktop CLS; Observatory F	Stabilize layout; deploy and validate baseline HTTP security headers; preserve modern TLS.

Code	Primary technical issue	Priority recommendation
M4	Excellent performance but only Observatory C / SecurityHeaders D	Preserve performance; strengthen CSP, frame/content-type/referrer/permissions policies.
M5	Mobile loading needs improvement; Observatory and SecurityHeaders F	Optimize mobile LCP; repair/expand HTTP hardening while maintaining strong TLS.
M6	Lowest mobile performance; high CLS; headers present but unsafe/unrecognized	Improve mobile loading/layout; correct CSP, HSTS, content-type, frame, and referrer configuration.
M7	Very slow mobile loading; weak HTTP header posture	Optimize image/resource delivery; add and validate CSP, frame, referrer, and permissions controls.

The recommendations derived from Table 8 emphasize three main improvement priorities. First, mobile performance optimization should become a primary focus, particularly for M2, M6, and M7, because these websites demonstrated substantial weaknesses in loading-related metrics. Improvements should focus on reducing unnecessary resource loading, optimizing media delivery, improving rendering efficiency, and minimizing factors that negatively affect LCP and Speed Index. Second, security improvements should prioritize configuration quality rather than only increasing the number of deployed security headers. CSP, Referrer-Policy, frame protection, and other browser-level controls should be reviewed and configured according to secure implementation practices. The findings demonstrate that incorrectly configured security mechanisms may provide limited protection despite appearing active.

Third, transport security modernization remains necessary for websites that still support outdated TLS versions. M1 and M2 should consider removing TLS 1.0 and TLS 1.1 support while maintaining compatibility with current TLS 1.2 and TLS 1.3 standards. Overall, the results indicate that improving mosque websites requires a balanced approach between technical performance, user experience, and security governance. A website that performs well but lacks appropriate security controls may reduce user trust, while a secure but poorly performing website may limit accessibility. Therefore, future improvement strategies should consider both dimensions simultaneously.

Limitations and Future Work

This study has several limitations that should be considered when interpreting the findings. First, the sample consisted of seven purposively selected mosque websites located on Java; therefore, the results should be interpreted as comparative technical case evidence rather than representative conclusions for all mosque websites in Indonesia. Second, the evaluation was limited to publicly accessible homepage pages, while other important service pages, such as donation systems, event pages, financial information pages, or administrative features, may demonstrate different performance and security characteristics. Third, the study relied on automated external tools, including Lighthouse, PageSpeed Insights, MDN Observatory, SecurityHeaders.com, and SSL Labs. Although repeated measurements and median aggregation were applied, the results may still be influenced by external factors such as server conditions, third-party resources, testing infrastructure, and website changes during the measurement period. In addition, the security evaluation was limited to non-invasive and externally observable indicators; therefore, the term security posture refers only to observable configuration practices and does not represent complete cybersecurity maturity, as application vulnerabilities, source-code issues, authentication mechanisms, access control, and server-level security were not examined.

Future research should expand the sample size by including mosque websites from different geographical regions and institutional categories to provide broader empirical evidence. Longitudinal measurements across multiple periods are also recommended to examine performance stability and security configuration changes over time. Future studies may further

evaluate additional website pages and user-oriented workflows to provide a more comprehensive understanding of digital service quality. Moreover, research conducted with appropriate authorization could incorporate deeper security assessments, including application security testing, dependency analysis, and configuration auditing. Future investigations may also examine how organizational factors, website management practices, institutional resources, and digital governance strategies influence the development of website performance, user trust, and security maturity.

CONCLUSIONS

The security findings reveal a distinct pattern. Although transport-layer security was generally strong, HTTP security-header implementation and configuration were less consistent. Differences between SecurityHeaders.com and the configuration-sensitive MDN HTTP Observatory further demonstrated that the presence of a security header should not automatically be interpreted as effective protection. Consequently, HTTPS status, header presence, and configuration quality should be treated as complementary rather than interchangeable security indicators. The principal contribution of this study is the use of an integrated evaluation framework that separates and cross-interprets laboratory performance, available real-user Core Web Vitals, HTTP security-header deployment and configuration quality, and TLS transport security. This approach provides a more informative technical profile than reliance on a single audit tool or technical dimension and offers practical evidence for prioritizing website maintenance and digital-service governance.

These conclusions should nevertheless be interpreted within the scope of the study. The seven websites were purposively selected and geographically concentrated on Java; therefore, the findings represent comparative case evidence and should not be generalized to Indonesian mosque websites as a whole. Future studies should examine larger and geographically diverse samples, conduct longitudinal measurements, evaluate service pages beyond the homepage, and, where explicit authorization is available, incorporate deeper application-security assessments. Such extensions would help determine whether the patterns identified in this study persist across the broader ecosystem of mosque and other public-interest digital platforms.

ACKNOWLEDGMENT

The author acknowledges the maintainers of Google PageSpeed Insights and Lighthouse, MDN HTTP Observatory, SecurityHeaders.com, and Qualys SSL Labs for providing publicly accessible tools used in this non-invasive technical evaluation.

AUTHOR CONTRIBUTION STATEMENT

T.A.P. and Suyono contributed to conceptualization, research design, website selection, data collection, validation, formal analysis, interpretation, visualization, and manuscript preparation. All authors reviewed the final manuscript and accept responsibility for the integrity and accuracy of the reported work.

AI DISCLOSURE STATEMENT

Generative artificial intelligence tools were used to assist with language refinement, manuscript organization, literature-search support, and verification of statistical calculations. The raw website measurements were collected by the author, and AI tools were not used to fabricate or alter research observations. All AI-assisted text, calculations, references, and interpretations were critically reviewed and remain the responsibility of the author.

REFERENCES

[1] D. Ardli, "Implementasi rapid application development pada sistem informasi layanan jamaah masjid berbasis website," Jurnal Informatika dan Teknik Elektro Terapan, vol. 14, no. 2, 2026, doi: 10.23960/jitet.v14i2.9356.
[2] R. Y. Fauzan, R. Wahyudi, M. Fahreza, R. R. E. Putra, and M. F. Falah, "Perancangan sistem informasi pengelolaan masjid berbasis website (Studi kasus: Masjid Al-Muttaqin Ketaping)," Jurnal Pustaka Data, vol. 4, no. 2, pp. 53–58, 2024, doi: 10.55382/jurnalpustakadata.v4i2.860.
[3] H. Herfandi and F. Hamdani, "Implementasi sistem informasi manajemen masjid berbasis web," INFORMAL: Informatics Journal, vol. 7, no. 3, p. 167, 2022, doi: 10.19184/isj.v7i3.34233.
[4] P. C. Verhoef et al., "Digital transformation: A multidisciplinary reflection and research agenda," Journal of Business Research, vol. 122, pp. 889–901, 2021, doi: 10.1016/j.jbusres.2019.09.022.
[5] G. Vial, "Understanding digital transformation: A review and a research agenda," The Journal of Strategic Information Systems, vol. 28, no. 2, pp. 118–144, 2019, doi: 10.1016/j.jsis.2019.01.003.
[6] Google Chrome Developers, "Lighthouse performance scoring," [Online]. Available: https://developer.chrome.com/docs/lighthouse/performance/performance-scoring.
[7] Google Web.dev, "How the Core Web Vitals metrics thresholds were defined," [Online]. Available: https://web.dev/articles/defining-core-web-vitals-thresholds.
[8] R. A. Farizqi and K. Haryono, "Evaluasi user experience pada sistem informasi manajemen masjid menggunakan metode usability testing (Studi kasus: Masjid Hidayatullah Kalasan)," Innovative: Journal of Social Science Research, vol. 4, no. 4, pp. 5724–5736, 2024, doi: 10.31004/innovative.v4i4.12653.
[9] A. Prambayun, M. A. Triawan, and F. Humam, "Analisis performa website karya usaha menggunakan Google Lighthouse dan GTmetrix," Jurnal Ilmu Komputer (JIK), vol. 10, no. 1, pp. 48–53, 2025, doi: 10.47007/komp.v10i01.9668.
[10] A. Setiawan and Y. Yamasari, "Evaluasi performa website Sistem Informasi Kesejahteraan Sosial (SIKS-NG) di Kelurahan Lembeyan Kulon Kabupaten Magetan dengan Google Lighthouse," Journal of Informatics and Computer Science (JINACS), vol. 7, no. 1, pp. 218–227, 2025, doi: 10.26740/jinacs.v7n01.p218-227.
[11] Syarifuddin and N. Annisa, "Analisis kualitas perangkat lunak pada website SARAH di Universitas Sari Mulia: Software quality analysis of the SARAH website at Universitas Sari Mulia," HOAQ (High Education of Organization Archive Quality): Jurnal Teknologi Informasi, vol. 17, no. 1, pp. 112–120, 2026, doi: 10.52972/hoaq.vol17no1.p112-120.
[12] T. A. Puspito, "Evaluation of website performance and usability using GTMetrix, usability testing, and System Usability Scale (SUS) methods," Jurnal Teknik Informatika, vol. 17, no. 2, pp. 162–170, 2024, doi: 10.15408/jti.v17i2.38530.
[13] S. Souders, High Performance Web Sites: Essential Knowledge for Frontend Engineers. Sebastopol, CA, USA: O'Reilly Media, 2007. ISBN: 978-0-596-52930-7.
[14] I. Grigorik, High Performance Browser Networking: What Every Web Developer Should Know about Networking and Web Performance. Sebastopol, CA, USA: O'Reilly Media, 2013. ISBN: 978-1-4493-4476-4.
[15] Google Web.dev, "How the Core Web Vitals metrics thresholds were defined," [Online]. Available: https://web.dev/articles/defining-core-web-vitals-thresholds.
[16] M. Al Khuwaitem and L. Hasan, "Clustering university websites based on usability metrics: Insights from web vitals analysis," Social Sciences & Humanities Open, vol. 13, p. 102608, 2026, doi: 10.1016/j.ssaho.2026.102608.
[17] J. Nielsen, Usability Engineering. San Francisco, CA, USA: Morgan Kaufmann Publishers, 1994. ISBN: 978-0-12-518406-9.

[18] F. F. Nah, "A study on tolerable waiting time: How long are Web users willing to wait?" Behaviour & Information Technology, vol. 23, no. 3, pp. 153–163, 2004, doi: 10.1080/01449290410001669914.
[19] W. J. Buchanan, S. Helme, and A. Woodward, "Analysis of the adoption of security headers in HTTP," IET Information Security, vol. 12, no. 2, pp. 118–126, 2018, doi: 10.1049/iet-ifs.2016.0621.
[20] A. Erden, "Modern web application security in practice: National-scale measurement and managerial insights from Türkiye," Computers & Security, vol. 164, p. 104847, 2026, doi: 10.1016/j.cose.2026.104847.
[21] A. Besmer, J. Watson, and D. Scibelli, "The death of the X-XSS-Protection header: A web security post-mortem," World Wide Web, vol. 29, no. 3, p. 23, 2026, doi: 10.1007/s11280-026-01410-1.
[22] Open Worldwide Application Security Project, "OWASP Top 10: The ten most critical web application security risks," [Online]. Available: https://owasp.org/www-project-top-ten/.
[23] N. Samarasinghe and M. Mannan, "Another look at TLS ecosystems in networked devices vs. web servers," Computers & Security, vol. 80, pp. 1–13, 2019, doi: 10.1016/j.cose.2018.09.001.
[24] I. Fragkiadakis, S. Gritzalis, and C. Lambrinoudakis, "Quantifying website privacy posture through technical and policy-based assessment," Future Internet, vol. 17, no. 10, p. 463, 2025, doi: 10.3390/fi17100463.
[25] E. Ciobanu, "Fast, stable, or credible? Mobile experience outcomes in certified luxury retail," Journal of Marketing Analytics, 2026, doi: 10.1057/s41270-026-00473-3.
[26] Google Chrome Developers, "Lighthouse performance scoring," [Online]. Available: https://developer.chrome.com/docs/lighthouse/performance/performance-scoring.
[27] A. Erden, "Modern web application security in practice: National-scale measurement and managerial insights from Türkiye," Computers & Security, vol. 164, p. 104847, 2026, doi: 10.1016/j.cose.2026.104847.
[28] W. J. Buchanan, S. Helme, and A. Woodward, "Analysis of the adoption of security headers in HTTP," IET Information Security, vol. 12, no. 2, pp. 118–126, 2018, doi: 10.1049/iet-ifs.2016.0621.
[29] N. Samarasinghe and M. Mannan, "Another look at TLS ecosystems in networked devices vs. Web servers," Computers & Security, vol. 80, pp. 1–13, 2019, doi: 10.1016/j.cose.2018.09.001.
[30] D. Rey and M. Neuhäuser, "Wilcoxon-Signed-Rank Test," in International Encyclopedia of Statistical Science, M. Lovric, Ed. Berlin, Heidelberg: Springer, 2011, pp. 1658–1659, doi: 10.1007/978-3-642-04898-2_616.
[31] A. Prambayun, M. A. Triawan, and F. Humam, "Analisis performa website karya usaha menggunakan Google Lighthouse dan GTmetrix," Jurnal Ilmu Komputer (JIK), vol. 10, no. 1, pp. 48–53, 2025, doi: 10.47007/komp.v10i01.9668.
[32] A. Setiawan and Y. Yamasari, "Evaluasi performa website Sistem Informasi Kesejahteraan Sosial (SIKS-NG) di Kelurahan Lembeyan Kulon Kabupaten Magetan dengan Google Lighthouse," JINACS, vol. 7, no. 1, pp. 218–227, 2025, doi: 10.26740/jinacs.v7n01.p218-227.
[33] Syarifuddin and N. Annisa, "Analisis kualitas perangkat lunak pada website SARAH di Universitas Sari Mulia: Software quality analysis of the SARAH website at Universitas Sari Mulia," HOAQ, vol. 17, no. 1, pp. 112–120, 2026, doi: 10.52972/hoaq.vol17no1.p112-120.
[34] M. Al Khuwaitem and L. Hasan, "Clustering university websites based on usability metrics: Insights from web vitals analysis," Social Sciences & Humanities Open, vol. 13, p. 102608, 2026, doi: 10.1016/j.ssaho.2026.102608.

[35] A. Besmer, J. Watson, and D. Scibelli, "The death of the X-XSS-Protection header: A web security post-mortem," World Wide Web, vol. 29, no. 3, p. 23, 2026, doi: 10.1007/s11280-026-01410-1.
[36] L. Waheed and A. Alazab, "Measuring baseline web security posture: Tier-1 HTTP security header adoption in the Maldives and the WSHS-B governance metric," Future Internet, vol. 18, no. 6, p. 313, 2026, doi: 10.3390/fi18060313.
[37] I. Fragkiadakis, S. Gritzalis, and C. Lambrinoudakis, "Quantifying website privacy posture through technical and policy-based assessment," Future Internet, vol. 17, no. 10, p. 463, 2025, doi: 10.3390/fi17100463.