



# THAISE: A Web Security Assessment Framework and Empirical Study of 126 Thai Higher Education Institutions

Tuul Triyason<sup>1</sup>

## ABSTRACT

The security of university websites is a vital but often overlooked issue, especially in developing countries. This work introduces THAISE (Thai Higher Education Institutions Security Evaluator), a system created to measure and score the web security levels of Thai universities. THAISE assesses seven key areas, including TLS configuration, certificate validity, and security headers such as HTTP Strict Transport Security (HSTS) and Content Security Policy (CSP). These factors are combined into a single Web Security Score (WSS). We used this framework to evaluate all 126 institutions under the Ministry of Higher Education, Science, Research and Innovation (MHESI). Our findings established a national baseline with an average score of 55.9. To ensure accuracy, we compared our results with industry tools like SecurityHeaders.com and Qualys SSL Labs, which showed consistent alignment. The results highlighted that Content Security Policy (CSP) is the most significant weakness, as 92.1% of universities failed to use it. Interestingly, exploratory analysis did not identify statistically significant associations between WSS and institutional budget per student, enrolment size, international ranking status, or Reinventing University group classification in the analyzed dataset. These findings suggest that web security posture may depend less on institutional resources or prestige than on deliberate configuration practices, though further research is needed to confirm this interpretation. These insights offer important directions for national cybersecurity policies in Thai higher education.

## Article information:

**Keywords:** Web Security Assessment, Higher Education Institutions, Content Security Policy, HTTPS, Security Headers, Thailand

## Article history:

Received: April 17, 2026

Revised: June 10, 2026

Accepted: July 6, 2026

Published: July 18, 2026

(Online)

DOI: 10.37936/ecti-cit.2026203.267289

## 1. INTRODUCTION

Higher education institutions (HEIs) have become increasingly attractive targets for cyber adversaries. The 2025 Verizon Data Breach Investigations Report recorded 3,336 cybersecurity incidents and 927 confirmed data disclosures in the educational services sector, with external actors responsible for 62% of attacks, of which 59% were carried out by organized criminal groups [1]. The consequences of such breaches are substantial: data breach costs in the higher education sector averaged USD 3.7 million in 2023, and universities face an estimated 2,300 cyberattacks per week globally [2]. These figures reflect the inherent value of university digital assets, including large volumes of student and staff personally identifiable information (PII), institutional credentials, and research data. In Thailand, the Personal Data Pro-

tection Act B.E. 2562 (PDPA) imposes legal obligations on all organizations handling personal data [3], making the web security posture of HEIs a matter of both operational and regulatory concern.

Despite the severity of the threat landscape, the web application layer remains much more exposed relative to lower-level network infrastructure. Large-scale empirical studies consistently report low adoption of fundamental HTTP security headers across the web: an analysis of 3,195 globally popular websites found that 55.66% received a failing security grade [4], while a survey of the top one million websites similarly revealed widespread absence of headers such as Content Security Policy (CSP) and HTTP Strict Transport Security (HSTS) [5]. Unlike operating systems and network appliances, which benefit from systematic vendor patching cycles, web applications are frequently developed under budget and time

<sup>1</sup>The author is with the School of Information Technology, King Mongkut University of Technology Thonburi, Bangkok, Thailand, Email: [tuul.tri@sit.kmutt.ac.th](mailto:tuul.tri@sit.kmutt.ac.th)

constraints, outsourced to third-party vendors, and subsequently maintained without dedicated security oversight, creating persistent misconfigurations that are both easy to introduce and difficult to detect.

Prior work examining the web security posture of HEIs has been largely confined to specific national contexts. Barreto *et al.* assessed web-related security practices among higher education institutions in Poland, identifying significant gaps in HTTPS configuration and security header adoption [6]. However, no equivalent study has established a systematic, national-scale empirical baseline for HEIs in Southeast Asia or Thailand specifically. Thai public universities face compounding structural challenges that motivate such a study: ongoing shortages of technical security staff, state budget allocations subject to lengthy procurement cycles across 126 institutions registered under the Ministry of Higher Education, Science, Research and Innovation (MHESI), and fragmented governance structures that make coordinated security improvements difficult to implement. These conditions suggest that institution-level web security posture may diverge substantially from Thailand's strong national cybersecurity standing, reflected in its ranking of 7th globally in the ITU Global Cybersecurity Index 2024 with a score of 99.22 [7].

This paper presents THAISE (Thai Higher Education Institutions Security Evaluator), a systematic web security assessment framework and its empirical application across all 126 MHESI-registered HEIs. The contributions of this work are fourfold: (1) a reproducible, standards-grounded framework that aggregates seven security dimensions, each anchored to RFC, NIST, or OWASP guidance, into a weighted Web Security Score (WSS); (2) a national empirical baseline for Thai HEI web security posture (mean WSS = 55.9, SD = 13.8); (3) external validation of the WSS against SecurityHeaders.com and Qualys SSL Labs; and (4) an exploratory analysis examining whether institutional factors commonly cited in Thai public policy discourse, including budget per student, enrolment size, international ranking status, and Reinventing University group classification, predict security outcomes. The exploratory analysis addresses four research questions: RQ1: Is there a significant association between budget per student and WSS among public institutions? RQ2: Do THE WUR-ranked institutions demonstrate significantly higher WSS than unranked institutions? RQ3: Is there a significant association between enrolment size and WSS? RQ4: Is there a significant difference in WSS across Reinventing University groups G1, G2, and G3? The remainder of this paper is organized as follows: Section 2 reviews related work; Section 3 describes the THAISE framework design; Section 4 details the dataset and methodology; Section 5 presents results; Section 6 discusses findings and implications; and Section 7 concludes with directions for future

work.

## 2. RELATED WORK

Large-scale empirical measurement of web security has demonstrated that fundamental security misconfigurations are pervasive across the global web. Lavrenovs and Melón conducted one of the most comprehensive baseline studies to date, analyzing HTTP security response headers across the Alexa top one million websites and finding widespread absence of security-critical headers including CSP and HSTS [5]. More recently, Kishnani and Das assessed 3,195 globally popular websites using the Mozilla Observatory and found that 55.66% received a failing security grade, indicating that weak HTTP header implementation remains an unresolved problem at scale [4]. The persistence of this weakness is particularly pronounced for CSP: Weissbacher *et al.* identified that CSP was deployed in enforcement mode by fewer than 1% of the Alexa Top 100 websites, attributing low adoption to the complexity of constructing and maintaining effective policies [8]. Subsequent work by Weichselbaum *et al.* further revealed that even among sites that do deploy CSP, 94.72% of policies contain allowlist-based bypasses that render the protection largely ineffective [9]. Collectively, these studies establish that security header misconfiguration is not an isolated phenomenon but a systemic condition across web infrastructure of all scales.

Research specifically examining cybersecurity in higher education has approached the problem primarily through risk management and policy lenses. Ulven and Wangen conducted a systematic review of cybersecurity risks in HEIs, synthesizing twelve years of literature and concluding that empirical research on the subject is scarce, with few studies providing quantitative measurement of actual security posture [10]. Fouad examined HEI cybersecurity as both an institutional risk and a national policy challenge, arguing that the peculiarities of universities as targets arising from open access cultures, large transient user populations, and decentralized governance create structural vulnerabilities that are frequently overlooked in policy discourse [11]. At the level of web infrastructure specifically, Barreto *et al.* assessed web-related security practices among higher education institutions in Poland, identifying significant gaps in HTTPS configuration and security header adoption and demonstrating that institutional web security posture can diverge substantially from an institution's broader IT governance maturity [6]. Beyond Europe, Barreto *et al.* subsequently extended their evaluation to 400 German HEIs in a two-wave study conducted across 2023 and 2025, finding that CSP adoption remained universally weak and HSTS configurations were classified as inadequate in the majority of institutions [12]. The same research group earlier assessed HTTPS and DNSSEC adop-

tion among Brazilian HEIs, demonstrating that insecure web protocol configurations are not confined to any single national context but represent a systemic condition across HEI ecosystems in multiple regions [13]. Collectively, these studies establish that empirical HEI web security measurement is an emerging but geographically narrow field, with no equivalent national-scale study conducted for Southeast Asia or Thailand prior to the present work. Table 1 summarizes the scope, method, and key limitations of prior studies most directly relevant to the present work, organized to highlight the cumulative gap that THAISE addresses.

**Table 1:** Summary of prior web security measurement and HEI-focused studies.

| Ref.      | Scope                                       | Method                                                 | Key Limitation                                                       |
|-----------|---------------------------------------------|--------------------------------------------------------|----------------------------------------------------------------------|
| [5]       | Top 1M websites (general web)               | Automated HTTP header analysis                         | No HEI context; no weighted scoring                                  |
| [4]       | 3,195 globally popular websites             | Mozilla Observatory grading                            | No HEI focus; no institutional factor analysis                       |
| [10]      | HEI cybersecurity risks (systematic review) | Literature review                                      | No empirical web measurement                                         |
| [11]      | HEI cybersecurity policy                    | Policy and risk analysis                               | No empirical web measurement; qualitative only                       |
| [6]       | HEIs in Poland                              | HTTPS and header assessment                            | Single national context; no composite score                          |
| [13]      | HEIs in Brazil                              | HTTPS and DNSSEC assessment                            | Limited to protocol layer; no multi-dimensional scoring              |
| [12]      | 400 HEIs in Germany (two-wave)              | Web standards evaluation                               | No weighted composite score; no institutional factor analysis        |
| This work | All 126 Thai HEIs (national)                | Weighted WSS framework + institutional factor analysis | Public institutions only for budget analysis; primary homepage scope |

The present work addresses this gap directly. While prior large-scale studies have characterized web security weaknesses across general web populations [4], [5], and prior HEI studies have identified the problem qualitatively or within narrow geographic scope [6], [10], [11], [12], [13] no study has combined a standards-grounded multi-dimensional scoring framework with complete national coverage of an HEI system in the region. THAISE is designed to fill this gap by providing a reproducible measurement instrument anchored to RFC, NIST, and OWASP standards, applied systematically across all 126 Thai HEIs registered with MHESI, yielding both an empirical national baseline and a reusable assessment methodology that can be extended to other national systems.

### 3. THE THAISE FRAMEWORK

This section describes the design of the THAISE framework, covering its overall architecture and scanning pipeline, the rationale for the selection and weighting of each security dimension, and the formula used to derive the Web Security Score.

#### 3.1 Framework Overview

THAISE (Thai Higher Education Institutions Security Evaluator) is an automated web security assessment framework designed to measure and score the security posture of institutional websites in a reproducible and standards-grounded manner. The framework operates as a multi-dimensional scanner that accepts an institutional homepage URL as input, evaluates it across seven independently weighted security dimensions, and produces a normalized Web Security Score (WSS) on a scale of 0 to 100. The overall pipeline is illustrated in Fig. 1.

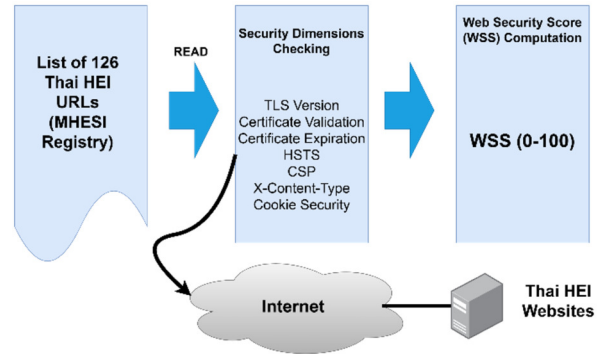


**Fig. 1:** The THAISE framework pipeline.

Each dimension is selected based on its direct measurability through passive HTTP and TLS inspection, its grounding in an established standard or industry guideline, and its relevance to the threat landscape facing public-facing web infrastructure. The scanner is implemented in Python and operates without requiring authentication or active exploitation, ensuring that the assessment is non-intrusive and deployable at national scale. Auto-save and resumable execution are supported to accommodate large-scale scanning campaigns across hundreds of institutions.

Although THAISE produces results that correlate moderately with existing tools such as SecurityHeaders.com and Qualys SSL Labs, it is not designed as a replacement for these services. Rather, THAISE differs in three key respects. First, it implements a transparent, standards-grounded weighting scheme that produces a single normalized score on a 0–100 scale, enabling direct quantitative comparison across institutions. Second, it is designed for reproducible, large-scale deployment without dependency on third-party APIs or rate limits, making it suitable for national-scale measurement campaigns. Third, the scoring rubric, dimension weights, and scanner

implementation are fully documented and open to scrutiny, allowing other researchers or national agencies to replicate, extend, or adapt the framework to different institutional populations or regulatory contexts.

### 3.2 Security Dimensions and Weighting

THAISE evaluates seven security dimensions, each assigned a weight reflecting its relative importance to overall web security posture. The dimensions, weights, maximum scoring levels, and grounding standards are summarized in Table 2. The weighting scheme follows a three-tier classification of security impact. Dimensions with weight 0.20, namely TLS Version, Certificate Validation, and Content Security Policy, are classified as high impact, as failures in these areas directly enable network-level interception, identity spoofing, and content injection attacks respectively, each constituting a fundamental breach of confidentiality or integrity. Dimensions with weight 0.15, namely HSTS and Cookie Security, are classified as medium impact; while their absence creates exploitable conditions, successful exploitation typically requires additional prerequisites such as active network positioning or authenticated sessions. Dimensions with weight 0.05, namely Certificate Expiration and X-Content-Type-Options, are classified as low impact; certificate expiration represents an operational lapse rather than a deliberate misconfiguration, and X-Content-Type-Options provides a narrow protective scope limited to MIME-sniffing attacks.

**Table 2:** THAISE security dimensions, weights, maximum scoring levels, and grounding standards.

| No. | Security Dimension     | Weight ( $w$ ) | Standard                 |
|-----|------------------------|----------------|--------------------------|
| 1   | TLS Version            | 0.20           | RFC 8996                 |
| 2   | Certificate Validation | 0.20           | RFC 5280                 |
| 3   | Certificate Expiration | 0.05           | CA/B Forum Baseline Req. |
| 4   | HSTS                   | 0.15           | NIST SP 800-44v2         |
| 5   | CSP                    | 0.20           | OWASP Secure Headers     |
| 6   | X-Content-Type-Options | 0.05           | OWASP Secure Headers     |
| 7   | Cookie Security        | 0.15           | OWASP Top 10 A07:2025    |
|     | <b>Total</b>           | <b>1.00</b>    |                          |

TLS Version ( $w = 0.20$ ). Transport Layer Security version compliance is assigned the highest weight alongside certificate validation and CSP, reflecting its role as the foundational encryption layer for all HTTPS communications. THAISE awards a maximum score for TLS 1.2 or TLS 1.3, a partial score for deprecated but still operational configurations, and zero for connections that fail entirely. This dimension is grounded in RFC 8996, which formally deprecates TLS 1.0 and TLS 1.1 [14]. It should be noted that THAISE evaluates TLS protocol version compliance

rather than cipher suite strength. While weak cipher suites can introduce vulnerabilities even under TLS 1.2, assessing cipher suite configuration requires active TLS handshake negotiation that varies by client implementation and cannot be reliably inferred from passive header inspection alone. Cipher suite analysis is therefore acknowledged as a limitation of the current framework and identified as a direction for future extension. Certificate Validation ( $w = 0.20$ ). A valid, trusted, and correctly chained X.509 certificate is a prerequisite for meaningful transport security. THAISE evaluates whether the presented certificate chains to a trusted root authority and is free from validation errors. The evaluation criteria follow RFC 5280 [15]. Certificate Expiration ( $w = 0.05$ ). While certificate expiration is a critical operational failure, it is assigned a lower weight because it represents a maintenance lapse rather than a deliberate security design choice. An expired certificate triggers a full score deduction for this dimension. Acceptable validity periods follow CA/Browser Forum Baseline Requirements [16]. HTTP Strict Transport Security ( $w = 0.15$ ). HSTS instructs browsers to enforce HTTPS connections and reject protocol downgrade attempts. THAISE evaluates the presence and configuration of the Strict-Transport-Security header, including the max-age directive. This dimension is grounded in NIST SP 800-44v2 guidance on HTTPS deployment [17].

Content Security Policy ( $w = 0.20$ ). CSP is the primary browser-side defence against content injection attacks including cross-site scripting (XSS). Despite its importance, CSP adoption has historically been low and frequently misconfigured [8], [9]. THAISE assigns the highest weight to this dimension alongside TLS and certificate validation, reflecting both the severity of the attacks CSP mitigates and the empirical finding that it represents the weakest dimension across the study population. THAISE evaluates CSP beyond mere header presence; a score of 2 is awarded only when the policy is deployed in enforcement mode (i.e., using the Content-Security-Policy header), while a report-only deployment (Content-Security-Policy-Report-Only) receives a partial score of 1, reflecting its lack of active protection. Evaluation criteria follow the OWASP Secure Headers Project [18]. X-Content-Type-Options ( $w = 0.05$ ). The X-Content-Type-Options: nosniff header prevents MIME-type sniffing attacks. Although its protective scope is narrower than CSP or HSTS, its implementation requires minimal effort, and its absence represents a straightforward configuration gap. This dimension is grounded in OWASP Secure Headers Project guidance [18]. Cookie Security ( $w = 0.15$ ). Session cookie misconfiguration is a persistent vulnerability class in web applications. THAISE evaluates the presence of the Secure and HttpOnly attributes on Set-Cookie headers. This dimension is grounded

in OWASP Top 10 A07:2025 (Identification and Authentication Failures) [19].

Several modern security headers not included in THAISE warrant explicit justification. X-Frame-Options, which mitigates clickjacking attacks, was excluded because its protective function is largely subsumed by the Content Security Policy frame-ancestors directive; institutions deploying CSP in enforcement mode with a frame-ancestors directive provide equivalent or stronger protection, making X-Frame-Options redundant in a framework that already assigns high weight to CSP. Permissions-Policy and Referrer-Policy were similarly excluded on the grounds that both headers govern feature access and referral metadata respectively, representing narrower protective scopes that are less directly tied to the confidentiality and integrity threats prioritised by THAISE. The seven dimensions selected collectively cover the foundational transport-layer and application-layer controls most consistently recommended across RFC, NIST, and OWASP guidance for public-facing web infrastructure. Incorporating additional headers such as Permissions-Policy and Referrer-Policy remains a direction for future framework extension.

### 3.3 Web Security Score Computation

The WSS for each institution is computed as a weighted proportion of the maximum achievable score across all dimensions, as defined in Equation (1):

$$WSS = \frac{\sum_{i=1}^7 w_i \times l_i}{\sum_{i=1}^7 w_i \times L_i} \times 100 \quad (1)$$

Where  $w_i$  is the weight assigned to dimension  $i$  as defined in Table 2,  $l_i$  is the score achieved at that dimension, and  $L_i$  is the maximum achievable level for dimension  $i$ . Each dimension is scored on an integer scale of 0 to  $L_i$ , where  $L_i = 2$  for six dimensions (TLS version, Certificate Validation, Certificate Expiration, HSTS, CSP, Cookie Security) and  $L_i = 1$  for X-Content-Type-Options, which is evaluated as a binary present/absent check. The denominator evaluates to a fixed maximum of 1.95, reflecting the sum of all weighted maximum levels across the seven dimensions. The resulting WSS is bounded on the interval  $[0, 100]$ , where 100 indicates full compliance across all dimensions and 0 indicates failure across all dimensions. This normalization ensures that scores are directly comparable across institutions regardless of which individual dimensions contribute to the total. The exact scoring criteria applied to each dimension are summarized in Table 3.

## 4. DATASET AND METHODOLOGY

This section describes the construction of the institutional dataset, the scanning procedure used to collect security measurements, the external validation

**Table 3:** Scoring rubric table.

| Security Dimension     | Score 0                         | Score 1                      | Score 2                          |
|------------------------|---------------------------------|------------------------------|----------------------------------|
| TLS Version            | Connection fails or TLS 1.0/SSL | TLS 1.1 or non-standard      | TLS 1.2 or TLS 1.3               |
| Certificate Validation | Chain error / untrusted CA      | Self-signed or partial chain | Valid, trusted, no errors        |
| Certificate Expiration | Expired                         | Expires within 30 days       | Valid, > 30 days remaining       |
| HSTS                   | Header absent                   | Present, max-age < 1 year    | Present, max-age ≥ 1 year        |
| CSP                    | Header absent                   | Present but report-only mode | Present in enforcement mode      |
| X-Content-Type-Options | Header absent                   | —                            | Present (nosniff)                |
| Cookie Security        | Secure and HttpOnly both absent | Only one flag present        | Both Secure and HttpOnly present |

approach, and the statistical methods applied to address the research questions.

### 4.1 Dataset Construction

The study population comprises all 126 higher education institutions registered with the Ministry of Higher Education, Science, Research and Innovation (MHESI) as of the 2023 academic year. Institutional URLs were collected manually from official MHESI registry records and verified through direct browser access to confirm that each URL resolves to the institution's primary homepage. The dataset composition by institutional subtype is summarized in Table 4.

**Table 4:** Dataset composition by institutional subtype.

| Subtype      | Count      | Percentages (%) |
|--------------|------------|-----------------|
| Private      | 44         | 34.9            |
| Rajabhat     | 38         | 30.2            |
| Autonomous   | 26         | 20.6            |
| State        | 9          | 7.1             |
| Rajamangala  | 9          | 7.1             |
| <b>Total</b> | <b>126</b> | <b>100.0</b>    |

In addition to the primary URL, the dataset records four institutional variables used in the exploratory analysis. Budget per student (THB) was derived from fiscal year 2569 (2026) government budget allocation documents for the 82 public institutions; private institutions were recorded as N/A as their budget data is not publicly disclosed. Enrolment figures were obtained from MHESI statistics for academic year 2569 (2026). International ranking status was encoded as a binary indicator based on the Times Higher Education World University Rankings

2026 (THE WUR 2026), which covers 21 Thai institutions in the dataset [20]. Reinventing University group classification (G1–G5) was assigned according to the Ministerial Regulation B.E. 2564, which categorizes public HEIs into five mission-oriented groups; 36 private institutions for which this classification does not apply were recorded as N/A.

Although the institutional URL registry reflects MHESI records from the 2023 academic year, all institutional variables, including budget allocation, enrolment figures, THE WUR ranking status, and Reinventing University classification, are drawn from the most recently available official sources at the time of the study. This temporal proximity is not expected to introduce material inconsistencies, as institutional characteristics such as mission classification and ranking status change infrequently over short intervals.

#### 4.2 Scanning Procedure

All 126 institutions were scanned using the THAISE scanner described in Section 3. Data collection was conducted between 7 and 14 April 2026 to ensure temporal consistency across the dataset, minimizing the effect of configuration changes that may occur over time. For each institution, the scanner establishes a TLS connection to the primary homepage URL, retrieves HTTP response headers, inspects the X.509 certificate chain, and evaluates cookie attributes from the Set-Cookie header where present. Institutions for which the primary URL was unreachable were retried up to three times before being flagged; all 126 institutions returned valid responses in the final dataset. The scanner implements auto-save functionality, recording results incrementally to prevent data loss in the event of interruption during large-scale runs.

#### 4.3 External Validation

To assess the construct validity of the WSS, scores were compared against three external web security tools: SecurityHeaders.com [21], Qualys SSL Labs [22], and Sucuri SiteCheck [23]. SecurityHeaders.com evaluates HTTP response headers and assigns a letter grade (A+ to F), which was converted to a numeric ordinal scale for correlation analysis. Qualys SSL Labs assesses TLS configuration quality and assigns a grade (A+ to F, T, or M), similarly converted to an ordinal scale; data were available for 108 of the 126 institutions, as Qualys declined to score sites with certificate trust failures. Sucuri SiteCheck scans for malware presence and domain blocklisting, assigning a risk score that reflects a fundamentally different security dimension from the WSS. Spearman rank correlation was selected over Pearson for all three comparisons because the external tools produce ordinal grades rather than continuous scores, making a rank-based measure the appropriate choice [24].

#### 4.4 Statistical Analysis

Four research questions guide the exploratory analysis of institutional factors associated with WSS. RQ1: Is there a significant association between budget per student and WSS among public institutions for which budget data are available ( $n = 82$ )? RQ2: Do THE WUR 2026-ranked institutions demonstrate significantly higher WSS than unranked institutions? RQ3: Is there a significant association between enrolment size and WSS across all 126 Thai institutions? RQ4: Is there a significant difference in WSS across Reinventing University groups G1, G2, and G3? Statistical test selection was guided by distributional properties of the data. WSS was assessed for normality using the Shapiro-Wilk test prior to analysis. For pairwise continuous associations (RQ1, RQ3), Spearman rank correlation was used as a non-parametric alternative to Pearson correlation given that normality could not be assumed for all variables. For the two-group comparison (RQ2), the Mann-Whitney U test was applied. For the multi-group comparison (RQ4), the Kruskal-Wallis test was used, with effect size reported as epsilon-squared ( $\epsilon^2$ ). All analyses were conducted in Python using the SciPy and penguin libraries. The significance threshold was set at  $\alpha = 0.05$  for all tests. To examine whether the institutional predictors jointly account for variance in WSS while controlling for potential confounding, a multiple linear regression model was estimated with WSS as the dependent variable. The predictor variables comprised: (1) log-transformed budget per student (natural logarithm of THB budget divided by enrolment), (2) log-transformed enrolment, (3) THE WUR 2026 ranking status (binary: 1 = ranked, 0 = unranked), and (4) Reinventing University group membership, encoded as dummy variables with G1 as the reference category. Continuous predictors were log-transformed prior to analysis to reduce the influence of right-skewed distributions. The analysis was restricted to the 79 of 82 public institutions for which complete predictor data were available, after excluding three institutions with missing Reinventing University classification; private institutions were excluded as their budget figures are not publicly disclosed. Ordinary Least Squares (OLS) regression was estimated using the statsmodels library. Three standard regression diagnostics were applied: residual normality was assessed using the Shapiro-Wilk test, homoscedasticity was assessed using the Breusch-Pagan test, and multicollinearity was assessed using Variance Inflation Factors (VIF). Heteroscedasticity-consistent standard errors (HC3) were additionally computed as a robustness check against potential violations of homoscedasticity.

### 5. RESULTS

This section presents the empirical findings of applying the THAISE framework across all 126 Thai

HEIs. Results are organized into four parts: the overall distribution of WSS, dimension-level analysis identifying specific security weaknesses, external validation of the WSS against third-party tools, and the outcomes of the four exploratory research questions.

### 5.1 Overall WSS Distribution

The distribution of WSS across the 126 institutions yielded a mean of 55.9 (SD = 13.8), a median of 61.5, and a range of 10.3 to 97.4, indicating substantial variation in web security posture across Thai HEIs. The distribution is illustrated in Fig. 2. The relatively wide gap between the mean and median suggests a left-skewed distribution in which a subset of institutions with very low scores pulls the mean downward. No institution achieved a perfect score of 100, and only a small number scored above 90, indicating that full compliance across all seven dimensions remains rare even among the strongest performers. At the lower end, the minimum score of 10.3 reflects near-total absence of security controls beyond basic TLS connectivity.

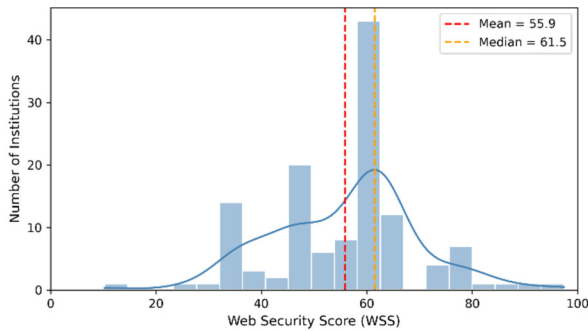


**Fig.2:** Distribution of Web Security Score (WSS) across 126 Thai HEIs.

### 5.2 Dimension-Level Analysis

Table 5 presents the failure rate for each of the seven security dimensions across the 126 institutions. TLS Version exhibited the lowest failure rate at 0.0%, confirming that all institutions in the dataset support at least a minimally acceptable TLS configuration. Certificate validation failures were limited to 7.9% of institutions, consistent with the overall strong TLS baseline.

In contrast, security header adoption was markedly poor. CSP emerged as the most critical weakness in the dataset, with 92.1% of institutions failing to implement it; a finding consistent with prior large-scale studies demonstrating low global CSP adoption [8], [9]. HSTS and X-Content-Type-Options exhibited similarly high failure rates of 75.4% and 74.6% respectively. Cookie security failures affected 40.5% of institutions, indicating that session management misconfiguration remains widespread despite its inclusion in OWASP Top 10 guidance [19].

**Table 5:** Dimension-level failure rates across 126 Thai HEIs.

| Security Dimension     | Weight ( $w$ ) | Failure Rate (%) |
|------------------------|----------------|------------------|
| TLS Version            | 0.20           | 0.0              |
| Certificate Validation | 0.20           | 7.9              |
| Certificate Expiration | 0.05           | 3.2              |
| HSTS                   | 0.15           | 75.4             |
| CSP                    | 0.20           | 92.1             |
| X-Content-Type-Options | 0.05           | 74.6             |
| Cookie Security        | 0.15           | 40.5             |

### 5.3 External Validation

Table 6 presents Spearman rank correlation coefficients between WSS and scores from three external tools. WSS showed moderate and statistically significant agreement with both SecurityHeaders.com ( $\rho = 0.510$ ,  $p < 0.001$ ,  $n = 126$ ) and Qualys SSL Labs ( $\rho = 0.483$ ,  $p < 0.001$ ,  $n = 108$ ), supporting the construct validity of the WSS as a meaningful measure of web security posture. The moderate rather than strong correlation reflects expected divergence arising from differences in scoring methodology, dimension coverage, and weighting schemes between THAISE and the external tools.

**Table 6:** Dimension-level failure rates across 126 Thai HEIs.

| External Tools      | n   | Spearman $\rho$ | p-value |
|---------------------|-----|-----------------|---------|
| SecurityHeaders.com | 126 | 0.510           | <0.001  |
| Qualys SSL Labs     | 108 | 0.483           | <0.001  |
| Sucuri SiteCheck    | 126 | 0.106           | 0.237   |

The correlation with Sucuri SiteCheck was negligible and non-significant ( $\rho = 0.106$ ,  $p = 0.237$ ,  $n = 126$ ). This result is not unexpected; because Sucuri measures malware presence and domain block-listing, which represent a fundamentally different security dimension from the configuration-based factors assessed by THAISE. The near-zero correlation thus shows that the WSS measures a different aspect of security, rather than undermining its validity.

### 5.4 Exploratory Analysis

Table 7 summarizes the results of the four research questions. All four analyses returned non-significant results at  $\alpha = 0.05$ , indicating that none of the institutional factors examined are significantly associated with WSS in this dataset.

#### 5.4.1 Bivariate Analyses (RQ1-RQ4)

RQ1: Budget per student vs. WSS. The Spearman correlation between budget per student (THB) and WSS among the 82 public institutions yielded  $\rho = 0.070$  ( $p = 0.534$ ), indicating no meaningful association between financial resource allocation and web security posture.

**Table 7:** Exploratory analysis results (RQ1-RQ4).

| RQ                  | Test           | Stat.                   | p-value |
|---------------------|----------------|-------------------------|---------|
| RQ1: Budget/student | Spearman       | $\rho = 0.070$          | 0.534   |
| RQ2: THE ranking    | Mann-Whitney   | $d = 0.186$             | 0.316   |
| RQ3: Enrolment      | Spearman       | $\rho = 0.032$          | 0.720   |
| RQ4: Reinventing    | Kruskal-Wallis | $\varepsilon^2 = 0.012$ | 0.242   |

RQ2: THE WUR 2026 ranking status vs. WSS. The Mann-Whitney U test comparing WSS between the 21 THE-ranked institutions and the 105 unranked institutions returned  $p = 0.316$ , with a negligible effect size (Cohen's  $d = 0.186$ ). The sample size imbalance between the two groups (1:5 ratio) warrants caution in interpreting this result; a post-hoc power analysis indicated that the test had limited statistical power (approximately 0.25) to detect a small effect at  $\alpha = 0.05$ , given the ranked group size of  $n = 21$ . Accordingly, the non-significant result should be interpreted as insufficient evidence to confirm an association rather than as evidence of absence.

RQ3: Enrolment size vs. WSS. The Spearman correlation between enrolments and WSS across all 126 institutions yielded  $\rho = 0.032$  ( $p = 0.720$ ), indicating no association between institutional size and security posture.

RQ4: Reinventing University group vs. WSS. The Kruskal-Wallis test comparing WSS across groups G1 ( $n = 15$ ), G2 ( $n = 16$ ), and G3 ( $n = 43$ ) returned  $p = 0.242$  with a negligible effect size ( $\varepsilon^2 = 0.012$ ), indicating no significant difference in WSS across mission-oriented institutional classifications.

#### 5.4.2 Multivariate Regression Analysis

To complement the bivariate analyses reported in Section 5.4.1 and address the possibility that institutional predictors jointly or interactively explain variance in WSS, a multiple linear regression model was estimated across the 79 public institutions for which complete predictor data were available. Table 8 presents the regression coefficients, HC3-corrected standard errors, and corresponding p-values for all predictors.

The overall model was not statistically significant ( $F = 0.799$ ,  $p = 0.590$ ), with an  $R^2$  of 0.093 and an adjusted  $R^2$  of 0.003, indicating that the full set of institutional predictors collectively explains a negligible proportion of variance in WSS. No individual predictor reached conventional significance under HC3-corrected standard errors: log-transformed budget per student ( $\beta = 10.065$ ,  $SE = 5.869$ ,  $p = 0.086$ ), log-transformed enrolment ( $\beta = 7.765$ ,  $SE = 4.881$ ,  $p = 0.112$ ), THE WUR ranking status ( $\beta = -11.157$ ,  $SE = 7.899$ ,  $p = 0.158$ ), and all Reinventing University group dummy variables (all  $p \geq 0.548$ ). Regression diagnostics confirmed that model assumptions were adequately satisfied: residuals were approximately normally distributed (Shapiro-Wilk  $W = 0.978$ ,  $p = 0.193$ ), no significant heteroscedasticity was detected

**Table 8:** Multiple linear regression results predicting WSS from institutional characteristics ( $N = 79$ , HC3-robust standard errors).

| Predictor                | $\beta$  | SE (HC3) | z      | p-value | VIF  |
|--------------------------|----------|----------|--------|---------|------|
| Constant                 | -126.240 | 107.214  | -1.177 | 0.239   | -    |
| Log budget per student   | 10.065   | 5.869    | 1.715  | 0.086   | 4.42 |
| Log enrolment            | 7.765    | 4.881    | 1.591  | 0.112   | 5.69 |
| The WUR ranked (binary)  | -11.157  | 7.899    | -1.412 | 0.158   | 4.00 |
| Reinventing G2 (ref: G1) | -2.931   | 6.898    | -0.425 | 0.671   | 2.81 |
| Reinventing G3 (ref: G1) | -2.383   | 6.994    | -0.341 | 0.733   | 5.32 |
| Reinventing G4 (ref: G1) | -14.321  | 23.835   | -0.601 | 0.548   | 1.40 |
| Reinventing G5 (ref: G1) | -3.762   | 9.399    | -0.400 | 0.689   | 2.53 |

(Breusch-Pagan LM = 3.034,  $p = 0.882$ ), and all VIF values were below 6.0, indicating that multicollinearity was not a concern (Table 8). These results corroborate and extend the bivariate findings reported for RQ1–RQ4. Even when all institutional predictors are considered jointly and potential confounding is controlled, no significant association with WSS is detected. The near-zero adjusted  $R^2$  further indicates that the model explains virtually no variance in web security posture beyond chance, reinforcing the interpretation that institutional resource and classification variables are not meaningful predictors of web security outcomes in this dataset.

## 6. DISCUSSION

This section interprets the empirical findings presented in Section 5 in the context of prior work and the broader landscape of web security in higher education. The discussion addresses three interconnected themes: the current state of web security posture among Thai HEIs, the relationship between institutional characteristics and security outcomes, and the implications of these findings for policy and practice.

### 6.1 Web Security Posture of Thai HEIs

The national mean WSS of 55.9 indicates that Thai HEIs, on average, satisfy approximately half of the security controls evaluated by THAISE, suggesting a security posture that is functional at the transport layer but substantially incomplete at the application layer. The strong TLS baseline, which is reflected in a 0.0% failure rate, is consistent with the broader global trend of near-universal HTTPS adoption driven by browser enforcement policies and free certificate authority services. However, this transport-layer strength masks significant weaknesses at the header configuration level, which require deliberate and informed implementation rather than automated infrastructure provisioning.

The most critical finding is the CSP failure rate

of 92.1%, which substantially exceeds the already-low global adoption rates documented in prior large-scale studies [8], [9] and aligns with the pattern of poor CSP implementation observed in European HEI contexts [6]. CSP misconfiguration is particularly concerning because it represents the primary browser-side defence against XSS attacks, which remain among the most prevalent web application vulnerabilities [19]. The similarly high failure rates for HSTS (75.4%) and X-Content-Type-Options (74.6%) further indicate that security header configuration is not being treated as a standard component of web deployment practice across Thai HEIs. Collectively, these findings suggest that the web security gap in Thai higher education is concentrated in deliberate, policy-driven controls rather than in foundational infrastructure.

The moderate external validation results ( $\rho = 0.510$  with SecurityHeaders.com and  $\rho = 0.483$  with Qualys SSL Labs) confirm that the WSS captures a meaningful and externally consistent signal of security posture. The divergence from perfect correlation is expected given methodological differences between THAISE and the external tools in dimension coverage, weighting, and scoring granularity. The near-zero correlation with Sucuri SiteCheck ( $\rho = 0.106$ ,  $p = 0.237$ ) corroborates the discriminant validity of the WSS, as Sucuri measures malware and blocklisting status, which is conceptually orthogonal to the configuration-based dimensions assessed by THAISE.

## 6.2 Security as Intentional Practice

The consistent lack of statistically significant results across all four research questions is a key finding. Together, RQ1 and RQ3 show that neither an institution's budget nor its student population size can predict its web security level. RQ2 demonstrates that international ranking, which usually reflects research quality and reputation, provides no measurable advantage in security. Similarly, RQ4 shows that an institution's specific mission under the Reinventing University framework does not influence its security outcomes. These results collectively suggest that web security is not simply a matter of having more resources. Instead, they support the view by Fouad [11] that cybersecurity gaps in higher education may reflect structural and governance factors rather than financial constraints alone. This conclusion is further supported by the multivariate regression analysis (Section 5.4.2), which confirmed that these predictors remain non-significant even when examined jointly, with the full model explaining less than 1% of WSS variance after adjustment.

This interpretation is further supported by how WSS scores are distributed. High-scoring and low-scoring institutions are found in every category, including autonomous, Rajabhat, and private universities. This implies that these results are consistent

with the interpretation that security posture may depend less on institutional resources or prestige and more on deliberate configuration practices and governance routines, though further qualitative or longitudinal research is needed to test this explanation directly. For national policy, these findings suggest that providing more budget alone may not be enough. Instead, more effective ways to improve national security would include setting mandatory configuration standards, offering centralized technical advice, or conducting regular automated audits.

## 6.3 Implications and Limitations

The THAISE framework is a useful tool that can be used in other contexts. Its scoring formula (WSS), the factors it measures, and its weighting system are all clearly explained so that other researchers or government agencies can use the same method. They could apply it to different groups of organizations or use it to track security improvements over time. Additionally, the automated scanner is designed to work on a large scale with very little human help, which makes it ideal for national monitoring programs.

However, this study has some limitations. First, the measurements represent a point-in-time snapshot. Since web security settings can change quickly, these findings show the state of Thai university websites at the time of the scan, not a long-term trend. Second, THAISE assessed only the primary homepage of each institution. Other parts of their systems, such as student portals or administrative information systems, may exhibit different security profiles. Third, the budget information for the first research question only included public universities and was based on general government funding rather than the money spent on IT security. Finally, while the results for the research questions were consistent, they should be seen as an initial exploration. This is because some groups in the study, such as top-ranked universities or specific categories under the Reinventing University framework, had a relatively small number of institutions available for analysis.

## 7. CONCLUSION

This paper presented THAISE, a systematic web security assessment framework designed to measure and score the web security posture of higher education institutions through automated, passive inspection of seven standards-grounded security dimensions. Applying THAISE across all 126 Thai HEIs registered with MHESI established the first national empirical baseline for this population, yielding a mean WSS of 55.9 (SD = 13.8, range: 10.3–97.4). The framework demonstrated moderate external validity against SecurityHeaders.com ( $\rho = 0.510$ ,  $p < 0.001$ ) and Qualys SSL Labs ( $\rho = 0.483$ ,  $p < 0.001$ ), confirming that the WSS captures a meaningful and

externally consistent signal of institutional web security posture.

The most critical empirical finding is the widespread failure to implement Content Security Policy, with 92.1% of institutions scoring zero on this dimension. Combined with high failure rates for HSTS (75.4%) and X-Content-Type-Options (74.6%), the results indicate that the web security gap in Thai higher education is concentrated in deliberate, policy-driven controls rather than in foundational transport-layer infrastructure, where Thai HEIs perform comparatively well. Exploratory analysis revealed no significant association between WSS and institutional budget per student, enrolment size, international ranking status, or Reinventing University group classification, suggesting that web security posture may depend less on institutional resources or prestige than on deliberate configuration practices, though further research is needed to confirm this interpretation.

These findings carry direct implications for national cybersecurity policy in Thai higher education. The absence of resource-based predictors suggests that targeted interventions such as mandatory web security configuration standards, centralized technical guidance from MHESI or NCSA, and periodic automated auditing are likely to be more effective levers for raising the national baseline than budget increases alone. The THAISE framework is fully documented and reproducible, making it easy to re-run periodically to track improvement over time or for adaptation to HEI in other countries.

Future work should address the current limitations of the study through several directions. Periodic measurement using THAISE would enable tracking of security posture trends over time and evaluation of the impact of policy interventions. Expanding the scan scope beyond primary homepages to include subdomains and student-facing portals would provide a more comprehensive institutional security profile. Incorporating additional dimensions such as DNSSEC adoption and HTTP/2 or HTTP/3 configuration would extend the framework's coverage of the modern web security landscape. Finally, qualitative investigation into the governance and procurement processes of high-scoring institutions could illuminate the specific organizational practices that underpin strong web security performance, complementing the quantitative baseline established by this study.

## ACKNOWLEDGEMENT

The authors would like to thank three undergraduate students of the Information Technology programme for their contributions to data collection and software development during the initial phase of the THAISE project: Mr. Nitisak Kangkhan, Mr. Pongsapat Charoencharuskul, and Mr. Phatcharadol Thangplub.

## AUTHOR CONTRIBUTIONS

Conceptualization, methodology, software, validation, formal analysis, investigation, data curation, writing (original draft preparation), writing (review and editing), visualization, supervision, and funding acquisition, T.T. The author has read and agreed to the published version of the manuscript.

## References

- [1] Verizon, "2025 Data Breach Investigations Report," Verizon Communications Inc., 2025. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>
- [2] S. Grajek and the 2023–2024 EDUCAUSE Top 10 Panel, "2024 EDUCAUSE Top 10: Cybersecurity as a Core Competency," *EDUCAUSE*, 2023. [Online]. Available: <https://er.educause.edu/articles/2023/10/2024-educause-top-10-1-cybersecurity-as-a-core-competency>
- [3] Royal Thai Government, *Personal Data Protection Act B.E. 2562*, 2019. Accessed: Apr. 13, 2026. [Online]. Available: <https://ratchakitcha.soc.go.th/documents/17082307.pdf>
- [4] U. Kishnani and S. Das, "Securing the Web: Analysis of HTTP Security Headers in Popular Global Websites," in *Information Systems Security*, V. T. Patil, R. Krishnan, and R. K. Shyamasundar, Eds. Cham, Switzerland: Springer Nature Switzerland, pp. 87–106, 2025.
- [5] A. Lavrenovs and F. J. R. Melón, "HTTP security headers analysis of top one million websites," in *Proceedings of the 2018 10th International Conference on Cyber Conflict (CyCon)*, pp. 345–370, May 2018.
- [6] J. Barreto, P. Rutecka, K. Cicha and P. Pinto, "The Status and Management of Web-Related Security at Higher Education Institutions in Poland," in *Proceedings of the 10th International Conference on Information Systems Security and Privacy*, Rome, Italy: SCITEPRESS - Science and Technology Publications, pp. 789–798, 2024.
- [7] International Telecommunication Union, "Global Cybersecurity Index 2024," International Telecommunication Union (ITU), Jun. 2024. Accessed: Apr. 13, 2026. [Online]. Available: <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>
- [8] M. Weissbacher, T. Lauinger and W. Robertson, "Why Is CSP Failing? Trends and Challenges in CSP Adoption," in *Research in Attacks, Intrusions and Defenses*, Lecture Notes in Computer Science, vol. 8688, pp. 212–233, 2014.
- [9] L. Weichselbaum, M. Spagnuolo, S. Lekies and A. Janc, "CSP Is Dead, Long Live CSP! On the Insecurity of Whitelists and the Future of

- Content Security Policy,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*, New York, NY, USA: Association for Computing Machinery, pp. 1376–1387, Oct. 2016.
- [10] J. B. Ulven and G. Wangen, “A Systematic Review of Cybersecurity Risks in Higher Education,” *Future Internet*, vol. 13, no. 2, p. 39, Feb. 2021.
- [11] N. S. Fouad, “Securing higher education against cyberthreats: from an institutional risk to a national policy challenge,” *Journal of Cyber Policy*, vol. 6, no. 2, pp. 137–154, May 2021.
- [12] J. Barreto, S. Neef and P. Pinto, “A Two-Wave Evaluation of the Web-Related Security Standards Implemented by Higher Education Institutions in Germany,” in *IEEE Access*, vol. 14, pp. 41552–41578, 2026.
- [13] J. Barreto, H. Almeida and P. Pinto, “An Overview of HTTPS and DNSSEC Services Adoption in Higher Education Institutions in Brazil,” *2023 25th International Conference on Advanced Communication Technology (ICACT)*, Pyeongchang, Korea, Republic of, pp. 180–185, 2023.
- [14] K. Moriarty and S. Farrell, “Deprecating TLS 1.0 and TLS 1.1,” *Internet Engineering Task Force, Request for Comments RFC 8996*, Mar. 2021.
- [15] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell and D. Cooper, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” *Internet Engineering Task Force, Request for Comments RFC 5280*, May 2008.
- [16] “Baseline Requirements,” CA/Browser Forum. Accessed: Apr. 13, 2026. [Online]. Available: <https://cabforum.org/working-groups/server/baseline-requirements/>
- [17] M. Tracy, W. Jansen, K. Scarfone and T. Winograd, “Guidelines on Securing Public Web Servers,” *National Institute of Standards and Technology, NIST Special Publication (SP) 800-44 Version 2*, Oct. 2007.
- [18] “OWASP Secure Headers Project — OWASP Foundation.” Accessed: Apr. 13, 2026. [Online]. Available: <https://owasp.org/www-project-secure-headers/>
- [19] “OWASP Top 10:2025.” Accessed: Apr. 13, 2026. [Online]. Available: <https://owasp.org/Top10/2025/>
- [20] “World University Rankings 2026,” Times Higher Education (THE). Accessed: Apr. 16, 2026. [Online]. Available: <https://www.timeshighereducation.com/world-university-rankings/latest/world-ranking>
- [21] S. Helme, “Analyse your HTTP response headers.” Accessed: Apr. 16, 2026. [Online]. Available: <https://securityheaders.com/>
- [22] “SSL Server Test (Powered by Qualys SSL Labs).” Accessed: Apr. 16, 2026. [Online]. Available: <https://www.ssllabs.com/ssltest/>
- [23] sucuri.net, “Sucuri Security,” Sucuri Security. Accessed: Apr. 16, 2026. [Online]. Available: <https://sitecheck.sucuri.net>
- [24] A. Field, *Discovering Statistics Using IBM SPSS Statistics*. London, U.K.: SAGE Publications Ltd, 2024.



**Tuul Triyason** is an Assistant Professor at the School of Information Technology, King Mongkut's University of Technology Thonburi (KMUTT), Thailand. He holds a B.Sc. in Physics from Mahidol University and M.Sc. and Ph.D. degrees in Information Technology from KMUTT. His research and teaching focus on cybersecurity and computer networks. He serves as an IT consultant to multiple Thai government

agencies, including the Thai Customs Department, the Department of Land Transport, the Office of the Attorney General, and the Department of Foreign Trade. His research interests include public sector IT procurement policy, digital infrastructure governance, and anti-corruption in government IT investment.