INTERNATIONAL JOURNAL OF SOCIAL SCIENCE, EDUCATIONAL, ECONOMICS, AGRICULTURE RESEARCH AND TECHNOLOGY (IJSET) | ISSN (E): 2827-766X
Website: https://ijset.org/ | Volumes 5 No. 7 (2026)

SECURITY ANALYSIS OF SUPERAPPS HERITAGE USING OWASP AND ISSAF

Abdul Rozak Nurdiansyah[1], Setiadi Yazid[2]
[123]Fakultas Ilmu Komputer, Universitas Indonesia, Jakarta, Indonesia
E-mail: abdul.rozak3@ui.ac.id* , author_2@mail.com[2]

Received: 22/04/2026 | **Revised** : 01/05/2026 | **Accepted:** 15/05/2026 | **Published** :26/05/2026

Abstract

Pusaka Super Apps is an integrated digital platform owned by the Ministry of Religious Affairs of the Republic of Indonesia (Kemenag) that provides various religious services for millions of users. Along with the increasing reliance on government digital services, threats to information system security are becoming more complex. This study conducts a security assessment of the Pusaka Super Apps web application (https://pusaka-v3.kemenag.go.id) using two complementary frameworks, namely OWASP Top 10 2025 and the Information Systems Security Assessment Framework (ISSAF). The research method is qualitative descriptive with black-box testing and gray-box testing approaches that include the stages of reconnaissance, scanning, enumeration, vulnerability assessment, and impact analysis. The results of the study identified several medium vulnerabilities, including Content Security Policy Header Not Set, Missing Anti-clickjacking Header, and Missing Sub Resource Integrity Attribute. This study provides structured remediation recommendations and serves as a contribution to efforts in strengthening cyber security for government applications in Indonesia.

Keywords: *Cybersecurity, OWASP Top 10, ISSAF, Pusaka Super Apps, Ministry of Religion, Penetration Testing, Vulnerability Assessment*

INTRODUCTION

Digital technology has become commonplace, influencing and changing the way society operates. As a result, governments around the world have prioritized digital transformation to improve the efficiency of public services for their citizens (Desai & Manoharan, 2024) [1] . In Indonesia itself, digital transformation in the public sector is carried out through the implementation of the Electronic-Based Government System (SPBE). SPBE is very important to realize clean, effective, transparent, and accountable governance, as well as quality and reliable public services. In the implementation of digital transformation, there are several factors that drive success, especially in the process of digitizing public services in Indonesia, including public service innovation, human resource capabilities, and work experience (Sisilianingsih et al., 2023) [2] . Cybersecurity has become an important issue for individuals, small organizations, and large organizations from various sectors (Budiyanto & Mabruri, 2025) [3] . A total of 330,527,636 anomalous traffic in Indonesia in 2024 indicates a high level of suspicious activity and potential cyber threats that can cause a decrease in device and network performance, sensitive data leaks, and a decrease in public trust in an organization (BSSN, 2024) [4] . Various cyber attacks that occurred in the public sector in Indonesia have had a significant material and economic impact (Alfi et al., 2023) [5] . Global losses due to cybercrime are expected to continue to increase to reach $ 12.2 trillion per year in 2031, with a growth rate of around 2.5 percent per year (Cybersecurity Ventures, 2025) [6] . The high frequency and complexity of cyber attacks indicate that Indonesia is also one of the main targets of cyber attacks that attempt to disrupt vital infrastructure, steal sensitive information, and influence public opinion (Wulandari et al., 2025) [7] . Collaboration and coordination between the government and the private sector are key to ensuring the success of cyber defense strategies across various sectors (Adma et al., 2023) [8] . 56,128,160 exposure data findings were recorded, impacting 461 agencies in Indonesia.

The Ministry of Religious Affairs (Kemenag) responded to the trend of digital transformation in the public sector by launching the Religious Service Center (Pusaka) Kemenag Superapps. First launched on November 1, 2022, Pusaka Superapps is now in version 3.0, released on November 1, 2024. Its aim is to integrate all religious services under the Ministry's jurisdiction, making it easier for the public to access services. Pusaka Superapps currently serves millions of users accessing services such as marriage management, madrasah data management,

waqf information, and various other religious administration services. The concentration of services in a single platform creates a high-value target for cybercriminals. Incidents of cyberattacks on government digital infrastructure are projected to increase by 23% by 2023, with web applications being the primary attack vector. Vulnerabilities in systems like Pusaka Superapps not only have the potential to cause service disruptions but can also result in the leakage of sensitive personal data of citizens, including National Identity Numbers (NIK), financial information, marriage-related information, and family data.

In implementing SPBE itself, the Ministry of Religious Affairs has enacted the Information Security Management System (Ministerial Decree of Religious Affairs, 2023) [9] . This regulation establishes technical standards and SPBE security procedures that require every web-based application to be released to the public to undergo a security testing phase. Because these testing instruments are generally only implemented temporarily at launch and not through regular monitoring, a detailed and structured methodological framework is required. Adopting standardized testing methods is crucial to ensure the consistency, validity, and accuracy of vulnerability identification results before the system is fully operational in a public environment.

This study integrates two security frameworks, the OWASP framework and the ISSAF framework, as a comprehensive information system security assessment methodology. The combination of these two frameworks enables analysis that not only identifies technical vulnerabilities but also evaluates them in the context of organizational risk and operational impact. The objective of this study is to identify security vulnerabilities in the Pusaka Superapps platform based on OWASP categories. Then, assess the risk level of each vulnerability using the ISSAF methodology and scoring scheme and formulate measurable improvement recommendations for the organization.

LITERATURE REVIEW

OWASP

OWASP, short for Open Web Application Security Project, is an international organization focused on application security. Its primary goal is to improve software security by providing resources, guidelines, and tools that developers, security professionals, and organizations can use to identify security vulnerabilities in web applications (OWASP Foundation, 2026) [10] . Among the various instruments it has developed, OWASP ZAP (Zed Attack Proxy) is a popular penetration testing tool. This tool also allows users to perform fuzzing attacks and manual web system searches (Nurelasari & Al Farabi, 2024) [11] . OWASP ZAP has an intuitive graphical user interface (GUI), making it easy to use by developers and security researchers. Furthermore, OWASP ZAP also supports automation through a command-line interface, allowing integration with existing security testing processes. The organization also compiles the OWASP Top 10, a list of the most frequently encountered and potentially dangerous web application security vulnerabilities. This list is updated regularly and provides guidance on web application security vulnerabilities. OWASP also holds local conferences and events in various countries to promote web application security awareness and share knowledge on best practices for addressing security vulnerabilities. It also provides the necessary resources and tools. The latest version (OWASP Foundation, 2025) [12] , released in 2025, identifies ten key risk categories:

1. A01:2025, Broken Access Control, Access control implements policies to prevent users from acting beyond their defined permissions. Failure to do so typically results in unauthorized disclosure of information, modification or destruction of all data, or the execution of business functions beyond the user's capabilities.
2. A02:2025, Security Misconfiguration, Security misconfiguration is a condition where a system, application, or cloud service is configured incorrectly from a security perspective, resulting in a vulnerability gap.
3. A03:2025, Software Supply Chain Failures, A software supply chain failure is a failure or other compromise in the process of creating, distributing, or updating software. These failures are often caused by vulnerabilities or malicious changes in third-party code, tools, or other dependencies that the system relies on.
4. A04:2025, Cryptographic Failures, In general, all data in transit must be encrypted at the transport layer (OSI Layer 4). Previous bottlenecks, such as CPU performance and private key/certificate management, have now been overcome thanks to CPU instructions specifically designed to speed up the encryption process.
5. A05:2025, Injection, In general, an injection vulnerability is a weakness in an application that allows untrusted user input to be sent to a command interpreter (such as a browser, database, or command line), causing the interpreter to execute some of the input as if it were a legitimate command.
6. A06:2025, Insecure Design, Insecure design is a broad category that represents a variety of different weaknesses, expressed as missing or ineffective design controls. There is a distinction between insecure design and insecure implementation. OWASP distinguishes between design flaws and implementation defects for a

reason; they have different root causes, occur at different times in the development process, and have different remediation steps. A secure design can still have implementation flaws that lead to exploitable vulnerabilities. Conversely, an insecure design cannot be fixed by even a perfect implementation, because the necessary security controls were never built in to defend the system from a particular attack.

7. A07:2025, Authentication Failures, When an attacker is able to trick the system into recognizing an invalid or false user as a legitimate user, this vulnerability is known as Identification and Authentication Failure.
8. A08:2025, Software or Data Integrity Failures, Software and data integrity failures relate to code and infrastructure that does not provide protection against the introduction of invalid or untrusted code or data, but is perceived as valid and trustworthy.
9. A09:2025, Security Logging & Alerting Failures , Without logging and monitoring, attacks and security breaches will go undetected. Furthermore, without an alerting system, it will be extremely difficult to respond quickly and effectively when a security incident occurs. Deficiencies in logging, continuous monitoring, detection, and alerting to initiate an active response can occur at any time.
10. A10:2025, Mishandling of Exceptional Conditions, Mishandling of exceptional conditions in software occurs when a program fails to prevent, detect, and respond to unusual and unexpected situations, ultimately causing the system to crash, behave erratically, and sometimes introduce security holes. This can involve one or more of the following three failures: the application does not prevent the unusual situation from occurring, the application does not identify the situation as it is occurring, and/or the application responds poorly or does not respond at all after the situation occurs.

Information Systems Security Assessment Framework (ISSAF)

ISSAF is a comprehensive framework developed by the Open Information Systems Security Group (OISSG) to provide structured guidance in conducting penetration testing and information system security testing. (Dirgahayu et al., 2015; Riandhanu, 2022) [13] [14] . ISSAF divides the process into three testing phases. The phases in this method include Information Gathering, which is the process of obtaining information from a website whose security will be checked. This is then continued with the Assessment phase, which is an examination of website security holes that are vulnerable to hacking issues. The final phase of this method is CleanUp and Destroy. ISSAF's advantage over similar frameworks such as PTES lies in its holistic approach that considers managerial and technical aspects simultaneously.

Government Web Application Security in Indonesia

Indonesian cybersecurity regulations have undergone significant developments with the issuance of Presidential Regulation No. 82 of 2022 concerning the Protection of Vital Information Infrastructure and BSSN Regulation No. 1 of 2024 concerning Cyber Incident Management. These regulations require government electronic system administrators to conduct regular security testing. Despite these regulations, implementation in the field still faces various challenges. Cybersecurity incidents affecting government agencies are caused by known but unaddressed vulnerabilities. This gap between vulnerability identification and remediation is a structural problem that needs to be addressed through a systematic approach based on a standards framework.

RESEARCH METHODS

Research Design

The research was conducted with Pusaka Superapps as the test target. This study used a descriptive qualitative approach with an interpretive paradigm in the cybersecurity domain. The qualitative approach was chosen because this study aims to deeply understand the characteristics of vulnerabilities, their risk context within the government service ecosystem, and their potential implications. Data were collected through direct observation of the target system and analysis of technical documentation. The research was conducted using black-box and grey-box testing methods. Black-box testing is conducted without internal system knowledge to simulate the perspective of an external attacker, while grey-box testing utilizes limited publicly available information for more targeted testing. All testing is conducted in a controlled environment and does not disrupt service availability for real users.

Research Methodology Framework

The research began with an initiation phase, which included problem formulation and research objectives. Next, a literature review was conducted to strengthen the theoretical foundation, along with relevant data collection.

The core phase of the research integrated the ISSAF stages with the OWASP Top 10 2025 testing categories, followed by analysis of the results and discussion, documented in a report using the following research flow:

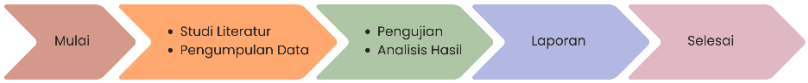

Figure 1Research flow

Literature Study and Data Collection

A literature review of the literature provided the necessary information for the Pusaka Superapps website analysis, including scientific books, research journals, research articles, and technology documentation. Data collection was conducted in three stages. First, publicly available information regarding the target infrastructure was gathered, including DNS record analysis and website metadata inspection. Second, active analysis was limited to examining HTTP header configurations, server response analysis, and mapping the application navigation structure using the OWASP ZAP tool. Third, publicly available technical documentation related to the platform's technology was reviewed. The ethical boundaries of the research were strictly defined. The research did not actively exploit discovered vulnerabilities, access or extract user data, or modify system configurations. The focus of the research was on identifying and documenting potential vulnerabilities, not on demonstrating exploits.

RESULTS AND DISCUSSION

At this stage, information is searched for on the website to be researched, namely Pusaka superapps, with activities explained in the following table:

Table 1Phase Integration Matrix and OWASP Categories

ISSAF Phase	Activity	OWASP Linkages
Phase 1: Information Gathering	Information gathering with *Netcraft, and Nmap*	-
Phase 2: Assessment	Perform *vulnerability scanning* and simulate security hole exploitation.	A01:2025 - A10:2025
Phase 3: Cleanup and destroy	System cleaning of test files (*cleanup*), document destruction (*destroy*), and preparation of reporting documentation.	As per findings (A01:2025 - A10:2025)

Pusaka Superapps V3 is the third version of the Ministry of Religion's digital platform built on a modern microservices architecture.

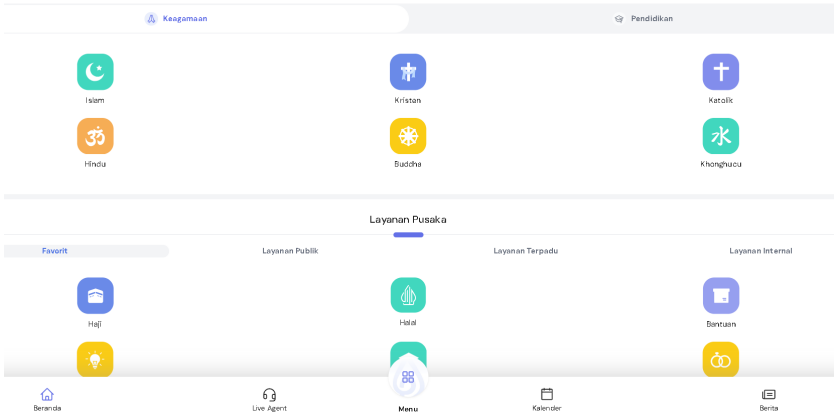

Figure 2Pusaka Superapps (https://pusaka-v3.kemenag.go.id/)

At the information gathering stage, information searches were carried out related to the website being studied. The results of the Pusaka superapps website netcraft are presented in the following table:

Table 2Findings with netcraft

No.	Findings	Description
1.	Domain	kemenag.go.id
2.	Nameserver	dns.kemenag.go.id
3.	Domain registrar	pandi.id
4.	Top Level Domain	Indonesia (.go.id)
5.	IP Address	8.215.xxx.xxx

Next, a port scan is performed to determine which ports are open. The results of the port scan on the Pusaka Superapps website are shown in the table below.

Table 3Port Scanning Results with nmap

Port	State	Service	Version
80/tcp	open	http	Nginx reverse proxy
443/tcp	open	http	httpd engine

Based on table 3, the scanning results using nmap obtained results regarding open ports, namely ports 80 and 443. Fingerprinting analysis and response header inspection, this platform uses modern JavaScript *framework- based web technology* for the frontend, with the backend configured behind a reverse proxy. This platform serves various user segments of the general public for religious services, the Ministry of Religious Affairs' State Civil Apparatus (ASN) for internal management, and partner institutions such as Islamic boarding schools and madrasas. It was identified that the platform uses various subdomains to separate different services, indicating an architecture that has implemented the principle of separation of concerns. However, higher architectural complexity also means a wider attack surface and a greater potential for misconfiguration.

Vulnerability Findings Based on OWASP Top 10

The system vulnerability identification stage in this study utilizes OWASP ZAP software. The above steps represent the Spider process, or the identification of all indexes. After completing and obtaining the indexes from the target website, the system automatically proceeds to the next stage, the Active Scan, shown in Figure 3. The purpose of this step is to identify security vulnerabilities on the target website.

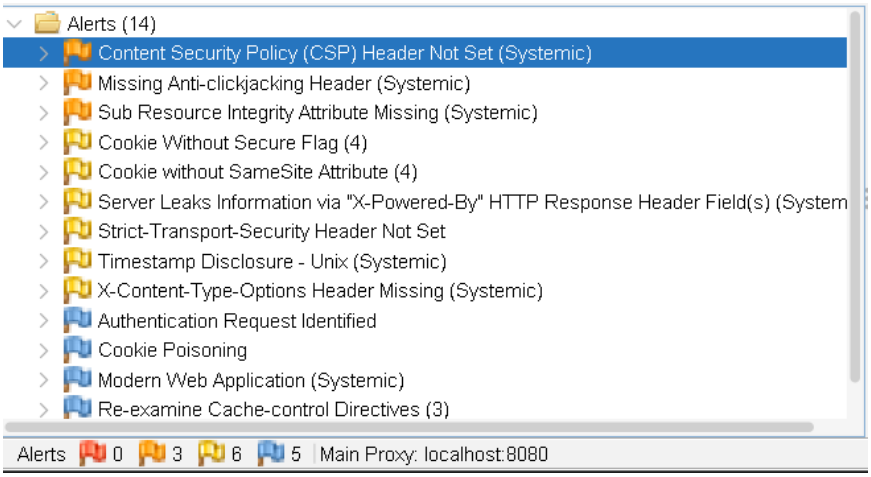

Figure 3Results of the OWASP ZAP Scanning Process

The image is the result of the scanning process on the Pusaka superapps *website* , the scan resulted in 14 vulnerabilities that were successfully identified. With details of 3 *medium* , 6 *low* and 5 *informational* . The *medium category* will be the focus of categorization and *reporting* using OWASP TOP 10. The findings from the scanning process are then grouped based on the OWASP Top 10 category. To measure the magnitude of the potential impact of further attacks on the website, a more in-depth risk evaluation is carried out using the OWASP Risk Rating method.

Table 4Categorization of vulnerabilities against OWASP TOP 10

No	Vulnerability	**OWASP Categories**
1.	Content Security Policy (CSP) Header Not Set	A02:2025
2.	Missing Anti-clickjacking Header	A02:2025
3.	Sub Resource Integrity Attribute Missing	A08:2025

Table 4 lists the vulnerabilities that have been categorized based on the OWASP TOP 10, and then these vulnerabilities are assessed using the OWASP *Risk Rating method* . *Risk Rating* has four stages in determining *likelihood* and *impact* : threat agent factors, vulnerability factors, technical impact , *and business impact* (Aryanti et al., 2021) .

Table 5Factor Scoring

Risk Rating	Factor 1	Factor 2	Factor 3	Factor 4	Total	Risk
threat agent factor	7	3	5	2	4.25	Medium
vulnerability factors	7	2	2	3	3.5	Medium
technical impact	6	2	3	7	4.5	Medium
business impact	1	4	5	7	4.25	Medium

The assumed score results based on the OWASP *Risk Rating provisions* are calculated to determine the value of *the threat agent factor, vulnerability factors, technical impact, and business impact.* The overall score can be seen in Table 5. Meanwhile, formulas (1) and (2) are the formulas for calculating the overall likelihood and impact scores.

$$\text{Likelihood} = \frac{\text{Threat Agent Factor} + \text{Vulnerability Factors}}{2} \quad (1)$$

$$\text{Impact} = \frac{\text{Technical Impact} + \text{Business Impact}}{2} \quad (2)$$

The assessment yielded an overall *likelihood* and *impact score* for the Pusaka Superapps information system of 3.875 *and* 4.375, respectively . Both risks are considered *medium* , indicating a low impact on the *website* . After going through the scanning and vulnerability assessment phase, all security vulnerabilities found in the target system were documented in detail. The mapping of these vulnerabilities into the 2025 OWASP Top 10 categories, risk levels (*ratings*), and recommended technical solutions are outlined in Table 6 below.

Table 6Vulnerabilities based on Owasp Top 10:2025

No	Rating	Vulnerability	OWASP Categories	Solution
1.	Medium	Content Security Policy (CSP) Header Not Set	A02:2025	Configure the web server to add a content security policy so that the browser only loads content from trusted sources.
2.	Medium	Missing Anti-clickjacking Header	A02:2025	Configure the web server to add security headers that prevent web pages from being loaded inside frames or iframes from other sites.
3.	Medium	Sub Resource Integrity Attribute Missing	A08:2025	Ensure that every external resource loaded is equipped with integrity verification so that the loaded content cannot be manipulated by third parties.

Testing with the ISSAF method

Information Gathering

This phase is the initial stage of gathering information from the target. This phase consists of *information gathering* and *network mapping* . The results of the initial information gathering on the target domain using the *Whois method* are summarized into network parameter aspects. The technical data identified during this initial testing phase can be seen in Table 7 below.

Table 7Information Gathering with Whois

No.	Findings	Description
1.	Registrar	Ministry of Communication and Digital of the Republic of Indonesia IANA ID: 1 URL: domain.go.id Whois Server: —
2.	Registrar Status	autoRenewPeriod
3.	Dates	5,847 days old Created on 2010-05-17 Expires on 2027-05-19 Updated on 2025-11-15
4.	Name Servers	DNS.KEMENAG.GO.ID (has 2 domains) DNS2.KEMENAG.GO.ID (has 2 domains) DNS3.KEMENAG.GO.ID (has 2 domains) DNS4.KEMENAG.GO.ID (has 2 domains)
5.	IP Address	103.xxx.xxx.xxx is hosted on a dedicated server
6.	**IP Location**	Greater Jakarta - Jakarta - Ministry of Religion (Kemenag)

Assessment

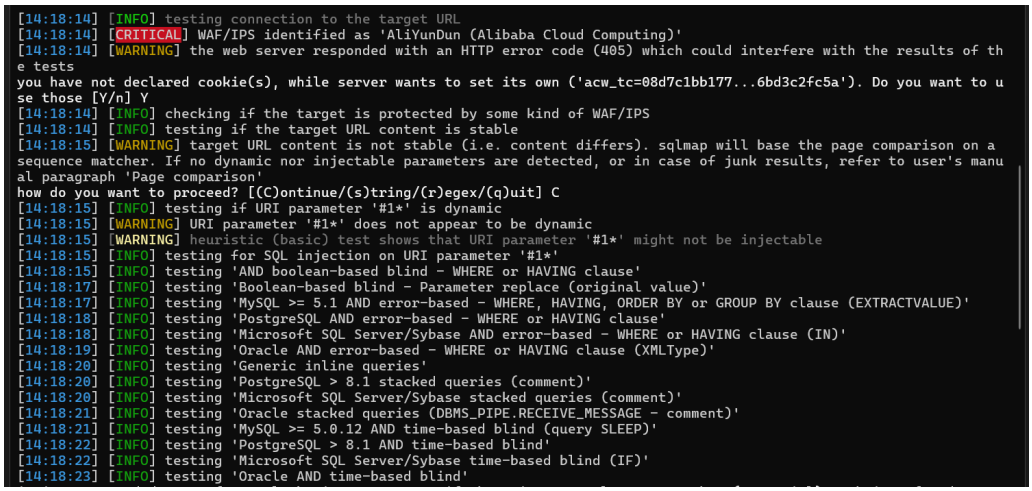

Figure 4SQLmap test results

Testing the injection security vulnerability on Pusaka superapps using SQLmap software, obtained analysis results that indicate that the target system has a solid level of defense. During the vulnerability assessment process, the test instrument successfully identified the presence of an active protection mechanism in the form of a Web Application Firewall / Intrusion Prevention System. In addition, the load loading test through a heuristic test on the URI parameter showed a not injectable status, accompanied by an HTTP Error 405 (Method Not Allowed) code response from the web server. It can be concluded that for category A05:2025, Injection on the OWASP Top 10 standard, the Pusaka website on the menu is in a protected condition due to restrictions on access methods and strict traffic filtering on the upstream side of the server network.

Cleanup and destroy

This phase is the final step after the entire testing process has been completed. At this stage, researchers ensure that all information from the testing process is permanently deleted from the target system. This cleanup and destruction of traces is mandatory to restore the web server to its original state and prevent new security vulnerabilities or residual artifacts that could be exploited by malicious parties.

DISCUSSION

The results of a vulnerability scan on the Pusaka Superapps website using the OWASP ZAP application showed 14 security vulnerabilities. Based on the threat impact, the findings consisted of 3 *Medium- level vulnerabilities, 6 Low*- level vulnerabilities , and 5 *Informational* category findings . The OWASP Top 10 method in

2025 is still ideal for use as a basis for conducting website security testing. Testing using the ISSAF framework with the SQL Injection technique using sqlmap was unsuccessful. This study has several limitations: First, the study limitations prevent verification of active exploitation, so some findings are indicative based on pattern analysis rather than full technical confirmation. Second, this study did not include testing of the backend infrastructure, databases, and internal APIs that are not accessible from the public interface. Potentially more critical vulnerabilities at this layer are outside the scope of the study. Third, the resulting security snapshot is temporary; the platform's security condition can change as the Ministry of Religious Affairs team updates the system. This limitation opens up the direction of further research that can be conducted with broader access, such as whitebox testing involving source code review, or verified penetration testing conducted with the official approval of the Ministry of Religious Affairs.

REFERENCES

[1] Desai, A., & Manoharan, A. P. (2024). Digital Transformation and Public Administration: The Impacts of India's Digital Public Infrastructure. In *International Journal of Public Administration* (Vol. 47, Issue 9, pp. 575–578). Routledge. https://doi.org/10.1080/01900692.2024.2350762
[2] Sisilianingsih, S., Purwandari, B., Eitiveni, I., Purwaningsih, M., & Korespondensi, P. (2023). ANALISIS FAKTOR TRANSFORMASI DIGITAL PELAYANAN PUBLIK PEMERINTAH DI ERA PANDEMI. https://doi.org/10.25126/jtiik2023107059
[3] Deny Budiyanto and Muhammad Mabruri, "PENTINGNYA KEAMANAN SIBER DALAM ERA DIGITAL:: TINJAUAN GLOBAL DAN KONDISI DI INDONESIA," Prosiding Seminar Nasional Sains Dan Teknologi "SainTek" 2, no. 1 (February 2025): 981–94, https://conference.ut.ac.id/index.php/saintek/article/view/5134
[4] Badan Siber dan Sandi Negara (BSSN), Lanskap Keamanan Siber Indonesia 2024 (2024).
[5] Muhammad Alfi, Ni Yundari, and Ahnaf Tsaqif, "Analisis Risiko Keamanan Siber Dalam Transformasi Digital Pelayanan Publik Di Indonesia," Jurnal Kajian Stratejik Ketahanan Nasional 6, no. 2 (December 2023): 1–11, https://doi.org/10.7454/jkskn.v6i2.10082.
[6] Cybersecurity Ventures, Cybersecurity Ventures Report on Cybercrime, November 25, 2025, https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime.
[7] Ria Wulandari, Priyanto Priyanto, and Afrizal Hendra, "The Indonesia's Cyber Security Strategy in the Face of Evolving Modern Warfare Threats," Formosa Journal of Applied Sciences 4, no. 2 (February 2025): 615–26, https://doi.org/10.55927/fjas.v4i2.5.
[8] Arinaldo Adma, Yusuf Surbakti, and Puspita Sari, "Transformasi Sistem Pertahanan Siber Indonesia Dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri Di Masa Depan," Jurnal Kajian Stratejik Ketahanan Nasional 6, no. 1 (June 2023): 1–14, https://doi.org/10.7454/jkskn.v6i1.10077.
[9] Keputusan Menteri Agama Republik Indonesia Nomor 412 Tahun 2023 Tentang Sistem Manajemen Keamanan Informasi.
[10] OWASP Foundation. (2026). About the OWASP Foundation. https://owasp.org/about/
[11]Nurelasari, E., & Al Farabi, D. G. (2024). Analisis keamanan sistem website menggunakan metode Open Web Application Security Project (OWASP) pada SIMANTEP.ID. JATI (Jurnal Mahasiswa Teknik Informatika), 8(3), 3049–3054
[12] OWASP Foundation. (2025). OWASP Top 10: 2025: The Ten Most Critical Web Application Security Risks. https://owasp.org/Top10/2025/0x00_2025-Introduction/
[13] R. T. Dirgahayu, Y. Prayudi, and A. Fajaryanto, "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," J. Ilm. NERO, vol. 1, no. 3, pp. 190–197, 2015, [Online]. Available: http://nero.trunojoyo.ac.id/index.php/nero/article/download/29/27
[14] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," J. Inf. dan Teknol., vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.
[15] Aryanti, D., Dan, N., & Utamajaya, J. N. (2021). ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA. Jurnal Nasional Indonesia, 1(3), 15–25