Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	1 1
Assignment title:	No repository 012
Submission title:	jurnal eng ver.pdf
File name:	jurnal_eng_ver.pdf
File size:	425.57K
Page count:	10
Word count:	6,132
Character count:	35,607
Submission date:	23-Jan-2025 04:26PM (UTC+0700)
Submission ID:	2569632617

JIKO (Jurnal Informatika dan Komputer) Accredited KEMENDIKBUD RISTEK, No.105/E/KPT/2022
Vol. x, No. x, April 2024, pp. x-x p-ISSN: 2614-8897
DOI: 10.33387/jiko e-ISSN: 2656-1948

SECURITY AND PERFORMANCE EVALUATION OF POST-DIVORCE WOMEN'S AND CHILDREN'S RIGHTS FUNDING APPLICATION USING OWASP TOP TEN AND ISO 25010:2023

Deta Oktariani[1], Ema Utami [2]

[1]Magister of Informatics, Universitas Amikom Yogyakarta
[2] Magister of Informatics, Universitas Amikom Yogyakarta
*Email: [1]detaoktariani@students.amikom.ac.id, [2]ema.u@amikom.ac.id
(Received: dd mmm yyyy, Revised: dd mmm yyyy, Accepted: dd mmm yyyy)

Abstract

Evaluating an information system from both performance and security aspects is crucial for anticipating and improving the quality of the information system. A High Religious Court in collaboration with the Provincial Government developed a web-based application to support one of its services, to monitor court decisions regarding alimony payments from former husbands to former wives and children in divorce cases involving civil servants. This is certainly very important because before the existence of this application, there were many complaints filed due to the non-payment of alimony. To ensure that the application runs in accordance with its purpose and that the data is secure, a comprehensive system evaluation is required. The main objective of this evaluation is to identify vulnerabilities and their mitigations, as well as to ensure that the functions in the application work as expected, so that the application's goals are achieved. To achieve this goal, this study uses the ISO 25010:2023 information system standard integrated with OWASP Top Ten to evaluate its security This study uses five ISO 25010:2023 characteristics selected according to the system's goals. The results show that the combination of ISO 25010:2023 and OWASP Top Ten effectively identifies vulnerabilities in the application's functions and security comprehensively. Overall, the functions in the application have run as expected, although there are still several things that need to be improved to enhance the quality and secure its data.
Keywords: *IT Audit, OWASP Top Ten, ISO, Security, Information System*

This is an open access article under the CC BY license.

**Corresponding Author: Author1*

1. INTRODUCTION

The rapid pace of digital transformation has led to an increasing adoption of information systems across various sectors, especially those closely tied to public services. The High Religious Court has leveraged information technology to improve its services by developing an electronic application that monitors the execution of funding for women's and children's rights post-divorce, specifically designed for civil servants. The application was designed to function as a monitoring mechanism that ensures divorced male civil servants comply with their obligations as stipulated in the religious court's ruling in response to the numerous complaints filed with relevant authorities concerning former husbands who default on their responsibilities.

There has been a growing trend of study on information system audits, driven by the escalating incidence of cyberattacks. A study conducted by [1] leveraged a combined OWASP Testing Guide and ISO 31000 approach for information system auditing. The study concentrated on assessing security risks via the OWASP Testing Guide, whereas ISO 31000 was applied for risk mitigation purposes.

Study [2] focuses on detecting Cross-Site Scripting (XSS) vulnerabilities using OWASP Security Shepherd, while research [3] targeted SQL Injection (SQLi) attacks using OWASP ZAP. The key difference between OWASP Security Shepherd and OWASP ZAP lies in their penetration testing approaches. OWASP Security Shepherd facilitates manual testing and OWASP ZAP conducts automated audits.

From a functional perspective, studies [4, 5, 6] have conducted evaluations using ISO 25010:2011. Study [4] utilized ISO 25010:2011 security characteristics to compare the security of paid password manager applications. In contrast, study [5, 6] employed ISO 25010:2011 for evaluating application quality. However, the difference lies in the methodology used:

1