

# EVALUATION OF DATA CONFIDENTIALITY SECURITY USING THE OWASP ON THE XYZ WEB APPLICATION

By

**I Komang Wahyu Ambara Putra, NIM 2215101055**

**Informatics Engineering Department**

**Computer Science Study Program**

## ABSTRACT

The XYZ Web Application manages sensitive academic and personal student data, making robust data confidentiality protections essential. This study evaluates the system's confidentiality controls using the Open Worldwide Application Security Project (OWASP) framework. Employing a Grey Box Testing approach based on the OWASP Web Security Testing Guide (WSTG) v4.2, the assessment focused on authentication, authorization, session management, and weak cryptography mechanisms. The OWASP Risk Rating methodology was utilized to assess the severity of discovered flaws. The evaluation identified 11 valid vulnerabilities: two Critical, six High, and three Medium risk. Mapped against the OWASP Top 10 2021, these vulnerabilities fall primarily under Identification and Authentication Failures and Broken Access Control. The findings reveal fundamental flaws in the system's business logic, specifically regarding identity verification and user privilege validation. Strategic remediation steps are provided to address these architectural weaknesses and secure the XYZ Web Application against unauthorized data access.

**Keywords:** Web Security, Data Confidentiality, OWASP WSTG, OWASP Top 10, OWASP Risk Rating, XYZ Web Application, Grey Box Testing.

# EVALUASI KEAMANAN KERAHASIAAN DATA MENGGUNAKAN OWASP PADA APLIKASI WEB XYZ

Oleh

**I Komang Wahyu Ambara Putra, NIM 2215101055**

**Jurusan Teknik Informatika**

**Program Studi Ilmu Komputer**

## ABSTRAK

Aplikasi Web XYZ mengelola data akademik dan pribadi siswa yang sensitif, sehingga perlindungan kerahasiaan data yang kuat sangat penting. Studi ini mengevaluasi kontrol kerahasiaan sistem menggunakan kerangka kerja *Open Worldwide Application Security Project* (OWASP). Dengan menggunakan pendekatan *Grey Box Testing* berdasarkan OWASP *Web Security Testing Guide* (WSTG) v4.2, penilaian difokuskan pada otentikasi, otorisasi, manajemen sesi, dan mekanisme kriptografi yang lemah. Metodologi OWASP *Risk Rating* digunakan untuk menilai tingkat keparahan kelemahan yang ditemukan. Evaluasi mengidentifikasi 11 kerentanan yang valid: dua Kritis, enam Tinggi, dan tiga risiko Sedang. Dipetakan terhadap OWASP *Top 10* 2021, kerentanan ini terutama termasuk dalam Kegagalan Identifikasi dan Otentikasi serta Kontrol Akses yang Rusak. Temuan tersebut mengungkapkan kelemahan mendasar dalam logika bisnis sistem, khususnya mengenai verifikasi identitas dan validasi hak akses pengguna. Langkah-langkah perbaikan strategis diberikan untuk mengatasi kelemahan arsitektur ini dan mengamankan Aplikasi Web XYZ dari akses data yang tidak sah.

**Kata Kunci:** Keamanan Web, Kerahasiaan Data, OWASP WSTG, OWASP *Top 10*, OWASP Risk Rating, Aplikasi Web XYZ, *Grey Box Testing*.