ABSTRAK

Judul : Pengujian Keamanan Aplikasi *Mobile* Berbasis Android Dengan Metode OWASP *Mobile Application Security Testing Guide* (MASTG) (Studi Kasus : PT PRIFAT TALENTA INDONESIA)
Nama : Mochamad Haviz Tasmara
Program Studi : Teknik Informatika

Aplikasi PRIFAT adalah aplikasi mobile berbasis android yang dikembangkan oleh PT PRIFAT TALENTA INDONESIA sebagai platform penyedia jasa instruktur/pengajaran. Aplikasi ini menyediakan beranekaragam jasa instruktur, mulai dari olahraga, musik, hingga kesenian. Dalam penggunaannya aplikasi PRIFAT meminta beberapa data pengguna untuk kebutuhan aplikasi dalam menyediakan platform jasa instruktur/pengajaran. Mengingat hal tersebut serangan terhadap aplikasi mobile berbasis android juga meningkat, bahkan tercatat terdapat 1.3 juta serangan siber pada aplikasi mobile di Indonesia dalam 3 tahun terakhir menurut data National Cyber Security Index (NCSI). Oleh karena itu perlu dilakukan pengujian keamanan aplikasi android untuk mengetahui kerentanan yang terdapat pada aplikasi android yang dapat mengurangi serangan siber dan kebocoran data. Pada penelitian ini dilakukan pengujian keamanan pada aplikasi PRIFAT berbasis android menggunakan metode OWASP Mobile Application Testing Guide (MASTG) yang terdiri dari 5 langkah yaitu preparation, intelligence gathering, mapping the application, exploitation, dan reporting. Pengujian akan dilakukan dengan menggunakan pendekatan gray-box dengan mengacu pada kerentanan berdasarkan OWAPS mobile top ten 2016. Berdasarkan hasil pengujian keamanan teridentifikasi tujuh kerentanan pada aplikasi PRIFAT. Rincian kerentanan yang ditemukan *insecure data storage(allow backup vulnerabillity dan temporary file vulnerability)* dengan kategori kerentanan *high* dan *medium*, *insecure communication* dengan kategori kerentanan *high*, *reverse engineering* dengan kategori kerentanan *high*, *OTP code on*

response leads to account takeover dengan kategori kerentanan *critical*, *bypass OTP code* dengan kategori kerentanan *high*, *Bruteforce OTP* dengan kategori kerentanan *high*, *no rate limit OTP code* dengan kategori kerentanan *none*. Kerentanan yang teridentifikasi sebagian besar berdampak pada hilangnya aspek *confidentiallity* mulai dari terungkapnya data sensitif pengguna hingga dapat mengambil alih akun dari pengguna lain. Berdasarkan kerentanan tersebut, diberikan rekomendasi keamanan berupa menerapkan *obfuscation* pada *source code*, melakukan enkripsi data pada *storage*, menerapkan limitasi pada saat melakukan *request* pada kode OTP, melakukan perbaikan pada kode dan logika aplikasi untuk mencegah adanya kerentanan.

Kata Kunci – pengujian keamanan, android, aplikasi *mobile, OWASP MASTG*

ABSTRACT

Tittle : *Penetration Testing of Android-based Mobile Applications with OWASP Mobile Application Security Testing Guide (MASTG) Method (Case Study: PT PRIFAT TALENTA INDONESIA)*

Name : *Mochamad Haviz Tasmara*

Study Programme : *Informatics Engineering*

PRIFAT application is an android-based mobile application developed by PT PRIFAT TALENTA INDONESIA as an instructor/teaching service provider platform. This application provides a variety of instructor services, ranging from sports, music, to the arts. In using the PRIFAT application, it requests some user data for application needs in providing an instructor/teaching service platform. Given this, attacks on Android-based mobile applications have also increased, in fact there have been 1.3 million cyber attacks on mobile applications in Indonesia in the last 3 years according to data from the National Cyber Security Index (NCSI). Therefore it is necessary to test the security of android applications to find out the vulnerabilities contained in android applications that can reduce cyber attacks and data leaks. In this study, security testing was carried out on the Android-based PRIFAT application using the OWASP Mobile Application Testing Guide (MASTG) method which consists of 5 steps, namely preparation, intelligence gathering, mapping the application, exploitation, and reporting. Testing will be carried out using a gray-box approach with reference to vulnerabilities based on the 2016 OWAPS mobile top ten. Based on the security testing results, seven vulnerabilities have been identified in the PRIFAT application. The vulnerability details are as follows: insecure data storage (allow backup vulnerability and temporary file vulnerability) categorized as high and medium vulnerabilities, insecure communication categorized as a high vulnerability, reverse engineering categorized as a high vulnerability, OTP code on response leads to account takeover categorized as a critical vulnerability, bypass OTP code categorized as a high

vulnerability, brute force OTP categorized as a high vulnerability, and no rate limit OTP code categorized as no vulnerability. The identified vulnerabilities mostly impact the confidentiality aspect, ranging from the exposure of sensitive user data to the ability to hijack other users' accounts. Based on these vulnerabilities, the following security recommendations are provided: implementing obfuscation on the source code, encrypting data in storage, applying limitations when making requests for OTP codes, and making improvements to the application's code and logic to prevent vulnerabilities.

Keywords *— penetration testing, android, mobile applications, OWASP MASTG*