ABSTRAK

Kesadaran dan kewaspadaan mengenai keamanan informasi terhadap aplikasi harus diterapkan oleh perusahaan atau organisasi, terutama terhadap informasi yang bersifat rahasia. Akan tetapi dalam pendaftaran akun wi-fi di website hotspot unpas terdapat suatu celah baik itu dari integrasi data maupun bug pada program sehingga dibutuhkan keamanan informasi.

Keamanan informasi perlu diterapkan untuk menjaga kerahasiaan data, agar data tidak dapat diubah oleh orang yang tidak berwenang dan data dapat diakses bila dibutuhkan. Penelitan ini menggunakan OWASP sebagai acuan untuk mengembangkan tingkat keamanan sebuah aplikasi.

Hasil dari penelitian ini berupa implementasi aplikasi yang telah dikembangkan tingkat keamanannya dari segi integrasi menggunakan API serta penggunaan verifikasi token dengan CSRF untuk menangani bug pada program website pendaftaran akun wi-fi captive portal.

Kata Kunci : *keamanan informasi, OWASP, C.I.A, Website Hotspot, API, CSRF.*

ABSTRACT

Awareness and care of the information security of the application must be applied by the company or organization, especially to confidential information. However, in the registration of wi-fi accounts on the unpas hotspot website there is a gap either from the integration of data or bugs in the program so that required information security.

Information security needs to be applied to maintain data confidentiality, so that data can not be changed by unauthorized persons and data can be accessed when needed. This research uses OWASP as a reference to develop an application's security level.

The result of this research is the implementation of the application that has been developed in terms of security level of integration using the API and the use of token verification with CSRF to handle the bug in the website registration program wi-fi captive portal account.

Keywords : *information security, OWASP, C.I.A, Website Hotspot, API, CSRF.*