ABSTRACT

Web-based Academic Information System (web-based AIS) has been used by all students of Faculty of Engineering, Diponegoro University, Semarang. Therefore, all student academic records through the campus network needs to be done research on the security system is established so that safe. The study was conducted by the steps of the analysis and testing of the system is installed, needs analysis, solution design problems, making improvements to the module, the module installation and repair module re-testing. From the results of research conducted can be concluded that there are weaknesses in the login system. Weaknesses include the use of the Students number identification (NIM), as a default user name and password, the data the user name and password is not encrypted before sent to the server through the network, track a user name and password left behind in browser as a manager in the cache or password can be seen as a simple text (plaintext) is not encrypted. From the results of the analysis of the security, login system of AIS can be improved by implementation of HMAC MD5 encryption technology and Challenge Handshake Authentication Protocol (CHAP). Challenge raised by the server randomly and used as an encryption key in the process of HMAC MD5. With the use of the challenge your password sent a hash value will always be different at each session. Javascript in the client-side encryption used to do so before the data is sent to the server is encrypted.

Key word: Academic Information System, login system, cryptography, security