NEWTON: Networking and Information Technology
Vol. 3 No. 1 June 2023, Page. 27- 31
E-ISSN: 2797-0728

Web-based Academic Information System Security

Tholib Hariono[1], Muhammad Iqbal[2*], Nurul Yaqin[3], Hilyah Ashoumi[4]
[1,2,3]Information System, Universitas KH. A. Wahab Hasbullah
[4]Islamic Religious Education, Universitas KH. A. Wahab Hasbullah
*Email: iqbal99@gmail.com

ABSTRACT

Web-based Academic Information System (SIA) has been used by all students of the Faculty of Information Technology KH. A. Wahab Unwaha Jombang University. Because all student academic records are stored through the campus network, it is necessary to conduct research on security so that a secure system is obtained. This research was conducted with steps including analysis and testing of installed systems, analyzing needs, designing problem solutions, making repair modules, installing modules and retesting repair modules. From the results of the research conducted, it can be concluded that there are weaknesses in the login system. The weaknesses include the use of the Student Identification Number (NIM) as the default username and password, username and password data is not encrypted before being sent to the server over the network, traces of usernames and passwords left in the browser as a cache or in the password manager can be seen as unencrypted plaintext. From the security analysis results, the SIA login system can be improved by applying HMAC MD5 encryption technology and Challenge Handshake Authentication Protocol (CHAP). Challenge is generated by the server randomly and used as a key in the HMAC MD5 encryption process. With the use of challenge passwords sent in the form of hash values will always be different in each session. Javascript on the client side is used to perform encryption so that the data before being sent to the server is already in an encrypted state.

***Keywords**: Academic Information System, login system, security.*

INTRODUCTION

The online Academic Information System (AIS) makes it easy for the academic community to access information related to academic needs. Information can be accessed from any computer connected to the campus network if the required account name and password are known. account name and password are known. One of the weaknesses is the login system. The login system in the AIS version 0.4 is currently thought to be very vulnerable to password breaches by unauthorized people. unauthorized persons.

Academic Information System (AIS) is software used to present information and organize administration related to present information and organize administration related to academic activities. academic activities. With the use of software like this, it is expected that academic academic administration activities can be managed properly and the necessary information can be obtained easily and quickly. obtained easily and quickly. The features available in the SIA application of the Faculty of Engineering Undip version 0.4 are user groups, Internet ready, SMS-based ready, online banking ready, Dikti Selfevaluation Ready, guest facilities, student facilities, lecturer facilities, BAA facilities, and supervisor facilities. (Academic Administration Section) and supervisor facilities (Satoto, 2006).

System login (login, also commonly referred to as log in, log on, signon, sign on, signin, sign in) is the process of accessing a computer by entering the identity of a user account and password to gain access rights to use the resources of the destination computer (Johnston, 2005). Logging into a system usually requires a user account and password pair. The pair must be precise and the two are inseparable. The password can be changed as needed, while the user account is never changed because it is a unique identity that refers to a specific user.

Cryptography is the study of mathematical techniques that deal with aspects of information security such as validity, data integrity, and data authentication. The process used to secure a message (called plaintext) into a hidden message (called ciphertext). Encryption is used to encode data or information so that it cannot be read by unauthorized people. A hash function is a function that efficiently converts an input string of a fixed length into an output string of a fixed length called a hash value. hash value. MD5 is one of a series of message-digest algorithms that were designed by Professor Ronald Rivest of the Massachusetts Institute of Technology (MIT). When analytical work showed that MD5's predecessor - MD4 - was starting to become insecure, MD5 was then designed in 1991 as a replacement for MD4. MD5 hash 128-bit (16-byte) long, also known as the message digest, is typically displayed in hex numbers. is typically displayed in a 32-digit hexadecimal number. Keyed-Hash-Message-Authentication-Code, also known as HMAC, is a one of the message authentication code (MAC) methods that is based on cryptographic hash functions (Krawczyk, 1997). The message along with the key is entered in the HMAC function which produces one hash value output.

The stateless nature of the web - the server and client immediately disconnect when the data has finished being sent - while the application needs status or data that will continue to be used while the application is running. will continue to be used while the application is running. This nature of the web can be handled by using sessions. The relationship status and data in the application are stored in session on the server (Rickyanto, 2003). Cookies are used to store session identities that reside in each browser. The session identity is unique and cannot be duplicated. When a web application is first accessed by a browser, a new session is created by the server with a unique session identity. The session identity is used to recognize the client making the request and maintain the relationship status between the client and the server. When a user navigates the same site, the session identity is sent along with the HTTP request data and the server responds with the same session identity. There are two types of cookies. Persistent and non-persistent cookies. Persistent cookies are stored on the user's computer. Non-persistent cookies are used to record authentic user activity at the time of opening the website. When the session ends, non-persistent cookies are deleted (Burnett, 2005). The identity of the session status will be recorded as an authentic user when the user has logged in correctly. When logging out of the system, the session identity is recorded on the server as an inauthentic visitor.

JavaScript is a cross-platform language first introduced by Netscape. It is one of the object-oriented scripting languages. It provides a means to run applications over the Internet. Client applications run in a browser such as Netscape Navigator and server applications run on a server such as Netscape Enterprise Server. such as Netscape Enterprise Server. Javascript can be used to create dynamic HTML that process user input and maintain data using specialized objects (Holzner, 2002). The CHAP (Challenge Handshake Authentication Protocol) login system is a type of authentication protocol where a key - random data - is sent to the client authentication agent which is used to encrypt the password before it is sent to the server.

Content Management System (CMS) is a system that is used to organize a website. Usually, a CMS contains two elements: Content Management Application (CMA) and Content Delivery Application (CDA). CMA is the element element that makes it easy for a content manager or writer - without having to know know Hypertext Markup Language (HTML) - to create, organize, change and delete content from a website. The CDA element is used to organize information to update the content of the website.

METHOD

In conducting the analysis, several methods were used, namely literature study, testing of existing systems, formulation of problem solutions and application of problem solutions. problem solution. Each method has a relationship with one another. User data can be taken from the list of registered NIMs because NIM is used as a user name in SIA version 0.4. The easiest way to collect NIM data is from the list of students contained in the SIA. There are two ways to get student data using SIA. First on the menu Search for student data and second on the menu List of course participants. Password data can be retrieved in two ways. The first is using the default password. The default password for SIA version 0.4 is the same as the user's NIM. Second with the social engineering method, namely the method of approaching users. This method requires special expertise not only in technical terms but also in terms of psychology. An easy way to do social engineering in this case is to trap the username and password to be stored in Firefox.

RESULT AND DISCUSSION

- System Analysis And Testing

The first test is the login system problem. Password data theft can be done by scanning data that passes through the network between the client and the server. The next test is to see the data traces left on the terminal computer (client). The terminal computers provided mostly use the Firefox browser so the research target is the Firefox browser. The Firefox browser has a facility to store passwords. in Firefox 1.0 *the default* button of the password saving dialog is *Yes* which means it will save the password in *the password manager*. This may be less vulnerable in Firefox 1.5 because the default dialog button for saving passwords is not *Yes* but *Not Now*. Pressing *the Yes* button in Firefox 1.0 (Remember button in Firefox 1.5) button will cause the password to be saved in the password manager. The Never for this site button is used to note that the password for the site visited (in this case SIA) will never be saved into the password manager SIA will never be saved into the password manager. The No button button in Firefox 1.0 (Not Now button in Firefox 1.5) is used to not save the passwords into the password manager only when the No button is pressed. Saved passwords can be viewed simply by pressing the View Saved Passwords button in the Options → Privacy → Passwords window. In this way, the password username data of all users who have used the terminal computer either for the purpose of accessing SIA or other Internet services can be easily viewed. Internet services can be viewed easily.

- Problem Solution Implementation
  Based on the results of the test analysis, literature study and the formulation of the problem solution, a model for the solution to be used is created. From the model, a simple program code is then created to be tested. If the test results are successful, the part of the program code is then attached to the part of the project that has weaknesses.
- System Retesting
  The final stage is testing to get maximum results. Final testing is intended to find weaknesses that are still found in the solution provided. From the test results if errors are found, then the solution is re-evaluated and corrected to get the best results. and improved to get the best results.
- Authentication System Testing
  Authentication system testing is done in various ways, namely with default passwords, theft of passwords that cross the network, SQL injection techniques and theft of passwords. default password, password theft across the network, SQL injection techniques and password trace search on the terminal computer searching for password traces on the terminal computer. Each technique has its own level of difficulty.
- User List Search
  Obtaining the user list is not difficult. In the SIA log system version 0.4, Student Identification Number (NIM) is used as the user name. One way is by looking at the list of students on the attendance sheet or the list of students from other published sources. from other published sources. Another way is to see the list of students from the SIA application.
- Testing The Login System With Default Password
  One of the weaknesses of SIA version 0.4 is the use of default passwords. The The default password of SIA version 0.4 is the same as the username. From the test results using the object of a list of students who take the course Database course, thirteen out of forty-four (29.5%) students still use the default password. using the default password. Another default password testing technique is to use tools. This tool is basically just a computer program that can automatically test the login system automatically based on a set value and generate a success report. This tool was created to speed up the analysis of users who still use the SIA default password.
- Session Monitoring
  Session monitoring aims to obtain test data on a local computer. Session monitoring on the Internet Explorer browser can be done using Fiddler by opening the SIA address at the site address http://http://sia.unwaha.ac.id//elektroext/.
- Scanning Using Ethereal
  The list of captured data frames is shown in the top box, the translation of the data frame is shown in the middle box, while the bottom box is used to display the frame in hexadecimal format. From the data obtained, there are some usernames and passwords were captured.
- Password Trace Search On Terminal
  Testing on the Firefox browser was done by performing a system login. After pressing the Login button, the browser asks if the password will be remembered by the password manager as shown in will be remembered by the password manager as shown in Figure 1. In the test, the Yes button was

pressed to save the password into the password manager. The test was conducted on seven different usernames. After the password manager, the password is saved and can be viewed easily.

- Authentication System Improvement
  The SIA authentication system installed at this time was created using the PHP language and MySQL The creation of the improvement module also used the same language and database. To be able to create an authentication system, there must be a system that runs as a test material. The Drupal Content Management System (CMS) is used as the system to be tested and also as a framework in building a complete system.
- Design
  At this stage a flow chart is used to help describe the process that occurs. There are two flow charts, namely the client-side flow chart and the server-side flow chart. Both have a reciprocal relationship between the server and the client. When the browser first requests the server, a new session is created by the server and sends the system login form along with a random data challenge used for the authentication process. The client part of the flow chart requires In the client part of the flow chart, several functions are needed including retrieving username, password, challenge data, HMAC MD5 encryption and sending data to the server.
- Module Creation
  The module was created in the form of a block module as a replacement for Drupal's native userlogin module. The module is named chaplogin and is stored in the chaplogin.module file. The module chaplogin module was created with the HMAC MD5 encryption algorithm. There are two former used for encryption on the client side, namely chaplogin.js and md5.js.
- Module Installation, Activation And Configuration
  The module is installed as a replacement for the original module by removing the original module and then installing the chaplogin module and activating it. The steps for steps can be found in the Drupal documentation at http://www.drupal.org/. In this study, Drupal was installed in the root directory of the web, namely /www/ on the server sia.phpnet.us server so that it can be accessed directly using the address http://sia.phpnet.us/. The installation of the chaplogin module is done by uploading the module files (chaplogin.js, chaplogin.module and md5.js) using FTP to the directory /www/modules/chaplogin/.
- Chaplogin Module Testing
  Testing the authentication module was done in various ways, the same as testing the previous system, namely with default passwords, password theft across the network, SQL injection techniques and password tracing on terminal computers, crossing the network, SQL injection techniques and searching for password traces on the terminal computer.
- Default Password Testing
  In the default password test, the chaplogin module passed the test because each user registers himself with his own user account name and password. In the system, there is no default password, so there is no possibility of intrusion using the default password.
- Session Monitoring
  With the help of Fiddler, sessions can be monitored to obtain user and password data. The test was carried out by monitoring HTTP POST sessions that may contain username and password.
- Data Sniffing
  From the scanning results it can be concluded that the data is more secure as it traverses the transmission path. The data is encrypted in the browser with Javascript before being sent to the server.
- SQL Injection Technique
  Testing with this technique was done by entering the user name as "cahnom' OR 1=1 --" (without double quotes) without password. From the result. It was found that this technique could not be used to penetrate the login system.
- Password Trace Search On Terminal
  Five sample users with different usernames and the same password "secret" (without double quotes) were used. The passwords were encrypted for all users who attempted to log in to the system with the URL address http://sia.phpnet.us/

CONCLUSIONS

Security Analysis of the Academic Information System of the Faculty of Information Technology Unwaha Version 0.4 has been carried out with the results stating that;

- Password data on the login system is not encrypted before being sent to the server,
- The use of the default password is the same as the user name making the system prone to intruders, prone to intruders,
- Session data sent from the browser to the server is not encrypted,
- Attacks with SQL injection techniques cannot be carried out on the login system or query strings on the address line,
- Traces of usernames and passwords can be seen in the Firefox browser password manager as unencrypted text.

Improvements to system weaknesses that have been made include;

- Password data in the login system has been encrypted before being sent to the server,
- The default password is not used but the password is created by the user himself,
- Password data in the session sent to the server has been encrypted with the CHAP method and the HMAC MD5 encryption algorithm, 3. CHAP and HMAC MD5 encryption algorithms,
- Trace the user name and password in the password manager as a hash value.

REFERENCES

Burnett, M., Hacking the Code: ASP.NET Web Application Security, California, 2005.

Holzner, S., Inside JavaScript, Indianapolis, 2002.

Johnston, P. A., Login System, http://pajhome.org.uk, Oktober 2005.

Krawczyk, H., Keyed-Hashing for Message Authentication, http://www.ietf.org/rfc/rfc2104.txt, Februari 1997.

Rickyanto, I., Membuat Aplikasi Web dengan ASP.NET, Jakarta, 2003.

Satoto, K. I., Tentang Sistem Informasi Akademik Fakultas Teknik Undip, http://siaft.undip.ac.id/, Maret 2006.