ANALYSIS AND DESIGN OF WEB SERVER SECURITY SYSTEMS FROM XSS AND CSRF DEFACEMENT

Muhd. Iqbal*,1, Umam Farizan2, Rasudin Abubakar3
[1, 2, 3] *Syiah Kuala University Banda Aceh*
*Corresponding Author : iqbal@unsyiah.ac.id

ABSTRACT

This study aims to identify the signs of defacement in detail and design web-server security system Automatic Interactive Reactive Intuition Detection System (AIRIDS) method to maintain the confidentiality of data from irresponsible parties and improve the security and filtering of data traffic on the web-server. The method used in this research is network and web-server analysis method which is done by analyzing existing web-server and website that has been active using Acunetix wvs 10.5 software, method of attacking web-server system done with scenario I (web attack local defacement) and scenario II (outside defacement). The parameters observed are the web server security topology, the designed system, the prevention of XSS and CSRF as well as the installation of AIRIDS. The results show that the website and web-server prior to installation of AIRIDS can be attacked by defacing techniques and high-level web server vulnerabilities (high = 3), but after installation of web-server security system, website and web-server cannot be attacked with defacing technique and not get back gap that status high (high = 0). It can be concluded that the installation of web-server security system AIRIDS method can prevent and minimize the level of vulnerability of attacks on websites and web-server, but it also can prevent the leakage of confidential information.

KEY WORDS: AIRIDS;web server;defacement

INTRODUCTION

Various telecommunications facilities in the era of information technology are currently experiencing very rapid progress. These technological advances can change human lifestyles more easily and practically (Madcoms, 2012). The advancement of information and communication technology that directly affects the lives of humanity is cellular phones and the internet. The use of cellular telephones as one of the information technology media that has progressed makes it easier for humans to communicate and obtain information quickly (Purbo and Wiharjito, 2010).

According to Agarwal and Tayal (2009) advances in information and other communication technologies are characterized by the presence of internet services. The presence of internet services as one of the telecommunications facilities used to process, produce, send and receive all forms of information without knowing the limitations of space, distance and time. One of the facilities of internet technology that is widely used today is the web browsing. This is because of the web browsing has various advantages and benefits, namely in terms of cost and easy to use in everyday life.

Website development (website) that is very fast and wide has an unbalanced impact. A very visible impact is the insecurity of data and information contained on sites. This is because its development is not in line with the development of its security system. The effort that can be done to handle this imbalance is the web-server. Web-servers are used to set up a site or several addresses that require a server (Medvet et al., 2007). However, with the development of techniques defacement web-server becomes one of the toughest problems that must be faced due to its development which has no solution to anticipate it (Bartoli et al., 2009). Of the several types of defacement that are the most commonly used attackers are cross-site scripting (XSS) and cross-site request forgery (CSRF) techniques, these two techniques can cause various problems for security web-server. Therefore, this research needs to be done to identify signs of XSS defacement and CSRF and design a security system on the web-server so as to provide solutions to these problems. This research is expected to provide information to identify signs of defacement XSS and CSRF type as a whole and improve security systems and filter data traffic on web-servers.

Problem Formulation

Based on the description above, it can be formulated problems that will be discussed to be completed in this study. First recognize the topology, network security used and the various obstacles contained in it. Furthermore, knowing how to recognize web-servers that are affected by defacing, especially in the XSS and CSRF types. In the end build security system of web-server method AIRIDS of two types of attacks.

Research Objectives

Purpose of this study is to identify signs of defacement over all and design a security system web-server with method AIRIDS to maintain the confidentiality of data from irresponsible parties and improve security and filtering data traffic on web-servers.

Research Benefits

This research is useful to provide information in recognizing signs of defacement overall and improving the security system and filtering data traffic on web-servers so as to maintain the confidentiality of data from irresponsible parties and avoid theft of access rights on a web page for users of services hosting.

METHODOLOGY

Place and Time of Research

The place where the research was conducted was PT. Pupuk Iskandar Muda, having his address at the Medan-Banda Aceh Road, Krueng Geukuh, North Aceh District, Aceh Province. The main reason for the research was at PT. Pupuk Iskandar Muda (PT. PIM) is because PT. PIM has a long history of development of departments engaged in the field of technology with a very significant increase over time - time.

Tools and Materials

To analyze and design a security system, tools and materials are needed to help data collection and processing. Tools and materials for analyzing research and designing security systems web-server from defacement can be in the form of hardware and software, as follows:

1. space Data centre in this case PT data centre. PIM with Tier III.
2. Computer devices are Lenovo G470 laptops with Intel Core i3 2.2 Ghz processor and have RAM 6 GB and capacity of 1 TB hard drive.
3. Web-server in this case the web-server that is used in the Linux operating system means running the web-server Apache.
4. The firewall in this case is the watchguard XTM 8600.
5. Active-directory server in this case IBM system X with operating system Windows Server 2003.
6. The website that has been active in this case is http: //www,pim.co.id.
7. software Acunetix WVS 10.5.
8. Security System AIRIDS

How it works

This research has been carried out using 3 main methods to produce an optimal security system web-server. Here are the main methods:

1. Methods of analysis and network web-server
2. attack step system web-server
3. design of security system web-server
   Methods of network analysis and web-server

Process first thing to do is to analyze the web-server is already there and website that has been active with software acunetix wvs 10.5. The following stages of analysis were carried out in this study, as follows:

1. Analyze computer network topology.
   - Network lines.
   - Hardware used and settings contained in
2. Network security analysis
   - Hardware and software firewall.
   - Active-directory server used.
3. Analysis Web-server web server
   - operating system
   - Access rights on the web-server.
   - Services used by web-servers.
   - arrangement Resource control.

The steps to attack the system web-server

The steps and steps that must be carried out in this research are 2 scenarios that will be implemented. Scenario I is attacking the web-server from within (local defacement) that will attack a web-server on the local area network or directly from the web-server itself. Scenario II is outside. Attacking the web-server from the outside will certainly be more difficult to do by looking for loopholes contained in the web-server and uploading data script that works to run on the web-server. Of the several techniques for carrying out attacks defacing, two techniques will be carried out in each scenario. In both techniques, done by manual scripting.

a. Scenario I

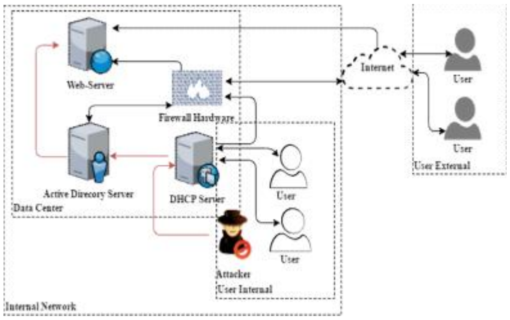

Fig. 3.1 Topology of attack scenario 1

Scenario I: Topology Scenario 1 can be seen in Fig. 3.1. The explanation of the attack process was carried out by connecting a computer device used as a media for attacking the internal network. The attack is carried out with stages - very detailed and careful because it can be ascertained that the person doing is having a relationship with the place where the web-server is located. scripts are XSS injection and CSRF injection prepared first. Connect a computer with a server active-directory to be registered as a user who has access to the server - the server is active. The website contained on the web server is accessed through browser an existing. Scripts are uploaded or sent to web-servers through security holes found on the website. A security gap on the website can be found on the login, form search and form registration. After the script is uploaded it will open the script by script accessing the through the browser.

b. Scenario II

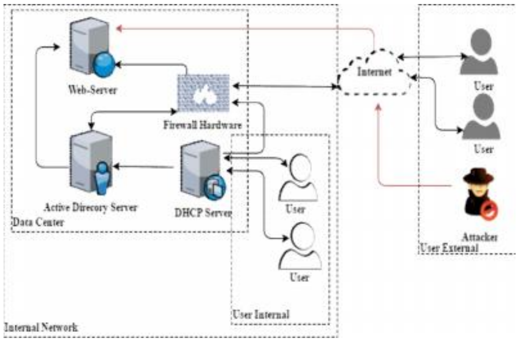

Fig. 3.2 Topology of attack scenario II

Scenario II: Topology Scenario II can be seen in Fig. 3.2. The attack is carried out with perfect stages to get optimal results. High level of difficulty and complicated to carry out attacks from outside the local area network. Script XSS injection and CSRF injection are prepared first. Connecting a computer with server active directory to be registered as a user who has access to the server - the server is active. The website contained on the web-server is accessed through a browser. Scripts are uploaded or sent to web-servers through security holes found on the website. A security gap on the website can be found on the form login, form search and form. the registration. After the script is uploaded it will open the script by script accessing through the browser.

Stage of designing the AIRIDS web-server

Security system This security system aims to protect the web-server with the ability to respond in accordance with security policies. Architecture system security Web-server can be seen in Fig. 3.3.

To realize this method, it is necessary to design the components of the security system web-server in the form of:

1. Intrusion detection system (IDS)
   a. Sensor module
   b. Analyzer module
2. Database system
3. monitoring system
4. Firewall system

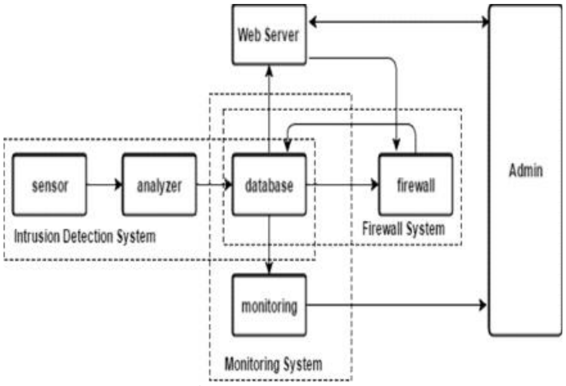

Fig. 3.3 architecture of security system AIRIDS web-server

1. Intrusion Detection System (IDS) in this final project implementation consists of component components and blocking diagrams of IDS, namely sensors, analyzers and databases system as shown in Fig. 3.3.
   a. The sensor module is built with the linux bin bash program that downloads the website content files stored in the baseline directory and detects the threat of defacement by comparing the results of the download of the site's page contents with those on the webpage at the actual time (Real Time) stored in the temporary directory (tmp).
   b. The Analyzer module is built using the linux bin bash program and the command line wdiff is applied to compare each word in the file downloaded from the website with the file that is on the real time page. The results of the comparison of the file are stored in the results directory with the file format that is compared and contains the results of the comparison in percent form.
2. The database system is built with the database files contained in the directory results (Fig. 3.4) and named according to the file name that is compared and contains the results of the comparison in percent (%) form.
3. Monitoring system is built using the linux bin bash program. The program is built looping on Sensor and Analyzer module that has been built and notified if there is a difference greater than or equal to the limit allowed(Threshold)in the form of percent (%) and printed to the linux terminal that

the presence of file content pages in the site has changed. Notifications are also made by applying the API bot to be able to send a message to the Admin that there has been a change in the contents of the site page.

4. Firewall system is used by XTM 8600 watchguard hardware and firebox software that has been found in Data Centre PT. Pupuk Iskandar Muda. The system firewall is ServerLock used to prevent users from sending scripts that can change the contents of the site pages on the web-server.

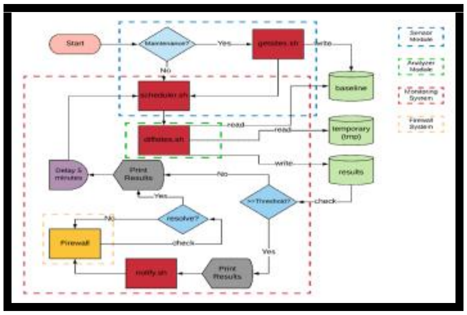

Fig. 3.4 flowchart of security system AIRIDS web-server

RESULTS AND DISCUSSION

Network System Analysis (Topology, Network Security System, and Web-server).

System analysis is a system that describes parts of the components of an information system in an original and complete manner with the aim of identifying and evaluating a problem, barriers, opportunities, and needs of the system so that an improvement is found in accordance with what is expected.

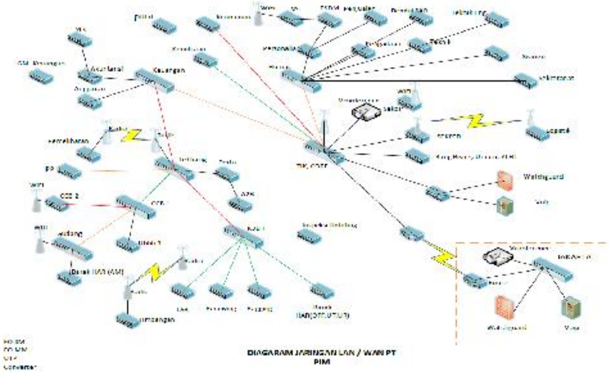

Fig. 4.1 Network topology of PT. Pupuk Iskandar Muda

Analysis of the Impact of XSS and CSRF Attacks

Impact of attack with scenario I

Attacks through scenario I are carried out using software Acunetix wvs 10.5. The results obtained under scenario I are that there are XSS and CSRF attack loopholes with attack vulnerability level that is high 3, or for a security system web-server with very low results, and followed by 5 attack vulnerabilities medium and some placement errors. script and arrangement directory on the web-server. In addition, in scenario I it is found that the active directory server and server log can be attacked with the level of damage is High 2, and found the writing password on each computer name employee's in the description column User. Especially on the form html login on the PT. PIM so it's very easy to attack CSRF and accompanied by Brute Force.

Impact of attacks with scenario II

Results from scanning before installing a system network security in Fig. 4.2. Attacks through scenario II using Acunetix Software, obtained results that are close to scenario I, where the level of vulnerability with XSS and CSRF attacks is in position high 3, but there is also a level of vulnerability in the position medium same that is 5. In addition, there is an error in placement of scripts and directory arrangement on the web-server. In scenario II there is no access to be able to attack the active directory server, this is because in order to get verification from the firewall, the user must use the VPN PT. PIM or by entering from the same subnet as PT. PIM.

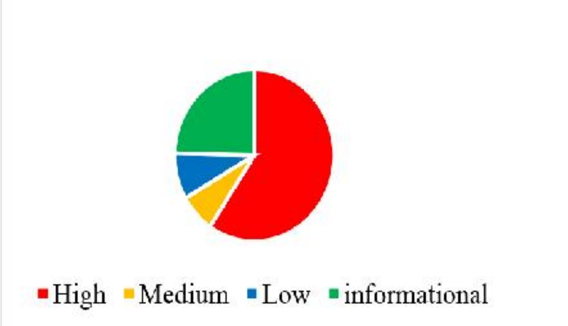

Fig. 4.2 Security gap web-server before installing the security system AIRIDS web-server

Status High: this vulnerability is categorized as the most dangerous, which places the scanning target as the maximum risk for data attacks, hacking and theft.

Status Medium: This vulnerability is caused by a configuration error server and a lack of errors in site coding, which allows intrusion and interference server.

Status Low: This vulnerability is caused by a lack of encryption of data traffic or the appearance of a directory structure.

Status Informational: items found at the time of scanning and considered attractive, for example the possibility of an internal IP address or e-mail address being displayed, or matching strings search that match the Google Hacking Database, information about services.

Application of the Security System Network in Web-Server

The results of scanning after installation system of a network security in Fig. 4.3. The AIRIDS network security system is carried out by installing a security system that has been created on the web-server of PT. PIM, and when testing using the software Acunetix found a decrease in the level of vulnerability to 100% and did not recover the status gap high- (Appendix 2). However, only a gap with a status medium of 10 was obtained and there were errors in the preparation of scripts and directories on the web-server. For active servers, directory there is no XSS and CSRF attack gap with both Scenario I and II.

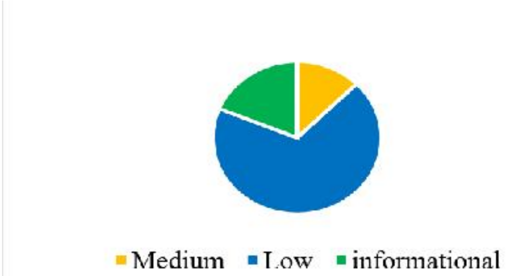

Fig. 4.3 Security gap Web-server after installing system security the AIRIDS web-server

CONCLUSIONS AND SUGGESTIONS

Conclusion

Based on the research that has been done can be concluded that:

1. Installation of system security web-server method AIRIDS on a web-server can prevent attacks defacement types of XSS and CSRF and the rate gap with the status of High, in addition to the parts contained loopholes attack XSS and CSRF reduced up to 100%, namely from 41 slots to 0.
2. Installation system of the security for web-server the AIRIDS method on the web-server can minimize the level of the attack medium and prevent confidential information leakage, this is indicated by the reduction in status. informational 82% that is, from 17 slots to 3.

Suggestions

Need to do further research to find out and maximize the configuration of the firewall on the web-server, so that it can further minimize the existing attack gap. In addition, it is necessary to test attacks flooding (such as DDOS and Brute Force) and build a security system to survive these types of attacks.

REFERENCES

Agarwal, BB and Tayal, SP 2009. Computer Network First Edition. University Science Press, USA.

Bartoli, A., Davanzo, G., Medvet, E. 2009. The reaction time to Web Site Defacements Internet Computing. IEEE. University of Trieste, Italy.

Borgolte, K., Kruegel, C., and Vigna, G. 2013. Delta: Automatic Identification of Unknown Web-based Infection Campaigns. SIGSAC Conference on Computer and Communications Security (CCS), ACM.

Davanzo, G., Medvet, E. and Bartoli, A. 2011. Anomaly Detection Techniques for a Web Defacement Monitoring Service Expert Systems with Applications. Vol. 38 (10).

Madcoms. 2012. Computer Network System for Beginners 1. Edition Andi Publisher, Yogyakarta.

Medvet, E., Fillon, C., and Bartoli, A. 2007. Detection of Web Deficiencies by Means of Genetic Programming. Proceedings of the 3rd International Symposium on Information Assurance and Security, IEEE Computer Society.

Prasad, Prakhar. 2016. Catering Modern Web Penetration Testing. Packt Publishing, UK.

Purbo, OW, and Wiharjito, T. 2010. Internet Network Security. Elex Media Komputindo.

Sugiantoro, B., and Istianto, JE 2010. System Analysis of Intrusion Detection System (Ids) Security System, Database System and Monitoring System Using Moving Agents. National Seminar on Informatics for Computer Science Postgraduate Program at FMIPA UGM, Yogyakarta.