Website Vulnerability Scan for Information System of Toddler's Growth and Development

Endah Sudarmilah, Universitas Muhammadiyah Surakarta, Indonesia
Wiwien Dinar Pratisti, Universitas Muhammadiyah Surakarta, Indonesia
Umi Fadlilah, Universitas Muhammadiyah Surakarta, Indonesia
Geri Gebyar Giwangkoro, Universitas Muhammadiyah Surakarta, Indonesia

The Asian Conference on Society, Education & Technology 2014
Official Conference Proceedings

Abstract
Web-Based Information System of Toddler's Growth and Development is a client server application which has been information source as monitoring tools for the growth and development. It also be accessed easier by parents, posyandu and medical personnel that has been implemented.

On the other hand, the more easily to access this website also the more raises the security issue of information systems. Therefore, this study aimed to test the security of information systems Web-Based Information System of Toddler's Growth and Development which in turn to give recommendations on the issues raised by the application. Method used in this research was testing vulnerabilities that allow a cracker attacked system using a vulnerability software scanner.

The testing results that have been conduct was known that Web-Based Information System of Toddler's Growth and Development is unsafe, it shows the pages with the vulnerability of the High-level with malicious web alerts and the most vulnerable to attack by cracker is on the login page. It derives a recommendation on this system paying attention to security and performance on application and also solving the system vulnerabilities.

Keywords: Website, Vulnerability, Information System

Introduction

Currently, Information systems in the medical world are so needed, but there still have lack of using information systems to assist the work of the medical personnel, especially in helping the development of toddlers.

In this research, web-based information and monitoring systems for toddler growth was designed and built for help medical personnel as well as posyandu (an integrated service post for toddler's monitoring growth) personnel in assisting parents in monitoring growth by looking at the nutritional status with the method of Anthropometry for measuring nutritional status toddler is weight, height or length and age (Indonesian Ministry of Health, 2010) (Indonesian Ministry of Health, 2011) (Wijaya, Awi Muliadi, 2011). As well as the development of toddlers who monitored her mental and motor development, and has more goals to become the portal database on child growth and development rates of posyandu and health centers which now is still done manually. Architecture of information systems and monitoring growing swell toddlers are web based which will then be implemented to work with the data governance posyandu and health centers (Sudarmilah, Endah, et al. 2013). This article will discuss the results of scanning the information system website vulnerabilities.

Related Research

Information and monitoring system is made with some of the software supporting the programming language PHP (Personal Home Page) is a scripting language embedded in HTML (Hypertext Markup Language) for the execution of server-side. PHP is used to extract the data/information that is desired by the user from the database and display it on a Web page (Nugroho, 2006).

Database Management System (DBMS) is software to manage and query database (Garry et al, 2009) that is used is MySQL which is an implementation of a relational database management system (RDBMS). SQL (Structured Query Language) is a database operations concept, especially for election or selection and data entry, which allows the operation of the data is done automatically with ease. (Nugroho, 2008).

This system using AHP decision support system (Analytical Hierarchy Process) is a method of decision making with multiple criteria, i.e. a comprehensive decision-making model, because it takes into account things both qualitative and quantitative. One of reliability of AHP is able to perform simultaneous and integrated analysis of qualitative parameters of quantitative or even that. The concept of AHP method is changing the values of qualitative quantitative values, so decisions taken can be more objective (Yuniartini, 2010).

Method

This researcher on testing using tools that are run with the specific measures used to test the security and performance of information systems. To conduct the analysis of information system in terms of security software used Acunetix vulnerability scanner for testing performance (Dukes, L. et al, 2013).

Result and Discussion

The implementation of this system has been feasibility tested online that can be accessed by anyone and everywhere with a domain and a particular web address. The system can be accessed online information systems hosting is done with web hosting, *siposyandu.com*.

Furthermore the results of the scan using the Acunetix vulnerability of this web application with the address *http://siposyandu.com/* which showed vulnerability at level 3 (High) that provides information 240 alerts namely, 45 alerts on High alert, 166 alerts on category Medium, 17 alerts on Low category, and the 12 alerts on Informational categories. From the results of scanning using Acunetix in Figure 1 was showed the analysis of vulnerability in *siposyandu.com* information system based on the type of these.

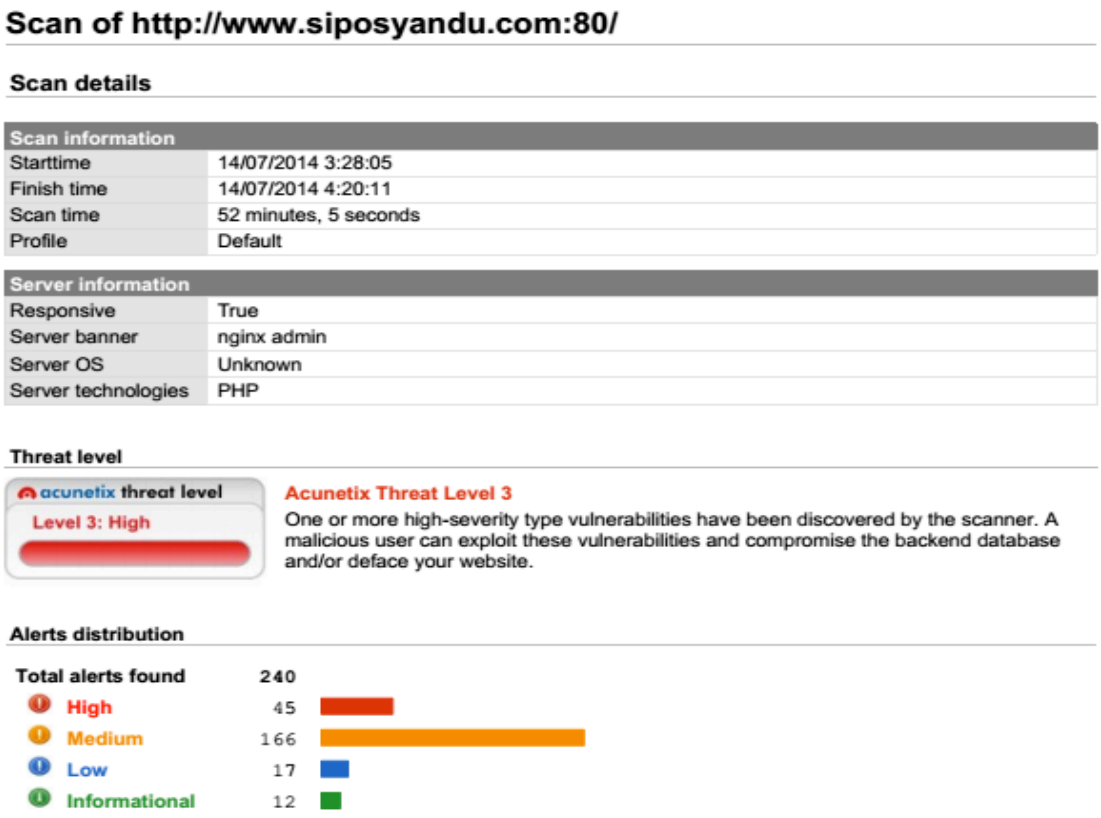

Figure 1: The Scanning Results Using Acunetix *siposyandu.com*.

The granting of a security risk level refers to the recommendations of Acunetix application are described as follows.

a. *Blind SQL Injection*
   Threat level: High
   Risks:
   - Blind SQL Injection allows a person can log into the system without having to have an account.
   - Allows one to modify, delete, and add data that resides in the database.

- Shutting down the database, so can't give a service to the web server.

Recommendation:

- The script should be able to do the filtering parameters that can be used for the process of Blind SQL Injection.
- Limit the length of the input box.
- Hide error messages out of the SQL Server that is running.

Alert group	Blind SQL Injection
Severity	**High**
Description	This script is possibly vulnerable to SQL Injection attacks. SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters. This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
Recommendations	Your script should filter metacharacters from user input. Check detailed information for more information about fixing this vulnerability.

Figure 2 Recommendations for Blind SQL Injection

b. *Cross Site Scripting*

Threat level: High

Risks:

- An attacker can perform against cookie theft.
- Allows attackers to deface or change the display either temporary or permanent nature of the website.

Recommendation:

- Perform filtering against meta character from user input.
- Using the POST method is a method of data delivery started where variables are submitted are not included in the link that is used.

Alert group	Cross Site Scripting (verified)
Severity	**High**
Description	This script is possibly vulnerable to Cross Site Scripting (XSS) attacks. Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.
Recommendations	Your script should filter metacharacters from user input.

Figure 3 Recommendations for Cross Site Scripting

c. *Weak Passwords*

Threat level: High

Risks:

- An attacker can easily break into the information system and utilize the information contained therein after gaining access.

Recommendation:

- Enforce a strong password policy.
- Do not permit weak passwords or passwords based on words in the dictionary.

Alert group	Weak Password
Severity	High
Description	Manual confirmation is required for this alert. This page is using a weak password. Acunetix WVS was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.
Recommendations	Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.
Alert variants	
Details	Username: admin, Password: admin

Figure 4 Recommendations for Weak Passwords

d. *HTML forms without CSRF protection*

Threat level: Medium

Risks:

- Changing the victim's e-mail password, account information, or perform logout.
- Victims of "buying" stuff from the usual shopping sites visited.
- Victims conduct financial transactions without realizing it.
- Victims of the polls to vote a certain website with an options preset assailant.

Recommendation:

- Do not rely on the "Remember Me", "Stay Signed in" and "Save Password" in the use of services on the internet.
- Do not store passwords in your web browser.
- Always Logout from the website once completed using the service and delete all traces (History, saved passwords, cookies and authenticated sessions) from the browser.

Alert group	HTML form without CSRF protection
Severity	**Medium**
Description	This alert may be a false positive, manual confirmation is required. Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.
Recommendations	Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.
Alert variants	
Details	Form name: <empty> Form action: http://www.siposyandu.com/ Form method: GET Form inputs: - key [Text]

Figure 5 Recommendations for CSRF

e. *User credentials are sent in clear text*
Threat level: Medium
Risks:
- The occurrence of attacks on data such as a user or password sent to the server to intercept over an unencrypted HTTP connection or not through HTTPS.

Recommendation:
- It is recommended to transfer data over an encrypted connection such as HTTPS.

Alert group	User credentials are sent in clear text
Severity	**Medium**
Description	User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
Recommendations	Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).
Alert variants	
Details	Form name: <empty> Form action: http://www.siposyandu.com/~admin/admin/login.php Form method: POST Form inputs: - userid [Text] - password [Password] - remember [Checkbox]

Figure 6 Recommendations for User Credentials Are Sent In Clear Text

f. Login page password-guessing attack
Threat level: Low
Risks:
- Attackers can perform Brute-force attack to find the password by trying every possible password guessing there.

Recommendation:

- It is recommended to implement some kind of account lockout after experimenting login with a password that is not right.

Alert group	Login page password-guessing attack
Severity	Low
Description	A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.
Recommendations	It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.
Alert variants	
Details	The scanner tested 10 invalid credentials and no account lockout was detected.

Figure 7 Recommendations to Login Page Password-Guessing Attacks

g. *Session Cookies without HttpOnly flag set and Secure Session Cookies without flag set*
Threat level: Low
Risks:
- An attacker can log in without a password by using "cookie name" and "Domain name" which will be filled with cookies and domain victim.

Alert group	Session Cookie without HttpOnly flag set
Severity	Low
Description	This session cookie doesn't have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.
Recommendations	If possible, you should set the HTTPOnly flag for this cookie.
Alert variants	
Details	Cookie name: "PHPSESSID" Cookie domain: "www.siposyandu.com"
Alert group	**Session Cookie without Secure flag set**
Severity	Low
Description	This session cookie doesn't have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.
Recommendations	If possible, you should set the Secure flag for this cookie.
Alert variants	
Details	Cookie name: "PHPSESSID" Cookie domain: "www.siposyandu.com"

Figure 8 Recommendations for Session Cookies without Http Only flag set and Secure Session Cookies without flag set

h. *Broken links*
Threat level: Informational
Risks:

- Broken links can make information systems exposed to a penalty from Google. And if exposed to penalties google Pagerank it will affect information systems and indexing by search engines.
- Broken links can degrade the quality of SEO blogs.
- Information systems may be considered spam by the search engines when too many broken links.
- And the loss of visitors are not able to find the information sought. And if like this, then the visitors slowly, reluctant to come back to the earlier information systems.

Recommendation:

- Deleting files indicated broken link.
- Replace dead links with new links and are still functioning.

Alert group	Broken links
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	No details are available.

Figure 9 Recommendations for Broken links

i. *Password type input with auto-complete enabled*

Threat level: Informational

Risks:

- It allows attackers to find and commit abuse of passwords.

Recommendation:

- Disable autocomplete passwords on sensitive pages such as the login page.

Alert group	Password type input with autocomplete enabled
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Recommendations	The password autocomplete should be disabled in sensitive applications. To disable autocomplete, you may use a code similar to: <INPUT TYPE="password" AUTOCOMPLETE="off">
Alert variants	
Details	Password type input named password from form named login_form with action cek_login.php?op=in has autocomplete enabled.

Figure 10 Recommendations for the Password type input with auto-complete enabled

Conclusion

The results of vulnerability scans using Acunetix for information systems of toddler's growth and development in address http://siposyandu.com/ toddler who showed susceptibility to level 3 (high), which provides information 240 alerts covering 45 alerts in the category of High, Medium 166 alerts in the category, 17 alerts on Low category, and 12 in the category of Informational alerts. Vulnerability analysis on *siposyandu.com* information system based on the type of vulnerability can be recommended to repair the system.

References

Dukes, L; Xiaohong Yuan; Akowuah, F.. (2013). *A case study on web application security testing with tools and manual testing*. Southeastcon, 2013 Proceedings of IEEE. pp:1-6.

Garry, et al. 2009. *Database.* http://www.scribd.com/doc/30914906/Pengertian-Database#, Accessed on 15 April 2014

Indonesia's health ministry. (2011). *Early Stimulating, Detection and Intervention for Toddler's Growth Sevices*. http://www.depkes.go.id/1137-pelayanan-stimulasi-deteksi-intervensi-dini-tumbuh-kembang-anak.html. Accessed on 15 April 2014.

Indonesia's health ministry. 2010. *Child health Volunteers Book Series*. http://www.gizikia.depkes.go.id/download/Buku-Kader-Seri-Kesehatan-Anak.pdf. Accessed on 15 April 2011.

Nugroho, Adi. (2006). *E-commerce Understand The Modern Trading in Cyberspace*. Bandung: Informatika.

Nugroho, Bunafit. (2008). *Dynamic Web Applications with PHP programming and MySQL (Case Study: Create Data Processing Information on Books Systems)*. Yogyakarta: Gava media.

Sudarmilah, Endah, et al. (2013). *Prototyping on Web-Based Information System of Toddler's Growth and Development*. Proceeding of International Conference on Information Systems for Business Competitiveness (ICISBC 2013).

Wijaya, Awi Muliadi. (2011). *Basic Needs For Optimal Growth of Kids*. http://www.gizikia.depkes.go.id/archives/741. Accessed on 15 April 2014.

Yuniartini, Rika. 2010. *AHP (Analytical Hierarchy Process) Method Session 1*. http://jihadi.staff.umm.ac.id/files/2010/01/spk4.ppt. Accessed on 7 March 2014.

Contact email: Endah.Sudarmilah@ums.ac.id