SAVMDS: A Software Application Vulnerability Management Dashboard System

Mauranda Elliott, Huiming Yu, Xiaohong Yuan and Justin Zhan

***Abstract*-A vulnerability management tool, named A Software Application Vulnerability Management Dashboard System (SAVMDS), has been developed. The SAVMDS provides a user-friendly mechanism for managing software application products vulnerabilities. It provides functions to support Administrator, Chief Information Security Officer, Information Security Officer, Business Line Owner and Business Manager to record software application products vulnerabilities, analyze possible risks based on existing vulnerabilities and make smart decisions. The system has been implemented and tested. The experimental results demonstrate that due to its simplicity, a user with limited computer technical skills and knowledge can use it easily. It provides visual presentation to allow users to see different views of information in a single place and generate results that are easy to understand.**

***Index Terms*-software applications, vulnerability, risk, dashboard**

I. INTRODUCTION

Software vulnerability is a security flaw, glitch, or weakness found in software products that can lead to successfully application attacks and cause serious damages for a system or application. Vulnerabilities that are commonly encountered errors become a security concern when attackers discover the vulnerability, conduct research about it, and create a malicious code or exploit that targets this glitch to launch their schemes. These schemes may cause many different attacks such as gaining administrator privileges which gives attackers control over the vulnerable system. Vulnerability in PHP applications can easily cause remote code execution, SQL injection, format string vulnerabilities and Cross Site Scripting (XSS), Username enumeration. Buffer overflow may occur when users open a file that may be too big for the program to read [2, 3, 5, 7]. Software vulnerabilities have serious security implications and can cause unpredicted damages. It is very important for Web developers and administrators to have a thorough knowledge of software vulnerability and possible attacks caused by software application vulnerabilities.

Appropriately managing vulnerability and preventing attacks are critical jobs for System Administrator (admin), Chief Information Security Officer (CISO), Information Security Officer (ISO), Business Line Owner (BLO) and Business Manager (Manager) to ensure computer security and information assurance in a company/organization. Dashboards are powerful because they can pull together different views of information in a single place and provide one of the most impactful ways to visualize data [4, 6]. Vulnerability management dashboards can help companies/organizations track software products strengths and weaknesses, and show possible risks and direct future planning. They could also be critical tools for company's decision makers to be the best predictors of success. A vulnerability dashboard allows sharing of vulnerability, strength and weakness of applications security information among different departments in a company to ensure that they are all aligned toward the company's core value proposition [2, 4, 6]. Using a vulnerability dashboard a user is able to look at it and immediately get information of software application vulnerabilities and possible threats. Managers, Chief Information Security Officers, Information Security Officers, and Business Line Owners do not have to weed through pages of unnecessary data. Instead, a vulnerability dashboard can identify and display data based on advanced analysis by using right metrics. It can generate well-informed, evidence-based decisions derived from the information in a dashboard. Focused drill-downs into the data within a dashboard also allows these charge in the departments to focus their attention on a specific area and, if possible, to fix identified weaknesses. With information in the vulnerability dashboard they will pay attention to the different vulnerable applications.

Vulnerability management is a continuous information security process. A lot of organizations and companies just use a paper report as their way of managing vulnerabilities. In this way it is questionable how much it helps with actually action taking and really drilling in on what and where the problem is coming from. Based on the demands a vulnerability management tool, named A Software Application Vulnerability Management Dashboard System (SAVMDS), has been designed and implemented to help companies/organizations easily record software application products vulnerabilities, analyze existing risks, produce reports and make smart decisions. In the second part of this paper, the details of the SAVMDS will be presented. Implementation and experimental results will be discussed in

Manuscript received February 26, 2014; revised March 28, 2014. This work was partially supported by National Science Foundation under the award numbers DUE-0830686, CNS-0909980 and DUE-1129136.

Mauranda Elliott is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: melliott22.me@gmail.com).

Huiming Yu is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: cshmyu@ncat.edu).

Xiaohong Yuan is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: xhyuan@ncat.edu).

Justin Zhan is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: zzhan@ncat.edu).

section 3. The conclusion and future work will be given in section 4.

II. THE SOFTWARE APPLICATION VULNERABILITY MANAGEMENT DASHBOARD SYSTEM

A Software Application Vulnerability Management Dashboard System has been designed and implemented to allow users to successfully record application products vulnerabilities, to analyze existing risks and produce reports in a less complex manner than other methods. This dashboard is powerful because it pulls together different views of vulnerability information in a single place and provides one of the most impactful ways to visualize data. The dashboard is designed around what the CISO, ISO, BLO, and Manager desire. It provides more effective and easy ways for CISO, ISO, BLO and Business Manager to manage software applications vulnerabilities. The visualization technology is used to support drill downs, visualized views and a closer look of vulnerability related issues in a company/organization [1, 4, 8]. The dashboard has been designed to show the trends of vulnerabilities of applications within in companies/organizations. It helps to consolidate information from reports on vulnerabilities.

A. Design Considerations

The design considerations of the SAVMDS are that it must be simple, user friendly, interactive, easy to access and use. This tool is designed for different officers and managers who may not be computer experts and do not have lots of computer knowledge and skills. A user can simply read a few pages of instructions, then he/she can use this tool to know the application products vulnerabilities and distributed situation, analyze data, produce reports and make smart decisions. We also keep in mind to choose correct metrics for risks assessment, keep information visual and make it interactive with users.

B. The System Architecture

The Software Application Vulnerability Management Dashboard System consists of the user interface, functional components of Administer, CISO, ISO BLO and Business Manager. The functions of each component will be described in the following sections.

B.1. The User Interface

The design principle of the user interface is that it should be user friendly. One important consideration is how long a user who does not have computer knowledge and skills needs to learn and use this tool. The second consideration is to easily view the results. Visualization technology has been used to display the trends of vulnerabilities, to drill down deep if necessary, the accountability, time frame and what may cause worries in a company/organization. The third consideration is that the user interface has to be clear, concise, interactive and easy to be used.

Based on these considerations the SAVMDS provides a better way of monitoring for vulnerabilities of a company/organization's software products by using the categories; External and Internal. It allows business owners to keep and get a closer look and check on the different application vulnerabilities and the progress trends easily. It also helps the senior level personnel better understand existing vulnerabilities, risks and threats. The functions of the SAVMDS are requirements driven.

B.2. The Functional Components

The SAVMDS contains five major functional components to support different types of users that are Administrator (Admin), Chief Information Security Officer (CISO), Information Security Officer (ISO), Business Line Owner (BLO) and Business Manager (Manager). According to the specific requirements of each type of users the SAVMDS provides various functions and displays results in special formats. The systems functions used are buttons for navigating a user to either another page, sign out, sign in as an admin, CISO, ISO, BLO, and Manager. Figure 1 shows the system architecture and functional components. There are several dashboard databases that include different tables. One database named Login table that stores user names and encrypted passwords as well as type of users. Another database named Vulnerability Tables store all critical security informations such as product name, business unit, location, type vulnerability, severity level, status, etc.

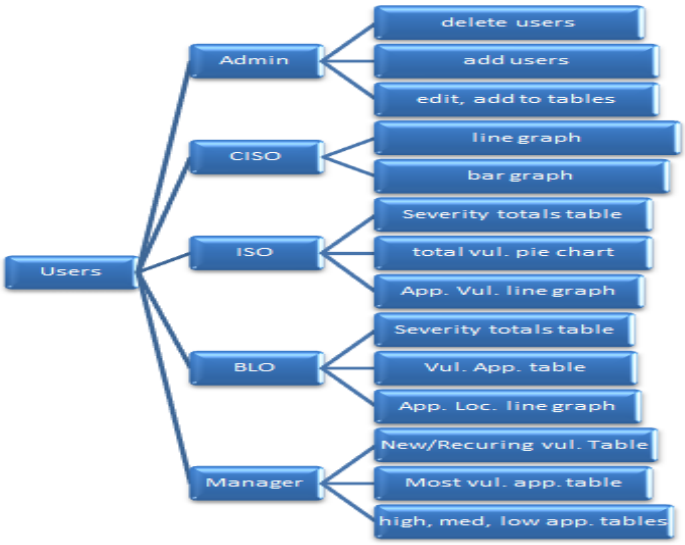

Figure 1. The System Functional Components Diagram

- The Functional Component of Administrator

An Administrator is the person who maintains the system, sets up users' login information, controls user access privilege, records software applications vulnerabilities, etc. The functional component of Administrator allows the administrator to add a user, delete a user, change a user

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

privilege, add new applications' information, update an application vulnerabilities, etc. Figure 2 is a snapshot that exhibits the user database structure and information. Figure 2 (a) is the administrator login information and (b) is other users login information that are encrypted. The login type will decide a user's access privilege.

username	password	type
elliott4499	cce5a79fd82fee8ef25429cac4a9a08b	admin

(a)

username	password	type
shimika24	f6945805845549a51dfeab80d0230918	CISO
malcome03	8d3322a1153d510e8391c032b5b6006e	ISO
macey07	d6b0ba2b1ef7a2ab8154a524b662c2a8	BLO
megan34	1b9d7c08398b6b0853d3f9ebed7f43fb	Manager
password	14c4b06b824ec593239362517f538b29	CISO

(b)

Figure 2. User Login and Access Privilege Information

- The Functional Component of Chief Information Security Officer

In general a Chief Information Security officer is the senior-level executive in a company/organization. He/she is responsible for information security and information assurance, information risk management, cybersecurity, information privacy, identity and access management, IT investigation, digital forensics, eDiscovery, disaster recovery, etc. Based on existing situation a Chief Information Security Officer must make effective and accurate decisions to enhance the company/organization's security. The SAVMDS supports a CISO in several ways. Based on the CISO requests it displays all products and associated vulnerabilities that occurred in the company, how many times these vulnerabilities occurred every year/total, numbers of vulnerabilities that occurred in different locations and total vulnerabilities by business units in a pie, etc. A CISO can also retrieve information from the Vulnerability Tables, analyze existing risks, make a smart decision and produce reports.

- The Functional Component of Information Security Officer

An Information Security Officer may direct the information security support, direct the management and support of day to day information security administration, provide technical and problem support, direct development, maintenance and distribution of all information security related polices, standards, guidelines and procedures, etc. He/she may oversight the risk management tools and risk assessments to ensure accuracy and completeness of information and security practices, and the changes to the environment that have security components. The SAVMDS provides various functions to support an ISO. The ISO can request information and the SAVMDS will display them in different formats. The SAVMDS also allows an ISO to select different year as shown in Figure 3. It supports an ISO to view vulnerabilities by business units, conduct comparison among different districts, look at business unit severity levels, etc. A user can select different parameters to get expected results. The results can be displayed as a pie chat with calculated percentages or a bar chart.

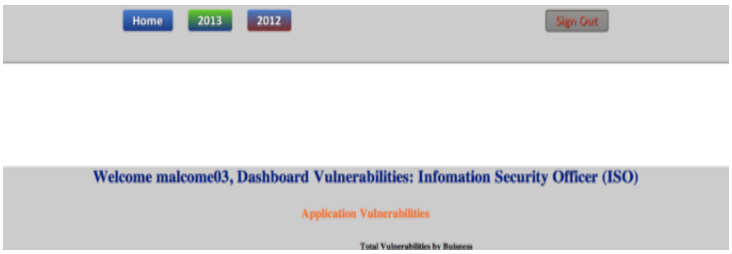

Figure 3. A Page allows the ISO to Select a Year

- The Functional Component of Business Line Owner

In general a Line of Business Owner often refers to an internal corporate business unit. It refers to a set of one or more highly related products which service a particular customer transaction or business need. In some industry sectors, it also has a regulatory and accounting definition to mean a statutory set of policies. In this paper a Business Line Owner (BLO) is a person who is in charge of an internal business unit. He/she may be responsible for shared services that may include communications, program supports; for operations and business continuity that may include implementation, training and customer support. Figure 4 is an example that demonstrates that the SAVMDS provides functions to allow a BLO to view vulnerabilities in the business unit that includes software application product names and the type of vulnerabilities occurred.

- The Functional Component of Business Manager

Business managers are responsible for overseeing and supervising a company's activities, and ensuring employees adhere to company's policy and regulations. Business managers may also oversee company/organization security related activities. The SAVMDS is designed to allow a business manager to see all vulnerabilities that occurred in the company/organization and estimate the level of existing risks. One display can show the status of vulnerability that can be new or recurring, vulnerability name, application name and the date that the vulnerability occurred. It also allows a manager to see high severity, medium severity and low severity vulnerabilities separately. A user can use Retrieve and Sort capability to get views he/she wants to see. One table contains the information for the new/recurring vulnerabilities with their status, severity, application, id number, and date. This table can be found on the Manager's page when they login.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

App/System	*Vulnerabilities*
Transaction Control	Buffer overflow
Customer Information Service	SQL injection
Customer On-line Help System	Denial of Service
…	…

Figure 4. Applications and Vulnerabilities in a Business Unit

III. IMPLEMENTATION AND EXPERIMENTAL RESULTS

We have implemented the Software Application Vulnerability Management Dashboard System and tested it in the laboratory environment. The technologies used include visualization technique, Web application design and implementation techniques, MySQL database, XAMMP, PHP and Perl programming languages and Apache. XAMMP is a free and open source cross-platform Web server solution stack package that consists of the Apache HTTP Server, MySQL database, and interpreters for scripts written in the PHP and Perl programming languages. We also used Jpgraph to create and display the graphs.

The languages that were used were HTML, JQUERY, PHP, CSS (Cascading Style Sheets), and Java Script. Hyper Text Markup Language which is the main markup language for creating web pages and other information that can be displayed in a web browser was used to code the webpages and CSS was used to define the style to display the code in HTML elements. Java Script was used by JQUERY to define a table in knowing what to call from the tables that were put in the database as shown in Figure 5. MySQL is the database that was used for creating the tables and storing application products and vulnerabilities related information.

```
<?php
    $sql_query = "SELECT * from vulnerabilities;";
    $result = mysql_query($sql_query);
    while ($row = mysql_fetch_array($result))
        {
            $status = $row["Status"];
            $Vul = $row["Vulnerability"];
            $App = $row["Application"];
            $Date = $row["Date"];
            echo "<tr>";
                echo "<td style='padding:0 15px 0 15px; '> $status";
                    echo "</td>";
                echo "<td style='padding:0 15px 0 15px;'> $Vul";
                    echo "</td>";
                echo "<td style='padding:0 15px 0 15px;'> $App";
                    echo "</td>";
                echo "<td style='padding:0 15px 0 15px;'> $Date";
                    echo "</td>";
            echo "</tr>";
        }
    echo "</table>";
?>
```

Figure 5. Retrieve Required Information

The Software Application Vulnerability Management Dashboard System has been run successfully in a laboratory environment. A set of experiments has been conducted to test the functions of the SAVMDS. The experiment results demonstrate it is easy to use, generates graphic views, displays analyzing results and produces reports. Figure 6 is the login screen to allow users to login with their username, password, and choose from the options under user type (admin, CISO, ISO, BLO, and Manger), it will then navigate them to the next page. Figure 7 shows an ISO's view that is the result of comparing the numbers of vulnerability in twelve business units between 2012 and 2013.

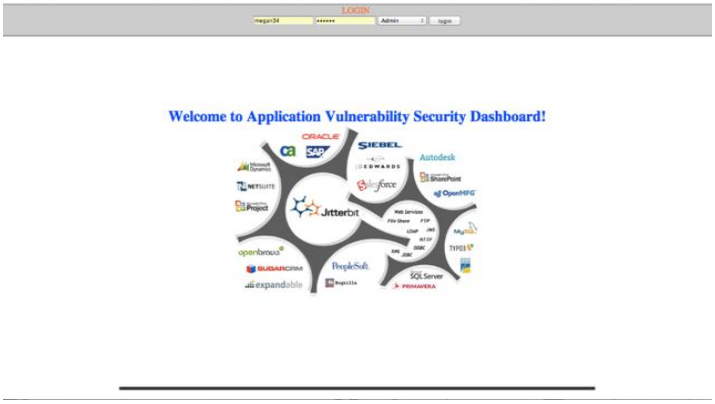

Figure 6. Login Page

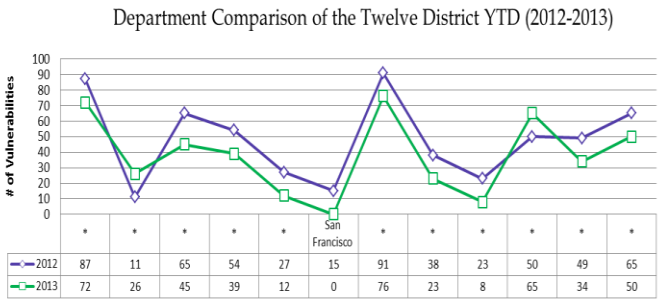

Figure 7. An Example of ISO View

IV. CONCLUSION AND FUTURE WORK

We have designed and implemented a Software Application Vulnerability Management Dashboard System. It provides a user-friendly visualized mechanism for managing software application products vulnerabilities. The SAVMDS was developed to make the company/organization more aware of the vulnerabilities that are being tracked on the applications running in the company/organization daily and risks caused by these vulnerabilities. It provides functions to record software application vulnerabilities, analyze existing risks, compare existing vulnerabilities among applications or business units, generate reports and help users to make smart decisions.

We have tested the SAVMDS in a laboratory successfully. The experimental results demonstrate that the SAVMDS is a user friendly tool that helps administrators, CISO, ISO, BLO and Business Managers to record and trace

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

applications vulnerabilities, view different results in an easier manner.

In the future we will contact external companies and organizations to use the Software Application Vulnerability Management Dashboard System. Based on users' feedback we will modify and update it.

ACKNOWLEDGEMENTS

This work was partially supported by National Science Foundation under the award numbers DUE-0830686, CNS-0909980, DUE-1129136.

REFERENCES

[1] R. Batchelor, "Executive dashboard: a decision maker's favorite", *Franchising World, Vol. 37 Issue 10*, October 2005.

[2] Y. Chang, P. Zavarsky, R. Ruhl and D. Lindskog, "Trend analysis of the CVE for software vulnerability management", *IEEE International Conference on Privacy, Security, Risk, and Trust*, 2011.

[3] P. Foreman, Vulnerability management, Auerbach Publications, Taylor & Francis Group, 2010.

[4] D. Hoang, T. Nguyen and A. Tjoa, "Dashboard by-example: a hypergraph-based approach to on-demand data warehouse systems", IEEE International Conference on systems, man, and cybermetics, October 2012.

[5] ISO/IEC, "Information technology: security techniques-information security risk management", ISO/IEC FIDIS 27005: 2011.

[6] J. Korczak, H. Dudycz and M. Dyczkkowski, "Intelligent dashboard for SME managers, architecture and functions", The Federated Conference on Computer Science and Information Systems, 2012.

[7] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems", *NIST SP 800-30*, July 2002.

[8] Tableau Software, "Top 5 practices for creating effective dashboards", http://www.tableausoftware.com/sites/default/files/whitepapers/dashboards-for-financial-services.pdf, 2012.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)