International Journal of the Physical Sciences Vol. 7(7), pp. 1057 - 1061, 9 February, 2012
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS11.1220
ISSN 1992 - 1950 © 2012 Academic Journals

*Full Length Research Paper*

# Web's critical survey analysis with respect to current loopholes

**Maqsood Mahmud* and Abdurrahman Alkarim Mirza**

Department of Information Systems, King Saud University, Riyadh, Kingdom of Saudi Arabia.

Accepted 23 January, 2012

**Vulnerabilities are the loopholes that arise due to poor programming. Web applications are considered to be very vulnerable to attack as compared to desktop programs on sole computers. Keeping this thing in our minds, we decided to find out all the possible vulnerabilities in Saudi Arabian organization's web servers. To assess these vulnerabilities, we selected number of open source tools and tested about 169 most popular web servers of government, financial and academic organizations and commercial organizations. This problem seemed interesting to us because of two reasons, first, security is a burning issue of the world and it can be minimized by finding out the vulnerabilities. By finding out vulnerabilities, it becomes easy to fix them. Secondly, it is in the interest of Saudi Arabian national goals. This problem was not addressed before for Saudi Arabian organizations web servers, so, that is why it carries high importance. Our solution to this problem is to check each server with two different vulnerabilities assessment tools. The purpose of using two different tools is to avoid false positive and false negative. Our purpose is not to hack these respectable organizations but to assess them with respect to security so that these may not be the victim of future cyber attacks. We will enlist all the vulnerabilities found by the tools with respect to their organizations. The vulnerabilities will be shown anonymously and with the level of severity. These vulnerabilities will be followed by a graph showing the "organization versus vulnerabilities" relationship. A graph on "recommended patches versus vulnerable organization server" is also included for those organizations that are conscious about their organization privacy and confidentiality. Saudi organization may contact us to know about their web server vulnerabilities to fix them in time.**

**Key words:** Saudi Arabia, critical analysis, websites, loopholes, assessment.

## INTRODUCTION

Web sites and web applications are rapidly growing in today's business complex environment. As more and more security critical applications, such as banking systems, governmental transaction interfaces and e-commerce platforms, are becoming directly accessible via the web, the role of web application security and defense has been gaining importance (Kals and Kirda, 2005). These applications are now delivered over the web (HTTP). The increased "web hacking" activities, worms on the web have made the lives of business environment miserable. E-commerce/E-government/Web hacking is unfettered. Web traffic is the most commonly allowed of protocols through internet firewalls. Hyper text transfer protocol (HTTP) is perceived as "friendly" traffic. Content/Application based attacks are still perceived as rare (Livshits and Erlingsson, 2007). A web hacker needs only three things to exploit the web application.

Hyper text transfer protocol secure (HTTPS) is a secure version of the hyper text transfer protocol (http). It is a secured means of transferring data using the *https protocol* in the World Wide Web where secure e-commerce transactions, such as online banking transactions and other financial transactions are involved. In other words, HTTPS encrypts the session with a digital certificate, that is, HTTP over secure sockets layer (SSL) which can be used by web browsers and HTTPS-capable client programs. So, if the website begins with https:// instead of http://, it is a secure site. Almost 99% of the browsers can connect to web servers either using http or https. The address bar in the browser will begin with https

*Corresponding author. E-mail: maqsood.m@ksu.edu.sa.

instead of http, if a web site is secured. Web browsers like IE, Firefox, etc, display a pad ”lock” icon to indicate the website is secure, which also displays https in the address bar. This padlock icon is displayed only when an SSL certificate is installed by their web server. If the padlock icon and the web link begin with https, then it can be concluded that the site is legitimate and secure to provide confidential information or carry financial transactions. Hence the HTTPS Protocol work with the combination of programs including the browser programs which takes care of the encryption/decryption routines that exist on the web hosting servers. Most typically, HTTP data is sent over transmission control protocol/internet protocol (TCP/IP) port 80, whereas SSL HTTP data is sent over port 443 (Tripunitara and Dutta, 2010).

Vulnerabilities provide the entry gate for computer attacks. Vulnerabilities persist for a number of reasons, including poor security practices and procedures, inadequate training for individuals responsible for network security and software products of poor quality (Bush, 1999). For example, within some enterprises and government agencies, an important security patch might not be scheduled for installation on computers until sometime after the patches are made available by the vendor. This delay tends to happen if a company or government agency fails to enforce its security policy, if the security function is under resourced, or if the patch disrupts the computer when it is installed, causing the system administrator an inordinate amount of time to fix the computer configuration to receive the new patch (Guirguis, 2007).

Threats are the potential means by which the value of information can be degraded. Information security comes down to three primary concepts: confidentiality, privacy and reliability. Information represents a value to your organization according to how it contributes to your objectives. In the case of business, the final value relates to how information supports the generation of revenue and profits. From this perspective, the final goal of information security is to preserve the value of information (Huang et al., 2003; Jaffar et al, 2011). The value of information can be degraded by several means. Information security should deal effectively with threat, risk and impact relative to the value of information. Threats are the potential means by which the value of information can be degraded. Risk is the probability that a specific threat will occur. Impact is the degree to which the value of information is degraded should a threat be realized.

Our objectives are based on the following three elements. Assessment of Saudi Arabian web Servers is to be conducted in such a way that information about holes, warnings, open ports and notes may be analytically viewed with different perspectives and goals.

Categorization of the most common vulnerabilities with respect to the number of organizations and vulnerability names, their symptoms, explanations, solutions and risk factors. The main goal of this research is the raising of flag and awareness about the security threats in Saudi society and all the organizations that are victim of intruders and viruses (Alhazmi and Malaiya, 2004). Awareness in the upcoming softwares and web servers threats, reviews and assessment of web servers on annual basis and to raise the security measures in Saudi organizations are our future perspectives.

## METHODOLOGY

The methodology followed is described as: the collection of web server names from popular websites of Saudi Arabia (Jovanovic, et al., 2006) and their corresponding IP address using website and ping and whois DOS commands. 169 diverse web servers of all Saudi Arabia organizations were assessed, which includes educational, commercial, financial, banks and governmental organizations. The earlier described tools were used on each web server to assess their vulnerabilities and to check, open ports, holes, warnings and notes. Then graphical results were made on the basis of scanning results above 169 web servers. The comparison graphs were based as holes (or open ports or notes or warnings) versus total averages holes (or open ports or notes or warnings) per sector (like education or finance, etc) Seo et al., 2004. Graphs on comparing the vulnerability versus number of web server (victim) were also made (Swiler et al., 2002). Graphs on the dependency of holes and warnings are drawn to show that holes generate warnings or threats for web servers. Comparison graph of web server tools is drawn to guide the security professional in selection of tools for their organization to judge the pros and cons of the tools with respect to usability comfort, effectiveness and avoid false positive (Ritchey and Ammann, 2000).

The organization names were not in the graphical results because of the organization's privacy and confidentialness. Organizations are numbered as Org1, Org2 and Org3, etc. In our research paper, we will use two tools (open source) for assessing the vulnerabilities of government organizations in Saudi Arabia. The purpose of selecting two tools rather than one is to avoid false positives and false negatives. We will assess about one hundred different web servers of the organizations according to the vulnerabilities which they possess. The purpose of finding the vulnerabilities is to facilitate the web administrators of the organizations to fix it before these has been exploited by the attackers. We will draw two graphs; one will be showing a relationship between “vulnerabilities versus organization”, the second would be showing the relationship between the “vulnerabilities versus patches”.

## FINDINGS

For carrying out our research work on the vulnerability assessment of the Saudi Arabian organizations, we choose the following two tools, that is, Nessus and Nikto (Myerson, 2002). Graphical results were made on several conceptual elements in mind. Diverse statistical and graphical analyses were brought into consideration to achieve maximum output on the research conducted. The following diverse graphical results were extracted from the scanning of the 169 web servers. We did not use the Numbers of graphs based on the scanning results were

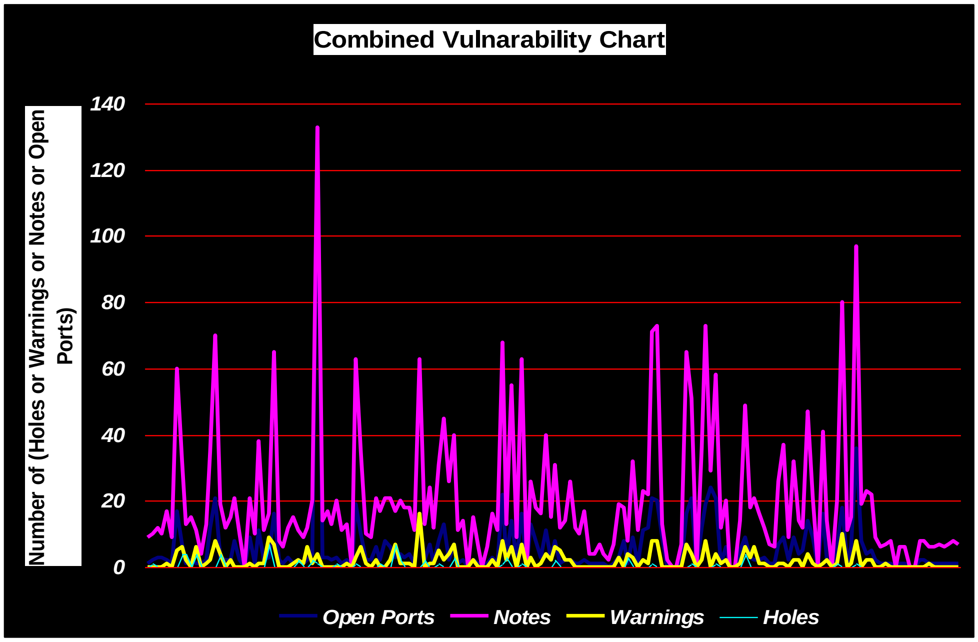

**Figure 1.** Combined (H, N, W and O.P).

dangerous option/plug-in Nessus, because that would have defaced or damaged the websites made as follows. The graph as shown in Figure 1 reveals the whole view of all open ports, warnings, notes and holes in all web servers of Saudi Arabia. One can easily judge the overall web security strength of the whole Saudi Arabia organizations from the following graph.

X-axis of the figure shows the organizations name anonymously as (Org1, Org2, Org3, etc). The figure shows holes with light green, warnings with yellow, open ports with blue and notes with pink color lines. Y-axis shows the number of H, W, O.P or N. Notes exist more as compared to H, W and O.P. Open ports are in second number to notes. Yellow color lines of warnings are third in majority, while the holes are in minority in all Saudi Arabian organizations in totality.

## Most known vulnerabilities charts

Here, is dedicated to the most known Saudi Arabian web servers holes, warnings, notes and open ports. The graph of Figure 2 shows vulnerability names in Saudi Arabian web servers on its x-axis, and on y-axis, it shows the number of organizations that are the victim of the respective vulnerabilities. These are the vulnerably that causes holes in web servers. Most of the web servers in Saudi Arabia are the victim of the vulnerability named (PHP < 5.2.5). About 27 web servers in Saudi Arabia are the victim of this vulnerability as shown in the graph. The lowest number of organizations is victim by the vulnerability named (PASSWORDLESS). Other vulnerability details, that is, begins with heading of vulnerability names, its synopsis, solution, risk factor, description and explanation with dangerous vulnerabilities. This is for the purpose of reference in case of problems on daily routine scanning of your web servers.

## Overall vulnerability graph readings

The pie chart in Figure 3 depicts the overall overview of the averages of all Saudi Arabia organizations. It shows that in the Kingdom of Saudi Arabia, the average percent of holes (shown in light green color) are lesser as compared to warnings, open ports and notes. Warnings are shown in yellow portion of the pie chart. Bringer color portion in the chart shows the open ports in all Saudi Arabia which is not good indeed (Vidalis and Jones, 2003).

Organization in Saudi Arabia must close the unused ports of communications so that people from outside may not be connected in an unauthorized way for malicious deeds. Since Microsoft Windows comes with ports opened when install on a PC. So, network administrators are advised to close the ports first and then open those ports that are unavoidably needed by the organizations, while the other open source operating systems like UNIX, Sun Solaris Mac or Linux and its flavors come with all ports closed by default. So, in case of operating system (OS), the open source OS are considered more secure by default. The light red (or maroon) color portion in graph informs us about notes.

The overall findings that we observed from the pie chart,

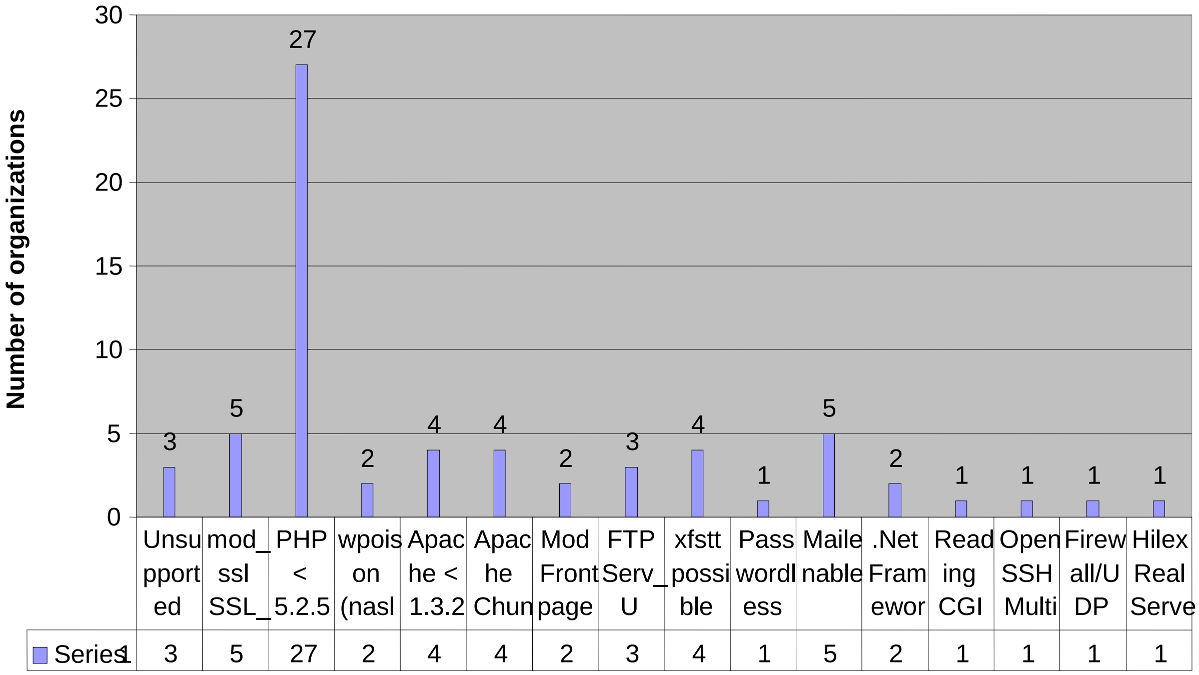

**Figure 2.** Holes vulnerabilities versus number of organizations.

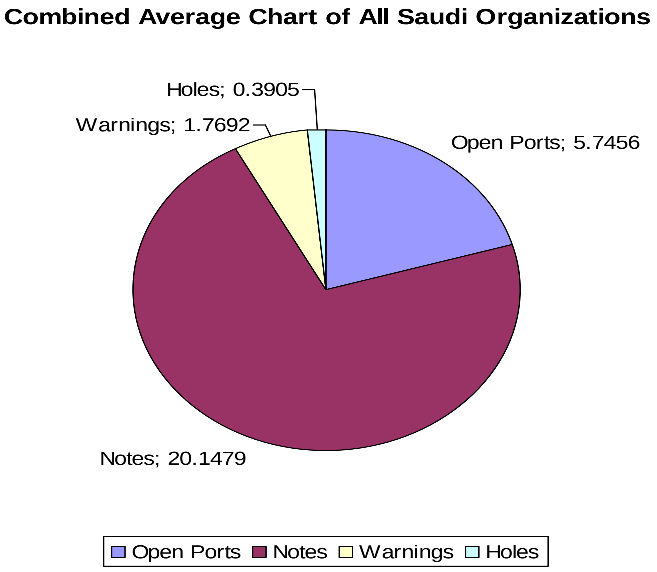

**Figure 3.** Resultant vulnerability graph.

that is, notes are in majority, then open ports comes in the second position, warnings are third in positions, while overall holes with respect to W, O.P and N are less in Saudi Arabian organizations.

## CONCLUSION AND FUTURE WORK

We need to create heightened levels of security awareness. The use of formal software engineering methods for developing web applications should be emphasized and implemented. The use of secure coding practices should be brought into high consideration. Thorough application testing must be made to assess the security aspects. Moreover, there is no patch for carelessness. So, a little care can save us from the hazards of cyber threats. The unused open ports must be closed to avoid unauthorized access by intruders remotely in all organization of Saudi Arabia especially in governmental and finance, because of their privacy and confidentiality. Similar assessment survey study can be made on yearly or quarterly basis to know about time to time situations of security of Saudi Arabia. This assessment study may not be limited to this country. Similar survey can be conducted on every country level by the governmental agencies or authorized consultants to know the situations of the web security and their strengths. We also intend to develop our own tool in open source that may be having the potentialities of all the tools that we studied and used. Some extra features related to IDS will also be introduced in the tool.

## ACKNOWLEDGEMENT

This work was supported by the Research Center of College of Computer and Information Sciences, King Saud University. The authors are grateful for this support.

### REFERENCES

Alhazmi OH, Malaiya YK (2004). Quantitative Vulnerability Assessment of Systems Software”, Colorado State University.

Bush SF (1999). Network Vulnerability Analysis Tool Precis”, General Electric corporate research and development, KWC-512, Niskayuna, NY p. 12309,

Guirguis M (2007). Computer science department, Texas State University, San Marocs USA, Bestavros, Azer and Matta, Ibrahim, Computer Science Department, Boston University, Boston USA, and Zhang, Yuting, Computer Science Department, Allegheny College, Meadville USA.

Huang Y-W, Huang S-k, Lin T-P, Tsai C-H (2003). Web Application Security Assessment by Fault Injection and Behavior Monitoring” institute of Information Sciences, Academia Sinica Nankang 115 Taipei and Department of Computer science and information Engineering, National Chiao Tung University 300 Hsinchu, Taiwan.

Jovanovic N, Kruegel C, Kirda E (2006). Pixy: A static Analysis Tool for Detecting Web Application Vulnerabilities” Technical University of Vienna Secure System Labs.

Kals S, Kirda E (2005). SecuBat: A web Vulnerability scanner” secure systems lab technical university of Vienna.

Livshits B, Erlingsson U (2007). Using Web Application Construction Framework to Protect Against Code Injection Attacks”, Microsoft Research.

Myerson JM (2002). Identifying Enterprise network vulnerabilities” Int. J. Network Manage., (12): 135-144.

Ritchey RW, Ammann P (2000). Using Model Checking to Analyze Network Vulnerabilities”, National Security Team, Booz Allen & Hamilton Falls church, Virginia and Information and Software engineering Department, George Mason University Fairfax, Virginia.

Seo J, Kim H-S, Cho S, Cha S (2004). Web server attack categorization based on root causes and their locations” Division of computer science, Department of EECS, KAIST and AITrc/IIRTRC/SPIC 373-1, Kusong-dong, Yusong-gu, Daejon, South Korea

Swiler LP, Phillips C, Ellis D, Chakerian S (2002). Computer-Attack Graph Generation Tool”, Sandia National Laboratories, Albuquerque, NM p. 87185.

Tripunitara MV, Dutta P (2010). Security Assessment of IP-Based Networks: A Holistic Approach”, AT&T Labs USA.

Vidalis S, Jones A (2003). Using vulnerability trees for decision making in threat Assessment” School of computing, University of Glamorgan, Pontypridd, CF37 IDL, Wales, UK.