A Critical Survey of different Security aspects in Saudi Arabian Web Servers

Saleh M. Al-Saleem[1,2]

[1]Department of Information Systems, College of Computer and Information Sciences, King Saud University Riyadh, Saudi Arabia
[2]Department of Computerized Based Testing, National Center for Assessment in Higher Education, Riyadh, Saudi Arabia

Summary
Assessment of web servers on country level shows the overall sense of security for secure businesses, official and educational activities. In this research paper we decided to find out all possible vulnerabilities in Saudi Arabian web servers. To assess these vulnerabilities we selected number of open source tools and tested about 169 most popular web servers of government, Financial, Academic, and commercial organizations. The challenge of this work was the selection of an appropriate tool and proper assessment of the most popular web servers in every sector of the country. This assessment seemed to us interesting because of two reasons, first security is a burning issue of the world and it can be minimized by finding them out .Secondly it is in the interest of Saudi Arabian national goals. This way many unknown vulnerabilities can be known to the programmers easily. This problem was not addressed before for Saudi Arabian web servers according to our literature review, so that's why it carries high importance. The purpose of using different tools is to avoid false positive and false negative. We will analyze and enlist all the vulnerabilities found out by the tools with respect to their organizations. The vulnerabilities will be shown anonymously and with the level of severity. These will be followed by graphs showing the "organization vs. vulnerabilities" relationship. A graph on "recommended patches vs. vulnerable organization server" is also included for those organizations that are conscious about their Organization privacy and confidentiality.

Key words:
Vulnerability, Assessment, web server, Saudi Arabia.

1.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 [2]. 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. HTTP is perceived as "friendly" traffic [2].

1.1 Our Goals /Objectives

Our goals are based on the following elements.

1.1.1 Assessment

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.

1.1.2 Categorization

Categorization of most Common Vulnerabilities with respect to number of organizations and vulnerability names, their symptoms, explanations, solutions and risk factors.

1.1.3 Raising the Flag

Raising the flag and awareness about the security threats in Saudi Society and all the organizations that are the victim of intruders and viruses is the main goal of our research.

1.1.4 Future Perspectives

Awareness in the upcoming software 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.
The paper is organized as follows: A background study about the tools used is given in section 2. Methodology is elaborated in section 3. Results and discussion are provided in section 4. Comparison with similar projects is made in section 5. And finally Recommendations and Conclusion are offered in section 6.

2.Background

Some background knowledge has been specified about the tools used for those who are new in the field of security and web threats.

Manuscript received February 5, 2015
Manuscript revised February 20, 2015

2.1 Tools Used

For carrying out our research work on the vulnerability Assessment of the Saudi Arabian Organizations we chose the following two tools.

2.1.1 Nessus

This software offers the power of the vulnerability scanner for both Microsoft Windows platform and open source Operating Systems. It is ideal for usage by a security consultant who wishes to conduct a vulnerability audit, or by an administrator who wishes to audit their network. It is generally a network scanner tool in broad sense but has the facility to scan websites as well. It also works with Nikto in integrated form [10].

2.1.2 Nikto

Nikto is an open source common gateway interface (CGI) script scanner. Nikto not only checks for CGI vulnerabilities but does so in an evasive manner, so as to elude intrusion detection systems. It comes with thorough documentation which should be carefully reviewed prior to running the program. If you have Web servers serving up CGI scripts, Nikto can be an excellent resource for checking the security of these servers [4].

3.Our Methodology

The methodology followed is described as: The collection of web server names from popular websites of Saudi Arabia [11], [14] and their corresponding IP address using website [8] and ping and whois DOS commands. 169 diverse web servers of all Saudi Arabian organizations were assessed which including academic, commercial, financial, banks and governmental organizations. The above 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 of above 169 web servers. The comparison graphs were based as open ports or Warnings vs. total averages open ports or Warnings. Graphs on comparing the vulnerability vs. number of web server (victim) were also made.

Note: The organization names were not shown in the graphical results because of the organization's privacy and confidentialness. Organizations are numbered as Org1, Org2 and Org3 and so on.

We have divided our findings in the following way.

- Our main findings include, counting the number of Holes, Warnings and Open Ports per organization.
- To show the vulnerabilities causing Holes and Warnings versus number of organizations those are victim of it.

4. Results and Discussion

4.1 Open Ports Readings

The graph in Figure-1 shows the number of open ports in various organizations of Saudi Arabia. We can extract the information about the highest number of open ports in a particular organization. So we can know the web server that has high probability of being hacked by intruders. We can also calculate the average number of open ports per organization from the graph which is almost near to 10% per organization. A table of open ports along with their respective protocols is also included in the following. Relationship between ports and Holes/Warning along with their frequency is also shown through a table in this section.

4.2 Warning Readings

As evident from the chart in Figure-2, it gives us information about Number of Warnings in all 169 organizations. It shows the relationship between open ports and Holes or Warnings. Whenever a port is open there will be some kind of vulnerability on that port. The frequency shows the repetition of the same vulnerability for different organizations. The detail about some of the vulnerabilities is given in section 4.3.1.

4.3 Most Know Vulnerabilities

This section is dedicated to the most known Saudi Arabian Web servers Holes, Warnings, Notes and Open Ports .Below are the details with graphs.

4.3.1 Most Known Warnings Vulnerabilities w.r.t number of organizations

The graph in figure 3 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 warnings in web servers. Most of the web servers in Saudi Arabia are the victim of the vulnerability named (weak Supported SSL cipher suite).About 23 web servers in the Saudi Arabia are the victim of this vulnerability as obvious from the graph. The lowest number of organizations is victim by the vulnerability named (mail relaying),(doc directory browsable),(PHP 5.2.3 Multiple Vulnerabilities),(Apache) and so on with on web server affected till (private IP Address Leak in HTTP Header).

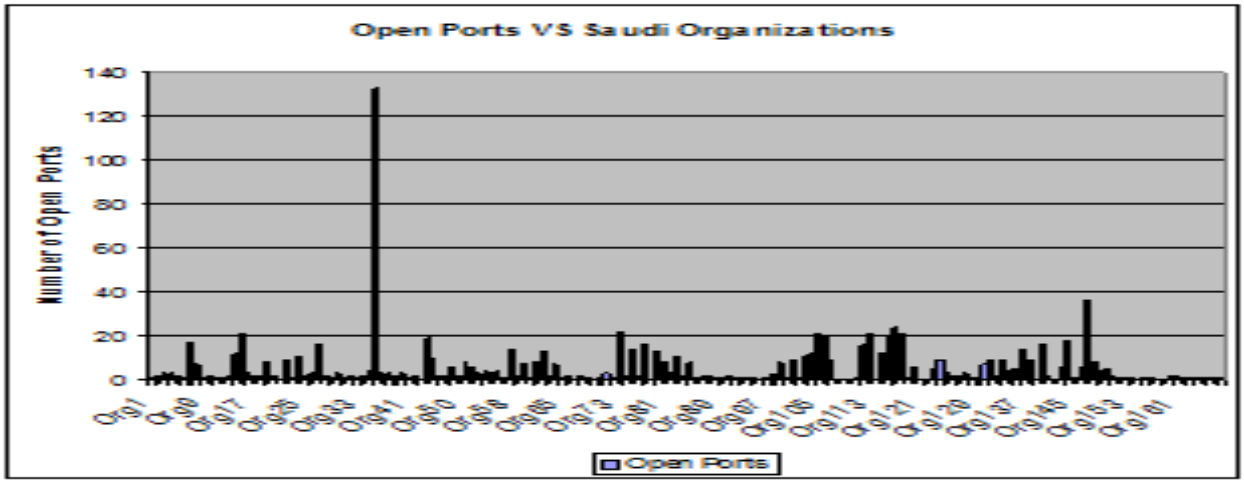

Figure 1: Open Ports VS Saudi Organization

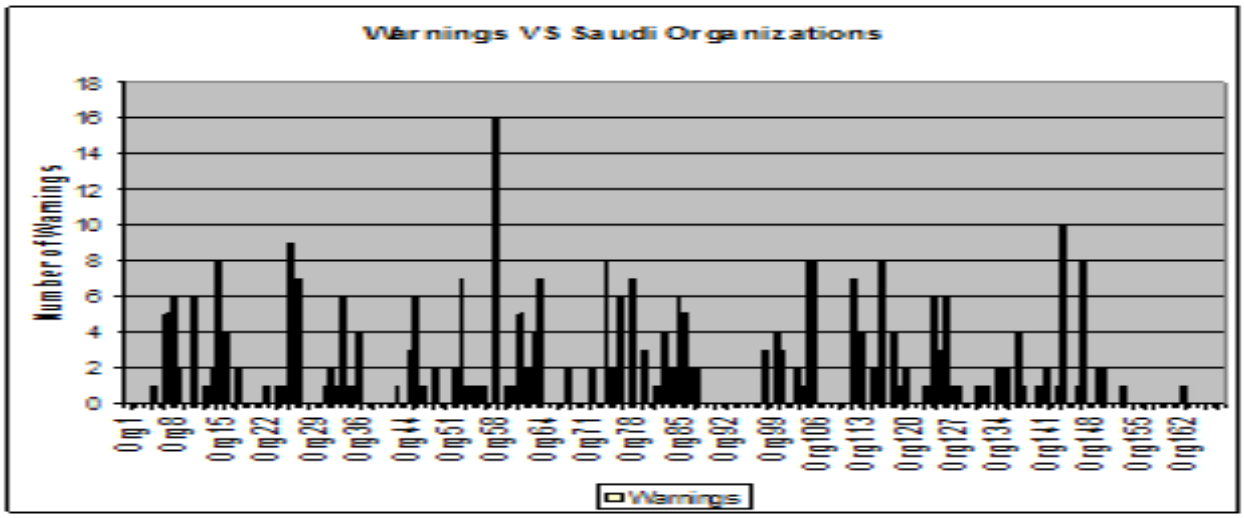

Figure 2: Warnings VS Saudi Organizations

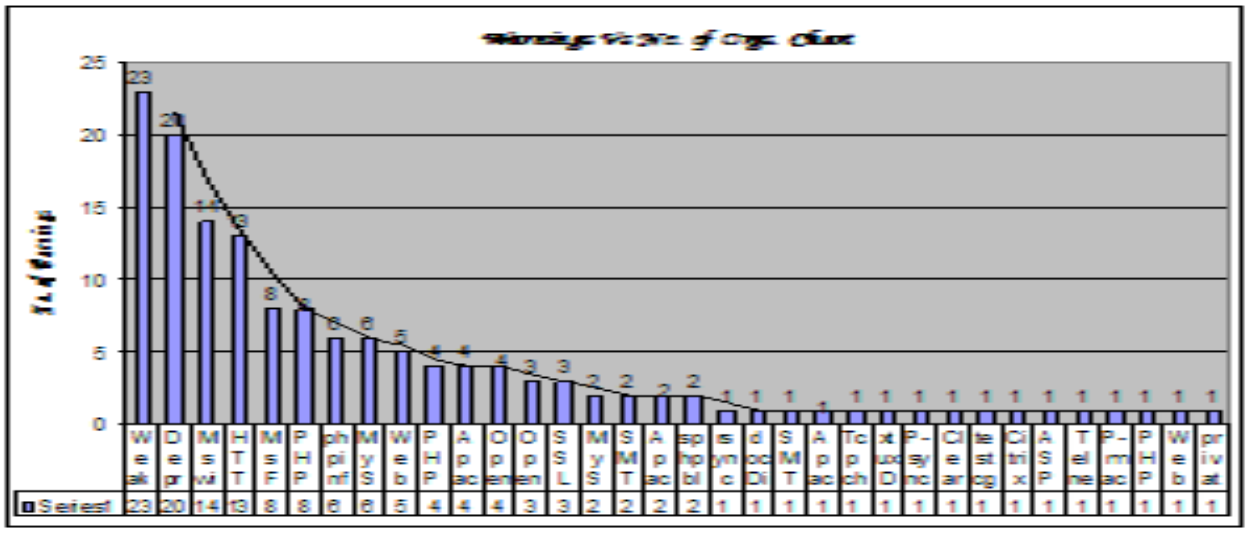

Figure 3: Vulnerabilities of Warnings Vs No. of Organizations

Other vulnerability details i.e. begins with the heading of Vulnerability Names, its Synopsis, Solution, and description. This is for the purpose to refer in case of facing it in daily routine scanning of your web servers. Here we have mentioned only the top ten vulnerabilities with respect to warnings.

4.3.1.1 Vulnerability Name: Weak Supported SSL Ciphers Suites

Synopsis: The remote service supports the use of weak SSL ciphers.

Description: The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all. The ciphers command converts textual OpenSSL cipher lists into ordered SSL cipher preference lists. It can be used as a test tool to determine the appropriate cipherlist.

Solution: Reconfigure the affected application if possible to avoid use of weak ciphers.

4.3.1.2 Vulnerability Name: Deprecated SSL Protocol Usage

Synopsis: The remote service encrypts traffic using a protocol with known weaknesses.
Description: The remote service accepts connections encrypted using SSL 2.0, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

Solution: Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead.

4.3.1.3 Vulnerability Name: Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure Vulnerability

Synopsis: It may be possible to get access to the remote host.
Description: The remote version of Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man in the middle attack. There is a bug in certain versions of Microsoft FTP server which can be exploited in this fashion. In addition, other FTP servers may react adversely to such a string. An attacker may exploit this flaw to decrypt communications between client and server and obtain sensitive information (passwords).

Solution: Force the use of SSL as a transport layer for this service.

4.3.1.4 Vulnerability Name: HTTP TRACE / TRACK Methods

Synopsis: Debugging functions are enabled on the remote web server.
Description: The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution: Disable these methods. OR Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy.

4.3.1.5 Vulnerability Name: MS FTPd DoS

Synopsis: It may be possible to make the remote FTP server crash by sending the command 'STAT? AAA...AAA.
Description: An attacker may use this flaw to prevent your site from distributing files
Solution: Apply the relevant hotfix from Microsoft

4.3.1.6 Vulnerability Name: phpinfo.php

Synopsis: The following files are calling the function phpinfo () which disclose potentially sensitive information to the remote attacker: /phpinfo.php.

Description: Many PHP installation tutorials instruct the user to create a file called phpinfo.php. This file is often times left in the root directory after completion. Some of the information that can be garnered from this file includes: The username of the user who installed php, if they are a SUDO user, the IP address of the host, the web server version, The system version(UNIX / Linux), and the root directory of the web server.

Solution: Delete them or restrict access to them

4.3.1.7 Vulnerability Name: MySQL Anonymous Login Handshake Information Leakage Vulnerability

Synopsis: The remote database server is affected by an information disclosure flaw.

Description: The MySQL database server on the remote host reads from uninitialized memory when processing a specially-crafted login packet. An unauthenticated attacker may be able to exploit this flaw to obtain sensitive information from the affected host as returned in an error packet.

Solution: Upgrade to MySQL 4.0.27 / 4.1.19 / 5.0.21 / 5.1.10 or later.

4.3.1.8 Vulnerability Name: Web Server Uses Plain Text Authentication Forms

Synopsis: The remote web server might transmit credentials over clear text

Description: The remote web server contains several HTML forms containing an input of type 'password' which transmit their information to a remote web server over plain text. An attacker eavesdropping the traffic might use this setup to obtain logins and passwords of valid users.

Solution: Make sure that every form transmits its results over HTTPS

4.3.1.9 Vulnerability Name: OpenSSL denial of service

Synopsis: The remote service is prone to a denial of service attack.

Description: According to its banner, the remote host is using a version of OpenSSL which is older than 0.9.6m / 0.9.7d. There are several bugs in such versions that may allow an attacker to cause a denial of service against the remote host.

Solution: Upgrade to version 0.9.6m / 0.9.7d or newer.

4.3.1.10 Vulnerability Name: OpenSSL password interception

Synopsis: The remote host is using a version of OpenSSL which is older than 0.9.6j or 0.9.7b

Description: This version is vulnerable to a timing based attack which may allow an attacker to guess the content of fixed data blocks and may eventually be able to guess the value of the private RSA key of the server.

An attacker may use this implementation flaw to sniff the data going to this host and decrypt some parts of it, as well as impersonate your server and perform man in the middle attacks.

Solution: Upgrade to version 0.9.6j (0.9.7b) or newer

5. Related Work

Tracy, Jansen, Scarfone and Winograd [18] have done the same work for securing public web servers. This document focuses on the security issues of Web servers [18]. Unfortunately, Web servers are often the most targeted and attacked hosts on organizations' networks. As a result, it is essential to secure Web servers and the network infrastructure that supports them. Web servers may also face indirect attacks to gain information from their users. In these attacks, the user is persuaded or automatically directed to visit a malicious Web site that appears to be legitimate. This paper is intended to assist organizations in installing, configuring, and maintaining secure public Web servers [18].

The work that we see relevant to our work is that of United States government accountability office done for the security assessment of Federal Agencies with respect to policies assessment methodologies and scope [20]. The paper is more theoretical and these theoretical policies are highlighted for the periodic assessment of risk in order to secure federal agencies data and system. The paper also stressed on risk based policies and procedures, subordinate plans for providing adequate information security for networks, security awareness training for agency personnel, periodic testing and evaluation of the effectiveness of information security policies, procedures and practices performed with a frequency depending on risk but no less than annually, procedures for detecting, reporting and responding to security incidents, and plans and procedures to ensure continuity of operations [20].

Mahesh Tripunitara and Partha Dutta [19] have done a security assessment of controlled attacks intended to find vulnerabilities in IP-Based networks. A network security assessment is a security assessment of a system conducted from across a network [19]. The goal of this paper is to discuss the shortcomings of current practices in network security assessment of IP-based networks and propose an approach that is more holistic [19].

6. CONCLUSION

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, confidentiality.

References

[1] Back Track 3.0 beta Linux Version, "www.remote-exploit.org/backtrack.html", accessed in March, 2008.

[2] Cailloux, Jean-Paul., and Roquilly, hristophe.," Legal Security of Web Sites: Proposal for a Legal Audit Methodology and a Legal Risks Profile Classification", 16th BILETA Annual Conference, University of Edinburgh, Scotland, (April 9th - 10th, 2001).

[3] Herzog, Pete.," Open-Source Security Testing Methodology Manual", ISECOM, (December, 2006)

[4] Hormat, Charles," The Meaning of Security", the infosec Writers Library, (09, 2002).

[5] http://www.infosecwriters.com/texts.php?op=display &id=17 "Article Paper: Meaning of Security" by "Charles Hornat" 05/09/02

[6] http://www.securitywriters.org accessed online 10/02/15

[7] InfosecWriters,http://www.swg.uklinux.net/cgi-bin/ultimatebb.cgi?ubb=get_topic&f=20&t=000002, date accessed 15/02/15
[8] IP Address Finder, “www.ip-adress.com”, accessed in Feb, 2008.
[9] Kals, Stefan. Kirda, Engin. “SecuBat: A web Vulnerability scanner”, secure systems lab technical university of Vienna
[10] Karro, Jared and Wang, Jie,” Protecting Web Servers from security Holes in Server-Side Includes”, Division of Computer Science, University of North Carolina at Greensboro.
[11] National State Auditors Association and the U. S. General Accounting Office A Joint Initiative,” Management Planning Guide for Information Systems Security Auditing”, (December 10, 2001).
[12] Nessus Website, “www.nessus.org”, accessed in February, 2015.
[13] Nikto Website, “www.cirt.net”, accessed in February, 2015.
[14] Ross, Ron., Johnson, Arnold., Katzke, Stu., Toth, Patricia., Stoneburner, Gary., and Rogers, George.,” Guide for Assessing the Security Controls in Federal Information Systems”, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, (June, 2007).
[15] Saudi Government Website,”www.saudi.gov.sa” accessed in January, 2015.
[16] Saudi Stock Exchange, “www.tadawul.com.sa”, accessed in January, 2015.
[17] Top Ten Web Attacks Book Name "WEB HACKING" by Saumil Shah Net-Square BlackHat Asia 2002, Singapore saumil@net-square.com ,http://www.net-square.com
[18] Tracy, Miles., Jansen, Wayne., Scarfone. Karen., and Winograd. Theodore,” Guidelines on Securing Public Web Servers (Draft)”, Recommendations of the National Institute of Standards and Technology, (May, 2007)
[19] Tripunitara, Mahesh V., Dutta, Partha.”Security Assessment of IP-Based Networks: A Holistic Approach”, AT & T Labs, USA.
[20] Wilshusen, Gregory C., “Agencies Report Progress, but Sensitive Data Remain at Risk”, United States Government Accountability Office, (June 7, 2007).

Dr. Saleh Al-Saleem is an Associate Professor in the College of Computer and Information Science, King Saud University, Riyadh, Saudi Arabia. He is also a Manager of the Computerized testing department at National Center for Assessment in Higher Education, Riyadh, Saudi Arabia. Dr. Saleh received his PhD degree from Wayne State University, Michigan, USA, in 2001, in the field of computer science (Evolutionary Computation). He received his Master degree in computer science from Ball State University, USA in 1996, and his BS degree in computer science from College of education, King Saud University, Saudi Arabia in 1991 respectively. He served as the dean of admission & registration as well as the head of IT and e-Learning in Shaqra University. Previously he worked as head of Information Technology department at Arab Open University. Before that he worked as the head of Computer Technology department and faculty member in Riyadh College of Technology. Dr. Saleh current research interest includes: evolutionary computation, Text Classification, ERP, BPM, and e-Learning.