Vol. (1) No. (1) March 2018

JK Research Journal in Mathematics and Computer Sciences

Security Analysis of Contemporary Web Server Systems

*Syed Mutahar Aaqib[1], Lalitsen Sharma[2]

[1]*Department of Computer Science, Amar Singh College Srinagar J&K- India*
[2] *Department of Computer Science & IT, University of Jammu, J&K-India*

Abstract: This paper presents a novel approach to study, identify and evaluate the security mechanisms in-place across various web server platforms. These security mechanisms are collected and compiled from various sources. A set of security checks are framed to identify the implementation these security mechanism in diverse web server platforms. The paper is concluded with a case study which implements this approach.

Keywords: *Web Server; Web Server Security; Information Security.*

Introduction

Security in computer science literature is considered to be the maintenance the confidentiality, integrity, and availability of information [4],[10],[11]. Security is a primary concern for World Wide Web researchers as the frequency of DDoS (Distributed Denial of Service) attacks, probability of exposure or compromise of sensitive information, data manipulation and spoofing have increased [4]. Initially, the architecture of web server was conceived to serve only static web pages, which was later extended into dynamic content [1],[3],[10].

Although this functionality delivers more customized content, it also implies that there is an increasing growth of security problems which needs to be mitigated while migrating to new supportive architectures. Web servers are therefore considered to be a vital backbone for web applications, from simple file transfer applications to delivery of confidential data for e-commerce applications. The security compromises of any type can thus cause heavy damage of data including economic and financial losses. The security of the web server is also characterized by the operating system interfaces, communication and security protocols, network configuration and its environment. The implementation of security features like SSL (Secure Socket Layer) within web servers is therefore mandatory for all contemporary web servers.

However, some of the web servers who have been claimed to be developed in adherence to various security guidelines still contain known and unknown

syed.auqib@gmail.com
*Syed Mutahar Aaqib

vulnerabilities[8]. The source of these vulnerabilities is sometimes the mis-configuration of the networking infrastructure such as Intrusion detection system and firewalls.

Thus, there is need to evaluate the security of a web server system by taking into consideration the holistic view of the system which includes the security features provided by the web server software, the operating system, the configuration of the networking infrastructure and its environment. Such an approach should allow the evaluation and comparison of the security mechanism in-place in web server systems. A standardized procedure should be adopted where tests can be applied and reapplied across various web server systems. These tests may also be repeated for reproducibility and validation. Comparing security of two web servers is a complicated issue. One obvious way to measure security of a web server is by checking the chances of violation of the confidentiality, integrity, and availability of information.Background and Related Work. A lot of work has focused to study the security of a computer system in general and security of web server in particular [8]. Bishop [4] in his work stressed about the three dimensions of security which viz, security requirements, security policy, and security mechanisms. A number of methodologies elaborating web security characteristics have been presented by numerous organizations [5]. These methodologies have gained international acceptance and are used as security policy standard in the development of web servers. The first security evaluation methods based on Common Criteria standard [5] was proposed by the United States Department of Defense [14]. This standard emphasized a set of security requirements that must be present in a web server system. Centre for Internet Security (CIS) presented a benchmark [6] which evaluates the security configuration settings for commonly used Apache and IIS Web Servers. The Department of Information Technology (DIT), Govt. of India, has also published a set of security recommendation for securing a web server [7]. National Informatics Centre (NIC), Govt. of India has published a manual [13] for enhancing the security of government websites. Such security recommendations have been found effective in preventing security hacks of government websites [13]. Researchers [8] have made vertical comparison between various generic servers based on the number of security flaws and severity and have also studied the vulnerabilities in operating systems [2], [15]. Others have used quantitative empirical models for the comparison of security vulnerabilities in Apache and IIS web servers [15]. Another technique reported in the literature is to characterize and count potential vulnerabilities that exist in a product [12]. In this paper, a different approach to evaluate the security of web servers across different web server platforms is presented.

Methodology

A comprehensive survey of technical security manuscripts published by various security organizations was done and a total of 390 best security mechanisms were compiled. The security mechanisms of web servers were evaluated by performing a test to verify whether a set of security mechanisms have been implemented on the target system. A security comparison was then performed between various web servers to identify which web server implements most of the security mechanisms. The number of steps involved in this process are listed below:

- Survey for identification of best security mechanisms for web servers.
- Categorization of security mechanisms in various classes.
- Execution of a number to tests to verify the implementation of security mechanisms in web servers.
- Case Study: Comparison of the security mechanisms implemented in various web servers.

A detailed study of the technical security manuscripts published by various organizations like CIS [6], NIST [14], Common Criteria [5], Web server security guidelines (DIT, Govt of India) [7] and web site security recommendation published by National Informatics Centre [13] were performed and a total of 390 best security mechanisms were identified. These security mechanisms were then divided into various classes for ease in the evaluation of security tests. A set of tests were then designed to identify whether these security mechanisms are implemented with a particular web server system. For the comparison of security of web servers, a case study of eight web server system installations was taken to implement this approach. Finally, a number of tests were performed for each web server, these tests verify whether the system implements the security mechanisms compiled.

Metrics

A simple metric employed in this approach is the count of the number of best security mechanism implemented in a particular web server. The final security score is thus the weighted percentage of the total security practices implemented, which implies the security level of the system. Till date, no consensus has been drawn about the set of best security mechanisms that should be applied to web server systems. The huge amount of diverse technical manuscripts in the form of books, manuals, reports and papers are available on the subject of web server security, but researchers have found no common ground for any agreement on the best standard mechanisms.

List of the technical documents included in this study are:-

- Apache Benchmark document.

- IIS benchmark document.
- Web server Common Criteria.
- Web server NIST document.
- DIT Web Server Guidelines.
- NIC Website Security Guidelines

After the end of the thorough study of all this literature and technical manuscripts, 390 security mechanisms were complied. Out of these 146 came from CIS documentation (Apache web server: 101, IIS web server: 45), 38 from DIT document, 11 from NIC, 39 from Common Criteria and 156 from NIST. Out of all the mechanisms compiled it was found that most of them are similar (equivalent) and deal with same security problems. The categorization of such similar security mechanisms was done and they were grouped together under a unique directive. After applying this method, the numbers of unique security mechanisms were counted and a total of 78 best security mechanisms were identified.

This set of 78 best security mechanisms were characterized into six categories based on an internationally valid standard for information security [9]. The characterization of security mechanisms into these six classes was done for ease in using them in evaluation. Table 1.1 lists the categories of security mechanisms grouped under six categories and the class assigned to each category.

Categories of Security Mechanisms	Class Assigned
Security policy.	Class A
Access control	Class B
Communication and operations management.	Class C
Human Resource security	Class D
Information System Acquisition development.	Class E
Physical environment security.	Class F

Table 1.1: *The characterization of security mechanisms into classes*

Web Server Tests

A set of tests were designed to identify whether or not this set of 78 of security mechanisms are implemented in a particular web server system. Based on the nature of the security mechanisms a set of tests were defined. These tests comprise of a set of questions with optional procedure to verify

presence of each security mechanisms within the system. The output of the test, yes/no would occur only after the execution of the optional procedure.

Case Study- Results & Discussion

To validate the approach used, a case study for the comparison of security of five different web servers was taken. Table 1.2 presents details about each web server tested, its version, the operating system and the number of applications running on the server. The results of these tests for web server are presented in the following tables (Table 1.3).'Test OK' in Table 1.3 refers to the successful execution of tests which implies presence of a set particular security mechanism in the web server under study. 'Test Fail' refers to the number of tests failed and Unknown refers to Unknown test, for each set of best mechanisms presented in Table 1.3. This case study was used to check the number of best security mechanism in place in these web server systems. A number of significant insights were gained from this study. One of the interesting observations was that the two web servers of different version from a same vendor, showed different results in this study. Such different results were obtained for a same web server while comparing their installations on different platforms.

S. No	Web Server	Operating System	Applications Running
1	*Apache HTTPd* 2	Windows XP	6
2	*Apache* Tomcat 6.0.13	Windows Server 2003	3
3	Microsoft *IIS* 6.0	Windows XP	2
4	*Apache* Tomcat 6.0.16	Windows Server 2003	2
5	*Apache HTTPd* 2	Scientific Linux SLC *CERN*	3
6	Microsoft *IIS* 7.0	Windows Server 2003	3
7	Nginx Web Server	Scientific Linux SLC *CERN*	2
8	Nginx Web Server	Windows Server 2003	2

Table 1.2*:* Web servers examined in the case study

The reason being the security of a web server is not dependent only on the web server software only but it is also characterized by the underlying operating system architecture, the network management and its configuration.

Case 1, *Apache HTTPd 2*	Test OK	Test Fail	Unknown	Case 2, *Apache* Tomcat 6.0.13	Test OK	Test Fail	Unknown	Case 3, Microsoft *IIS* 6.0	Test OK	Test Fail	Unknown
Class A	0	7	0	Class A	0	7	0	Class A	03	04	0
Class B	17	8	1	Class B	14	12	0	Class B	10	16	1
Class C	18	15	0	Class C	16	16	1	Class C	18	14	0
Class D	1	1	0	Class D	1	1	0	Class D	02	00	0
Class E	4	4	0	Class E	4	4	0	Class E	05	03	0
Class F	1	1	0	Class F	2	0	0	Class F	02	00	0
Total	**41**	**36**	**1**	Total	**37**	**40**	**1**	Total	**40**	**37**	**1**
Case 4, *Apache* Tomcat 6.0.16	**Test OK**	**Test Fail**	**Unknown**	**Case 5, *Apache HTTPd***	**Test OK**	**Test Fail**	**Unknown**	**Case 6, Microsoft *IIS* 7.0**	**Test OK**	**Test Fail**	**Unknown**
Class A	0	7	0	Class A	7	0	0	Class A	7	0	0
Class B	13	13	0	Class B	9	17	0	Class B	9	17	0
Class C	21	12	1	Class C	15	18	0	Class C	15	18	0
Class D	2	0	0	Class D	2	0	0	Class D	2	0	0
Class E	4	4	0	Class E	2	6	0	Class E	2	6	0
Class F	2	0	0	Class F	0	2	0	Class F	0	2	0
Total	**42**	**36**	**0**	Total	**35**	**43**	**0**	Total	**35**	**43**	**0**
Case 7, Nginx Server SLC	**Test OK**	**Test Fail**	**Unknown**	**Case 8, Nginx Server Windows**	**Test OK**	**Test Fail**	**Unknown**				
Class A	02	03	2	Class A	02	03	2				
Class B	07	15	4	Class B	07	16	3				
Class C	11	18	4	Class C	11	16	6				
Class D	02	00	0	Class D	02	00	0				
Class E	02	05	1	Class E	02	04	2				
Class F	01	01	0	Class F	01	01	0				
Total	**25**	**42**	**11**	Total	**25**	**40**	**13**				

Table 1.3: Results of case study for 8 different web server system installations

For example, while comparing the same Apache HTTPd server on Scientific Linux CERN and Windows XP 2000, it was found that Apache on SLC CERN system passed more tests and thus was more secure. Another aspect used in this study was the comparison of diverse web server systems, of different underlying operating systems. While comparing the security mechanism in Apache Tomcat 6.0.13 and Apache Tomcat 6.0.16 on Windows Server 2003 platform, it was revealed that Apache Tomcat 6.0.16 passed more tests and hence was more secure. Here also the explanation is the support provided by the underlying operating system platform and its security configuration. Among all the web servers under study, it was found that Microsoft IIS passed more number of tests than any other web server and thus implements higher number of security mechanisms. The only limitation of this approach is that the execution of these tests requires immense computer proficiency as this approach requires verification of mechanisms in-place for different web servers systems.

References

[1] Aaqib S.M., Sharma L.: Analysis of Delivery of Web Contents for Kernel-mode and User-mode Web Servers, International Journal of ComputerApplications, 12(9): 37–42, Foundation of Computer Science, New York, USA (2011)

[2] Alhazmi, O. H., Malaiya, Y. K., Ray, I.: Security vulnerabilities in software systems: A quantitative perspective. Proc. Ann. IFIP WG11.3 Working Conference on Data and Information Security , 281–294 (2005)

[3] Arlitt M. & Williamson C.: Understanding Web Server Configuration Issues. Software: Practice and Experience, 34(2): 163-186 (2004)

[4] Bishop, M.: What is Computer Security, IEEE Security & Privacy (2003)

[5] Common Criteria: US Government Protection Profile. Web Server for Basic Robustness Environments, Version 1.1 (2007)

[6] CIS. Centre for Internet Security 2008. Retrieved from CIS http://www.cisecurity.org/as accessed on June 2015

[7] CERT-In.: Web Server Guidelines 2004. Department of IT. Government of India (2004)

[8] Ford, R., Thompson, H., Casteran, F. Role comparison report-web server role. Technical Report, Security Innovation (2005).

[9] IEC-ISO. 17799:2005: Information technology -Security Technique - Code of practice for information security management. Retrieved from: http://www.iso.org/iso/ as on Oct 2012.

[10] Laprie, J. C.: Dependability of computer systems: concepts, limits, improvements, Proc. of the 6th Int. Symposium on Soft. Reliability Engineering (1995)

[11] Lin P.: So You Want High Performance (Tomcat Performance). Jakarta Tomcat. (2003).

[12] Neto, A.A., Mendes, N., Duraes, J., M., Madeira, H.: Assessing and Comparing Security of Web Servers, 14th IEEE Pacific Rim International on Dependable Computing (2008)

[13] NIC Guidelines for Indian Government Websites (2013).: National Informatics Centre. Retrieved from: http://darpg.gov.in as accessed on June 2015

[14] NIST.: National Institute of Standards and Technology, Guidelines on Securing Public Web Servers, Special Publication,800-44 Version 2 (2007)

[15] Rescorla, E. Is finding security holes a good idea? IEEE Security and Privacy 03, 1, 14–19 (2003)

[16] Web Server Protection Profile, Retrieved from, http://llniap.nist.govIcc-scheme (2001)

[17] Woo, S., Alhazmi, O.H., Malaiya, Y.K.: Assessing Vulnerabilities in Apache and IIS HTTP Servers, Colorado State University Fort Collins (2008)