Analysis of Web Site Security Measures Based on Network Database

Bo Xu*

Department of Electrical Engineering, Yingkou Institute of Technology, Liaoning 115014, China

*Corresponding Author email: vipxb01@163.com

Keywords: Network database; Web site; Security measures

Abstract: At present, with the rapid development of information technology, the security work of the network database and the overall guarantee of the integrity of the Web database are the key issues of the Web-based network database security technology. In the Internet era, people are demanding more and more storage of network database. We should pay attention to improving database security technology. Starting from the traditional sense of database security, this paper introduces the management principles and Strategies of traditional database combined with network security. Then it introduces the desktop-level and enterprise-level database security settings and database backup. Finally, the web-based database security control and management is described in combination with the web application, and the Web network database security solution is proposed. Based on the overall design, this paper completed the implementation of the system function module, and tested the function and performance of the system. The results show that the implemented system meets the requirements of website security detection and has good usability.

1. Introduction

In recent years, with the rapid development of information technology, information security has gradually become the focus of attention and discussion. In the planning and design of enterprise information security, most enterprises focus on network security, ignoring the security of the most important database itself [1]. In the information society, databases store the most real and valuable part of online resources. Once these data in the database are destroyed by security, it will bring unimaginable serious consequences. A lot of personal information is stored in the network database. Therefore, improving the security of the network database has become the main goal of current development [2]. With the development of Internet technology, the technology of Web sites has changed from traditional static services to dynamic and interactive services based on user needs [3]. Because of its convenient and fast features, dynamic Web sites have been widely used, but because of this feature, Web sites are more vulnerable to intrusions and attacks [4-5].

In the technology about network security, people first think of firewalls. Firewalls have been widely adopted on the Internet. Many enterprises have adopted firewalls to protect their own servers or data security. Firewalls have gradually been accepted by the public and become the first threshold to protect network security [6]. Therefore, the purpose of establishing website security protection measures is to ensure that data transmitted and exchanged over the network will not be added, modified, lost or leaked [7]. In 2015, researchers conducted research on the quantification of bypass information leakage based on data complexity measurement of web browsing [8]. Subsequently, in 2016, theoretical research on the collection and analysis of automated spyware was proposed [9]. Website security includes physical security and logical security. Physical safety refers to the safety of the system machinery and its peripherals to ensure that they are not subject to various physical damage, such as theft, fire, etc [10]. Logical security refers to the integrity, confidentiality and usability of the system and its data. These three points are important characteristics of computer security and important principles of website security construction [11]. Although database security is very important, most enterprises still do not intend to consider and solve the related security problems before they suffer irreparable losses [12].

Copyright © (2018) Francis Academic Press, UK DOI: 10.25236/eeems.2018.043

How to protect the security of Web sites is an important issue for every Web site developer. This paper discusses the security measures of Web sites from the aspects of Web server security, ASP application scripting and SQL Server database access security by analyzing the working principle of dynamic Web site based on ASP technology [13-14]. All messages are required to pass the check apricot here. The router can install IP-based packet filtering software to implement packet filtering [15]. Many routers have message filtering configuration options themselves, but they are generally relatively simple. The dangers of a firewall consisting solely of shielded routers include the router itself and the host that routers allow access to [16]. In the real-time security detection of network sites, it mainly detects whether the connection status of the website is normal, whether there are text or pictures tampered with, whether there are dead links, wrong links and other elements affecting network efficiency in the website, and whether the content of the web page contains sensitive words [17].

2. Materials and Methods

The security management of database refers to the system security protection measures taken to protect database from data leakage, change or destruction caused by illegal use. A powerful database security system should ensure the security of information and control it effectively. Web database refers to the way to access database resources in the Internet through the Web query interface [18-19]. This reduces the size of the relationship to be connected on each site, shortens the processing time on each site, and thus reduces the response time of the entire query. However, it is not difficult to see that when the query graph is more complex, the number of iterations of the improved algorithm may increase, but also involves data transmission between sites, which increases the communication cost of the entire query [20]. Web technology has played a big role in the development of the Internet. The development and improvement of Web technology has gone through a long process, realizing the development from static web pages to dynamic web pages. The client's server makes an HTTP request, IIS receives the request, calls the ASP engine, calls the corresponding ASP file, and interprets the execution script [21]. Accessing the database through the Active X component ADO automatically generates an HTML page based on the access result set to respond to the user's request. It also standardizes the information transfer format, communication methods, and standard APIs between components.

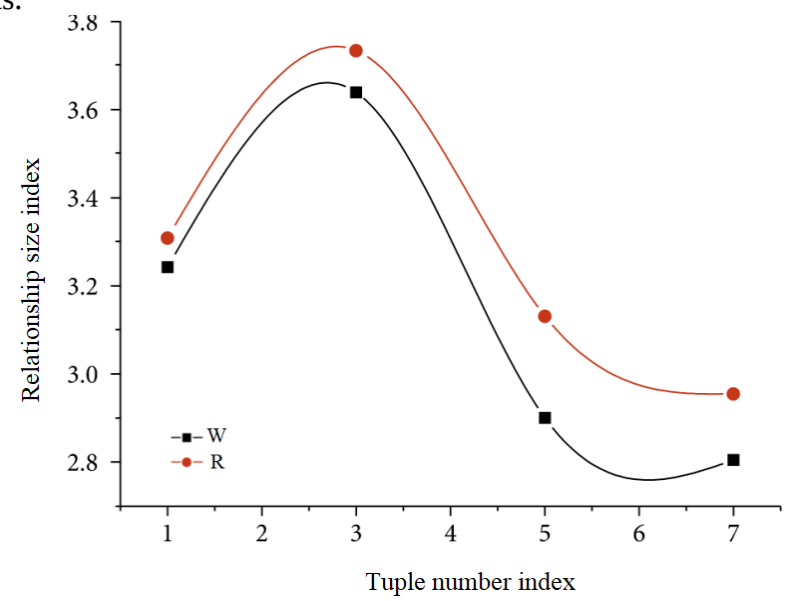

Figure 1 Relationship information

Two connection operations can be performed at Site 1 and Site 2, respectively, and the results are not removed. The results are shown in Table 1 and Figure 1. The subsequent processing is completely parallel processing. If you want to view the results on the site, you only need to transfer the results of

the two sites to Site 1 for a simple docking to generate the desired results, no need to do database connection operations.

Table 1 Relationship information table

Relationship	Number of tuples	Relationship size
W	150	986
R	130	893

The breadth-first search strategy refers to the next level of search after completing the current level of search in the crawling process. In order to cover as many web pages as possible, a breadth-first search method is generally used. There are also many studies that apply breadth-first search strategies to focused crawlers. The basic idea is that there is a high probability that a web page with a certain URL within a certain link distance has a topic relevance. During the cluster establishment phase, each sensor node sends its current location information to the sink node. In order to better form clusters, the aggregation node needs to ensure that the energy is load balanced across all sensor nodes. The sensor node sends an energy level to the sink node. The sink node calculates the average energy value of the node, and some nodes higher than the average energy value will have the opportunity to become the cluster head node of the round. The difference between event generators and analyzers is only the efficiency of data collection and analysis. For example, many manufacturers' IDS adopt more protocol analysis modules to enhance data analysis ability. Event libraries clearly reflect IDS's detection capability (not performance) and are closely related to the detection engine, because common false positives and false positives are clearly related to the definition of events. In addition to the addresses added to the list, we can authorize access to all other addresses, or deny access to all other addresses except those added to the list.

The neural network is trained with the data in Table 2 and Figure 2, and the matching mode between the input vector and the corresponding output vector is established. When the training accuracy of the neural network is reached, the same attributes between heterogeneous databases can be matched. The data indicators of attributes to be matched are input into the neural network, and the similarity of attributes is identified by comparing the output of the neural network.

Table 2 Sample data

Serial number	Input vector	Output vector
1	133	156
2	124	189

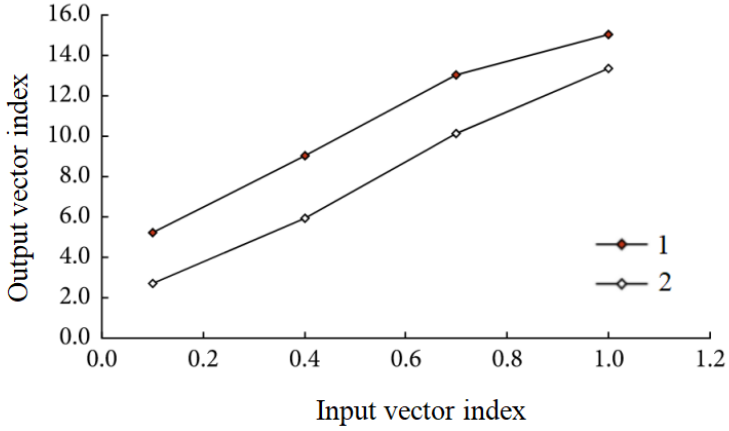

Figure 2 Sample data

User identification is a technology of network database. User identification technology can be used to protect user's peripheral security, so as to protect user's database security. User identification uses the client application program in the working process to achieve the purpose of protecting the user's data security. This creates a security vulnerability for most database servers. This enables some

people to use the obtained database administrator account to execute system commands and add administrator-level users through the call of system stored procedures, so that they can completely control the database server machine, which shows the importance of database security. Non-cluster-head nodes will keep listening at this stage and receive broadcasts from all cluster-head nodes. When this process is completed, each non-cluster head node will decide which cluster it belongs to based on the strength of the received signal. When the node decides to join a cluster, it will notify the cluster head node that it has become a member of the cluster. Each node will reply to the cluster head information using the CSMA/MAC protocol. All cluster head nodes must keep their receivers active. Login is usually the login of the username and user password. User password is a widely used method for user identification, which is faster. However, in the actual operation process, the user password is relatively simple and convenient, and there are many loopholes and high security risks. Illegal people can use some techniques and means to find out the loopholes in the program, resulting in user information leakage and loss.

3. Result Analysis and Discussion

Through the study of several mainstream security technologies, it is clear that firewall technology is one of the most important technologies in the security field, and it should be the core link in a security system. In fact, firewalls are now used in the network structure of many enterprises and institutions or in the networking of WEB websites. However, network security cannot be achieved by firewall alone. The firewall must be combined with other products, such as IDS and anti-virus products, to build a security system with a fire wall as the core. When using the system, users can choose the content and frequency they want to detect according to their own needs. When there is an exception, the system will notify users by sending short messages or e-mails. Managers need to constantly upgrade and maintain identification libraries. Increasing recognition libraries will require firewalls to improve performance or reserve larger processing capacity. Completing intrusion detection and other functions will require firewalls to be able to detect attacks in the packet buffer queue, and the packet buffer queue can not be too long, otherwise it will show a long delay.

As shown in Table 3, given two different initial states (only considering the change of spatial credibility), in the first case, the initial state is LSR, and finally reaches the OSR state through two rounds of adaptive adjustment; in the second case, the initial state is HSR, and finally reaches the OSR state through three rounds of adaptive adjustment. Combining the above results, we can know that the expected reliability state can be achieved in any initial state, and the correlation threshold will be adjusted to the optimal state adaptively, which will reduce the energy consumption of wireless sensor networks to the minimum.

Table 3Variation of correlation threshold with different initial states

Initial state	Threshold	Energy consumption
LSR	24	33
OSR	19	15

Application layer attacks have been a serious threat to network security for many years because it is always after a technically legitimate connection is established. Because of the flexibility and interoperability of HTTP, HTTP-based communication is allowed in most networks because everything a user needs can be found through a web service. As a result, HTTP-based automation software is booming to meet the needs of Internet users. Unfortunately, in addition to normal automatic testing such as operating systems or software updates, in recent years, cyber criminals have used the network as a medium of communication environment, through the dissemination of malicious HTTP self-guided software, such as fraudulent advertising software, spyware, BOT, etc., hidden a variety of prohibited or illegal activities. As shown in Figure 3, HTTP traffic and auToware can be divided into several categories.

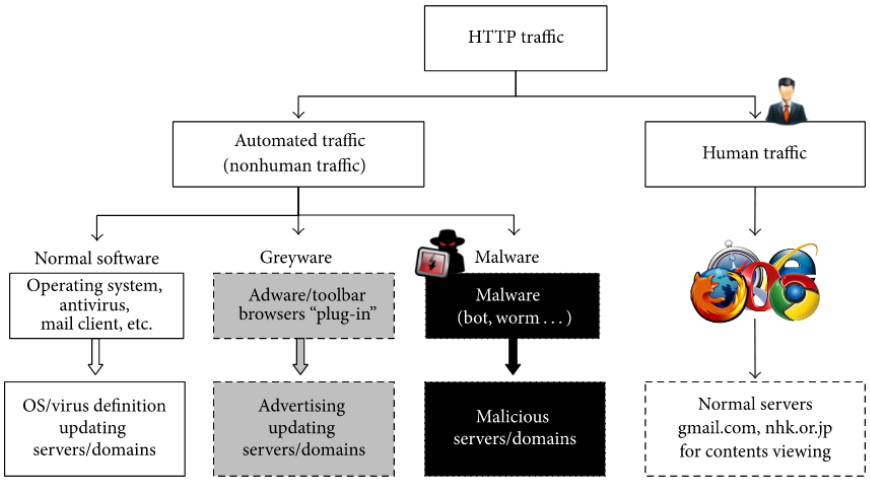

Figure 3 Http traffic and automation software category

When the hidden layer output vector is x, the connection weight of n to the output layer node is E. The output is now:

$$E(x)=\sum_{j=1}^{n}E_j \tag{1}$$

Similarly, when the input vector is i, the connection weight from X to the node in the output layer is still E. At this point, the output expression is:

$$HWt=\frac{\sum_{i=1}^{N}D_i(x)}{N} \tag{2}$$

It can be seen from the above formula that the equation has multiple sets of solutions to satisfy the meaning of the question. That is, there are different inputs corresponding to the same output. Let the number of output layer nodes be n, which are denoted as i and j, respectively. Then the connection weight matrix from the hidden layer to the output layer is:

$$D_i=a+\sum_{j=1}^{n}b_j p_j+r_i Y+u \tag{3}$$

When the hidden layer output vectors are n and a, respectively, the problem of whether the output layer output vectors i and j are equal is converted into a problem of whether the equations have a solution. At this point there is an expression:

$$D_i=a+\sum_{j=1}^{n}b_j\,ln(p_j)+r_i\,ln(Y)+u \tag{4}$$

When i< j, the rank u of matrix a must have a basic solution system containing n vectors. Assuming that Y is a basic solution system of the equation system, the solution of the equation can be expressed as:

$$ln(D_i)=a+\sum_{j=1}^{n}b_j\,ln(p_j)+r_i\,ln(Y)+u \tag{5}$$

In the WAN environment, the transmission speed of data on the network is much slower than that of the database on the computer. In the distributed database query operation of the WAN, how to reduce the total cost of network transmission is often the target of query optimization. Suppose w1 and w2 are two relationships, which are located at site v1 and site v2, respectively, and p1 and p2 are

two attributes on A and D respectively, then the semi-join operation of its attributes can be expressed as:

$$D(p_1) = A \cdot w_1 \left[1 - \frac{p_1}{v_1} \left(\frac{p_1 w_1 + p_2 w_2 - m(1-r)}{\frac{w_1}{v_1} {p_1}^2 + \frac{w_2}{v_2} {p_2}^2} \right) \right] \tag{6}$$

According to the calculation of the above formula, the core functions of the clustering phase are realized and deployed in the middle part between the database and Hadoop Map Reduce. This module will archive the results from the first phase, and the URLs are aggregated in Map Reduce through distributed processing paradigms. Finally, the results of the second phase are returned to the Mark Logic database through the cluster XDBC application server. Data exchange between Mark Logic and Map Reduce of Hadoop will be done by a connector. Figure 4 depicts the detailed flow of this phase.

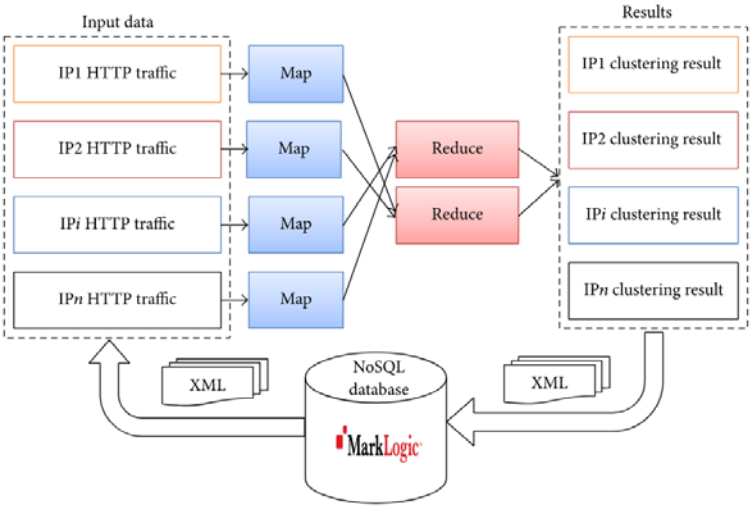

Figure 4 Cluster stage process

ASP can realize access to files and databases. At the same time, the password of the website or the password of the database connection can be directly written into the ASP source file, so the confidentiality of the source code of the ASP file is very important. Although the ASP program runs on the server side, the general client does not see the source program. It is convenient for enterprises to implement more users to use remote network resources in different places. Due to the low requirements of client devices, configuration costs and operating costs can be effectively controlled. From the current development situation, SSL VPN is mainly used to meet three application requirements: remote access platform, unified authentication portal and platform conversion gateway. With the increasing of information resources and the increasing of various types of databases, it is no longer applicable to simply use backup files to backup data. Whether the required data can be extracted from the huge database files for backup is an important part of network database backup.

Through monitoring the content of the website, we can determine whether the website has been maliciously tampered with by hackers and whether there is a page byte mutation. If the page is tampered with, the user will be notified by short message or email, and the user can view the results in the report. If the text is tampered with, the label where the text is located will be saved together with the text to facilitate user error correction. To a great extent, this security system can guarantee the security of WEB website system. Nowadays, many enterprises and government agencies' website architectures are formally established under the security mechanism with firewall as the core. I might as well call it the traditional security architecture. However, this traditional security system is still not enough for the protection of a WEB website system, because a WEB website system needs to be maintained and updated frequently. If you understand the directory structure of the web server, use it

to view the important ASP files on the web server. It not only includes SSL VPN technology, but also covers other VPN technologies. During the user's use, you need to set a password and authentication through a third-party system, and then you can use the SSLVPN technology to achieve remote access.

4. Conclusions

The development of Internet technology has greatly facilitated people's production and life, and has occupied an increasingly important position in people's daily life. However, while Web technology is rapidly developing, it also brings some problems, the most important of which is the security of network databases. In the process of running the database, the security of the database is not guaranteed, which brings a lot of trouble to the user. Therefore, it is very important and necessary to be familiar with the security operation of the Web database system, to understand the security vulnerabilities of the system, and to solve the security problem of the web database system in the first time. Of course, in order to maximize the security of Web-based database, it is better to migrate existing script-based web applications to compiled ASP.NET applications under the framework of NET Framework. Of course, with the continuous development of the network, some new technologies, new operation modes and methods will emerge, and the system needs to be constantly updated and upgraded.

References

[1] Boue S, Talikka M, Westra J W, et al. Causal biological network database: a comprehensive platform of causal biological network models focused on the pulmonary and vascular systems [J]. Database, 2015, 2015:bav030-bav030.

[2] Yue, Ying. Database Design of Pop Music Website Development [J]. Applied Mechanics and Materials, 2014, 687-691:3023-3026.

[3] Ying-Chiang C, Jen-Yi P, Francesco P. Design and Implementation of Website Information Disclosure Assessment System [J]. PLOS ONE, 2015, 10(3):71-88.

[3] Yao M H, Wang N, Li J S. The Multi-Server Load Balancing Systems Research in Large-Website Construction [J]. Applied Mechanics and Materials, 2015, 713-715:4.

[4] Frey L J, Sward K A, Newth C J, et al. Virtualization of open-source secure web services to support data exchange in a pediatric critical care research network [J]. Journal of the American Medical Informatics Association, 2015, 22(6):1271-1276.

[5] Li C. Design of Graduate Employment Network SMS Platform [J]. Applied Mechanics and Materials, 2014, 608-609:326-330.

[6] Peltoniemi M, Aurela M, Böttcher, Kristin, et al. Webcam network and image database for studies of phenological changes of vegetation and snow cover in Finland, image time series from 2014 to 2016[J]. Earth System Science Data, 2018, 10:1-23.

[7] Yan X Y, Lin Z P, Zhang X M, et al. Design and Realization of Alfresco Database of the Micro-Information System[J]. Advanced Materials Research, 2014, 989-994:4643-4649.

[8] Quantification of side-channel information leaks based on data complexity measures for web browsing [J]. International Journal of Machine Learning and Cybernetics, 2015, 6(4):607-619.

[9] Stamminger A , Kruegel C , Vigna G , et al. Automated Spyware Collection and Analysis[J]. Lecture Notes in Computer Science, 2016, 5735:202-217.

[10] Zhao X, Wang N, Ou J, et al. Research on public participant urban infrastructure safety monitoring system using smartphone[J]. Proceedings of the Spie, 2017, 169:101.

[11] Yu R. Design and Realization of the Personalized Data in Tourism Business Website [J].

Applied Mechanics and Materials, 2014, 556-562:5780-5782.

[12] Calzavara S, Tolomei G, Casini A, et al. A Supervised Learning Approach to Protect Client Authentication on the Web [J]. ACM Transactions on the Web, 2015, 9(3):1-30.

[13] Mao J, Tian W, Li P, et al. Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity [J]. IEEE Access, 2017, 5(99):17020-17030.

[14] Zhou W, Jia W, Wen S, et al. Detection and defense of application-layer DDoS attacks in backbone web traffic [J]. Future Generation Computer Systems, 2014, 38:36-46.

[15] Tan C H, Sutanto J, Tan B C Y. Empirical investigation of relational social capital in a virtual community for website programming[J]. Acm Sigmis Database, 2015, 46(2):43-60.

[16] Ben-Asher N, Gonzalez C. Effects of cyber security knowledge on attack detection[J]. Computers in Human Behavior, 2015, 48:51-61.

[17] Santos O. Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security [J]. Issues in Information Systems, 2015, 13(1):23-34.

[18] Peng Y, Tudor C O, Torii M, et al. iSimp in BioC standard format: enhancing the interoperability of a sentence simplification system [J]. Database, 2014, 2014:38-48.

[19] Kasten A, Scherp A. Ontology-Based Information Flow Control of Network-Level Internet Communication [J]. International Journal of Semantic Computing, 2015, 09(01):1-45.

[20] Annuessuman K. An Analysis on the Regulation of Grey Market Cyber Materials [J]. Survey Sampling & Measurement, 2014, 82(3):201-216.

[21] Onarlioglu K, Buyukkayhan A S, Robertson W, et al. SENTINEL: Securing Legacy Firefox Extensions [J]. Computers & Security, 2015, 49:147-161.