A Middleware for Web Database Security

Zhenhui Wang

College of Technology and Engineering, Xi'an Fanyi University, Xi'an 710105, China

9502wzh@163.com

Keywords: Web database; Middleware; Security; Vulnerability; Audit; Encryption and decryption

Abstract: In order to solve the increasingly serious security problem of web database, we established a Web database security middleware between web application program and web database. The platform independence and maintainability of middleware are realized by using the design concept based on web services and components and Java technology. Web database is controlled and managed by security middleware from four aspects: identity authentication, data encryption/decryption, and vulnerability detection and operation audit. It effectively improves the security of Web database in the network environment.

1. Introduction

With the development of Internet technology, the concept of enterprise sharing information regionalization has been broken, the demand of information network management is increasingly strong, and web information management system has become the main part of software system development. However, the increasingly serious network information security problems, not only the internet enterprises, institutions and users have suffered huge economic losses, but also the national security and sovereignty is facing a serious threat [1]. In recent years, many well-known websites at home and abroad have leaked tens of millions of user information due to security loopholes. The status quo of information management system construction "only focus on business, ignore security" needs to be improved. The database is the core component of the information system, facing double threats from the outside and inside of the enterprise, and its security processing is an effective means of data protection. Although there was no blackmail virus in 2018 that caused panic among people around the world as in 2017, the number of data leaks exposed by the media was far greater than in previous years, and the number of people whose sensitive data were leaked was counted in the hundreds of millions[2].

2. Research Status

Different people have different opinions on how to protect the security of network database. The main methods adopted are hardware firewall, host security protection, database vulnerability detection and evaluation, application access control, security system guarantee, etc.

In recent years, researchers have proposed more effective identity authentication technology. For example, smart cards, UKEY, fingerprint identification and other high-strength authentication technologies are becoming more and more mature, and many application results have been achieved [3-5], but due to its technical, economic and other reasons cannot be widely promoted, password is still popular. At the same time, more researches are still focused on digital signature, data encryption, data certificate and other fields to prevent data security. Some research papers also have a lot to learn from.

In conclusion, the current database security processing is mainly focused on the database access interface control and application login verification methods. But the location for the database user login, the login time, vulnerabilities and operational auditing lack of effective control, the lack of direct way makes the database application and database is very fragile, hackers can legal user's

  DOI: 10.25236/isrme.2019.014

identity or bypass the login check to access the database. Data tampering and leakage have occurred from time to time.

Security middleware is a kind of middleware technology which adopts many mature middleware technology and security technology to shield the complexity of security. Cross-platform and highly scalable middleware technology is adopted to realize the security application in the web database. Users and developers can directly invoke the security control function in the middleware, and can also extend the function of the middleware to realize the customized requirements of enterprise security application.

3. Design of Web Database Security Middleware

3.1. Design ideas.

There are three ways to access a database. The first way is to access the database server through the server, mainly for employees within the enterprise, to carry out online office business. In the second way, the C/S structure is used to connect the database directly by the application software. The third way is the terminal host structure. Users can log on to the database server by using remote terminals to complete the operation of the database. The main users are database administrators and network hackers.

Because all three methods are direct connection and service between database server and users and Web server, they are vulnerable to all kinds of attacks. Moreover, the database system has unknown hidden channels, which are easy to be exploited by attackers. In order to solve the above problems, the fourth layer (security layer) is designed on the basis of the three-tier B/S structure, which acts as a software firewall in the software structure and is implemented by the Web database security middleware.

The database security middleware is located between the application and RDBMS and performs security filtering and auditing on the clearances of various connection and operation on databases. Considering the destructive and difficult of remote login, it is restricted to connect to the database in database security middleware. Figure 1 shows the architecture diagram after adding the database security middleware.

As you can see in figure 1, the database server is isolated from the application through middleware. All access to the database must go through the middleware. All kinds of hidden channels are blocked accordingly and will not be directly used by attackers.

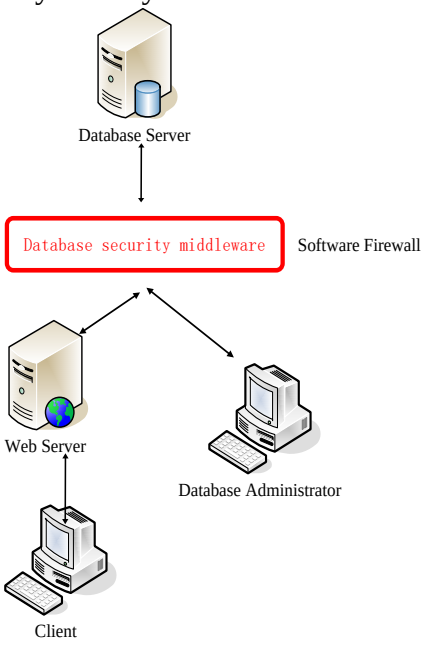

Figure 1. Improved database security solution

3.2. Model of Web Database Security Middleware.

There are four main requirements for web database security: user identity authentication, data encryption and decryption, vulnerability detection and operation audit. In response to these four requirements, corresponding web services are designed in the web database security middleware. Figure 2 shows the web database security middleware model.

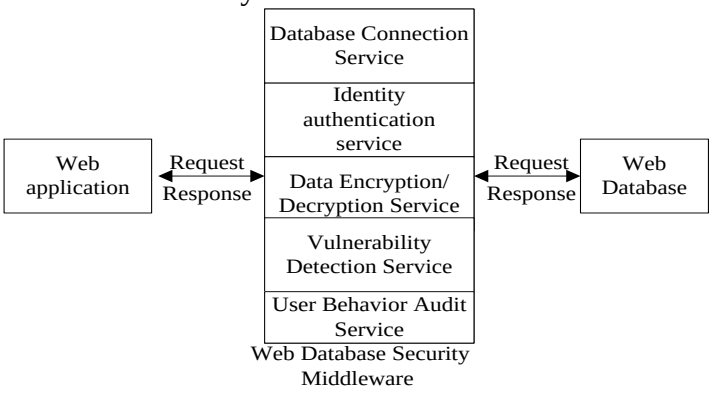

Figure 2. Web database security middleware function model

This web database security middleware model is based on EJB technology. In order to realize the four functions provided by the middleware, mature web service technology is used to realize the transparent use of services.

The four functional requirements in the model are independent. According to the security verification requirements of web pages, one or more web service interfaces can be invoked in one application or page.

The technical scheme in this paper has the following innovations and improvements.

3.2.1. Security level allows user customization.

When using the services designed in the middleware, users can choose which security functions are enabled and which ones are disabled at any time. In this way, security level is defined according to different users.

3.2.2. Technological solutions differentiate between threats within and outside the enterprise.

Because threats to web databases come from inside and outside the enterprise, therefore, different algorithms are adopted according to different regions. Internal access is controlled by binding IP with MAC address. If the user's security requirement is higher, technologies such as hard disk serial number and client name, user operation audit, secret data salt processing can be added. External users are protected by log, account audit and operation audit, and black and white list functions.

3.2.3. Secondary user login verification.

The web application first logs on to the security middleware, then logs on to the web database, and use the second login mechanism to solve the login security problem.

3.2.4. Hybrid encryption.

According to the importance of data, different data encryption methods are used to prevent data leakage. For key data such as user password, asymmetric encryption algorithm and data salt technology are used, while for other secret data with slightly lower security level, symmetric encryption algorithm is used.

4. Analysis of experimental results.

In order to verify the feasibility and practicability of the security middleware, this paper takes the student score management system as an example to test. The student score management system was

built five years ago with JSP technology. It only pays attention to the function, and the security is not considered thoroughly. Therefore, there are many hidden dangers in data security.

We take typical data threat behaviors as test scenarios: system destruction, information stealing and electronic fraud. We determine test points and test identities respectively, and verify the detection and audit functions of security middleware. In order to compare the degree of system and data damage before and after security middleware system deployment. We carried out two groups of experiments, each group of three attack tests, a total of 40 students were invited to carry out 240 validations.

Through six different experimental results of the two groups, it is proved that after deploying the security middleware system, the ability of student achievement management system to avoid and trace data threat events has been improved qualitatively. Table 1 shows the different test results before and after the deployment of the security middleware system.

Table 1 List of system test results

Group number	Test scenario	Type of attack	Attack technology	Attack consequences
1	Before deploying Security Middleware System	Information System Destruction	SQL injection	Enter the system and delete key data
		information theft	sybil attack	Enter the system, leak the information of student
		Electronic fraud	IP fraud	Enter the system and modify the score
2	After deploying the security middleware system	Information System Destruction	SQL injection	SQL Injection Vulnerability Scanning, Unable to Log in, Write Log Files
		information theft	sybil attack	Subject Information Authentication, Can't Log in, Record User Behavior
		Electronic fraud	IP fraud	Enter the system, back up the score before modifying the results, record suspicious operations, and alarm

In terms of performance, due to the existence of security middleware system, the access delay of student score management system is caused. Performance analysis delay is caused by the delay of data acquisition, verification process and communication in the middleware system. To reduce system latency, the user experience can be improved by improving the hardware performance of the middleware system or by using asynchronous processing techniques.

5. Conclusions

It is an indisputable fact that data security problems arise from internal or external attacks in the use of web databases. In order to improve the security level of information system, this paper uses database security middleware to protect the confidentiality, integrity and availability of enterprise data. According to the strategy of "pre-detection, in-process control and post-remedy", the middleware manages and controls database identity authentication, data encryption and decryption, vulnerability detection and operation audit. The effective management of database security is realized.

Database security is an eternal topic, and this topic is also lasting and new under the premise of continuous innovation of network and computer technology. How to face the future and adopt reasonable technology to realize enterprise data security in network era is also a persistent problem. Security middleware technology that provides security detection, prevention and control in a service

way will also be improved and perfected continuously. At the same time, the development trend of data security monitoring technology is based on the concept of data-driven security management and the establishment of real-time response mechanism and rapid analysis technology driven by data changes in big data environment [7-10].

Acknowledgements

This research was supported by Scientific research team in Xi'an Fanyi University (XFU17KYTDB02).

References

[1] Information on.http://www.sohu.com/a/240410995_786964

[2] D.N. Wang. Data Leakage: Unbearable Safety [J]. China Information Security [J].(2018)No 3,p.56.

[3] W.D Fang, W.X Zhang and Y Yang ,et al.Biometric-Based Three-Factor User Authentication Protocol for Wireless Sensor Network[J]. Acta Electronica Sinica, Vol.3 (2018) No.3,p702.

[4] R Jiang, A Bouridane and D Crookes, et al. Privacy-Protected Facial Biometric Verification Using Fuzzy Forest Learning[J]. IEEE Transactions on Fuzzy Systems, Vol.24 (2016) No.4,p779.

[5] Y.N Dong, X.J Liu and B Li.Click Fraud Detection Method Based on User Behavior Feature Selection [J].Computer Science, Vol.43（2016）No.10,p145.

[6] L Qian, W Zhu and J Li, et al. Research and Development of Drilling Assistant Design System Based on B/S Structure [J]. Procedia Engineering, Vol.73 (2014) No.1,p160.

[7] Cardenas A A, Manadhata P K, Rajan S P. Big Data Analytics for Security [J]. IEEE Security & Privacy, 2013, 11(6):74-76.

[8] Xu L, Jiang C, Wang J, et al. Information Security in Big Data: Privacy and Data Mining[J]. IEEE Access, 2017, 2(2):1149-1176.

[9] Zhou Q, Luo J. The Study on Evaluation Method of Urban Network Security in the Big Data Era [J]. Intelligent Automation & Soft Computing, 2017(5):1-6.

[10] Gang C, Wu S, Yuan W. The Evolvement of Big Data Systems: From the Perspective of an Information Security Application ☆[J]. Big Data Research, 2015, 2(2):65-73.