Measurement: Sensors 27 (2023) 100779

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

Neural network based single index evaluation for SQL injection attack detection in health care data

N. Nagabhooshanam [a,*], N. Bala sundara ganapathy [b], C. Ravindra Murthy [c], Al Ansari Mohammed Saleh [d], Ricardo Fernando CosioBorda [e]

[a] Aditya Engineering College, Surampalem, Andhra Pradesh, India
[b] Department of IT, Panimalar Engineering College, Chennai, India
[c] Department of EIE, Sreevidyanikethan Engineering College, Tirupati, India
[d] College of Engineering, Department of Chemical Engineering University of Bahrain, Bahrain
[e] Universidad Privada del Norte, Peru

ARTICLE INFO

Keywords:
Network security
Artificial Neural Networks
SQL Injection
QoS

ABSTRACT

In recent years, there are a lot of security risks in the network, and there is the combination intersection between the computer network security problems and security evaluation. The scale of computer network is very large with vast information, so there are many loopholes in the system network. At present, many have established a computer network security evaluation system to monitor the network security vulnerabilities, viruses, and defects in healthcare. However, many places simply analyzed the risk assessment of network security, but there is no assessment of network security situation. For the network security evaluation system, there is no complete evaluation system of network information security. Therefore, a network security evaluation system must be constructed to develop an effective and practical simulation model of computer network security evaluation. Through the simulation model, the effect of network security can be improved. Since the reform and opening up, the simulation of computer network security evaluation in our country is a new subject. It can directly study the network security evaluation, build a network security evaluation model, and study the network security in detail. In the computer network simulation system, it can analyze, study, design, and plan various stages, so as to play an important role.

1. Introduction

Since the 80s of last century, the research of artificial neural network has entered a stage of rapid development. On 1989, Haight Nielsen proposed the multi level BP network approximation and computing theorem, and determined the theoretical basis of neural network function approximation [1–4]. A variety of theories with practical significances were born in 1990s, such as the radial basis function network and the cerebellar model control network model, and they have been applied to the system identification, the simulation, the optimization, and the automatic control range [5]. In 2000, He Xingui proposed the theory of process and weighted neural network, and opened up a more extensive application prospect for the research of artificial neural network.

The analysis and completion of this topic is to develop the base station patrol management system based on Web for the company, the above system is a Web system with a typical exemplary B/S architecture, and the background uses the MySQL database. The system sets the server inside the company, and uses the network to carry out data transfer and function optimizing and upgrading, therefore, MySQL which is regarded as the backend database of the system will inevitably be interfered with by many external factors, and will often be confronted with the risk of malicious reading, modification and so on. The above databases of system reserve internal staff information, base station information and inspection data and other important information content, the above information is all important information of the company, if the attacker uses the system to carry out malicious attacks on the background MySQL database, the company will face their reparable losses [6].

In the authentication, the security database has the strict identification of legal identity for the users who declare database connection, the user must prepare the corresponding user name and password to

* Corresponding author.
E-mail addresses: sainaga90@gmail.com (N. Nagabhooshanam), balabsg@gmail.com (N.B. ganapathy), ravins.ch@gmail.com (C. Ravindra Murthy), malansari.uob@gmail.com (A.A. Mohammed Saleh), ricardo.cosio.borda@gmail.com (R.F. CosioBorda).

https://doi.org/10.1016/j.measen.2023.100779
Received 24 February 2023; Accepted 4 May 2023
Available online 14 May 2023

enter the database, and then enter the database for operation. Authentication is the most basic form of protection that a database needs to prepare. In addition, SSL data certificates can be used to prepare more rigorous means. Access control generally means the control of operation authority of users who access to the database through authentication [6]. Based on the current situation of MySQL database, the association database should also carry out permission test on many requests made by users, finally, the test permissions are to the column level of the database table, when the request of user can't get permission, and it's difficult for the database to expand the preparation of the service. For the security audit of the database, this aspect represents the supervision and recording of the relevant actions taken by the user of the data, and all the operations are stored in the log data associated with them. Log data specifically covers the time, category and other of implementation [7]. According to the audit log, the administrators of system can accurately understand the relevant access information, as well as the specific operation of database, so that they can know exactly the problems and shortcomings in the system, and take specific measures to deal with them by means of the analysis of logs. As for database encryption, it's generally considered that a database with higher security can have the function of information encryption, the corresponding encryption operations are carried out for the stored data information, and usually implemented in accordance with a specific encryption algorithm, so as to effectively prevent illegal users who obtain the relevant information in the database passes through the Web system [8]. Normally, the information encrypted by the database covers the relevant encryption of tables, attributes, records and so on. Based on the purpose of weakening the functionality of the database, encryption algorithms must be made more efficient and transparent in the phase of encryption, thus preventing data from being illegally cracked. In terms of the backup in the database, under the condition that system is disturbed by the network, the database needs to have the appropriate recovery function in case of that the data in the backstage of the database is damaged, or the problems caused by non-resistance factors, such as the external disasters and other parts of the database. Web system can complete the automatic backup function of database, when the database is attacked or the information is maliciously tampered, the database can be recovered using the information previously backed up, thereby further reducing the loss.

2. Research background

2.1. Web system architecture

The previous Web system architecture is the two-tier design patterns, client and server mode (C/S), in this way, the advantages of the client and server hardware can be used, proper classification of the work is achieved, and communication burden of the system is reduced. However, the rapid development of the network causes many problems of the C/S architecture. To highlight that the features of Web system are easy to be used, extended and maintained, B/S structure is proposed to complete the sharing of system information. The lightweight J2EE platform now takes advantage of research for Web systems of the company. The architecture of the J2EE framework is shown in Fig. 1.

In conjunction with the of research base station patrol management system of company, the scheme to enhance the security of MySQL database in the system was described. The scheme is generally divided into the following sections. Firstly, the rigorous database configuration and the development of the permission list are carried out; secondly, the security of MySQL is promoted by preventing SQL injection attacks. To further grasp the system usage scenarios, the company needs to carry out field analysis, generate specific requirements and exploration documents, select the most appropriate system architecture, and make the permissions distribution of database more reasonable. Based on many of the features of the system, perhaps SQL injection attack vulnerabilities are explored, the goals of preventing SQL injection attacks are realized, and the system consists of many storage engines. This layer is the implementation step of storage operation of the underlying data, and all the information stored in the database is effectively managed. Because of the differences in types, the features displayed by the storage engine are different, the type of engine selected for implementing data storage operations can be determined through a systematic analysis of the characteristics of the stored data as well as the advantages and disadvantages of the engine [9].

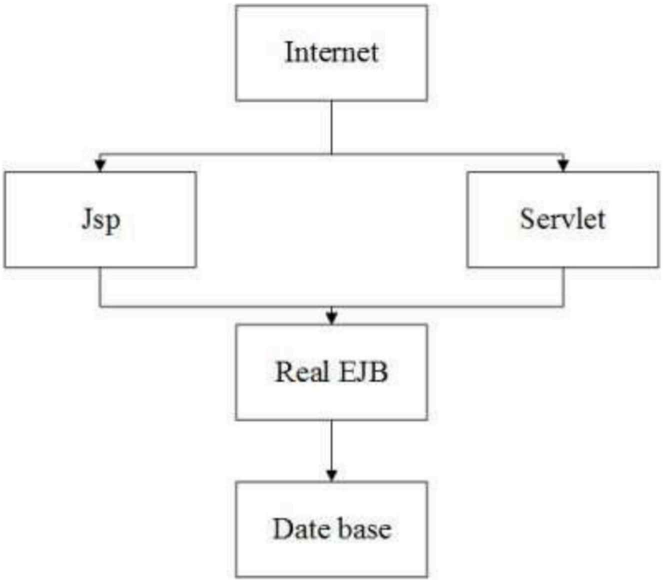

Fig. 1. The framework of the J2EEframework.

2.2. Overall design of the system

The management system of base station inspection adopting B/S mode is designed and developed under the Java platform, its framework is the native JSP + Servlet + JavaBean of Java, which is typical of the MVC mode. JavaBean is the Model layer, responsible for the business logic implementation of the system; JSP is the View layer, which is responsible for interacting with the user and displaying the data objects to the user through the page; Servlet is the Control layer that connects the Model layer to the View layer, can distribute the user's request and select the appropriate view to display the request, and also explain the user's input and map it to the executable operations of Model layer.

In the system, the three-layer architecture of MVC mode can divide the most data, the business logic and the user interface of the web system into three parts in essence, in the actual research and development, factories and single instance mode can be integrated to accomplish the high cohesion and low coupling of the system, which is convenient to the extension and protection of the program. The topology of the intranet is shown in Fig. 2.

The goal of the research on the management system of base station patrol is to help the patrol inspector of base station to carry out the corresponding patrol, use GPS positioning function to supervise the inspection activities of inspector, use mobile terminals to replace the paper inspection table, improve high-tech supervision, and send pictures in

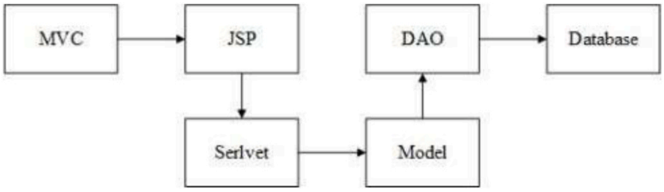

Fig. 2. MVC topology.

terms of the abnormal problems. In addition, the operator of system needs to carry on the classified research and the examination for the inspection information of base station, export the data form which is needed according to the demand, and searches the unusual base station from the inspection information, so as to improve the efficiency of saving abnormal problems of the base station [10]. The integrated system involves system administrators and senior administrators who are generally responsible for maintenance and management activities, in particular, the senior administrators of system need to manage the maintenance of server to ensure data of system is stable and running smoothly. The integrated system is based on the needs of operators and responds to the principle of energy saving and emission reduction, the users of different systems have clear operation authority. The comprehensive management module of the system is generally responsible for the supervision of the base station information, patrol personnel and news pictures, the function of this module includes the implementation of the database, preparation of the inquiry of many data tables in the database, adding, deleting and correcting the base station, patrol staff, patrol personnel, work assignment and so on. In addition, in the above module, the channels are prepared for administrators to enter the system, and multiple logins are used to ensure the security of system.

2.3. Optimization for the database design of the system

MySQL is as the back-end server of the Web system, attacker uses the lookup tools to explore the Web system, after using the MySQL database, the network communication system of MySQL is explored, persistent analysis is carried out for the related versions and content of database, as well as the SQL injection vulnerabilities that appear, the information obtained can be used to help the attacker to understand the related content of database, and then the injected attack plan can be revised according to the above content. According to the TCP/IP communication protocol, the monitoring port recognized by MySQL is 3306; the 3306 port of server of system realizes the data sharing with client. Understanding the details of the MySQL server's way of delivering information can help the attackers to perform attacks more effectively at a specific level.

In order to ensure the internal stability of MySQL, the development of ensuring the external security of MySQL is described. The external network attack encountered by the management system of base station inspection is usually SQL injection attack. According to the needs of the inquiry, the performance model of different functional modules is different; the SQL injection attack vulnerabilities are also different. In order to enhance the security of the MySQL database, a more efficient way is developed based on different functional modules to prevent SQL injection attacks. Prevention of SQL injection attacks generally are implemented on the client and server, many internal function modules of the system adopt the same methods for comprehensive prevention when they are researched, the client and server are ready to take precautions against the SQL injection process attack to resist a large number of attackers, and provide the appropriate basis for the stable operation of the MySQL database. The detailed procedure is shown in Fig. 3.

The support module of the security inspection of the base station covers the following two aspects, firstly, in the background support, patrol personnel uses GPS positioning in the mobile terminal to access to the system and determine the parts to be checked, and realizes the data sharing with mobile terminals, the relevant content of the mobile terminal declared by the patrol personnel is transmitted to the server through the wireless network, and the server gets the content and the content is explored, finally, the data is stored in the background database, and in this part, the system module completes a certain task. Secondly, the managers of system review the month patrol situation of various base stations in the PC, covering the patrol progress and detailed inspection content [11].

After the function of this module is completed, the GET mode is used in the page jumping, the goal of communication parameters is to facilitate the user to find relevant content, and user doesn't need to search the database for second times, so as to improve the efficiency of comprehensive operation. Even though URL can be encoded, English name is often chosen for the propagation parameter, which makes the process is more efficient and the garbled problems can be avoided. In general, Base64 coding can't work for English. Combined with the analysis of all kinds of circumstances, it's concluded that if the established purpose is achieved, the implementation of the GET request parameters will be verified. Like the number and the corresponding name of base station, the page has to check the information before it gets the data. If the parameter covers the sensitive character of the SQL injection, and the error page appears, then the system only needs to deal with the parameters that are up to standard, as shown in Table 1.

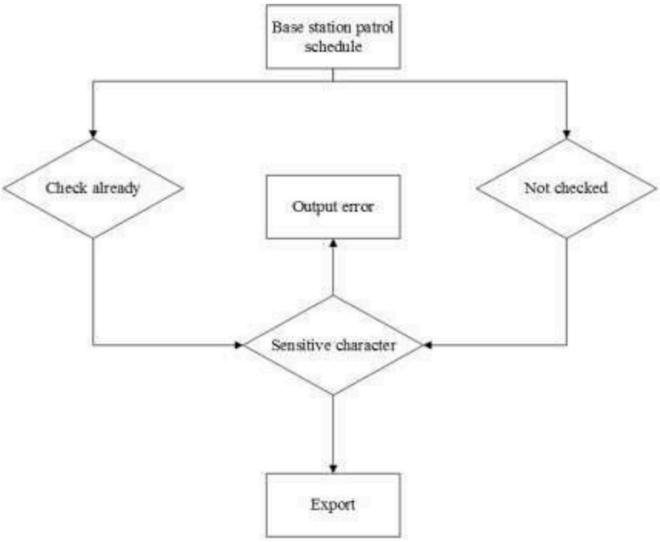

Fig. 3. Process of SQL injection.

This module includes the logins of system management, two logins are to maintain the stability as well as security of system, after the login of system, and the admin page contains all the functions that the system administrator can manage (see Table 2). In this process, the key difference between the system administrator and the supervision of the patrol personnel is the introduction of the ownership difference of the human rights.

Compared with the traditional model, neural network has a higher fault tolerance. It is less sensitive to the incomplete information, and in particular, it is less susceptible for it to be damaged in a quiet environment. Due to the specific characteristics of this model, it can effectively reduce the negative impact of distributed information. At the same time, its adaptability is very strong, and it also has good learning abilities. In the construction process of computer security evaluation system, it can also reduce the error through self-adjustment, and carry out training after the self-calculation law. In this process, costs of people, money, material, time and other aspects are relatively high, but in terms of the efficiency of work, it is a big leap. The operating process is now more concise, and the results can be quickly acquired [12].

3. Methodology

At present, many software systems have been applied in the field of

Table 1
Parameter processing statistics.

	Name	Tape	Limit
ID	Num	Int	10
Date	Timestamp	Int	20
Message	Varchar	Out	10

Table 2
Different types of neurons.

Hyperbolic tangent function	$1-e^{-x}$ $f(x)=$ $1+e^{-x}$
Gauss function	$f(x) = e-(x2\sigma2)$

computer network security evaluation. They can detect network security vulnerabilities, but they lack the assessment of network security risks. Up to now, there is no formation of a truly support network information security assessment platform. Some current systems are unable to be combining the evaluation technology with the testing technology, so they are unable to guide the network security risk assessment and testing. Therefore, on the basis of BP neural network and genetic algorithm, a simulation system model of network security assessment was studied and designed in this paper, covering the detection and evaluation.

3.1. *Construction of evaluation system for network security*

In fact, many factors can affect the security of computer network. In order to solve this problem, a safety evaluation system was established to evaluate its security situation [13].

According to the standards of accuracy, timeliness and independence, a safety evaluation system was built up to reduce the correlation between the evaluation indexes. And the indexes were selected comprehensively, so as to reasonably reflect the safety degree of the computer network operation, and fully consider the work load and work efficiency of the computer. During this evaluation, the scientific and reasonable analysis was completed according to the actual situation of the computer, so as to adopt the standard analysis model and classification approach to distinguish the safety of computer network operation. According to the actual situation of computer network security, quantitative evaluation indexes were used to ensure the effective solution of the problem. Due to the difference of the measurement units, the range of the value of quantitative evaluation was determined. Subsequently, the results were compared with the results of qualitative evaluation, and the standard treatment was applied comprehensively.

3.2. *Network security evaluation system under neural network*

The emergence of neural network has provided a general standard model for the construction of computer simulation model. According to the application of classification, the neural network has several functions: it can be directly used as the simulation model to be used in the study; it can be used as part of a recognition simulation model to carry out the pattern recognition; the simulation model can be used as part of the optimization function; it can be combined with other simulation models to promote other fusion models; it can be regarded as a whole to form the control system of identification and process, and it can integrate all kinds of information to simulate and control the nonlinear system [14].

The computer network security evaluation system constructed by neural network was composed of three parts: the input layer, the hidden layer and the output layer. Among them, the number of nodes in the input layer must be consistent with the evaluation index of the computer network security evaluation system [11]. The BP neural network mainly adopted one way implicit hierarchy. Too few nodes will have an impact on the fault tolerance of the evaluation system, and the excessive number of nodes will extend the learning time of the system. Therefore, in order to ensure the stable operation of the safety evaluation system, the number of nodes should be set as 5.

3.3. *System simulation*

The system simulation is a new discipline which emerged and developed in the late last century, and it can study, design, and transform a model which can reflect the characteristics of the system and meet the requirements of the system, so as to reveal the existing or future characteristics of the system and the operating rules, and it also can predict the future. Initially, it used to be applied in the experimental stage of the system, but now it has been gradually applied to training. Now, its applications have been extended to the system research, forecasting, the design and development, testing and evaluation, training and forecasting, and other aspects, covering many important areas of the national economy [15].

The construction of the system simulation model is based on two main methods: the mechanism modeling and the identification modeling. But these two kinds of traditional modeling methods have problems in two aspects: the modeling objects are extremely complex with too many uncertain factors, so the establishment of a complete mathematical model is almost impossible; the requirement for system modeling is becoming higher and higher, so the ability to describe of the system model and the adaptive performance of the modeling process need to be improved.

4. Result analysis and discussion

4.1. *Performance analysis of single index evaluation*

After the completion of the simulation model, the initial connection permissions were exploited. Effective learning can ensure that the computer network security evaluation results were as much as possible consistent with the requirements of the agreement.

According to the fair standard of the industry safety evaluation, the computer network security can be divided into A, B, C, and D these four levels, indicating the level of safety. In the model system of this study, 17 specific points of the computer network security indexes were listed as input values, and the score of the safety comprehensive evaluation was regarded as the expected output value of the network. In this process, a consistent sample was required. At the same time, a network that was already trained was needed. In the comprehensive evaluation, the analytic hierarchy process (AHP)was used to test whether the design simulation model was equipped with an ideal safety evaluation effect [16].

4.2. *Test results of simulation model*

In this study, the Matlab computing language was used. Through Table 4, a sample evaluation was conducted. After 1000 times of training, the results were less than the expected error range. It can be concluded that the simulation model designed in this study was reliable and effective. The difference of actual and expected output values was less than 3.5%, and it represented the safety level of B [17].

Neural network has strong robustness, and in the increasingly complex information age, the application of computer network security simulation is gradually expanding. In this study, the simulation model of neural network was studied, and it can be proved that neural network can promote the use of computer simulation [18,19].

4.3. *Targeted SystemTest based on web application*

The system is tested and the test environment is listed below. The tested content includes functional tests for system modules, selection of tools to scan the system, and the presence of injection vulnerabilities, analog injection is provided for the regions where the attack potential is in the corresponding module, and the specific test results are shown in the function test of module.

Specific tested module includes the login function test of system, test

Table 3
Single evaluation index.

	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	$^{c}10$	$^{c}11$	$^{c}12$	$^{c}13$	$^{c}14$	$^{c}15$	$^{c}16$	$^{c}17$	Output
1	1	0.92	0.94	0.84	0.89	0.89	0.91	0.93	0.97	0.94	0.91	0.86	0.99	0.97	0.86	0.94	0.91	0.96
2	0.92	0.90	0.89	0.87	0.91	0.84	0.83	0.87	0.89	0.88	0.90	0.87	0.92	0.82	0.81	0.86	0.87	0.88
3	0.72	0.73	0.79	0077	0.80	0.75	0.79	0.71	0.73	0.84	0.71	0.76	0.89	0.76	0.76	0.85	0.74	0.73
4	0.65	0.64	0.59	0.64	0.68	0.66	0.76	0.66	0.60	0.61	0.65	0.64	0.60	0.70	0.66	0.42	0.65	0.59
5	0.97	0.91	0.87	0.91	0.70	0.87	0.97	0.89	0.95	0.88	0.89	0.79	0.61	0.62	0.85	0.91	0.85	0.93
6	0.86	0.82	0.80	0.83	0.88	0.90	0.85	0.79	0.78	0.82	0.88	0.87	0.91	0.82	0.79	0.79	0.95	0.82
7	0.74	0.71	0.73	0.80	0.82	0.69	0.61	0.67	0.74	0.79	0.61	0.83	0.75	0.77	0.66	0.61	0.68	0.71
8	0.61	0.53	0.67	0.66	0.71	0.52	0.58	0.57	0.55	0.63	0.60	0.67	0.71	0.63	0.64	0.66	0.63	0.57
9	0.93	0.92	0.88	0.64	0.76	0.92	0.90	0.60	0.71	0.83	0.81	0.71	0.92	0.66	0.92	0.87	0.92	0.94
10	0.79	0.82	0.83	0.77	0.63	0.81	0.89	0.88	0.87	0.81	0.73	0.80	0.77	0.75	0.71	0.92	0.91	0.77
11	0.63	0.61	0.59	0.63	0.68	0.64	0.59	0.7	0.65	0.66	0.71	0.59	0.66	0.67	0.51	0.71	0.68	0.64
12	0.62	0.66	0.67	0.48	0.55	0.59	0.64	0.69	0.60	0.71	0.65	0.63	0.49	0.58	0.62	0.71	0.68	0.61

Table 4
Testresults

	Expected output	Actual output	Error	Evaluation value	Output level
E_1	0.873	0.891	2.05	8.92	B
E_2	0.826	0.862	3.72	8.82	B
E_3	0.847	0.876	3.30	8.76	B
E_4	0.839	0.849	1.21	8.49	B
E_5	0.833	0.868	3.33	8.59	B
Average value	0.844	0.866	2.86	8.67	B

of support module for security patrol of base station, test on the statistical query module of the base station's patrol, test on the location module for abnormal fault of base station and so on. Because of the limitation of space, the test of support module for security patrol of base station was emphasized. The support module for security patrol of base station shows the progress of the patrol stations in the same month, indicates days to the end of the inspection cycle, gives the detailed business name, inspection location, the number of base stations with complete inspection and the incomplete inspection, and check the details of the patrol information. The basic architecture diagram of Web application is shown in Fig. 4.

Chrome browser's own developer tools are used to view the detailed address of the jumped page, when attackers jump to the list of information to browse the patrol details of base station, they can pass the parameters in GETmode, the number of completed inspections is taken as the example, the attacker can get the path http://10.110.161.85:8080/jizhan/front/get checked action by looking at the relevant developer tools. According to category = 0&level = A, the request passes two parameters which are cate and level respectively, and the meaning of the two fields can be guessed, if attackers try to obtain the name and version of the database used by the system, the system will jump to the page, the quantity of input points generated by SQL command statement in the background is shown in Table 6 (see Table 5) (see Table 3) (See Table 7).

Table 5
System test environment.

System test environment	Concrete condition
System platform test environment	Java:JDK1.7Server:Tomcat 7.0Storage:2GB2.8GHzOS:Windows7 Database:mySQL5.0
Mobile terminal test environment	CPU: Pentium(R)Dual-Core2.00 GHz
System hardware test environment	Memory:2 GB Harddisk:500 GB

Table 6
The number of input points of webpage (interactive channel).

A Webpage with a vulnerability	①	②	③	④	⑤	⑥	⑦	⑧	⑨
Number of input points	2	6	2	47	2	49	19	18	9

Table 7
Usage case input setting of penetration instantiation.

Test operator	Coverage criteria	Instantiated use case setting
▽DS	RCR coverage	Select 5 random characters/strings
▽SQLC·▽COMS	Command verb coverage	MV = {select, create, insert, update, delete, drop, alter} Eachverbconstructs1usecases
▽SP·▽COMS	RCR + command verb overlay	MV = {randomlyselects3storedprocedureverbs.} verbsgenerate1usecases
▽IE·▽CON,▽ NE· ▽CON,	Relational predicate coverage	OP = {<>,<,>,≤,> = ,between, IN, like} Eachpredicategenerates1 usecases
▽disg	Camouflage cover	DG = {Unicode encoding, ASCII encoding, case mixing}

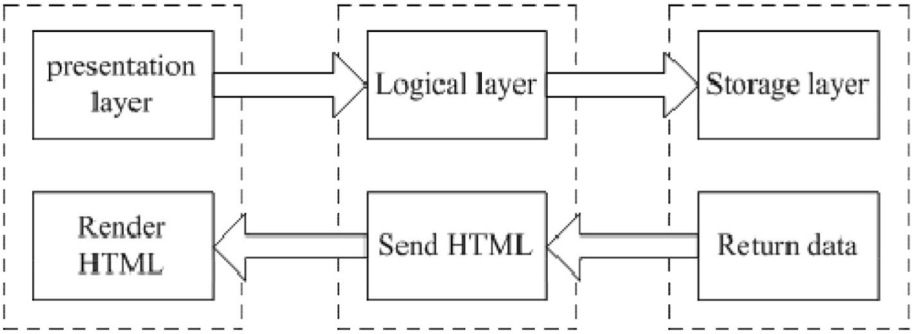

Fig. 4. The basic architecture of the targeted web application.

4.4. System testing based on SQL security vulnerabilities

The statistical inquiry module of the base station includes the name, the type, the work station, the patrol personnel, the start and end time, etc. of the base station; in accordance with the requirements of inquiry standards, the required elements aren't set; however, at least one factor should be selected, all conditions don't require manual input from the operator and completed according to the selection method. Query criteria are declared in the form of POST mode, the GET mode is used to transfer parameters only when looking for the list of patrol information and details, and the way to prevent SQL injection is the same as that of the security inspection support module of base station. Emphasis was placed on the use of JavaScript technology and string filtering to filter manually entered content from the attacker's level of creating malicious SQL statements to ensure the operation of database meets requirements. In addition, attackers may get sensitive data during network transmission. After the attacker's access to the relevant content of the legitimate user, sensitive data is encrypted when the system is upgraded, the encryption algorithm of database is deeply analyzed and the corresponding guarantee is provided for the security of MySQL database. MySQL database security system is fully explored, such as storage processes, even if the storage process can't prevent SQL injection attacks, however, the rational use generally can ensure the safety of the database in the program development period, and provide the appropriate basis for efficient operation of the system, in addition, maintainability is high and there are a few code flows appearing. The injection of the usage case model is input into the operator formula, and the instantiation is set as follows.

5. Conclusion

The use of MySQL databases in Web systems was incorporated during the learning period of author, the relevant research of improving database security under Web system was pointed out, and the research of patrol management system of base station was completed. The system used MVC mode and JSP + Servlet + JavaBean technology, firstly, MySQL features were exploited to carry out security configuration, the internal security system was utilized to ensure the stability of the MySQL database server; based on Web systems, the way to ensure the smooth operation of the MySQL database was continually analyzed. In the detailed research, the front-end used JavaScript technology to filter the user's input content, and background used string filtering to prevent SQL injection attacks, and feel the key to security. When the system was completed, especially the integrated management module showed the obvious repeatability in the operation of the database. In order to enhance readability and protection of code, the understood factory pattern was adopted to investigate functionality and enhance the extensibility of module. In the completion of the system, functional completion, extensibility and reasonable compatibility were fully analyzed, and the most suitable way was chosen to prevent SQL injection attacks. The system not only completed the information supervision of the base station inspection, but also ensured the information security in the database, and provided the foundation for the following development of Web system and the configuration of MySQL database. In this work, by analyzing the characteristics of neural network system and its algorithm, in terms of the weakness of convergence and search of the neural network, a new algorithm was adopted; on this basis, the simulation model of computer network security was designed; finally, the results of the evaluation were carried out by the corresponding test. The simulation results show that the performance of the simulation model is excellent with extremely abundant promotion value. From a global perspective, the neural network and system simulation both have more than 50 years of research history, while the neural network security evaluation of the computer network simulation system has only a history for 20 years. Therefore, whether from the theoretical, methodological, or technical point of view, it is not mature enough. In the future, the dynamic system simulation, the theory of the simulation algorithm, the evaluation of the simulation credibility, and the choice of the structure of the neural network should be studied continuously and deeply. Finally, we are firmly convinced that the simulation study of computer network security evaluation under the neural network will create a glorious era.

The security of the Web system is continually analyzed, and the key to this article is to analyze theSQL injection attacks that Web systems in PC side may suffer, and to prevent them when the system is completed. With the widespread use of mobile phones and the progress of the mobile Internet, the probability using of smart terminals to carry out SQL injection attacks continues to improve; in addition, there will be a security risk in the background MySQL database. The instantiated use case is output to the response module of the penetrated test link set and the developed by the OUT to determine the presence of SQL injection security vulnerabilities. Therefore, the system needs to be constantly improved so that the system can meet the requirements of the development of Internet science and technology and maintain the database from being violated.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] Li Haiyan, Xu Wenming, DragonTechnologyandapplicationRuixian.Web database security, Digital 6 (2016) 107–108, 60-64.

[2] Yun Woo, Security database mandatory access control research and implementation, Bus. Soc. Rev. (1) (2000) 56–57.

[3] Yang Zhang, Research and Application of Database Security Technology, Computer Disk Software and Application, vol. 1, 2013, pp. 143–144.

[4] Xiangbin Zhu, Security Database Mandatory Access Control Research and Implementation, vol. 11, Jilin University, 2010.

[5] Xiaodong Liu, Research on Network Database Security Technology Based on Web, vol. 5, Wuhan University of Technology, 2013, pp. 11–16.

[6] Jinqiu Lv, Web Database Security Technology Research and Application, vol. 4, JilinUniversity, 2014, pp. 56–59.

[7] Lei Yang, Design and Implementation of Database Security Audit and Detection System, vol. 7, Beijing Jiaotong University, 2014, pp. 88–102.

[8] N.A. AlSayid, D. Aldlaeen, in: Database,security,threats:survey,study.Computer, Science,and,Information,Technology(CSIT),5th,International,Conference,on,IEEE, 2013, pp. A60–A64.

[9] Lei Yang, Web network database security system to establish and perfect, the, J. Xichang Teach. Coll. 2 (2014) 69–72.

[10] Yongsheng Wang, Web. Application of SQL Injection Attacks Intrusion Detection Research Based of the Zheng Zhou University.Research and Implementation of, Northwestern University Zhouyan. SQL injection detection method, 2014, pp. 60–64, 2014.

[11] Jing Xiong, SQL Injection Detection Technology Research, Huazhong University of Science and Technology, 2015, pp. 60–64.

[12] A. Sadeghian, M. Zamani, A.A. Manaf, in: A Taxonomy of SQL Injection Detection andPreventionTechniques.InformaticsandCreativeMultimedia (ICICM),2013InternationalConferenceon, IEEE, 2013, pp. 53–56.

[13] Yuanpeng Li, SQL Injection Attack Scanning Analysis Tool Implementation and Attack Prevention Technology, vol. 9, Beijing Jiaotong University, 2016, pp. 60–64.

[14] hinges Liu, Multi Function SQL Injection Detection System and Attack Prevention Method, vol. 8, Beijing Jiaotong University, 2015, pp. 60–64.

[15] Tao Wang, Analysis of computer network security and preventive measures, Sci. Technol. Innov. Appl. (2) (2013), 45-45.

[16] Guoyin Wang, Fuchun Sun, Huadong Ma, To meet the era of intelligent"artificial intelligence" special article ", Comput. Sci. 43 (12) (2016) I0001–I0002.

[17] Licheng Jiao, Shuyuan Yang, Neural network for the past seventy years: review and Prospect, Chin. J. Comp. Sci. 39 (8) (2016) 1697–1716.

[18] Yongkang Xing, Yang Shi, Chao Mou, Multivariate Chebyshev Neural Network and its fast weight determination algorithm, Comp. Appl. Eng. 49 (13) (2013).

[19] Qiang Zhang, Dezhi Xu, In the sonorous, uncertain nonlinear system robust control adaptive terminal sliding mode, Self-Organiz. Wavelet Cerebell. Model Articulat. Controll. 33 (3) (2016) 387–397.