ABSTRACT: Research shows that with hundreds of application systems, the general colleges and universities have different developers in uneven professional levels, such as professional personnel from outside of the school, from independent departments, and even the students. The operating environment of application system is scattered in a managed way, by cloud services or directly in the office. The various application systems and the complex operating environment in colleges and universities, and some unprofessional developers would make bugs and difficult to manage. Nowadays, the universities have been widely deployed firewalls, intrusion and other network security equipment, so that hackers have been difficult to attack the websites through the traditional network layer. However, due to the widespread bugs of web application, hackers often use them to attack the sites. Thus, it is urgent to develop a set of security management service platform to help the information security administrator manage the basic information, find bugs before the attacker and timely repair. Based on the above reasons and combined with the actual needs, the campus network security management service platform is designed and developed.
The record management mainly include the integration of record information, modification, query, deletion and export. The record information mainly records the basic system information, such as system function, IP address, subordinate unit, manager and so on, to facilitate the information administrator.

The bugs management mainly include integration about two types of bugs (WEB bugs and system bugs), query of bugs, deletion of bugs, analysis of bugs and the comprehensive analysis report.

The off-campus access management can integrate information from off campus access to this platform, so that the information security administrator can view and modify off-campus access to each system server.

The security management is to generate comprehensive analysis report and issue security announcement. The bugs of all application systems are analyzed, and statistics on the distribution of campus network bugs is done, which are presented to the users in the histogram and pie charts.

And according to the relevant record information, a security rectification notice is issued to the person and his department in charge of the system.

2.2 System architecture design

Based on the functions of campus network security management service platform, this system takes advantage of B/S structure, and the architecture diagram is shown in figure 1. The work interface used by information security administrator is presented through the browser, the main logic part is shown in the server, and a little part is realized through the front.

3 DETAILED SYSTEM DESIGN

3.1 Record information management module

Integration of record information can be done through single import or mass integration. The single import requires the information security administrator to manually enter the relevant information of the application system, whose efficiency is relatively low. It is used for application system without filing in office automation system. The mass integration is used for the application system filing in office automation system. This method is based on the implementation of Excel middleware. The document of Excel format is used as intermediate media of data exchange between office automation system and this system. First of all, judge whether the record data about to import are normative, and modify it if not normative. If it is normative, manage the information and extract related data. Then make sure whether the record information of this system exists. If there is no similar information in the database, then add a record to the unique table and the historic table. If it exists, update the record information in the unique table, and add a record in the historic table.

The query of record information can be done through condition query and instant query. Condition query means that the random combination of IP, domain name and import time can be used as condition to search. Instant query means to enter anything as condition to search for all fields of the target data that has been queried. Users can search any data they have interest with these two methods. For the data having been queried, the user can also put them in order.

Modification and deletion module means that the record information can be modified and deleted. The modified information is updated to the unique table of the record information, and a record is added in historic table. When the information is deleted, it is deleted in unique table and the record in historic table cannot be deleted to provide resource for the later data search.

The filing information export module realizes the function that users can export the record information in the form of Excel file, and it is convenient for users to carry on the data statistics and report.

3.2 Bugs information management module

Bugs management module concludes integration of two types of bugs, query of bugs, deletion of bugs, analysis of bugs, and comprehensive analysis report.
The two types bugs integrated are Web bugs and system bugs. The two kind of bugs can be found through scanning the server and the system, which comes from the remote security assessment system of the green alliance. Due to the restriction of the authority, this system cannot get the data directly from the scan result database. Since bugs information report of excel form can be gotten based on remote security assessment system of green alliance, the excel file can be used as data exchange medium between the campus network security management service platform and remote security assessment. Because Excel files are from remote security assessment system, the format and content of the document cannot meet the needs of users, so this platform need special treatment for file format. Two types of bugs information files include two work tables. The system bugs information file is corresponding to the host profile and bugs information work table; Web application bugs information file is corresponding to the site profile and risk distribution table. In the process of integration, the system would analyze the four work table, extract required data, and put them into the corresponding database table. Bugs information integration process is shown in Figure 2. First read the bugs scanning information. The program verify the scanning information, modify the error data and verify it again, and extract the qualified. And then determine whether this bug is a new one. If it is new, add it to the bugs database, and the number of times the bug appears is initialized to 1, namely find count=1. If it is old, add 1 to the counters, namely find_count+1. After the bugs’ database is updated, take out the ID bugs and IP fields in the table of the database, and judge whether it has appeared in the application system based on these two kinds of information. If it does not exist, add a record in the application of the distribution table; if it exists, add 1 to counters in the distribution table, namely count+1. At the end, the import field is assigned to the recently discovered bugs time field.

3.3 Information security management module

Information security module includes comprehensive analysis report, monthly report, and safety notices and safety knowledge.

Monthly report means that system monthly analyzes bugs information of all application systems in subordinate units, and generates a monthly report, which is composed of safety notices. At first, the university information security administrator fill out monthly basic information and click the generate button, and after the system collects the monthly basic information, all iterators of subordinate units are removed. And then determine whether subordinate unit exists in the iterator. If existing, the subordinate and all the host and host bugs information should be extracted. Then judge whether the number of host bugs is above zero. If above zero, analyze the bugs and generate security notice. If not above zero, do not generate notice. Then go on judging whether there is subordinate unit in iterator, and generate monthly report if not. In order to save space, in the process a safety announcement is not generated, but to store the data required in a database table. When information security administrators and managers of subordinate units download the notice, the system extracts the data from the database and then generate notification file.

4 IMPLEMENTATION OF THE SYSTEM

The background of the system is developed by using JAVA programming language with good portability. The hardware is Intel Core 3.2 GHZ CPU and 4GB RAM; software is JDK1.8, Tomcat 8.0, and Mysql5.6. The system has been developed and put into use on the line.
The current campus network is booming, but there is no uniform standards and rules for the construction of university information. The application system is purchased and developed independently by the individual department. The department is also responsible for most daily operation and maintenance of the system. Due to the large number of campus network application systems and the scattered operation, universities cannot effectively manage them. Due to the lack of unified management, coupled with security risk of Web system, the application system is frequently attacked. The campus network security management platform can manage uniformly the record information and site of internal application system and help security managers find problems before the attacker and timely repair, to provide an important guarantee for the university personnel training and scientific innovation.

REFERENCES