Research on Key Technology of Web Application Security Test Platform

Yun-Lan Ruan and Xiao-Qing Yan

[Abstract] With the continuous deepening and popularization of Web applications, the corresponding Web vulnerabilities and malicious attacks emerge in an endless stream, making it efficient and accurate to evaluate the security of Web applications. In this paper, Web application security testing technology, building plug-in and extensible security testing technology framework, and the key technologies of unknown vulnerability intelligence discovery and supporting self defined test tool integration are studied. In the runtime and runtime of Web application, security scanning and risk discovery can be strengthened by platform. It can enhance the safety detection of Web application and ensure the safe and reliable operation of Web application.

[Key words] Web applications; security testing; plug-ins; integrated frameworks; vulnerability mining

1 Introduction

With the rapid development of information technology, more and more applications begin to be provided by the form of Web. Convenient and fast Web applications have been widely applied in government, enterprises and army. However, unsafe Web applications make China's financial, medical, national defense, energy and other important network architectures face a serious security threat. As the digital architecture becomes more complex and interrelated, the difficulty of realizing the security of Web applications has also increased exponentially. Web applications are becoming more and more complex, resulting in more and more inherent vulnerabilities and defects, and are facing more and more attacks from the network. At present, the security problem of Web application has become an important technological challenge in the development of information technology in China. We need to have targeted protection against Web application attacks, that is, different protection technologies for different attack behaviors.
Therefore, the research and design of Web application comprehensive testing platform for security testing and timely detection of Web application vulnerabilities is of great significance for preventing all kinds of Web application attacks.

2 research status and shortcomings
In Web application software analysis and testing research, Ricca and Tonella put forward a UML based model. Kung et al. Represented Web application or Web website by a graph. According to the navigation order of page browsing, we built test tree to generate test cases to detect state behavior errors. Kallepalli et al put forward a Unified Markov Model method based on statistics and data information for application testing, performance evaluation and reliability analysis.

In the aspect of automatic detection technology of Web application vulnerability, Microsoft divides security vulnerabilities into ten categories, and based on that, it clarifies the needs of Web application security framework. OWASP gives ten application vulnerability lists according to whether a few vulnerabilities are closely related, whether similar counteractions are used and whether they often appear in Web application architecture standard. Document [6, 7], aimed at dangerous data from untrusted sources, using dynamic Tainting Dynamic technology to detect dangerous data entering sensitive area efficiently.

Compared with foreign countries, the domestic research on Web application security testing is still relatively weak. A study of representative Lu Hong of Wuhan University and others from the state testing perspective on the testing of Web applications are discussed, the Tsinghua University Wuhai equal people developed a Web server performance test system and method of the HeFei University of Technology Wu Lei et al. Application environment error injection was investigated for safety testing. National University of Defense Technology Zheng Lihua, who is studying the evaluation system of Web application security testing based on network, the PLA University of Science and Technology Zhanwei Hui et al in the software security defects based on (SSD) is a useful exploration on Web application security testing method.

Through the analysis of the current situation at home and abroad, it is not difficult to find that our existing Web application security testing technology can not meet the urgent needs of information system construction, and the specific gap is manifested in several aspects.

(1) lack of integrated and unified framework for Web application security test. Currently, the mainstream Web application testing frameworks and tools are usually aimed at some specific Web application security vulnerabilities, which fail to carry out a comprehensive test of security flaws, and difficult to meet the requirements of Web application security testing.

(2) the lack of effective automatic scanning and discovery techniques for unknown vulnerabilities in Web applications. The current security tests of Web applications mainly use osmosis attacks to detect existing security vulnerabilities and lack a feasible method for detection of unknown security vulnerabilities.

In view of the practical needs of Web application security testing, aiming at the above shortcomings, this paper deeply studies the Web application security testing technology system, and establishes a plug-in, extensible, dynamic and interactive Web application security testing tool. In order to ensure the accuracy of safety testing and efficiency as the starting point, the key technology breakthroughs and intelligent method in finding unknown
vulnerabilities support custom testing tool integration method, finally lays the foundation for the Web application security test and provide a comprehensive test intelligent tools, a set of robust, and thus in Web application operation and before the operation, the security scanning and risk, to ensure safe and reliable operation of Web application.

3 Web application security.
Web application is a client / server application software system, including the client and server applications interact through the HTTP/HTTPS protocol, usually consists of five parts, namely the client (browser), Web server, application server, Web application, data source, between them to communicate through the mechanism of Web application architecture model as shown in figure 1.

Because the software system of Web application is relatively complex, and involves many ways, such as network, operation system, server and so on. At present, there is no uniform standard definition for Web application security at home and abroad. Strictly speaking, Web application security should include all the security issues involved in its architecture, such as network security, operation system security, browser security, Web server security, application server security and so on. Enterprises, governments and military units mostly use firewalls, SSL, anti-virus software, intrusion detection system and other measures to protect Web application security. But according to Gartner survey, most Web attacks are directly against Web application itself. Attackers build malicious HTML codes, such as XML, SOAP, Web Services and other data streams, and attack malicious vulnerabilities directly against Web application vulnerabilities. OWASP (Open Web Application Security Project) Web application security risk report released by SQL injection, cross site scripting has become a major threat to the security of Web applications, as shown in Figure 2, border protection, virus killing etc. the traditional means of security are insufficient.

Web application is the core part of developing and composing Web application. To protect Web application security, we need to adopt different protection technologies for different attack behaviors. This requires the timely discovery of various security vulnerabilities in Web applications and the corresponding precautions to be strengthened before real attacks occur. The WhiteHat survey reports that the sooner the vulnerability is found and the more timely it is made up, the smaller the attacker's chances of using the vulnerability to attack. Therefore, in-depth study of Web application security detection technology, development of evaluation tools for Web application security testing, timely detection of vulnerabilities in Web application, is of great significance for preventing Web application attacks.

4 Research on key technology of Web application security comprehensive test platform
4.1 Web application security test integration framework based on plug-in
The Web application security vulnerability has become a serious disaster area of the security risk of the application system, and presents a trend of increasing year by year. Although there are a wide variety of current Web application security testing tools, there are some defects without exception, and the operating efficiency is relatively low. To overcome these shortcomings, we design a plug-in based Web application security testing integration framework in Figure 3, which is composed of three parts: plug-in management unit, scanning management unit and global management unit.
The plug-in management unit is mainly responsible for the maintenance and management of vulnerability scanning plug-in, mainly includes the following modules: plug-in interface layer provides plug standard interface and specification for plug-in extension layer; plug-in management module, maintaining the integrity and timeliness of the plug-in library, to ensure the safety of the framework itself; plugin scheduling module based on business logic properties of Web application system, test the optimal scheduling of intelligent test, to ensure the efficiency and the detection rate of system vulnerabilities. On the basis of the three modules is the plug-in library and database maintenance module plug-in, plug-in library for storing various plug-ins, including two parts of local library and online library system, to facilitate fast retrieval and loading plug-ins, CVE vulnerability scanning plug-in, third party plugins include standard benchmarks (including interface compliance testing, etc. according to the system, and user plug-in) specific attribute definition vulnerability scanning plug-in. The plug-in library maintenance module is mainly responsible for the plug-in transmission between the local library and the online library, the plug-in audit, and the integrity maintenance of the plug-in library.

The scanning management unit is responsible for calling various scanning plug-ins, and using the plug-in to scan the Web application based on a variety of prior knowledge libraries and benchmark vulnerabilities. Which includes several modules: knowledge base / base vulnerability database used to store a variety of known or learned knowledge and reference basis as vulnerability scanning and heuristic learning; the application of Web information collection module, mainly used to intercept test framework and Web application of the message, in order to provide the data analysis as scanning plug-in plug-in; call the proxy module, as a specific plug-in in the scanning part in the abstract, through this module, the scanning component can call the corresponding plug-in, loose coupling and keep scanning component and plug-in management components; test report generation module, according to the results of the test generates the corresponding testing report and give feedback to the test personnel.

The global management component is responsible for monitoring and supporting the operation of the entire framework. Includes the following modules: system configuration module, the configuration of the various components of the whole system, guarantee system in accordance with the expected running test personnel; virtual user generated module and management module, virtual users to create and maintain different roles have different permissions, the user can use the virtual expansion approximation to the real environment to test Web applications; user interaction module friendly, for testers reading test results generated using the test report and test report generation module generates; error processing module, response and timely treatment of system error.

4.2 intelligent mining technology to support the discovery of unknown vulnerabilities

In order to explore new security vulnerabilities and detect security flaws that are closely related to specific Web applications, this paper proposes and designs an unknown vulnerability detection method based on intelligent mining.

In the detection of unknown vulnerabilities based on intelligent mining, the intelligent vulnerability mining module constantly learn and acquire specific business logic and application features in routine vulnerability detection method based on self learning service. Then, based on the known vulnerability database, under the guidance of the enlightening template,
we take the idea of "gene mutation", and generate new specific attack vectors for specific Web applications through unknown vulnerability services, and detect whether there are any unknown vulnerabilities outside the known vulnerabilities. For a variety of new Web application vulnerabilities and closely related with the specific application of the problem of unknown vulnerabilities emerge in an endless stream, intelligent mining detection technology based on the proposed, can use heuristic learning mechanism and self-learning mechanism to detect unknown vulnerabilities, enhance the ability to detect unknown vulnerabilities Web application, improve the automation and intelligence the detection ability of tools, can more effectively test application security. Intelligent vulnerability mining is based on conventional vulnerability detection and can not replace conventional vulnerability detection. Intelligent vulnerability mining requires routine vulnerability testing, obtaining input and output information of Web application, data flow and control flow information, and obtaining specific application characteristics before expanding test coverage and generating new attacks to detect new security vulnerabilities.

4.3 Web application security test tool implementation technology
According to the above theories and techniques, a comprehensive security testing tool for Web applications is implemented. The tool integrates the security testing of the known vulnerabilities of Web application interface, dynamic compliance, business security and unknown vulnerabilities to launch the comprehensive test, to ensure that most of the potential security vulnerabilities in the Web application on the front line, to ensure the safe and reliable operation of the new letter Web application information system based on. A typical Web application security test scenario using the tool. The tester using the console to configure and start the testing process of test tools, test framework according to the plug-in structure test agent testers configuration call the corresponding (i.e. a test tool tailored for instance), the agent generated a number of virtual characters with different identities and different roles, the role of virtual test launched a request to the Web application the test through the network, testing tools and service request response interception return, after using the configured plug-in security vulnerabilities of Web application and mining intelligent discovery, efficient discovery of Web application security vulnerabilities.

5 concluding remarks
This paper studies the Web application security testing technology, and constructs a plug-in and extensible security testing framework. In order to ensure the accuracy of safety testing and efficiency as the starting point, the key technology breakthroughs and intelligent method in finding unknown vulnerabilities support custom testing tool integration method, provides a set of comprehensive testing tool of intelligent robust, ultimately for the Web application security test in the construction of information system in the application of Web operation and before the operation, the the security scan and risk, to ensure safe and reliable operation of the Web application, to provide support and guarantee for the promotion of Web application security.
Reference