Design of Information System Vulnerability Governance Platform Based on Distributed Asset Acquisition and Vulnerability Verification Radar

Guiquan Shen¹, Jiangang Lu¹, Wuqiang Shen¹, Jingzhi Huang¹, Weiyan Ji²*
¹Information Center, Guangdong Power Grid Company Limited, Guangzhou, China
²Guangdong Information Technology Security Evaluation Center, Guangzhou, China
*Corresponding author’s e-mail: jiwy@gidtsec.org.cn

Abstract. There are a large number of information vulnerabilities in enterprise information systems. Many hackers use vulnerabilities to obtain enterprise or personal information, which greatly jeopardizes enterprise information security. This paper proposes a design method of integrated information system vulnerability governance platform based on distributed asset acquisition and vulnerability verification radar, discusses the business flow and architecture of the vulnerability governance platform, the logical relationship between modules, business function modules, and the technical framework for building platforms.

1. Introduction
In recent years, hackers have been attacking enterprise information systems more and more frequently, and enterprise information system security has become extremely important. The reason that enterprise information systems are attacked is that there are many information security vulnerabilities in information systems. If the vulnerability is exploited or traded on the black market, it is extremely harmful to businesses and users [1]. Therefore, information system vulnerability governance is the most important measure of information security protection, and it’s an important guarantee for enterprise information security.

Recent years, some vulnerability scanners were developed for searching information system vulnerabilities. Antunes propose a benchmarking approach to assess and compare the effectiveness of vulnerability detection tools in web services environments [2]. IBM Rational AppScan and HP WebInspect both are Commercial vulnerability scanning tool [3]. They can automatically scan the security vulnerability of Web applications, and help companies enhance the reliability of Web applications. IBM Rational AppScan is a leading suite of automated Web application security and compliance assessment tools that scan for common application vulnerabilities [4]. HP WebInspect performs web application security testing and assessment for today's complex Web applications, built on emerging Web 2.0 technologies. HP WebInspect delivers fast scanning capabilities, broad security assessment coverage and accurate web application security scanning results. WSDigger is a free open source tool designed by Foundstone to automate black-box web services security testing (also known as penetration testing). WSDigger is more than a tool, it is a web services testing framework. Version one of this framework contains sample attack plug-ins for SQL injection, cross site scripting and XPATH injection attacks. Doupé proposes a novel way of inferring the web application’s internal state machine from the outside—that is, by navigating through the web application, observing differences in output,
and incrementally producing a model representing the web application’s state [5]. Lukanta developed a vulnerability scanning tool extending an existing open source tool, namely Nikto, to detect session management vulnerabilities [6]. Pelizzi presents a new server-side defense against CSRF attacks, called JCSRF, operates as a server-side proxy, and does not require any server or browser modifications. Thus, it can be deployed by a site administrator without requiring access to web application source code, or the need to understand it [7]. You propose an improved CSRFGuard that the Servlet filter was used to intercept responses, and responses of pages' source codes were stored by a custom response wrapper class to add script tags, so that scripts were automatically inserted [8]. Recently, some enterprise information system vulnerability management platforms have been proposed [9-10].

Although there are many vulnerability scanners, different vulnerability scanners have different strengths and weaknesses. Information system vulnerabilities that a single vulnerability scanner can detect are limited. At the same time, it is not possible to embed an existing vulnerability scanner into an enterprise information system, and it is necessary to manually use an existing vulnerability scanner to test information system vulnerabilities, which is time consuming and laborious, and cannot detect new vulnerabilities in time. Existing Web application technology research can’t satisfy the requirement of information system development [11]. Therefore, enterprises urgently need to establish their own vulnerability testing platform, detect enterprise information systems in real time, discover enterprise information system vulnerabilities and fix vulnerabilities in a timely manner.

In view of the above problems, this paper presents the design of information system vulnerability governance platform based on distributed asset acquisition and vulnerability verification radar, discusses the business flow, architecture, business function design and technical framework.

2. Business process design

Enterprise information systems are often composed of multiple information subsystems, and each information subsystem may have security vulnerabilities. The Vulnerability Governance Platform should be able to handle all information subsystem information vulnerabilities. Internet vulnerability publishing platforms often publish new information system vulnerability information. The vulnerability management platform should be able to obtain these vulnerability information and update the platform vulnerability information so that new vulnerabilities in the information system can be discovered in time.

![Figure 1. business flow](image-url)
Business flow of Vulnerability Governance Platform is shown in figure 1. The vulnerability information management module has a common interface to support the connection with third-party vulnerability information platforms to obtain the latest vulnerabilities. The module has an automated inspection module that crawls the vulnerability information published by the Internet vulnerability publishing platform (including but not limited to: CNVD, CNNVD, National Internet Emergency Center website, CVE general vulnerability and disclosure website, etc.) according to the set vulnerability crawling rules. The module also supports batch import or manual entry to add vulnerability information.

Sources of information assets include: 1) Interfacing with existing asset information management related platforms (such as ITSM systems, etc.) to obtain asset-based data. 2) Dispatching the distributed asset collection radar, obtaining asset attributes and fingerprint information, and monitoring asset changes. 3) Support batch import or manual entry to add asset information.

Sources of threats include: 1) Establishing vulnerability scanning tasks on the platform, conducting vulnerability scanning, and exploiting vulnerability. Vulnerability scanning supports different granularity vulnerability scans, including: full vulnerability library scanning, scanning by vulnerability category, specifying scans for specific vulnerabilities, And more.2) When the vulnerability database or asset library changes, obtain the information in the internal network of the information through asset matching and rapid verification of the vulnerabilities in the network, and automatic measures threat levels, and form internal threat intelligence.

Visualization of internal threat intelligence is mainly based on map visualization, visualization based on different latitudes, visualization of vulnerability response based on different time points, recurring visualization based on the same type of vulnerability, visualization based on vulnerability validation, visualization based on the scope of the vulnerability.

3. Architecture of platform

3.1. Overall architecture design

![Figure 2. Overall architecture](image)

The architecture of Integrated vulnerability governance platform is shown in Figure 2. The Integrated vulnerability governance platform mainly includes several functional modules such as platform management, asset management, vulnerability database management, vulnerability management, and system configuration management. The Integrated vulnerability governance platform controls the radar
equipment information. Vulnerability verification radar detects system security and determines if there is a vulnerability in the system. Asset acquisition radar scan asset attribute information. Radar detection radar verifies vulnerability information by executing poc scripts. The platform docks the external system to obtain external system resources.

3.2. Logical architecture
At the functional level, the system includes process management, data resource management, component management, system management, and unified display management, as shown in Figure 3.

![Figure 3. Logical architecture](image)

Process management is invoked through data management, starting, stopping, and suspending various processes to control the definition and execution of processes.

Data management includes vulnerability information data, operational process resource data, and external system submission data, which is provided to the statistical data for statistical data foundation.

Component management provides asset scanning discovery, attribute identification, vulnerability scanning, and POC scanning.

Unified display management provides data statistics for different business types and provides a vulnerability security posture. System management provides users with functional rights and data permission controls, and strictly defines the data resources accessed by each user.

3.3. Functional structure
Business function architecture includes: system management, information asset management, vulnerability database management, vulnerability task management, system threat management which statistics report and internal threat intelligence analysis, as shown in figure 4.

System management includes role management, Authority management, user management, task policy management, and radar configuration management. The platform's asset data comes from three aspects, existing asset management platform, manually imported asset information, and asset information obtained by asset acquisition radar.
Vulnerability library information sources include subscribed vulnerability update library, vulnerability information obtained by docking security organization vendors and vulnerability validation radars. After obtaining the latest vulnerability information, the vulnerability validation radar quickly verifies the existing assets, obtains the intranet vulnerability threat. Among them, each area shares vulnerability information and vulnerability disposal suggestions. When a vulnerability threat is discovered, an internal threat information display is formed based on the existing vulnerability information, asset information, and threat information, and is presented by using a visual chart.

3.4. Technical framework

The technical architecture of the system is divided into four layers, namely user interaction layer, functional service layer, technical framework layer and system platform layer.

User interaction layer provides the ultimate human interaction framework. The functional service layer provides customized functional components that support system operation. The technical framework layer provides the general technology needed to implement functional components. The system platform layer provides the operating environment required for a common technical framework.

The technical framework layer provides the underlying component set for the system, ensuring that application system development only needs to focus on the implementation of business logic, without having to care too much about the underlying technology. The set of components provided by the technology framework layer covers all levels of the application system: data framework for data provision, process framework for process definition and control, security components for application security, business framework for business implementation, and UI framework for interface presentation.

The data framework function is divided into two parts: data access and data processing. MyBatis framework is used to access database. It converts database objects into program objects for access. The process framework provides the basic environment for the work approval process for the upper layer, including Workflow Engine, Spring, and Security. The workflow engine is responsible for maintaining the definition of the process and various process instances of the defined process, and is responsible for the flow control and business rule process. The security component provides the system with technical functions such as security filtering, secure transmission, and data security. These functions are completed by Security, SSL, AOP, Model, and Encrypt. The business data of the information system vulnerability governance platform mainly includes: task process management data, system management data, information asset management data, vulnerability database data, vulnerability task management data, POC task data, rule library file data, rule base data, and data dictionary data.
4. Results
To illustrate the applicability and scalability of the cross-regional vulnerability management and control platform, we use six different types of vulnerabilities to detect whether the vulnerability governance platform can detect vulnerabilities and conduct them in a timely manner. These six different types of vulnerabilities are SQL Injection, XPath Injection, Code Execution, Buffer Overflow, Username/Password Disclosure, and Server Path Disclosure.

We artificially created 60 information vulnerabilities in enterprise information systems, including 10 vulnerabilities for each type. The results show that all of these vulnerabilities have been successfully detected by the vulnerability governance platform.

5. Conclusion
The governance of information security vulnerabilities is an important guarantee for corporate information security. The vulnerability governance platform automatically updates vulnerability information from the subscribed vulnerability information website which realizes the early detection and disposal of high-risk vulnerabilities in enterprise information systems, improves the efficiency of vulnerability management and the security of enterprise assets.

Acknowledgments
This work was financially supported by GDKJXM20162130(037800KK52160003).

References
[1] Makino Y, Klyuev V. Evaluation of web vulnerability scanners[C]// IEEE, International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. IEEE, 2015:399-402.
[2] Antunes N, Vieira M. Benchmarking Vulnerability Detection Tools for Web Services[C]// IEEE International Conference on Web Services. IEEE, 2010:203-210.
[3] Vieira M, Antunes N, Madeira H. Using web security scanners to detect vulnerabilities in web services[C]// Ieee/ifip International Conference on Dependable Systems & Networks. IEEE, 2009:566-571.
[4] Dao T B, Shibayama E, Security Sensitive Data Flow Coverage Criterion for Automatic Security Testing of Web Applications[C]// International Conference on Engineering Secure Software and Systems. Springer-Verlag, 2011:101-113.
[5] Parimala G, Sangeeth a M, Andalpriyadharsini R, Efficient Web Vulnerability Detection Tool for Sleeping Giant-Cross Site Request Forgery[C]// National Conference on Mathematical Techniques and its Applications, 2018.
[6] Lukanta R, Asnar Y, Kistijantoro A I, A vulnerability scanning tool for session management vulnerabilities[C]// International Conference on Data and Software Engineering. IEEE, 2014:1-6.
[7] Pelizzi R., Sekar R. A server and browser-transparent CSRF defense for web 2.0 applications[C]// Proceedings of the 27th Annual Computer Security Applications Conference, New York, 2011, pp. 257-266.
[8] You J, Guo F. Improved CSRFGuard for CSRF attacks defense on Java EE platform[C]// International Conference on Computer Science & Education. IEEE, 2014:1115-1120.
[9] Gui-Ping L I, Xian Fanyi, Design of security vulnerability detection platform based on Wi-Fi[J]. Information Technology, 2016.
[10] So I G, Setiadi N J, Papak B, et al. Action Design of Information Systems Security Governance for Bank Using COBIT 4.1 and Control Standard of ISO 27001[J]. Advanced Materials Research, 2014, 905:663-668.
[11] Sun Y, Liang D Y, Wang W J, Enhancement of Test Platform for Web Application Security[J]. Applied Mechanics & Materials, 2014, 511-512(5):1205-1210.