Research on web security test based on kali Linux

Qiuyang Zhu, Na Li
Anhui University of Science and Technology, Chuzhou 233100, Anhui Province

Abstract: web security is mainly divided into server security and client security, in B/S architecture occupies half of the Internet service today, the security level of the web level determines the user and enterprise information security protection level. The purpose of penetration testing is to help enterprises and companies find possible vulnerabilities, and carry out threat analysis of vulnerabilities, and provide vulnerabilities recurrence and repair suggestions. kali Linux, which redevelops BackTrack based on the Debian development standard, is a specialized penetration testing and security audit platform pre-installed with a wealth of penetration testing tools. Using kali Linux during penetration testing will greatly reduce the time and cost of testing, and the use of tools and scripts will make the penetration testing work more effective and effective. In this paper, the author will develop a simulation of the penetration test of simulated network services which based on kali Linux security tools and python scripts, and make principle analysis and repair suggestions on the existing vulnerabilities.

Key words: kali Linux; Penetration test; python; Scripts

Introduction With the vigorous development of Internet technology and economy, while the country and people enjoy the timeliness and convenience brought by network services, the promulgation of the cybersecurity Law of the People's Republic of China in 2017 has opened the curtain of the construction of national cybersecurity, and is also the most powerful backing for combating malicious attacks and criminal acts on the Internet. The effective means to ensure personal and enterprise information security and asset security is the network space security technology. In network security research, attackers often only need to seize the weak point of network services to detect and attack, while defenders need to monitor and reinforce the entire network services. The main significance of penetration testing is to find out the weak points that may be found by the attackers before the attack, analyze the causes of malicious attacks, cooperate with developers to strengthen network services, and protect the enterprise network.

At present, China's network security market exceeds supply, and the lack of talents leads to great potential and development space in the field of network security research. Penetration testing is to detect the dangerous behavior of the enterprise network, and to prepare for the malicious intrusion behavior of the network. To discover network security problems in advance and kill network security intrusion behaviors in the cradle, this is the main significance of penetration testing in the actual production environment.

1. The technical principle of network architecture analysis

1.1 Concept of wed application

In fact, web is a service application born with the development of the Internet. Its basic working principle is to integrate the Internet information resources scattered all over the world through the use of hypertext transmission technology, so that users can browse the application service technology quickly and easily through the browser. Web application is a holistic concept, it contains a variety of information resources: text, pictures, multimedia, databases and applications, these resources in the web can be linked to each other through the hypertext transmission protocol, to bring intuitive feelings and experience to users.

The Web application is logically connected through the globalization of information, so as to form a global information network on the Internet. The Internet and web application complement each other, but they are two completely different concepts. Web application is a kind of application service of Internet, and Internet is the basic platform for web application to be realized. Dividing the web business process into three layers is more helpful to understand and study, that is, "front-end layer + business logic layer + database layer", which is the three-layer architecture of the web program.

1.2 B/S architecture security analysis

The rapid development of Web applications benefits from the development and implementation of B/S architecture. With the maturity of Web applications, more and more enterprises, schools and governments are willing to use web applications as office and management platforms. The fact also proves that the web application in daily life and work has shown an irresistible convenience and timeliness. B/S architecture is different from C/S architecture, which works on the local area network. B/S architecture is a network service architecture established on the basis of wide area network. The wide area network makes the B/S architecture pay more attention to the user experience. Users usually only need to install the browser on the client, and they can make the browser show the intuitive page display through a few simple clicks. B/S architecture is a kind of web application in which a large amount of database information is exchanged between the browser and the server in the form of network, and the data information is visually presented in the browser in the form of css and html.

It is undeniable that although the B/S architecture has brought great convenience to daily life and work, the drawbacks of the B/S architecture itself have always brought troubles to the network information security of website applications. The main reason for these problems is that the website development technicians do not pay attention to the awareness of network security and the lack of their own hard power technology.

1.3 Website intrusion behavior way

The main reason for the website intrusion behavior is that there are vulnerabilities in the website or system, such as server

vulnerabilities, middleware vulnerabilities led by apache and tomcat, and application service vulnerabilities including database, web and other application services. This article focuses on the web vulnerability attack website intrusion behavior, first of all readers need to be clear that the Internet does not exist absolute security, security is a relative sense of security. A web developer with weak security awareness is far more likely to develop code with vulnerabilities than a development technician who knows network security. web applications need to be launched after the completion of development, and the acceptance environment of the system may change after the system is launched, causing some problems in the code that is not at all wrong. In addition, errors caused by service configuration, website administrator password leakage and other reasons will cause web security problems.

There are three major risk points in Web applications, and website intrusion is often based on these three risk directions. The three risk points of the Web server are as follows: First, C-segment penetration: attackers try to lurk or directly enter the same network segment and scan and penetrate the PC side of the network segment, so as to achieve the purpose of attack; Services, attackers through the discovery and matching of application service vulnerabilities, the use of existing or existing related vulnerabilities to complete the attack hypothesis, such as web vulnerabilities, FTP service vulnerabilities, etc.; Third, social engineering: through the use of the network environment for personal social communication and other aspects of information collection and use, to achieve the purpose of manipulating other people's information.

2. Analysis and simulation of vulnerability principle

SQL injection vulnerability is a high-risk vulnerability at the web level. The SQL injection vulnerability mainly exists in the dynamic input field of the website page: login field, registration field, password recovery field and search field. At present, with the change of the language framework of web application development and design and the development of the code audit industry, SQL injection vulnerabilities have been reduced, and the SQL injection vulnerabilities existing in the web level have become relatively difficult to detect and exploit. However, this does not affect the value of continuing to learn and study SQL injection vulnerabilities, nor can it rule out the possibility of the existence of SQL injection vulnerabilities at the web level.

2.1 Principle of SQL injection

The word "SQL" in SQL injection refers to the SQL database. SQL injection statements vary depending on the database. This paper mainly explains the SQL injection vulnerability based on MySQL database. SQL injection can be detected in many places.

SQL injection vulnerabilities can be subdivided into many types, but there are two main directions: data type and request type. First, according to the injection data type classification can be divided into: character injection, numeric injection. The second is classified according to the type of sending request: GET injection, POST injection and Cookie injection

Numeric injection vulnerabilities often appear at the level of weakly typed language code. If the web application uses a weakly typed language, then when the input parameter is id=1 after the SQL statement, the weakly typed language such as PHP will automatically determine that the parameter id is of type int; If the input parameter is id=1 and 1=1 after the input SQL statement, it will automatically determine the type of string. However, when web developers use a strongly typed language such as Java, there will be a typecast error message in the syntax structure and compilation processing. When you try to convert a string type to an int type, the program throws an exception and cannot continue top-down execution. This step occurs before the SQL statement is queried, so the probability of numerical injection vulnerability is much lower in strongly typed languages than in weakly typed languages.

2.2 File upload vulnerability

File upload vulnerability refers to the security risks of the upload function of the website application and is maliciously exploited by attackers to upload malicious attack files such as Trojan horses.

File upload vulnerabilities can be divided into direct upload vulnerabilities, middleware resolution vulnerabilities and bypass upload vulnerabilities. The main reason for the direct upload vulnerability is that the upload function is not strict enough to filter the file type, resulting in the script file can be directly uploaded. The "middleware" in the term middleware vulnerability refers to server components such as IIS, Apache, and Nginx. In a real production environment, server components are more or less vulnerable. The way to exploit a historical vulnerability in a server component for attack purposes is called a middleware vulnerability. There are two ways to exploit the upload vulnerability, namely, bypassing client-side detection and bypassing server-side detection. The realization of client and server side bypass requires familiar with the basic underlying architecture knowledge of these two levels to achieve the exact effect.

2.3 XSS cross-site scripting attack

XSS cross-site scripting attack refers to the problem that web applications output data to web pages, resulting in hackers to modify web pages based on the injection of web front-end, and insert JavaScript and HTML malicious code into the original page. Once the user accesses the web page through the browser, the malicious script implanted in the web page will be executed, so as to achieve the purpose of attack.

Generally speaking, XSS scripting vulnerability aims at stealing user Cookie values, stealing user accounts, and using user identities to publish false information. The victims of XSS scripting attacks involve two aspects: the attacked web browser and the website that has been inserted with malicious scripts. Due to the vulnerability of XSS attack in the attacked website, once an unwitting user enters the website and clicks on web page applications with malicious scripts, such as links and pictures, a vicious cycle of malicious attacks is likely to be formed.

2.4 Kali Linux penetration test

Kali Linux comes packaged with a list of out-of-the-box security tools such as SQLMap, Joomscan, Jhon, etc. Each tool targets different web security vulnerability scenarios. And the existence of every vulnerability in web security is very likely to be used as a

springboard for malicious attacks by criminals, thereby destroying network services and making profits from it. This experiment mainly takes a SQL injection vulnerability as an example to show how to use kali Linux to carry out penetration test research. At the same time, it reproduces and demonstrates the harmfulness and destructiveness of web security. Its simulation test ideas are mainly as follows:

(1) Build a network service target machine as the penetration test object of this subject

(2) Analyze the common vulnerability principle of penetration testing

(3) Systematic penetration testing of target aircraft based on kali Linux and python scripts

(4) Make reasonable repair suggestions for the penetration test results

(5) Provide reasonable and professional network information security defense measures

3. Security operation analysis

Enterprises tend to pay more attention to the security construction of the back end of the web (that is, the security of the server side), and ignore the possibility of large-scale attacks on the front end of the web. Attacks on the front end of Web 2.0 websites can allow hackers to obtain or destroy a variety of private data, which is still a more severe and difficult security problem at present.

Network attack and defense, there is an attack to be protected. It is the so-called “know yourself and know your enemy, only in a hundred battles”, understand the causes of vulnerabilities, and analyze from the principle level in order to have a more purposeful and organized targeted defense. Network attack is a stitch in the stitch type of attack, and security defense is a Great Wall like construction grade project. For enterprise security construction, physical isolation of the internal and external network, separation of business traffic from other traffic, separation of the front and back end of the web, security hardware equipment, security software deployment, are undoubtedly available means to enhance the security level of enterprises. And regular acceptance of the security assessment, network attack and defense drills, can also effectively and targeted to find network security defects, concretively to deal with such security problems.

References:

[1] Hui Tong,Xiaoguang Chen,Zuofeng Zhang. Basic course of Web Security [M]. Beijing: Beijing Normal University Press, 2017.10-16

[2] Tao Wu,Jiaming Fang,Rongde Wu,Yan Xu. Python Security Attack and Defense Penetration Test Practical Guide [M]. Beijing: China Machine Press, 2021.54-254

[3] Xiaoguang Chen,Bing Hu,Zuofeng Zhang. Web Business Security Practical Guide [M]. Beijing: Publishing House of Electronics Industry, 2018.11-12

[4] Stuart Mcclure, Joel Scambray, George Kurtz. Hackers expose Network security secrets and solutions [M]. Beijing: Tsinghua University Press, 2013.523-659

[5] ShaoFei Zhao,Fan Yang, Tian Guo-min. SQL Injection analysis based on website system [J]. Network Security Technology and Application, 2019 (11) : 28-29. (in Chinese

[6] Chuan Guo. Research on Penetration Test Platform based on Kali Linux [D]. Inner Mongolia Autonomous Region: Inner Mongolia University of Science and Technology, Master Dissertation, 2019

[7] Christian Armbruster. Hacker, Philipp, Datenprivatrecht[J]. Zeitschrift fur die gesamte Versicherungswis. 2021. PP 1-5

[8] Kirti Sharma; Shobha Bhatt. SQL injection attacks - a systematic review[J]. International Journal of Information and computer Security.2019(11):4-5

Anhui Province Higher Education Institutions Blockchain Technology Innovation Application Program 2020qkl12□Key R&D project of Anhui Province 202104f06020019