Research on Security Technology based on WEB Application

Fanxing Kong
[1] *Linyi University, Shandong China, 276000*

Keywords: WEB Application; Security Technology; Research.

Abstract: This article described the relevant technologies of web security, thoroughly analyzed the application security of Web in three aspects of security threats of Web client, security threats of Web server, security threats of data transmission, and accordingly studied the security technology based on WEB application. Hope the elaboration of this article could provide some reference to the relevant personnel in the field.

1 INTRODUCTION

With the advent of the information era, WEB application has entered into people's life and work, and the application programs based on WEB have been fully used in various fields, including Internet management, control of facilities, etc (Xiaojie X,2015).

For the current Internet, any information and data needs the WEB service. Now, WEB has been widely used, and the programs and data based on WEB application are the targets mostly attacked by network hackers. According to the relevant reports, the Internet data vulnerabilities are all the key ways of secure dissemination. Browser and WEB applications began to be hacked, in which, 75% of the Internet threats are related to WEB applications. These security risks have brought serious losses to the relevant areas. Then, the paper will further analyze and discuss the security technologies based on WEB application comprehensively (Ziqian W,2015).

2 RELATED TECHNOLOGIES OF WEB SECURITY

2.1 Authentication technology

The so-called authentication technology mainly refers the process that divide it into two subjects, and one of the subjects clear confirms the other. When one user's identity is taken as a subject, it requires to use authentication technology to verify its identity, if successful, it can continue to access, otherwise, it cannot (Dongjiao Z,2016).

2.2 Authorization technology

After authentication, if the subject has the right of follow-up access, the access rights involved, we can call it authorization. Authorization mainly contains two aspects, the first is the control information of resource access; the second is the information of subject.

2.3 Security and privacy technology

This technique is mainly hidden in the user information without authorization application, which mainly uses encryption technology, after encryption, users can transfer data, but other users can not view the transmitted information, even by the network protocol analyzer (Juan D,2014).

3 SECURITY ANALYSIS OF WEB APPLICATION

Web application mainly consists of two parts, the first is the client; the second is the server. It mainly draws support from the TCP/IP protocol layer to achieve data transmission and processing. The most widely used client program is the Web browser. The Web server has access to Web resources. Web resources mainly involve five aspects, the static text file, document of hypertext markup language, media file, client code and dynamic script. The mode of Web application is shown in figure 1 (Yi S,2014):

367

Kong F.
Research on Security Technology based on WEB Application.
DOI: 10.5220/0006450603670370
In *ISME 2016 - Information Science and Management Engineering IV (ISME 2016)*, pages 367-370
ISBN: 978-989-758-208-0

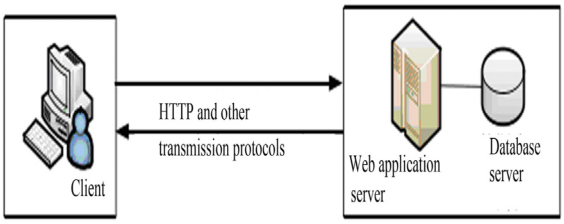

Figure 1: Mode of Web application

3.1 Security threat analysis of Web client

3.1.1 Security threats of browser

Browser usually refers to the program of client host, which is used to meet the needs of the Web server, while display and process the data and information given by Web server. The browser only needs to provide the display function for HTML static page before, but with the rapid development of scripts and plug-in technology, scripts and plug-in technology with ActiveX, FLASH model have been used comprehensively, which provides the conditions for the enhance of browser's performance, but followed by the gradually increasing security problems in the process of Web application. Browser is the key to the entire Internet, network hackers often use browser software to set the virus, attack the client, and which leads to Web client being threatened (Wang X,2008).

3.1.2 Cross-site scripting attacks

Usually, there are two kinds of XSS attack, one is persistent attack, and the other is a reflection attack. Persistent attack mainly refers that the attacker saves the virus in the database crossing with Web application program, when users access it, Web application will send the potential virus to the user. When the user executes the program, the relevant information of user will be sent to the attacker. Reflection attack mainly refers that the attackers do not save the virus in the server side, and reflect it directly to the user. They mainly use the malicious script sent by others, copy the virus into it, when the user links, it will steal user's information. This attack does not have persistence.

3.1.3 Clickjacking

Clickjacking mainly refers to a kind of visual deception, hackers mainly upload the transparent Web elements to a web page, when users link the web page, they don't they have clicked on the Web elements, and then information is operated or stolen. Network hackers mainly lure users to click the performance button of these Web elements without knowing the facts, and then achieve specific supply performance (Yubei Y,2015). For example, linkJacking attacks can not only hijack information, while after the implementation of a series of tedious actions, network hackers can eventually control the camera.

3.2 Security threat analysis of Web server side

Once the server side has security threats, it will lead to the security threats of Web applications, Web servers, as well as the database. Once the complicacy of Web applications gradually increases, the security awareness of Web programmers and the corresponding management personnel gradually reduces, and which will provide the conditions for the attacker's attack. In normal circumstances, the security threats of Web server side are mainly two aspects (Chuan L,2010).

(1) The security threats of server side's data and file, such as the leakage of bank accounts and credit card information, etc. Assuming that the intruders have obtained this information, they can cheat by the way of role playing, and then obtain the corresponding economic benefits.

(2) Web applications of server side are also affected by the preservation of malicious code, thereby attacked by the Trojan horse of Webpage. The Web threats we often encounter include SQL injection attacks, attacks of remote code execution, and so on (Chengyu H,2011).

3.3 Security threat analysis of data transmission

In the process of user side data transfer or server side data transfer, once there is improper operation, there is a security threat. The main attacks we often encounter are two kinds, one is the active attack, and the other is a passive attack. Active attack mainly refers to the data attack in the network. This attack mainly uses user side or server to revise user information, and then achieves the effect of attack. Passive attack mainly refers to reading data in the network, this kind of attacks mostly read the important information in the network, such as user names, user passwords and users' personal information, etc (Yongxiang W,2014)

Research on Security Technology based on WEB Application

4 SECURITY TECHNOLOGY OF WEB APPLICATION DATA

4.1 Security technology of client

For the security threats of browser and the host operating system, in order to enhance the security of the host operating system and browser, browser version and real time patch update of operating system should be well done in the link of security, and the vulnerabilities of browser and operating system should be timely repaired. For the security threat of Web client's script, Web client's ability of fighting against attacks should be strengthened, install detection system in the Web client script, and detect regularly. In general, there are two kinds of detection technologies for malicious web page, the first is static detection; the second is dynamic detection. Static detection detects malicious code on the webpage by code analysis. Compared to static detection, dynamic detection has relative low efficiency, but strong pertinence, which can effectively identify the malicious code in the page. If the malicious code is encrypted or changed, dynamic detection can read the relevant information in malicious code, analyze characteristics of the behavior, and then achieve the purpose of protection. Therefore, dynamic detection has good accuracy.

4.2 Security protection method of server

4.2.1 AJAX protection mechanism

Comparing the AJAX protection mechanism and original security system of Web application, there are certain similarities in nature, which contains the data query by interacting with data, response ability of data transfer, capability of data transmission and information call, etc.

4.2.2 Input validation

In order to prevent the phenomenon of only the user side is verified, all of the information of clients and servers should be verified, such as the verification of HTTP header, cookie verification, parameter verification, data validation, and the verification of length, specification of user data.

4.2.3 Security of client's program code

The protection mechanism mainly involves four aspects, first, the application system mechanism of user end; second, mechanism of third party's external program; third, the data call mechanism; fourth, the protection mechanism of data processing.

4.2.4 SOAP filtering and WSDL strengthening mechanism

Typically, before the filtering of firewall or HTTP layer, it is unable to defend the attack of Web services, and needs to play the effect of resistance in the filter and supervision of SOAP layer. While as one of key sources, information of WSDL date could not be leaked, its enforcement mechanism mainly includes two aspects, the first is in the process of program design, it needs to provide the corresponding function; second, it is only used in SSL.

4.2.5 Authentication, authorization and development mechanism of security program

The protection mechanism involves five aspects, first, R &D staff of the system carry out WSDL access control; second, apply security assertion markup language; third, WS-Security certificate; fourth, SOAP filtration; fifth, data transfer.

4.3 Security technology of data transmission

4.3.1 HTTPS protocol

HTTPS mainly refers to running HTTP based on SSL, the structure after fusion is called HTTPS, when building a TCP in HTTP, link to it, when the user side presents a demand server will give corresponding reply. In the process of applying SSL, the user side must build a TCP, link to it, build a SSL channel on it, send the same requirement in the SSL channel, and the server side will make corresponding response to the SSL channel. In terms of the traditional HTTP server, the information SSL accepts is equivalent to spam, because that not all of the servers can apply SSL. Therefore, in order to ensure the quality of the data, it needs to select the appropriate application channels in the application process. It needs to use the Web address starting with HTTPS to achieve the application of SSL.

4.3.2 SRTP protocol

SRTP protocol mainly researches and develops the safety performance of the two contents, the first is the voice stream; the second is the video stream, SRTP gives the encryption modes and cognitive methods corresponding to AES. So the main function of SRTP protocol is security and real time. SRTP can be used in

369

TCP/UDP, but people often use it in UDP, for the transmission of voice and video is mainly based on UDP.

Protection of data authentication and integrity: in general, the authentication algorithm used by RTP is MAC-SHA1. After the calculation results are sent to the data packet, the receiving side will choose a reasonable label value of M according to the calculation results, and compare it with the label value received (Hung-Bin C,2015).

4.3.3 RTMPS protocol

RTMPS protocol is also called security protocol, it is the protocol got after the SSL encryption. The protocol can support data transfer. The main function of secure sockets layer is to provide a security protocol with data integrity for network communication. SSL mainly uses the transmission layer to achieve the encryption of the network link. The default port is 443.

5 CONCLUDING REMARKS

All in all, with the rapid development of Internet technology, the application programs based on Web have steadily developed, and become an important standard of the current computing platform. With the appearance of Web mail, shopping and media, Web applications has entered our work, life and learning, become an indispensable part of our daily life, and played a key role in network information service. Because of the rapid development of Web technology, applications related to Web have become cumbersome, which also makes the security vulnerabilities gradually emerge. In order to ensure the safety of Internet applications, it is necessary to conduct a comprehensive security analysis of the Web application, and develop an efficient and reliable method to prevent attacks, so as to ensure the security of programs and data.

REFERENCE

Xiaojie X, Yang X, Shuo J., *Research and Design of Web Application Firewall Based on Feature Matching*. Netinfo security, (11)53-59,2015

Ziqian W, Bo W., *Research on technology taking use of vulnerability of information security in Web application system.* Electronic Product Reliability and Environmental Testing, (6):30-33, 2015

Dongjiao Z, Ping W., *Analysis on the security technology of Java Web application program*. Computer fan, (3):48-49,2016

Juan D, Yang X, Yuwei M., *Research and design of audit system of security log based on Web application*. Netinfo security, (10):70-76,2014

Yi S, Dongyun L, Wenjie W., *Research on the key technology of security testing platform of Web application program*. Information Security and Technology, (1):29-32, 2014,

Wang X.,*Desing of Secure Identity Authentication System Based on JAAS in the Web Application System*. Journal of Beijing University of Civl Engineering and Architecture, 24(2):55-59,2008

Yubei Y., *Application security of PGP encryption technology based on WEB in mail system*, Network Security Technology & Application,(6):38-40,2015

Chuan L., *Research on Application of Web J2EE system identity authentication security mechanism based on Unix authentication*. Journal of Chongqing University of Arts and Sciences,(4):65-67,2010

Chengyu H. *Research on the protection method of Web Java application software,* Software Guide,(11):57-58,2011

Yongxiang W, *On WEB website security optimization*. Network Security Technology & Application,(5):136-1137,2014

Linhai Y, Binying H., *Research on the content of Web code security artificial audit*, Jiangxi Science,(4):536-538,2014

Hung-Bin C, Izhak Rubin,Ofer Hadar., *Scalable Video Multicast for Multi-Cell Cellular Wireless Networks*. Journal of Communications, 10(9):715-727, 2015