ISSN 2635-8875
산업융합연구 제16권 제4호 pp. 47-52, 2018 https://doi.org/10.22678/JIC.2018.16.4.047

Study on defense countermeasures against Webshell attacks of the Industrial Information System

Sunghyuck Hong*
Professor, Div. Information & Communication, Baekseok University

산업정보시스템의 웹쉘공격에 대한 방어 대응책 연구

홍성혁*
백석대학교 정보통신학부 교수

요 약 WebShell is a web script file created by a hacker to remotely commands to a web server. The hacker can bypass the security system using the web shell, access the system, control the system such as file modification, copying and deletion, install malicious code in the web source code, attack the user's PC, And so on. There are many types of WebShell attack, but we study about attacks on PHP and JSP based web server which are used as representative ones. And we propose the method of web page management, method of development, and several other methods. By using these countermeasures, it is possible to effectively prevent damage caused by WebShell attacks.

Key Words : WebShell, Web Security, Information Protection, Hacking, Web Server

Abstract 웹쉘은 해커가 원격으로 웹 서버에 명령을 내릴 수 있도록 작성한 웹 스크립트 파일이다. 해커는 웹쉘을 이용하여 보안 시스템을 우회, 시스템에 접근하여 파일 수정, 복사, 삭제 등의 시스템 제어를 할 수 있고 웹 소스코드에 악성코드를 설치해 사용자들의 PC를 공격하거나 연결된 데이터베이스의 정보를 유출하는 등 큰 피해를 입힐 수 있다. 웹쉘 공격의 유형은 여러 가지가 있지만 그중 대표적으로 사용되는 PHP, JSP 기반 웹 서버에 대한 공격에 대해 연구하고 이런 유형의 웹쉘 공격에 대한 대응 방법인 웹페이지 관리차원에서의 방법과 개발과정에서의 방법, 그 외 몇 가지 방법을 제안하였다. 이런 대응 방법들을 활용한다면 웹쉘 공격에 의한 피해를 효과적으로 차단할 수 있다.

키워드 : 웹쉘, 웹보안, 정보보호, 해킹, 웹서버

1. Introduction

Hacking, which is an act of unauthorized intrusion into the system to extract information or destroy programs, has evolved over time. In the first generation attack technique, the internal attack which is an attack which breaks down the vulnerability of the OS itself is mainly performed, and in the second generation, the external attack which is an attack which is the attack of the daemon vulnerability is mainly performed. At the same time, the third generation of hacking

*Corresponding Author : Sunghyuck Hong (sunghyuck.hong@gmail.com)

Received December 3, 2018 Revised December 13, 2018
Accepted December 14, 2018 Published December 31, 2018

techniques exploited vulnerabilities in the TCP / IP protocol, and various attacks were launched[1].

According to the Korea Internet Development Agency, "homepage tampering", which is a type of web attack method that continuously increases with various attack techniques, is becoming a main type following simple intrusion attempts by worms and hackers[2]. A hacker who successfully exploited this method deletes the traces and symptoms of intrusions, causing the server administrator to ignore the infringement and leave it untouched, causing malicious code to be planted on a large number of user computers connected to the Web server and causing abnormal symptoms such as information leakage .

Although a hierarchical web security system is presented as a countermeasure against this problem, another attack technique that bypasses this security system has been developed and it has been difficult to solve this problem with existing web security systems and detection and blocking techniques.

In this paper, we discuss the WebShell technology and various variant patterns in Chapter 2, and analyze the results of Chapters 3 and 4 to study the defense countermeasures against WebShell. Finish it.

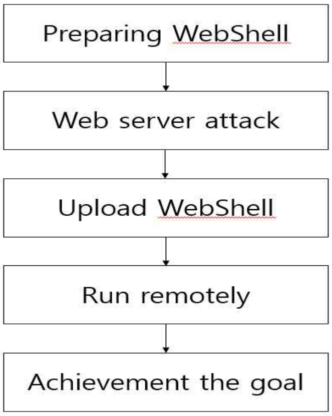
2. Related studies

2.1 WebShell

WebShell is a web script file created by a hacker to remotely execute commands on a web server. WebShell can be created in a variety of ways, but it is widely used to create simple server scripts such as jsp, php, and asp. These scripts are uploaded to the web server via a vulnerability in the web server, which in turn allows the hacker to execute arbitrary commands in the web server environment.

Once WebShell is installed, a hacker can easily bypass the security system and access the victim system without going through a separate authentication process. If you execute arbitrary command on the connected system, you can see that it is difficult to protect. In addition, system control such as file modification, deletion, and copying of the damaged system can be performed, malicious script is inserted into the web source code, attacked the PC of users connected to the web server, It is a tool that can be applied.

The damage caused by WebShell is so large that the web server where WebShell is found has a distribution of 91% among the hacked web servers that are damaged. It is difficult to detect. Because of this feature, WebShell is widely used for web server hacking[3].



[Fig. 1] WebShell attack process

2.2 WebShell attack techniques

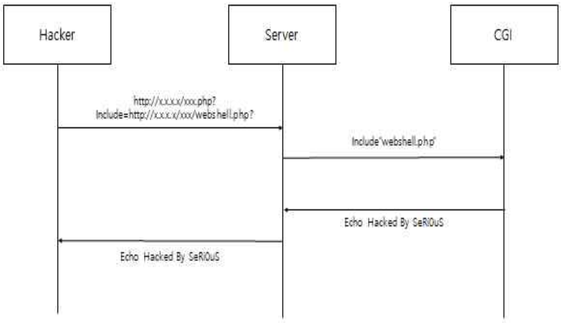
In addition to the explosive increase in Web-based services, hacking attacks, which were aimed at exploiting vulnerabilities in previous operating systems and application programs, have recently undergone a sudden change in system data hacking and hacking incidents through WebShell, A program running on the Web is called a CGI (Common Gateway Interface), which is a bulletin board or a shopping mall. WebShell mostly attacks such CGI[4].

WebShell attack technique analysis will examine WebShell attacks on Web sites based on PHP and JSP based websites.

2.2.1 PHP based WebShell attacks

In a PHP-based web site, a user's input is handled by referring to a file on another web server rather than being processed by a single server. This is called RFI (Remote File Include). This happens because of the lack of filtering on external reference parameters, which allows hackers to modify existing URLs to arbitrary URLs and run them on servers vulnerable to webshells.

The process of attacking the vulnerability of RFI, which is a method of processing data by referring to the file of the web server, is as follows. The hacker sends the modulated parameter value to the server, and the attacked web server recognizes the modulated value received from the hacker as the external file reference parameter in the CGI application, executes the web shell on the server, and returns it to the hacker.

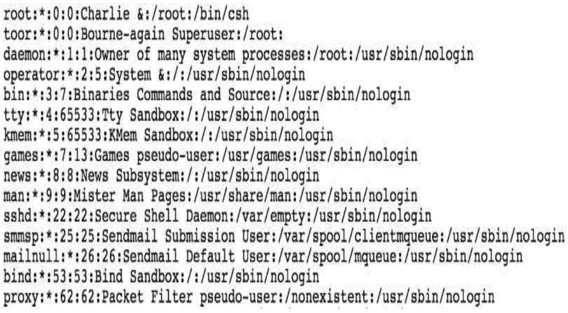


[Fig. 2] Flow of PHP Data

2.2.2 WebShell attacks based on JSP

JSP (JavaServerPages) is a Java-based scripting language that has the advantage of being more stable and easier to maintain than PHP.

In order to acquire the privileges of the server remotely, the jsp file based on the JSP is first uploaded from the administrator page of the bulletin board by the jsp file written in the CGI language to infer the path of the uploaded file, and then the uploaded file It attempts to access the path of. A vulnerability in file uploading occurs because the web server does not trust the user's file and does not filter on the validation and extension. In addition to uploading files, there are various attack methods such as Web shell access and execution, backdoor installation, elevation of privilege, and command transmission. If the attack is successful and the file path is successfully accessed and the web shell is executed, the hacker uses the executed web shell to send the command to the attack target server. The hacker can check the directory list of the target server and the target server which receives the command "cat / etc / passwd" from the hacker executes the command to send information of all accounts to the hacker[5].



```
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/usr/sbin/nologin
news:*:8:8:News Subsystem:/:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
```

[Fig. 3] Execution of cat/etc/passwd using the webshell

2.3 Causes of WebShell

The feature of the server that a Web shell attack occurs is the use of the file upload function. If a file is allowed to be uploaded, it is possible to upload a file existing on the client to the server, and a hacker generally tries to upload a webshell file using a bulletin board such as a file library where such a file can be uploaded.

2.4 Types of WebShell

WebShell can classify types according to file type or file type. As a typical classification method, it is possible to classify WebShell as a single file or add only an attack phrase that uses an existing file as WebShell. Web shell files are usually uploaded to the server through file uploads or vulnerabilities, so they are mostly used as single files. However, there are also cases where attack syntax used in WebShell is inserted into basic source code due to hacking etc. When used as a single file, it is divided into Text format and Image format. Text-based Webshell file consists of single-line WebShell composed of a single command, multiple webshell composed of multiple commands, and Multi Division Webshell. Image base can be categorized by adding attack syntax at the end of image file and adding attack syntax to image file attribute[6].

〈Table 1〉 OWASP TOP 10 Web Application Security Risks[7]

OWASP Top 10
A1:Injection
A2:Broken Authentication
A3:Sensitive Data Exposure
A4:XML External Entities (XXE)
A5:Broken Access Control
A6:Security Misconfiguration
A7:Cross-Site Scripting (XSS)
A8:Insecure Deserialization
A9:Using Components with Known Vulnerabilities
A10:Insufficient Logging&monitoring

3. Action Plan

The above-mentioned related research is based on the assumption that the web shell is uploaded and executed through a bulletin board where a vulnerability that is not set in the access restriction is not sufficiently verified in the file uploading process of the bulletin board, Respectively. Especially in recent years, a large number of website tampering accidents involving web hosting service providers have occurred, and it is known that the homepage tampering is rapidly increasing among cyber infringement accidents[8]. If so, what are some of the ways you can respond to WebShell attacks based on JSP or PHP?

The first is through HTTP outbound traffic monitoring. Web attacks such as WebShell, XSS, and Injection cause outbreak of malicious code with outbound traffic, leakage of information due to web shell, leakage of personal information, and XSS [9]. HTTP outbound traffic monitoring is a technique to detect whether or not a web attack is detected by detecting such anomaly. It can detect the intrusion by comparing the abnormal HTML tags and the code included in the HTTP traffic flowing from the server which is infringed by the web attack with the actual traffic.

Secondly, there is a way to block from the bulletin board which has the archive function which is used as the most path of the web shell attack. If the file upload function of the website is used to upload files with the extension .php, .html, the hacker can upload the web shell and obtain the authority of the web server. Therefore, when a web developer implements a bulletin board function capable of uploading a file, he or she should filter the files that can execute the web script language from being uploaded. It is better to implement the filtering method by blocking the extension of asp, php, jsp, etc., and checking it to upload only file extensions such as txt, hwp, doc, gif. This is because there are ways to bypass files when uploading files with specific extensions. If it is a bulletin board that does not require file uploading, it is recommended to remove the function of uploading.

Third, there is a way to detect the WebShell. WebShell can detect WebShell using the latest version of Kaspersky Anti-Virus or V3 vaccine when using Windows Server. However, in the case of Linux, it can be difficult to check the encrypted web shells of the source code. In this case, the whistle (Web Hacking Inspection Security Tool) provided by Korea Information Security Agency can easily detect it. There is also a way to detect WebShell programs in the actual victim system by using a specific string in the file.

Fourth is the use of Static Analysis Tools. This method is not a way to block the WebShell attack itself, but rather to detect Web servers that may be vulnerable to WebShell attacks, or to monitor Web pages modified periodically or in real time by webshell attacks, It is a way to block.

The fifth is SQL Injection attack prevention. WebShell attacks can be triggered not only by file upload vulnerability but also through SQL Injection. Therefore, special characters ('", - (space)) related to DB query are filtered to cause an error if the user's input value contains special characters. To prevent it from running. In all cases where you take user input, such as entering a user's login page or number of posts, and insert the variable into a DB query statement, you should apply this filter and be careful not to introduce SQL injection loopholes in even a single page. SQL Injection attacks are often done with reference to error messages, so you can prevent some error messages from being displayed.

4. Conclusion

Web-shell attack is mainly started from the vulnerability of Web-page bulletin file upload function. Even if attacked, it is difficult to detect and it causes great damage. The most common reason for the vulnerability in file upload is that there is a problem with RFI, which is a way of referring to other web server files without processing user input in one server in PHP based web server. The hacker modifies the existing URL to an arbitrary URL, sends the modulated value, and causes the server to execute the web shell. There are various WebShell attacks such as SQL Injection attack.

To protect the server from these attacks, the web server administrator uses an analysis tool to check for vulnerabilities on his server, and the developer puts a filtering feature so that when developing it can not upload a file that can run the web scripting language[10,11]. If the bulletin board does not require uploading, the file upload function itself should be deleted to enhance security so that the web shell attack does not cause damage.

REFERENCES

[1] M. S. Kim, J. B. Kim, H. C. Yang, Y. M. Kim & J. H Seo (2007). Web 2.0 and Ajax Security Vulnerabilities, *Communications of The Korea Information Science Society, 25(10),* 43-48

[2] KISA, (2010) “Korea Internet Incident Report of April 2010” Seoul : KISA.

[3] K. M. Kwon (2017.06.02) Web hacking begins with WebShell, dailysecu, https://www.dailysecu.com/

[4] J. G. Kim & S. C No (2012.03). A Study of Step-by-step Countermeasures Model through Analysis of SQL Injection Attacks Code. *Journal of Information and Security,* 12(1), 17-25.

[5] S. S. Shin, J. I. Kim & J. Y. Lee (2015.08). A Study on Secure Digital Convergence Curation System to WebShell. *Journal of the Korea Convergence Society,* 6(4) 187-195.

[6] IglooSecurity (2017.02.01.) “WebShell classification and countermeasures" https://www.igloosec.co.kr/

[7] OWASP (2017) “OWASP Top 10”

https://www.owasp.org/

[8] K. J. Shin & S. J. Lee (2007.12). Research about the Identification and Gathering of Digital Forensic Evidence by Cyber Intrusion Accident Types. *Journal of Information and Security,* 7(4),93-105.

[9] B. H. Choi, S. K. Choi & K. S. Cho (2011.1). An Efficient Detecting Scheme of Web-based Attacks through Monitoring HTTP Outbound Traffics. *Journal of the Korea Society of Computer and Information,* 16(1), 125-132.

[10] Information Protection News Coverage Team (2008.11). "Web server security whistle" Information Security News, 132(12) 14-18..

[11] Sunghyuck Hong. (2018). A Study on the Countermeasures against APT Attacks in Industrial Management Environment. *Journal of Industrial Convergence*, 16(2), 25-31.

Sunghyuck Hong [정회원]

- Aug, 2007: Texas Tech University, Computer Science (Ph.D)
- Sept, 2007~ Feb, 2012: Senior Programmer, Texas Tech University, Office of International Affairs
- March, 2012 ~ Present : Associate Professor at Baekseok University

- Research Interests: Network Security, Hacking, Anti-fishing technology
- E-Mail : sunghyuck.hong@gmail.com