http://dx.doi.org/10.14400/JDC.2014.12.10.259

Vulnerability of Directory List and Countermeasures

Sunghyuck Hong

Division of Information and Communication, Baekseok University

디렉토리 리스팅 취약점 및 대응책

홍성혁

백석대학교 정보통신학부

Abstract The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. The directory list have some serious vulnerability to show internal files and directory to outsider attackers. Therefore, the proposed countermeasure of directory list is presented to prevent unnecessary valuable information from outsider attackers.

Key Words : Directory listings, web server, IIS, Apache, vulnerabilities, and Google Search

요 약 본 논문은 디렉토리 리스팅이란 서버 시스템의 파일을 볼 수 있는 것으로 디렉토리 리스팅의 취약점을 갖고 있는 사이트를 찾는 방법과 보완하는 방법이 무엇이 있는지 알아본다. 검색 사이트인 구글을 이용하여 디렉토리 리스팅 취약점이 있는 사이트를 찾는 법, 구글 검색에 내가 운영하는 사이트가 검색되지 않는 방법과 웹 서버의 운영자가 할 수 있는 취약점 제거 방법을 제시한다.

주제어 : 디렉토리 리스팅, 웹서버, IIS, 아파치, 취약점, 구글 검색

1. Introduction

If the URL that you entered when a user enters a URL in the Web browser is enabled, when you want to display a Web page normal, additional settings are not a Web server, to show a list of files in a directory on the server I will be. At this time, when it is not in a regular page by the web publisher want to show to the user, indicating the contents of the directory, if the user requires the publisher to be able to view the data on the server When you are ready to browse and users' personal information and other important files, users who use the site, there would be no hackers but to try to exploit the information that has been published. A directory listing, you can browse a list of files in system user accidentally, but if a hacker with a malicious purpose, by using, for example, automated tools and search site, of the vulnerable site This is what you find, set the target of the attack the site. Examine how to find a website with the help of search

* This research is supported by 2014 Baekseok University research fund.
Received 12 July 2014, Revised 24 September 2014
Accepted 20 October 2014
Corresponding Author: Sunghyuck Hong
(Division of Information and Communication, Baekseok University)
Email: shong@bu.ac.kr
ISSN: 1738-1916

keywords in Google search site, has the vulnerability of a list of directories, and the way that are not exposed in the search, while running a Web server, list vulnerable to directory present a setting method can complement the.

2. Directory List

2.1 Vulnerabilities

It is a vulnerability that could be called a list of directories to show a list of files in a directory on the server system, occurs when you do not have a set of additional business for the Web server.

The information can be through a list of directories, attackers know, it is possible to through the information on the Web application information and operating system of the Web server, to inform the other vulnerabilities the system has, site Administrator and configuration files necessary for the operation of the site access is not possible, the information of other users or system files, such as backing up files, and temporary files that were created temporarily by running a site in the usual way it will be able to Once the access in a database file that was included, to take account of other users and administrator, it can be a vulnerability of the Web server.

2.2 Search vulnerability site through search engine

The other, IIS Microsoft's and (Internet Information Service), the pattern for each type of Web applications that are used to operate a web site, showing the contents of the directory is greater Apache HTTP of the Apache Software Foundation to three there is a server such as Tomcat and server.

Contents of the list pattern of an application-specific directory is the same as <Table 1>[1].

〈Table 1〉 Directory Listing Pattern

Web Application	Patterns
IIS	Parent Directory
Apache	Directory Listing
Tomcat	Directory Listing
Other	Index of /

By using the pattern of the list of directories, in the Google search site, see the site there is a vulnerability in the directory list.

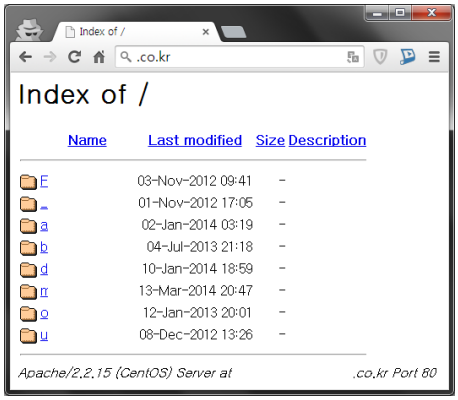
[Fig. 1] shows that the site where it was found by a Google search Index of / is either a pattern of a list of directories, unlike the Web page general, in the center of the site such as a file Explorer at the bottom, system information domain address and the version of the operating system and Web application you are using, such as the use port number is output a list of files on the server to come out.

If you click on the directory that will be displayed in the list page of the directory, go to that directory, you can list the files in the directory, click on the file, it is possible to or download the file, and check the Web browser. To move to the upper directory, just click the Parent Directory at the top in the list of files. If you click Name, Last Modified, Size, and Description at the top, the files are sorted in the order of each file name, last modified date, size, and description.

As [Fig.2], so that you can when you add specific keywords, such as <Table 2> when searching for Google, do a search for a specific site, but with the help of this, vulnerability of the list of directory it is possible to search data stored NAS products of several companies that have the (Network Attached Storage)[2][3].

Users by using the NAS recent, to use as the Web hard and Personal Web Server is increasing, but the point without any constraints outsider like this, search, that is access to, I can be very satisfied with the security.

When you search for a page that contains the keyword, which means administrators, such as admin as [Fig. 3], the page for the administrator or even come out, but the administrator account flows out to the hacker if the administrator for page If you become exposed, and using this hacker made available on its own and you remove the information of other users or confidential information of the site, the system will be able personal information to flow out.



[Fig. 1] Directory Listing Pattern Index of /

〈Table 2〉 Google Search keywords

Keywords	Contents
site	Search within a site or domain
inurl	Search URL in a string
filetype	Search by extension
intitle	Search for keyword int the title of page

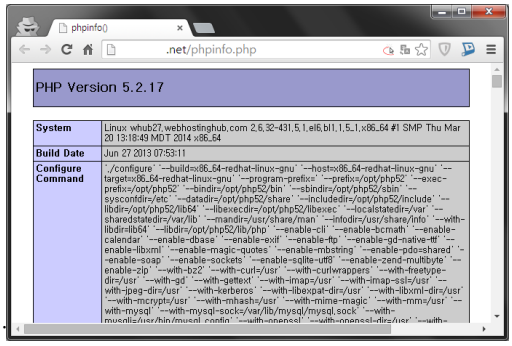
The following site in [Fig. 2], administrator pages are not open to the public, [Fig. 3]. Php.ini, phpinfo.php is a configuration file required to operate the server system as [Fig. 6] is exposed, but as important information for this hacker, vulnerabilities that exist in the version of the system because it is good information to inform.

In the above case, the configuration file, such as phpinfo.php was able to verify the configuration file to a directory listing can be inferred enough, it is necessary to set so as not to be able to view the file.

[Fig. 2] php.ini Configuration file

3. Remove the directory listing vulnerability

We are not the first to search by creating a robots.txt file is added to the directory of the Web server to use the robots.txt file in Google and other search engines for the search bots to collect site-specific directory is searched by You can search or not to be.



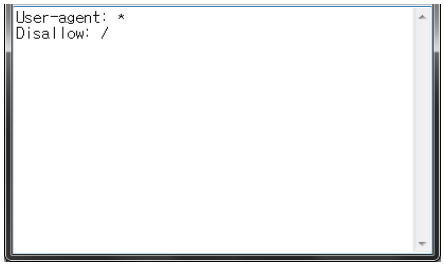
[Fig. 3] phpinfo.php Configuration file

How to use the robots.txt file to the root directory of a domain by creating a reference to the contents of <Table 3> set. About Google bot example in order to allow the search of all directories User-Agent: Googlebot and small parts

Disagllow: If left blank, as part of Conversely, with respect to all the bots will not allow the search of all directories, if User-Agent: * a small part Disagllow: part of the / give to the less top-level directory.

If you do not want to allow only specific directories to / instead of / directory name in case your.

Directory does not allow search for multiple Disallow: When you add the item in [Fig. 4].



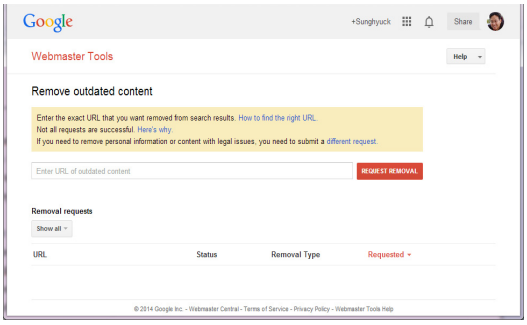
[Fig. 4] robots.txt Configuration file

〈Table 3〉 robots.txt Configuration

Item	Contents
User-Agent	Bot Name
Disallow	Directory Path

3.1 Removing vulnerabilities from a server operating

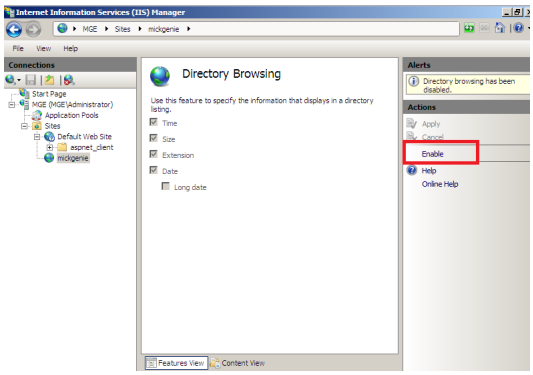
Directory listing of web application vulnerability does not change the initial settings of the web server administrator was infused to change that setting to give this problem is solved vulnerability[6].



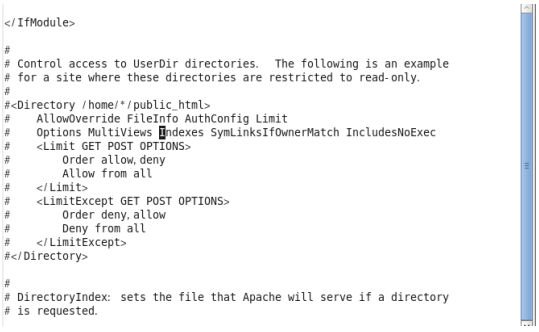
[Fig. 5] Remove Outdated Content on Google

In [Fig. 6], The. IIS (Internet Information Service) remove vulnerabilities [IIS (Internet Information Services)] Manager - Web site serving people] - [Directory Search] to get into the right tab, click Disable, and restart IIS[7][13].

Open the Apache httpd.conf configuration file of the directory server options after clearing the Indexes section to restart the service daemon. The settings may differ directory carefully[8][9][12]. [Fig. 5] shows that remove outdated content on Google. Fig, 6 and 7 shows that directory browsing option and removing a directory listing in Apache respectively.



[Fig. 6] Removing a directory listing in IIS



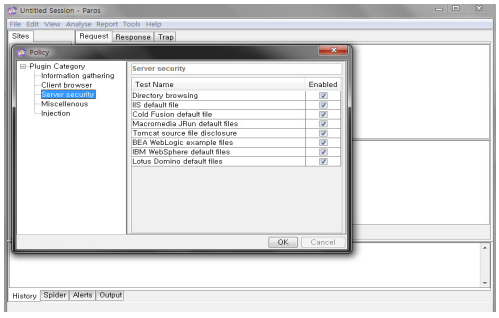
[Fig. 7] Removing a directory listing in Apache

4. Vulnerability Assessment

Check the main page of the website you wish to access the main page, while following the links to the

individual vulnerability exists in the directory, check to make sure the directory listing. First, check the directory where the destination directory does not exist, since the idea of an attacker can easily admin, root, home, upload, test, etc. The vulnerability also exists in the directory of inspection [10,11]. [Fig. 8] shows vulnerability assessment tools using Paros which is analysing packets over networks.

If the file being used by the Web site or many, a large scale, confirming the manual is difficult, be utilized inspection tools vulnerabilities such as Paros, to find vulnerabilities Web Site possible. Because you can check together well as a list of directories, multiple vulnerabilities in the basic pose a threat to the Web server and another managed, it is confirmed, the vulnerability checking tool of Paros is to build a Web server , it must be seen using all means. [Fig. 9] summarized and showed protection procedure for webserver.



[Fig. 8] Vulnerability assessment tools using Paros

[Fig. 9] Protection Procedure for Webserver

5. Conclusion

Vulnerability of large and small have been present in the Web application of what you need to do to run a web site for a long time. List of directories that were examined in this paper, will be able to vulnerabilities and not fatal as such, but, depending on whether to utilize a greater ripple effect. The large myself I thought that in the course of the study of the paper, we look at looking for a site that is vulnerable of Google, many sites are at risk of security really is frequently used I was surprised to see that there is a list of vulnerability directory site, personal files because it contains administrator of our site mentioned in it, I was surprised more. Where the people who run the web hard and Personal Web server through a device such as NAS recent has increased, but it was confirmed that the list vulnerable to directory of services of products of a particular company is present, the Web server application may not closely related to people who are using, but most people singing from personal photos of their own, copyright and other documents such as resumes, is applied as hard of a typical Web , I see that you have put a lot of files such as movies.

For example, if the situation called, or will be by chance, people are looking for some movies to see and resume personal information entered by accessing the web site does not occur, the web an individual run any site where several hundred people are also using the server, web server administrator must make management and interested in a little more security.

ACKNOWLEDGMENTS

This research is supported by 2014 Baekseok University research fund.

REFERENCES

[1] Kaiping Liu; Hee Beng Kuan Tan; Shar, L.K., Semi-Automated Verification of Defense against SQL Injection in Web Applications, Software Engineering Conference (APSEC), 2012 19th Asia-Pacific , vol.1, no., pp.91,96, 4-7 Dec. 2012.

[2] JOHNNY LONG, Google Hacking for Penetration Testers Vol., No., pp. 41-62, 2010.

[3] Beaver Kevin, Hacking for Dummies 4th Edition, Vol., No., pp. 281-282, 2012.

[4] Seungju Jang, Juneho Kim, Design of files and directories with security features within the Windows O. S. using Visual C++, Vol. 7, No. 1, pp 510-514, 2009

[5] Acevedo, B.; Bahler, L.; Elnozahy, E.N.; Ratan, V.; Segal, M. E., Highly available directory services in DCE, Fault Tolerant Computing, Proceedings of Annual Symposium on, vol., no., pp.387,391, 25-27 Jun 1996

[6] DOI: http://dx.doi.org/10.1109/HPCA.1999.744354

[7] DOI: http://dx.doi.org/10.1109/IEEESTD.1994.122164

[8] Jae-Nam Woo, Red Hat Fedora Linux Server & Network, Vol., No., pp. 573-575, 2010.

[9] S. B. Hong, Linux Server Security Management Practices 2nd Edition, Vol, 1. No., pp.85-86, 2008.

[10] KISA, Web Server Security Check's Guide, pp. 64-65, 2010

[11] B. Moore, E. Elleson, J. Strassner, A. Westerinen, "Policy Core Information Model", Request for Comments RFC 3060, February 2001.

[12] J.Halpern, S.Convery, R. Saville, "IPSec Virtual Private Networks in Depth VPN", Cisco Systems White Paper, June 2001.

[13] DOI: http://dx.doi.org/10.1109/TPDS.2005.4

홍 성 혁(Hong, Sunghyuck)

- 1995년 2월 : 명지대학교 컴퓨터공학과 (공학사)
- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 네트워크 보안, 해킹, 센서네트워크 보안, 해킹, 센서네트워크 보안
- E-Mail : shong@bu.ac.kr