YGN ETHICAL HACKER GROUP

Whitepaper

Sensitive Information Digging:

Directory Bruteforce Attack

By

d0ubl3_h3lix

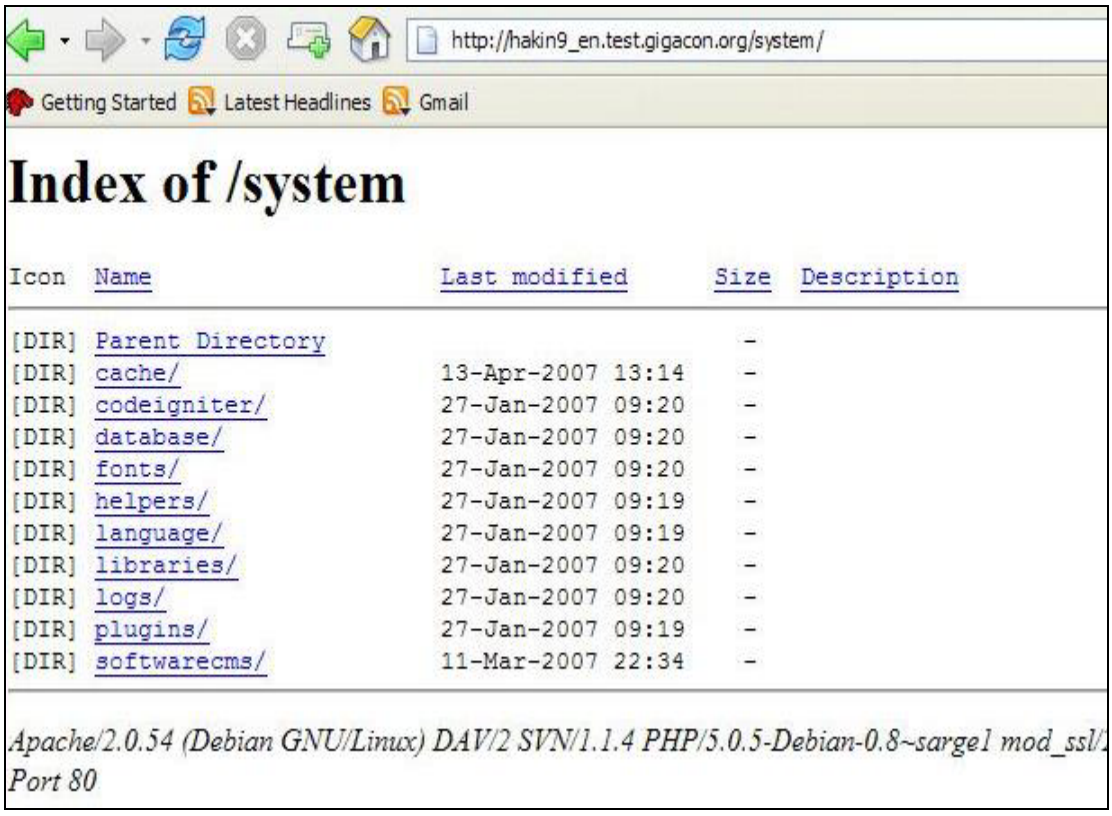
Wed Jan 09 2008

$ Revision 1.1 $

Abstract

Directory Bruteforce Attack is used to determine possible vulnerable directories (such as cgi-bin, _vti_bin) and find directory listings that may contain sensitive secret information or list of files to be used as hotlinking – which eats huge bandwidth. It is also used to determine targeted web site directory structures to understand more about its web application infrastructure. There are many tools (CGIScan, Paros, DirBuster from OWASP.org …etc) that aids in directory bruteforcing using predefined dictionary or vulnerable words list.

The following screenshot shows directory listing vulnerability of hackin9's mirror site. Hackin9 is a currently prominent Commercial Hacker E-zine site.



Defensive Measures

1. ***Using blank index.htm***

Putting blank index.htm simply prevent directory listings from displaying to site visitors. Write some texts like 'Your access has been logged' if you wish to fool script kiddies.

2. ***Preventing with .htaccess in Apache web server***

In .htaccess, write

Options –indexes

Note: Only .htaccess which is at **root** directory affects all subdirectories.

3. ***Suppressing error messages***

When an application fails to read non-existent files, it issues a 'file not found' error messages along with invalid path name. Attackers can deliberately make the application burst out noisy error messages by posting invalid requests. The following is an error message of hakin9 site that reveals server system directory:

The three above options may prevent directory listing.

But …

It will not stop bad guys. If they see certain directories exist because of directory listing denied message, they can also Bruteforce files names for digging possible sensitive files:

Dictionary Words + Common File Extensions (txt, htm, exe, pdf, xls, doc ...etc)

A tricky approach is to use error 403 Forbidden message exactly like error 404 Not Found message.

Attackers cannot get any clues about which directories actually exist or not. Nevertheless, smart attackers can write a simple script or program that easily determines actual existence of directories by analyzing server response headers.
Even if they Bruteforce file names, it will take them much longer. As their attempts are significant and are heavily logged in application firewall or web server logs. You can easily detect them by simply searching 404 in access logs.