

Forum:[Hack Forums](#)

Thread: [\[TUT\]Hacking Websites Through Directory Traversal Attack\[/TUT\]](#)

?????g?z - November 15, 2012, 9:18 pm

Hey HF here's another tutorial for you guys, this time we will be looking at directory traversal attacks.

A directory is basically a folder where web designer stores his website files(this is with respect to server). By directory traversal attack, i simply mean that hacker is able to navigate between the directories and files stored in those directories(say root which contains all config files, htaccess file, ini file and xquery files(all these files are most sensible files for any website, if any of these files security is not handled properly, then Hacker can own website)). In short by using directory traversal attack, hackers main aim is to get access to sensible file that i have mentioned above.

Nowadays attackers also use directory traversal attacks to view arbitrary files on web server like SSL private keys and password files.

Directory traversal is also known as the ../ (dot dot slash) attack, directory climbing, and backtracking.

What does ../ or ..\ (dot dot slash) mean ?

The ..\ instructs the system to go one directory(or simply called folder) up.

For example, we are at this location C:\Hacking\Hacking Tools\Bugtraq. Now on typing ..\ , we would reach at C:\Hacking\Hacking Tools.

Again on typing ..\ , we would reach at C:\Hacking and so on.

Lets again go at location C:\Hacking\Hacking Tools\Bugtraq. Now suppose we want to access a file abcfile.txt placed in folder Hacking. Just we need to type ../\abcfile.txt . Typing ../\ two times would take us two directories up (that is to directory Hacking) where abcfile.txt is stored.

I hope you got dot dot slash concept. Now lets proceed further..

So as of now, we have complete understanding what directory means and what dot dot slash means. Now lets understand clearly what directory traversal attack means.

Directory Traversal attack is an HTTP(or in simple terms web) exploit or vulnerability which allows attackers or hackers to access restricted directories (most hackers are interested in root directory access) and execute commands outside of the web server's root directory. The goal of this attack is to access sensitive files placed on web server by stepping inside root directory using dot dot slash technique. By exploiting a directory traversal vulnerability, an attacker can access files in directories other than the root directory. This can be harmful, since access to restricted files containing passwords or other private information may compromise the web server.

For example, by typing the following URL:

<http://www.samplesite.com/sample.php?item=../../../../web-config.php>

The attacker or hacker causes sample.php to retrieve the file ../../../../web-config.php and display it in the attacker's or hackers web browser. As i have already told you the character sequence "../" stands for "one directory up". So the string "../../../../web-config.php" therefore means "go four directories up, then down into root directory and retrieve the file web-config.php from there".

The attacker needs to guess how many directories to climb in order to get to the desired directory, but this can be easily done by trial and error.

Note Some web applications scan query string for dangerous characters such as:

..
..\
../

to prevent directory traversal attack.

However, the query string is usually URI decoded before use. Therefore these applications are vulnerable to percent encoded directory traversal such as:

%2e%2e%2f which translates to ../

%2e%2e/ which translates to ../

..%2f which translates to ../

%2e%2e%5c which translates to ..\

Also in windows internet explorer Microsoft added Unicode characters support, which introduced a new way of encoding ../, causing their attempts at directory traversal prevention to be bypassed.

Multiple percent encoding, such as

%c1%1c

%c0%af

are translated into / or \ characters.

Hope you guys learned something from this tutorial, please comment and rate! I learned this from a friend and thought it was neat to share!

lulzcat - November 15, 2012, 9:39 pm

Common sense, but legit contribution. Cheers bruv.

??????g?z - November 15, 2012, 9:45 pm

(Nov 15, 2012 10:39 PM)tehbunta Wrote: [\[CITE\]](#) Common sense, but legit contribution. Cheers bruv. Ye this was meant to help those who didn't know of the method. Glad you enjoyed it bud!

anish001 - January 10, 2013, 4:54 pm

Nice tutorial sir .. and could have more information in this post... nice post sir (Y) !!! to community

ProblemSolva - June 15, 2013, 12:22 pm

I doubt this still works on websites nowadays.

But nice tutorial thanks.

gsundeeep - January 20, 2014, 9:37 am

is there any dorks to find the directory traversal vulnerability ..?
and how to upload deface page using this attack