

**An Apache Trick to
Prevent Sensitive/Backup Files**

By

**Aung Khant
Nov 2008**

Sensitive files include backup files, sql files, and others that you don't want the world to access.

Backing up files is a well-known practice. Some web masters set cron (=scheduled) jobs for bi-weekly or monthly backup. Web developers create working backup files before critical changes. This is a daily or weekly occurrence during project activities. A common mistake found is they almost always place backup files in world-accessible directories; meaning anyone can download the files if they can guess file names. Some text editors like vi create backup files such as config.php~.

Blackbox security tools including my [WebPageFingerprint](#), [WebScarab](#) have been tailored to brute-force scan for backup files. How can you protect? You don't create backup files any more? Or immediately delete them after downloading them? Or you tell your fellow web developers not to create backup files in web accessible directories? Practically impossible for always.

The following .htaccess codes will solve this problem. You can extend it according to your needs.

```
# deny files like Copy of config.php
<FilesMatch "^(Copy of)">
  Order allow,deny
  Deny from all
</FilesMatch>

# deny files like fun.inc , data.sql, config.php-bk,config-bk.php,
# config-10Oct08-bk.php, yoursite.com-10Oct08-backup.tar.gz

<FilesMatch
"(\.inc|\.sql|\.*\~|\.*bk|\.*bak.php|.bk.php|.*\bakup.php|.*\bak|.*\bakup|.*\backup|.*\b
ackup.tgz|.*\backup.tar.gz|.*\backup.tar|.*\backup.gz|.*\backup.bz2|.*\backup.zip)$"
>
  Order allow,deny
  Deny from all
</FilesMatch>

#Deny directories whose names end with backup, bakup
<DirectoryMatch "(backup|bakup)$">
  Order allow,deny
  Deny from all
</DirectoryMatch>
```

In case you experience 500 Internal Server Error, ask your web server administrator to do this job for you. From now on, you can safely create backup files and directories

without needing to worry about potential backup file hunters and sensitive information diggers. Last but not least, you should never place your entire site backup in web accessible directory. The format auto-generated by cPanel is widely known:

YOURSITE-Month-4DigitYear.ZipExtension

yehg.net-10-2008.tar.gz

yehg.net-10-2008.tgz

yehg.net-10-2008.gz.gz