**Information disclosure**

* + Source code disclosure :  issues occur when the code of the backend environment of a web application is exposed to the public  ex the admin made a backup of the db or source code and put it on the server or the site so anyone can download it its usually compressed (zip/tar/sql/tgz/...)
    - **backup files extensions**
      * txt,log = log files with text
      * admin.php~ = hidden copies of editable files
      * .zip , .gz , .tar , tar.gz, .rar , .bz2 , .7z , .tgz , .php.bak = archives that may contain backup files (e.g., backup.zip, backup.tar.gz)
      * conf,cnf = config files (e.g., admin.conf)
      * .sql , .bak , .old= sql database backups
      * .git = version control system files
  + hidden files (.filename)  ex of hidden files source code repositories (.git , .svn) (git repository)
  + source code repositories (.git , .svn) if found on the website
  + source code files (.old/.bak/.php~)
  + javascript files (a lot of js files contains important info)
  + search in github for the website maybe we will find something
  + Tools that helps in info disclosure
  + Directory bruteforcing tools :
    - dirsearch/dirbuster/dirb tools
    - fuzz.txt  //world list that contains alot of dir names we can use it with dirb or anytool (by booM in git)
  + html the source code can sometimes reveal some information disclosure
  + ERROR MESSAGES
    - Script Error Messages
    - stack traces : is debugging information about the error which also includes information about the  path of files and often the piece of code where the error originated.
    - Informative Debug Message
    - Server and Database Message :they often disclose the query that generated the error, enabling   you  to ﬁne-tune a SQL injection attack
  + File Name & File Path Disclosure
    - A web application may disclose the structure of underlying infrastructure by revealing either file names or file paths or both. Due to inappropriate input handling, improper configuration management, or backend exceptions, a web application’s response may include such information in error pages.
  + Directory Listing: Related to filename and path disclosure is directory listing in web servers. This functionality is provided by default on web servers. When there is no default web page to show the web server shows the user a list of files and directories present on the website.
    - Therefore if the default filename on an Apache web server is *index.php*, and you have not uploaded a file called *index.php* in the root directory of your website, the server will show a directory listing of the root directory instead of parsing the php file
  + **Notes** 
    - what is dvcs pillage
      * (dump anywebsite that has git/svn repository on the server)
    - we can hide our server info from banner grabbing and use generic error messages ex : In Apache, custom error pages can be conﬁgured using the ErrorDocument directive in httpd.conf:
      * ErrorDocument 500 /generalerror.html
  + **How to Prevent Data Exposure**
    - Classify data processed, stored, or transmitted by an application.
    - Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs.
    - Apply controls as per the classification.
    - Don’t store sensitive data unnecessarily.
    - Discard it as soon as possible or use PCI DSS compliant tokenization or even truncation. Data that is not retained cannot be stolen.
    - Make sure to encrypt all sensitive data at rest.
    - Ensure up-to-date and strong standard algorithms, protocols, and keys are in place; use proper key management.
    - Encrypt all data in transit with secure protocols such as TLS with perfect forward secrecy (PFS) ciphers, cipher prioritization by the server, and secure parameters.
    - Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
    - Disable caching for responses that contain sensitive data.
    - Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as Argon2, scrypt, bcrypt, or PBKDF2.
    - Verify independently the effectiveness of configuration and settings.