[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@0e722c19ffd446b293739c9e37645e20?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Summary**

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the exposure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution, or sensitive user data.

A clear example is an execution file that is executable by unauthorized users. For another example, account information or a token value to access an API - increasingly seen in modern web services or microservices - may be stored in a configuration file whose permissions are set to world-readable from the installation by default. Such sensitive data can be exposed by internal malicious actors of the host or by a remote attacker who compromised the service with other vulnerabilities but obtained only a normal user privilege.

**Test Objectives**

* Review and identify any rogue file permissions.

**How to Test**

In Linux, use ls command to check the file permissions. Alternatively, namei can also be used to recursively list file permissions.

$ namei -l /PathToCheck/

The files and directories that require file permission testing include but are not limited to:

* Web files/directory
* Configuration files/directory
* Sensitive files (encrypted data, password, key)/directory
* Log files (security logs, operation logs, admin logs)/directory
* Executables (scripts, EXE, JAR, class, PHP, ASP)/directory
* Database files/directory
* Temp files /directory
* Upload files/directory

**Remediation**

Set the permissions of the files and directories properly so that unauthorized users cannot access critical resources unnecessarily.

**Tools**

* [Windows AccessEnum](https://technet.microsoft.com/en-us/sysinternals/accessenum)
* [Windows AccessChk](https://technet.microsoft.com/en-us/sysinternals/accesschk)
* [Linux namei](https://linux.die.net/man/1/namei)