**INADEQUATE APPLICATION SECURITY**

1. An application’s process is invoked with sensitive arguments, environment variables, or other elements that can be seen by other processes on the operating system. Many operating systems allow a user to list information about processes that are owned by other users. This information could include command line arguments or environment variable settings. When this data contains sensitive information such as credentials, it might allow other users to launch an attack against the software or related resources [1].
2. **Banner** **grabbing** or **active** **reconnaissance** is a type of attack during which the attackers send requests to the system they are attempting to attack in order to gather more information about it. If the system is not well configured, it may leak information about itself, such as the server version, PHP/ASP.NET version, OpenSSH version, etc. [2].

**REFERENCES**

1. “CWE - CWE-214: Information Exposure Through Process Environment (2.10)", Cwe.mitre.org, 2017. [Online]. Available: <https://cwe.mitre.org/data/definitions/214.html>
2. M. Hasan, "Information Disclosure Issues and Attacks in Web Applications", Netsparker.com, 2017. [Online]. Available: <https://www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/>.