A04:2021 – Insecure Design Prevention

SECURITY PRINCIPLES

1.Principle of least Privilege

Each program or user should operate only with the least amount of privilege required to achieve their goals.

SECURITY PRINCIPLES
2.Validation of Input

Every input from the user is validated to ensure it is in the expected format and reject it otherwise

SECURITY PRINCIPLES
3.Segregation of Tenants

Different environments such as live and test should be on separate networks and not share resources

SECURITY PRINCIPLES

4.Encryption

Data must be encrypted at all times
including during the resting phase

SECURITY PRINCIPLES
5.Fail Securely

Internal architectural details should be not be revealed in error messages

SECURITY PRINCIPLES

6.Observe

Running code should issue logs that reveal data such as type and volume of traffic as well as available bandwidth being used.