***Cryptographic failures OWASP A02:2021***

Ineffective execution & configuration of cryptograpy (FTP, HTTP, MD5, WEP)

Sensitive data exposure

* Never roll your own crypto use well known open source libraries
* Static code analysis tools can be discover this issue
* Key management (creation, destruction, distribution, storage and use)

***Insecure design OWASP A04: 2021***

A failure to use security by design methods/ principles resulting in a weak or insecure design

Breach of confidentiality, integrity and availability

* Secure lifecycle (embed security in each phase: requirements, design, development, test , deployment, maintenance, and decommissioning )
* Use manual (code review, threat modelling) and automated (SAST and DAST) methods to improve security

***Software and data integrity failures OWASP A08:2021***

An application that relies on updates from a trusted external source, however the update mechanism is compromised.

Supply chain attack; data exfiltration, ransomware, etc…

* Verify the input (in this case software updates with digital signature)
* Continuously check for vulnerabilities in dependencies
* Use software bill of materials
* Unconnected back up

***Server side request forgery OWASP A10:2021***

Misuse of prior established trust to access other resources. A web application is fetching a remote resource without validating the user supplied URL

Scan and connect to internal services. In some cases the attacker could access sensitive data.

* Sanitize and validate all client supplied input data
* Segment remote server access functionality in separate networks to reduce the impact
* Limiting connections to specific ports only (443 for https)