***XML external entities***

Many older or poorly configured XML processors evaluate external entity references within XML documents.

Extraction of data, remote code execution and denial of service attack

* Use JSON, avoiding serialization of sensitive data
* Patch or upgrade all XML processors and libraries
* Disable XXE and implement whitelisting
* Detect, resolve and verify XXE with static application security testing tools

***Insecure deserialization OWASP AB-2017***

Error in translation between objects

* Remote code execution, denial of service. Impact depends on type of data on that server
* Validate user input
* Implements digital signatures on serialized objects to enforce integrity
* Restrict usage and monitor deserialization and log exceptions and failures

***Insufficient logging and monitoring OWASP A10: 2017***

Not able to witness or discover an attack when it happens or happened

Allows attacker to persist and tamper, extract or destroy your data without you noticing it.

* Log login, access control and service-side input validation failures
* Ensure logs can be consumed easily, but cannot be tempered with
* Continious improvement monitoring and alerting process
* Migrate impact of branch: Rotate, Repave and Repair