# **Chapter 4 – Types of possible attacks?**

Within the structure described above, there can be a big number of attacks. In this chapter, I will be emphasizing some of the most prevalent. According to OWASP Top 10 API Security Risks – 2023 [25], the most problematic vulnerabilities are:

1. Broken Object Level Authorisation
2. Broken Authentification
3. Broken Object Property Level Authorisation
4. Unrestricted Resource Consumption
5. Broken Function Level Authorisation
6. Unrestricted Access to Sensitive Business Flows
7. Server Side Request Forgery
8. Security Misconfiguration
9. Improper Inventory Management
10. Unsafe Consumption of APIs

Besides all of the above mentioned problems when writing a software APIs, there exist a lot more misconfiguration and mismanagement problems when using third-party software and hardware.

## Chapter 4.1 – Third-party software and hardware security problems

Firstly, I would like to discuss about possible problems with third-party software and hardware.

--add database security here

## Chapter 4.2 – API problems

Asdasda

# **Chapter 5 – Prevention and mitigation of attacks?**

-- Description of this chapter

## Chapter 5.1 – Prevention and mitigation of third-party software and hardware security problems

According to the Plan-Do-Check-Act principle, any component must go through cycles of planning changes, implementing them, checking for issues (being security or otherwise) and acting to minimise the issues.

-- Risk avoidance

--database security

## Chapter 5.2 – Prevention and mitigation of API problems

-- Add API Prevention and Mitigation