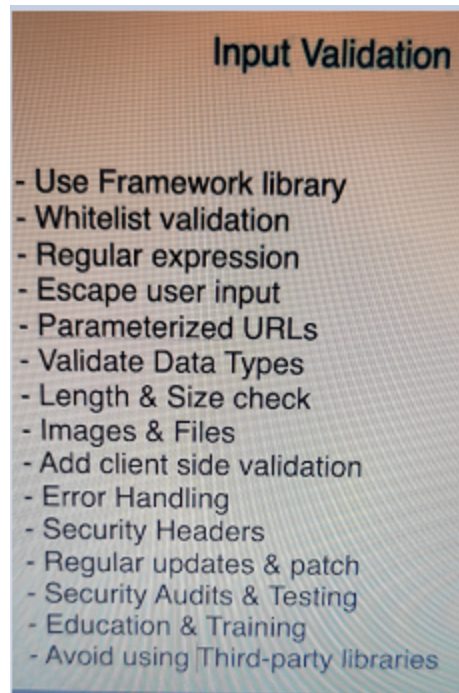


# Input Validation and Sanitization



## Use framework library

React, axios - they take care of some simple issues at their own level

## Whitelist validation

What data you get from user - what input keys/values are valid for data

## Regular expressions

input must fit right set of regular expressions

## **Escape user input**

## **Parameterized url's**

we need to specially take care of it because you may be taking some info from query params for doing somethings in your app

## **Validate data types always**

whether you were expecting number/string/etc

## **Length and size check**

you must always verify size of input

Real world example - DDOS attack using huge data - if we will not handle size - it can bring down server

## **Type/size of images/files needs to be checked/verified - take care of extensions**

## **Add client side validation**

don't just depend on server side validation(SSRF and SSJI type of attack can happen)

**Having proper error handling - specially global exceptions**

**You should never avoid Security Headers**

**Regular updates and patches for libraries used**

You should not take this lightly. Security related small things are constantly pushed. You must update if something is related to security

**Security Audits and Testing should be done**

**Third party library**

Avoid using third party libraries for everything because there can be security vulnerabilities

Don't use third party libraries for small things