SwipeRight OWASP Top 10 Checklist

A01:2021-Broken Access Control

Description

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

Solution/Plan

Make use of CORS, protect resources by default, logging and implement rate limiting.

A02:2021-Cryptographic Failures

Description

This failure is responsible for the exposure/leaking of data of critical and sensitive nature to ill-intended resources/people. Missing out on safeguarding such data leads to theft, public listing, breaches, and other problems.

Solution/Plan

Identify sensitive data, store only what needs to be stored, use encryption (TLS) and disable caching for sensitive data.

A03:2021-Injection

Description

Injection is an attacker's attempt to send data to an application in a way that will change the meaning of commands being sent to an interpreter

Solution/Plan

Use safe and well tested libraries for querying data, validate user input and test the application thoroughly.

A04:2021-Insecure Design

Description

Insecure design is a broad category representing different weaknesses, expressed as “missing or ineffective control design.

Solution/Plan

Mind security in the analysis phase, use secure design patterns, make use of unit and integration testing and segregate applications, layers and roles.

A05:2021-Security Misconfiguration

Description

Security misconfigurations are security controls that are inaccurately configured or left insecure, putting your systems and data at risk. Basically, any poorly documented configuration changes, default settings, or a technical issue across any component in your endpoints could lead to a misconfiguration

Solution/Plan

Use environments and automation, keep a minimal code spaces and delete unused features. Send security headers and implement automation which verifies the effectiveness of configurations and settings in every environment.

A06:2021-Vulnerable and Outdated Components

Description

Vulnerable and outdated components attacks target both client and server side components.

Solution/Plan

Remove unused dependencies, monitor libraries with external software/tools and try to use only official libraries/dependencies.

Note: I use Dependabot (GitHub) in order to scan for insecure/outdated dependencies. This will notify me by email as soon as something is found.

A07:2021-Identification and Authentication Failures

Description

Identification and authentication failures can occur when functions related to a user's identity, authentication, or session management are not implemented correctly or not adequately protected by an application.

Solution/Plan

Implement MFA/2FA, rate limiting, use secrets & implement password checks.

Note: I will use a cloud service for authentication in order to get a higher grade of security in my project.

A08:2021-Software and Data Integrity Failures

Description

Description. Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs)

Solution/Plan

Use trusted third-party software and encrypt serialized data where necessary.

A09:2021-Security Logging and Monitoring Failures

Description

Security logging and monitoring failures are frequently a factor in major security incidents. The BIG-IP system includes advanced logging and monitoring functionality and provides security features to protect against attacks that can result from insufficient system and application logging and monitoring

Solution/Plan

Sufficient logging, encode logs, have integrity control in high value transactions, integrate DevSecOps and report breaches within 72 hours (GDPR).

A10:2021-Server-Side Request Forgery

Description

A Server-Side Request Forgery (SSRF) attack involves an attacker abusing server functionality to access or modify resources. The attacker targets an application that supports data imports from URLs or allows them to read data from URLs.

Solution/Plan

Reduce remote access functionality and enforce deny by default (firewall).