Assignment: OWASP report

The OWASP top 10 is a solid way to start off analyzing your work in relation to possible security risks and their impact. In this assignment you will check your project for issues, creating awareness about security and offering you a chance to improve your application security.

Difficulty: ☆☆☆★★

Learning objectives:

- Get familiar with the OWASP foundation and top 10 security risks
- Analyze your individual track for potential issues vs the OWASP top 10.

Estimated time required: 120 minutes

Step 1: Check the OWAP top 10

Check the OWASP 2021 top 10: https://owasp.org/Top10/ See if you understand all 10 security risks.

Step 2: Analyze your own project against this top 10

Analyze your own project vs these security risks. Risk is defined as Probability X Impact. Higher risk problems should have higher priority. Create a document in which you write down your analysis using a table. Your table could look like this:

	Likelihood	**Impact**	**Risk**	**Actions possible**	**Planned**
A1: broken access control	High	Severe	High	N/A, fixed	Yes
A2: Cryptographic failure	Very unlikely	Severe	Low	No passwords or user data used	N/A
…					
A10: Server side request forgery	High	Moderate	Moderate	Improve framework implementation	No, risk accepted

Step 3: Add reasoning

Add a reasoning to the document indicating what you think the security risks means and what the impact on/chance of affecting your application will be.

Final step: Add a conclusion to the report

In the conclusion, write why you think your app is sufficiently secure, or might need more security improvements in the future.