Security by design

Author: Denny Cox
Class: S6-RB10
Semester: 6

Table of contents

Security vulnerabilities **3**

SQL injection *3*

Cross site scripting *3*

Insecure file upload *3*

Insecure deserialization *3*

Padding oracle *3*

Security vulnerabilities

During the security workshop, we discussed the following important security vulnerabilities and talked about how to prevent them:

SQL injection

Use an ORM in the framework that is used. For my project I will use Entity Framework.

Cross site scripting

Output encoding (use protection from used framework).

Insecure file upload

Only accept whitelisted file types, restrict file size, generate file names yourself, store files only in database, use library to verify zip files.

Insecure deserialization

Don't deserialize user input if possible, otherwise apply integrity checks.

Padding oracle

Encrypt using AES in GCM mode.

Closing tips from workshop:

- View Microsoft SDL: https://www.microsoft.com/en-us/securityengineering/sdl
- Implement security tests
- Follow OWASP top 10
- Follow security recommendation from the used framework
- Use tools like SonarQube in CI/CD
- Write security recommendations and implement them