

Desenvolvimento Seguro

Descrição do Projeto

Desenvolvimento Seguro

*A codificação segura é a prática de desenvolver software de computador de forma a **evitar** a introdução accidental de vulnerabilidades de segurança. **Defeitos, bugs, falhas lógicas e falta de padronização** são consistentemente a principal causa das vulnerabilidades de software comumente exploradas [CWE, 2021].*



Regras do Projeto

- Deverá ser desenvolvido individualmente ou duplas.
- Prazo de entrega: 13/10, até 23h59.



Regras do Projeto

- Existem diversas comunidades que oferecem suporte à codificação segura com padrões e regras para diversas linguagens de programação, como SEI CERT, OWASP, CWE, entre outros.

Regras do Projeto

- SEI CERT:
 - <https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java>

Regras do Projeto

- O SEI CERT Coding Standards é um conjunto de práticas de programação que visam aumentar a segurança e a robustez de códigos em várias linguagens de programação, incluindo Java.
- Essas diretrizes são publicadas pelo Software Engineering Institute (SEI) da Carnegie Mellon University.



Regras do Projeto

- Validação e Sanitização de Entrada:
 - IDS00-J. Prevent SQL injection (e XSS, caso web
 - IDS01-J. Normalize strings before validating them
 - IDS03-J. Do not log unsanitized user input
- Declarações:
 - DCLo1-J. Do not reuse public identifiers from the Java Standard Library
 - DCLo2-J. Do not modify the collection's elements during na enhanced for statement



Regras do Projeto

- Comportamento Excepcional:
 - ERR00-J. Do not suppress or ignore checked exceptions
 - ERR07-J. Do not throw RuntimeException, Exception, or Throwable
- Diversos:
 - MSCo1-J. Do not use an empty infinite loop
 - MSCo4-J. Do not leak memory
 - MSCo2-J. Generate strong random number
 - MSCo3-J. Never hard code sensitive information
 - MSCo7-J. Prevent multiple instantiations of singleton objects



Regras do Projeto

- Deverá desenvolver um projeto em Java (web ou console) e cadastrar as tarefas no Trello.
- Deverá possuir pelo menos 5 funcionalidades diferentes neste projeto, com persistência em banco de dados relacional.
- Cada equipe deverá pensar em um tema para implementação.
- Deverá desenvolver o projeto com MVC, DAO e Singleton para a classe de conexão ao banco de dados relacional.



Regras do Projeto

- Deverá considerar o Cognito para cadastro e autenticação dos usuários do projeto em um ou mais grupos.