Universidade do Minho
Escola de Engenharia

Desenvolvimento seguro de *software*

Práticas Fundamentais

Paulo Gameiro **A72067**
Pedro Rodrigues **PG41092**
Rafaela Soares **A79034**

Universidade do Minho
Escola de Engenharia

Introdução

Foi estudado um conjunto de orientações importantes para o desenvolvimento seguro de software - desde a fase inicial de conceptualização até à utilização.

Universidade do Minho
Escola de Engenharia

Introdução

Design	**Práticas de Desenvolvimento**	**Planeamento**
Gestão de Problemas	**Gestão de Riscos**	**Resposta às vulnerabilidades**
	Testes e Validação	

Universidade do Minho
Escola de Engenharia

Design

- ***Threat Modelling***

Representação abstrata de um sistema no intuito de se identificar as possíveis e hipotéticas ameaças, riscos, vulnerabilidades e contramedidas do sistema em questão.

Vantagens: aumento da consciência de segurança
Identificação e possível solução de hipotéticas falhas

Universidade do Minho
Escola de Engenharia

Design

- **Princípios de *design* seguro**
  - *Defense in depth*
  - *Fail securely*
  - *Design for updating*

Universidade do Minho
Escola de Engenharia

Design

- **Desenvolvimento de uma estratégia de criptografia**
  - Definições sobre o que proteger
  - Designação dos mecanismos a serem usados para criptografia
  - Decisão sobre uma solução de gestão de chaves e certificados
  - Implementação com agilidade criptográfica em mente

Universidade do Minho
Escola de Engenharia

Design

- **Padronização da gestão de identidade e acesso**
  - Mecanismo de autenticação
  - Mecanismos pelo quais um serviço ou componente lógico se autentica para outro e como as credenciais são armazenadas
  - Mecanismos que autorizam as ações de cada principal

Universidade do Minho
Escola de Engenharia

Design

- **Estabelecimento de requisitos de Log e práticas de auditoria**

Utilizar arquivos *log* de aplicações, sistemas e segurança é uma ótima forma de armazenar detalhes relativos a um hipotético incidente de segurança.

Contudo, é necessário ter em consideração algumas decisões face à criação e manutenção de *logs*.

Universidade do Minho
Escola de Engenharia

Práticas de Desenvolvimento

- Estabelecer padrões e convenções de codificação
- Utilizar apenas funções seguras
- Utilizar ferramentas de análise de código para localizar problemas de segurança antecipadamente
- Manipular dados com segurança
- Lidar com erros

Universidade do Minho
Escola de Engenharia

Gestão de Riscos

A utilização de *frameworks* e bibliotecas de terceiros, apesar das **vantagens que traz associadas** (reutilização de componentes que permite uma maior eficácia no desenvolvimento), traz também **riscos inerentes**, tendo em conta que normalmente **não é possível perceber o que contém o código** que está a ser importado.

Deve escolher-se *frameworks* e bibliotecas estáveis e conhecidas como seguras.

Universidade do Minho
Escola de Engenharia

Testes e Validação

Testes Automáticos

- Ferramentas de Análises Estaticas
- Análises Dinâmicas
- *Fuzz Parsers*
- Analizar Vulnerabilidades na Rede
- Configurações Seguras e Plataformas de Mitigação
- Testes Automáticos de Funcionalidades

Testes Manuais

- Verificações Manuais das Funcionalidades
- Testes de Penetração

Universidade do Minho
Escola de Engenharia

Gestão de Problemas

Definir Gravidade

Ex: **Muito Baixo** a **Muito Alto**

Aceitar Risco

É necessário uma aprovação de que é possível **lançar o produto com o risco inerente**

Universidade do Minho
Escola de Engenharia

Resposta às vulnerabilidades

- Políticas Internas e Externas
- Funções e Responsabilidades
- Gerir Repórteres de vulnerabilidades
- Garantir que repórteres de vulnerabilidades sabem quem contactar
- Gerir vulnerabilidades de componentes de terceiros
- Resolver vulnerabilidades
- Divulgar vulnerabilidades
- Feedback do ciclo de vida do desenvolvimento

Universidade do Minho
Escola de Engenharia

Planeamento

- Cultura da empresa
- Experiência da empresa
- Ciclo de vida e modelo do desenvolvimento do produto
- Âmbito do desenvolvimento inicial
- Propostas de valor

Universidade do Minho
Escola de Engenharia

Ferramentas

Universidade do Minho
Escola de Engenharia

Considerações finais

À medida que as ameaças e os métodos de ataque continuam a evoluir, também os processos, técnicas e ferramentas para desenvolver *software* seguro.

Universidade do Minho
Escola de Engenharia

Desenvolvimento seguro de *software*

Práticas Fundamentais

Paulo Gameiro **A72067**
Pedro Rodrigues **PG41092**
Rafaela Soares **A79034**