Desenvolvimento seguro.

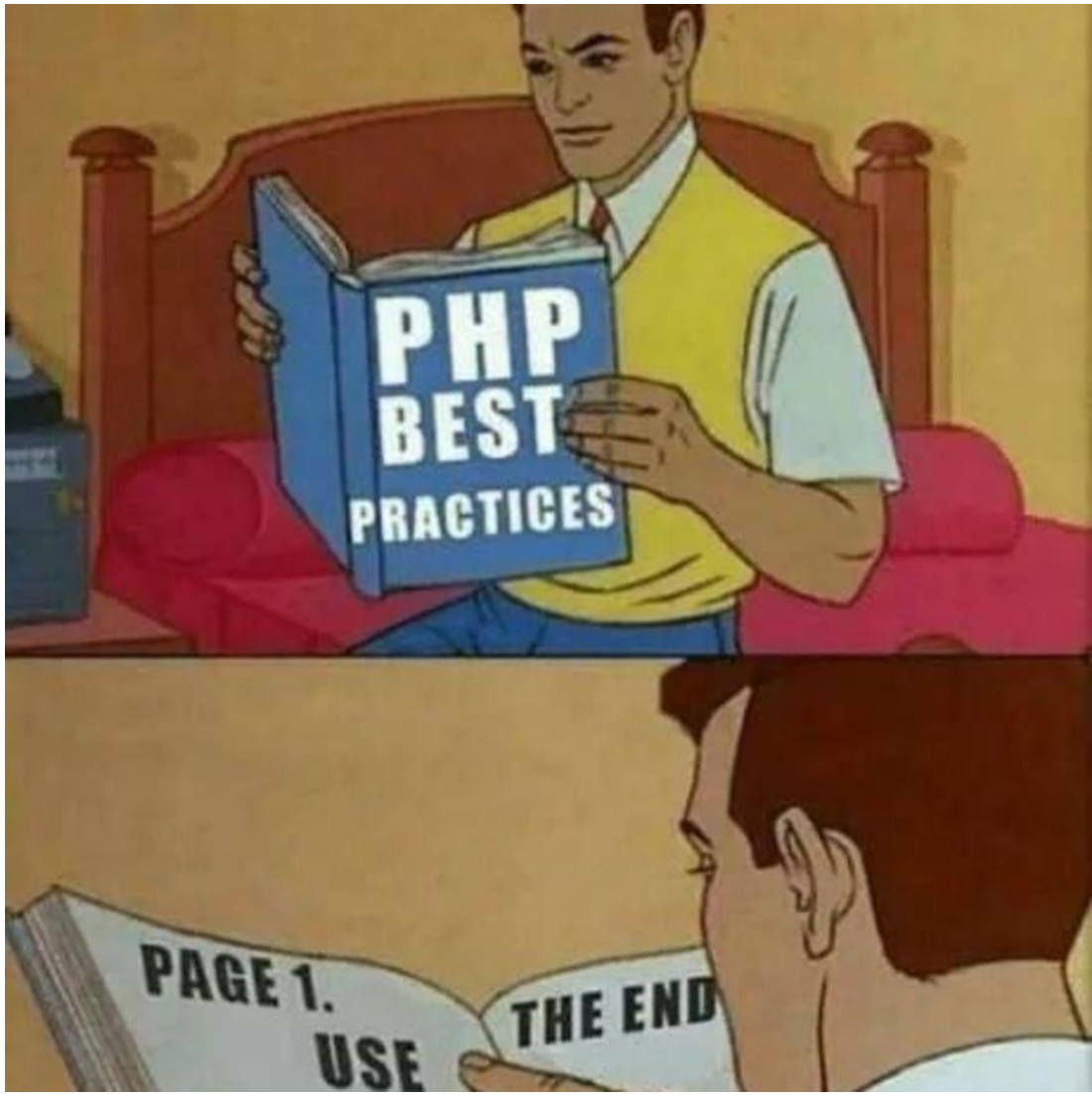
Tópicos 8.25 até 8.34 da ISO 27002
Auditoria e Segurança.

O que é desenvolvimento seguro?

O desenvolvimento seguro é uma metodologia para criar software que incorpora segurança em todas as fases do ciclo de vida de desenvolvimento de software (SDLC). A segurança é inserida no código desde o início.

Security by Design

Security by Design é sobre garantir que os sistemas e seus componentes sejam criados desde o início com a segurança em mente, como por exemplo: realização de testes de segurança da solução,
adoção de medidas mais seguras de autenticação, adoção das melhores práticas de programação para evitar vulnerabilidades.

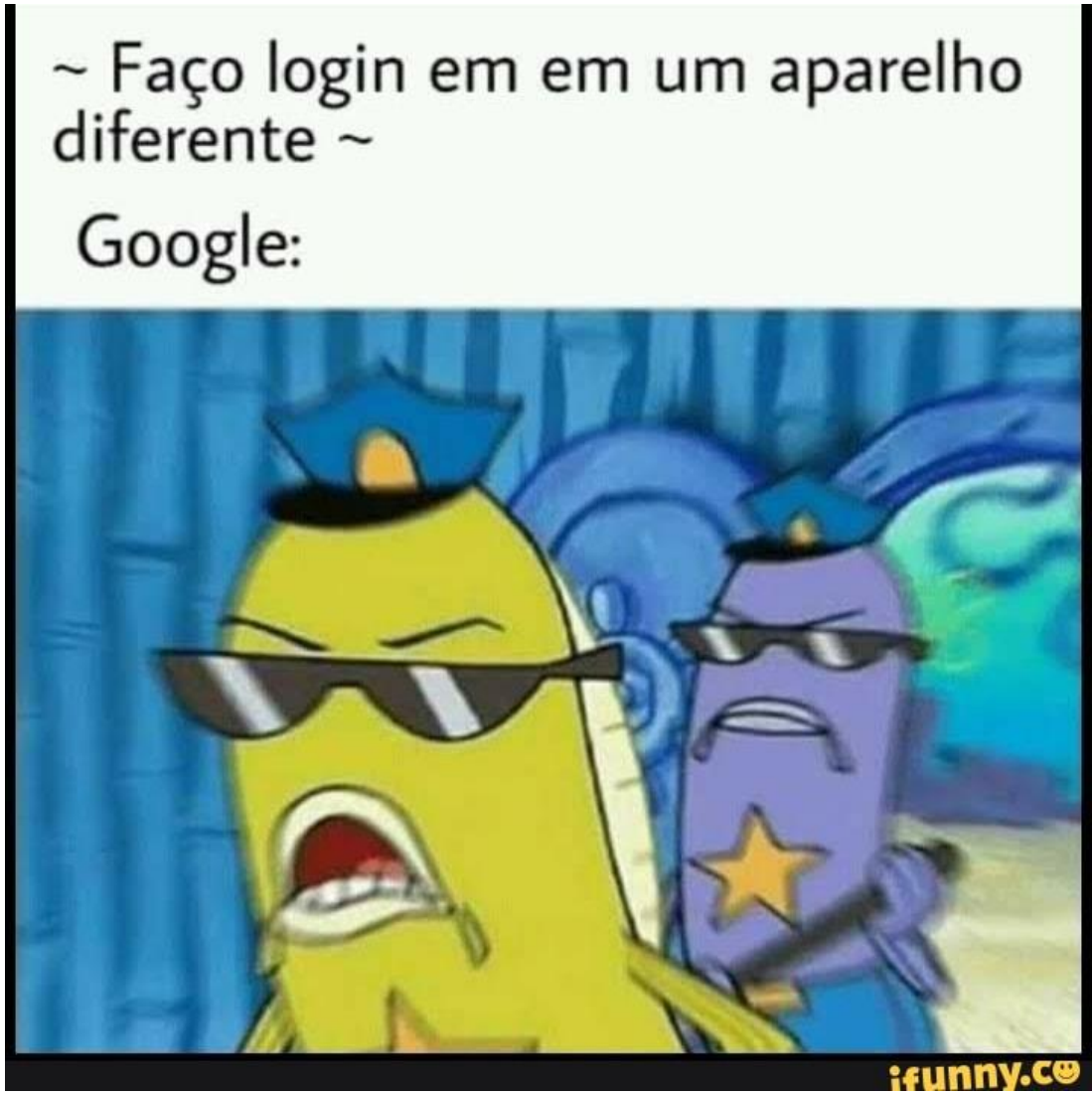


Ciclo de Vida do Desenvolvimento de Software Seguro (SSDLC)

É permitir que as aplicações sejam desenvolvidas tendo como base as melhores práticas de desenvolvimento seguro, o que ao final do processo entregaria uma aplicação mais segura.

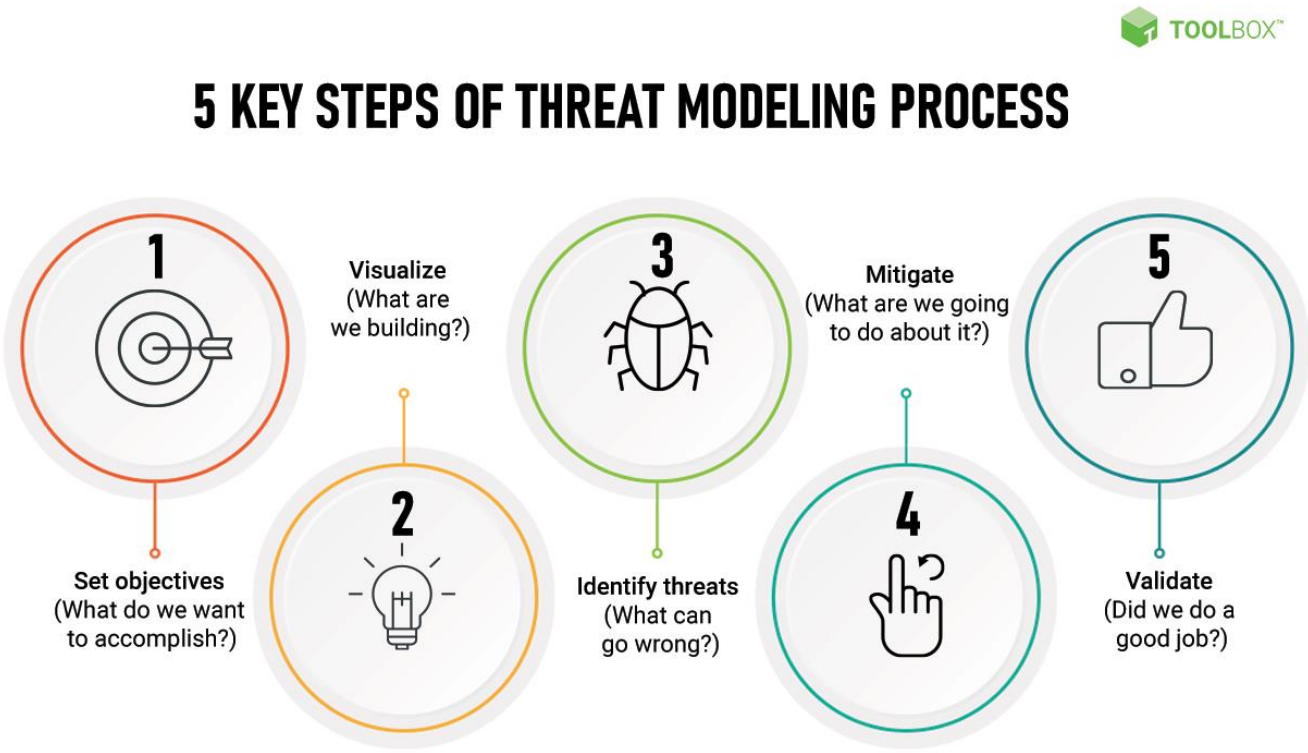
Requisitos de uma aplicação segura

- Segregação de acesso e nível de acesso;
- Resiliência contra ataques maliciosos;
- Atender a requisitos legais durante a transação, processamento e armazenamento;
- Criptografia das comunicações entre as partes envolvidas;
- Armazenar todas as movimentações.



Threat Modelling

A modelagem de ameaças é uma abordagem para identificar e priorizar possíveis ameaças a um sistema e determinar o valor que possíveis mitigações teriam na redução ou neutralização dessas ameaças.



Código seguro.

Na fase de desenvolvimento, é pensando em como evitar vulnerabilidades, como descritas na OWASP Top 10.

Aliado a isso há SAST (Teste estático), Teste dinâmico (DAST) e o Code Review.

Code Review, Dast e Sast

Code Review – avaliações de código projetadas para identificar bugs e aumentar a qualidade do código.

Sast – O teste de segurança de aplicativos estáticos (SAST) é uma ferramenta de segurança que identifica a causa das vulnerabilidades e ajuda a corrigir as falhas de segurança subjacentes.

Dast – O teste dinâmico de segurança de aplicativos (DAST) é o processo de análise de um aplicativo da Web por meio do front-end para encontrar vulnerabilidades por meio de ataques simulados.

E de que falhas estamos tentando fugir?

1. XSS (Cross Site Scripting;
2. Security Misconfiguration;
3. SQL Injection;
4. Cross-Site Request Forgery;
5. Outras inúmeras...

Pentesting

Procedimento para testar a segurança de um sistema ou aplicativo de software fazendo uma tentativa deliberada de comprometer sua segurança.

Imita as etapas que um agente de ameaça pode seguir para explorar suas vulnerabilidades. Em seguida, demonstra o impacto e fornece orientações claras para corrigi-los.

Hardening

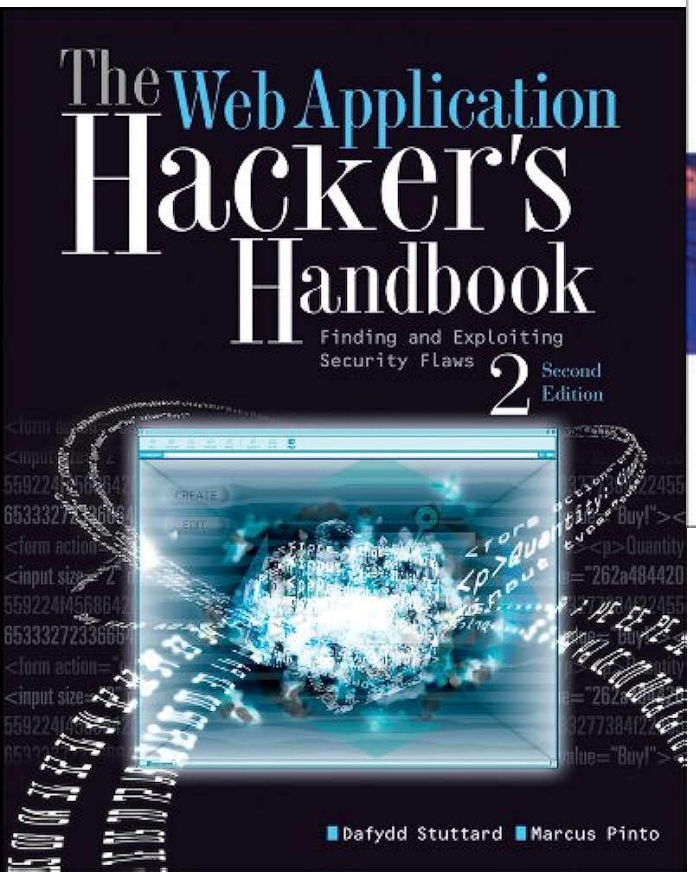
Um processo destinado a eliminar um meio de ataque corrigindo vulnerabilidades e desativando serviços não essenciais. Você fortalece um sistema reduzindo a superfície de ataque.

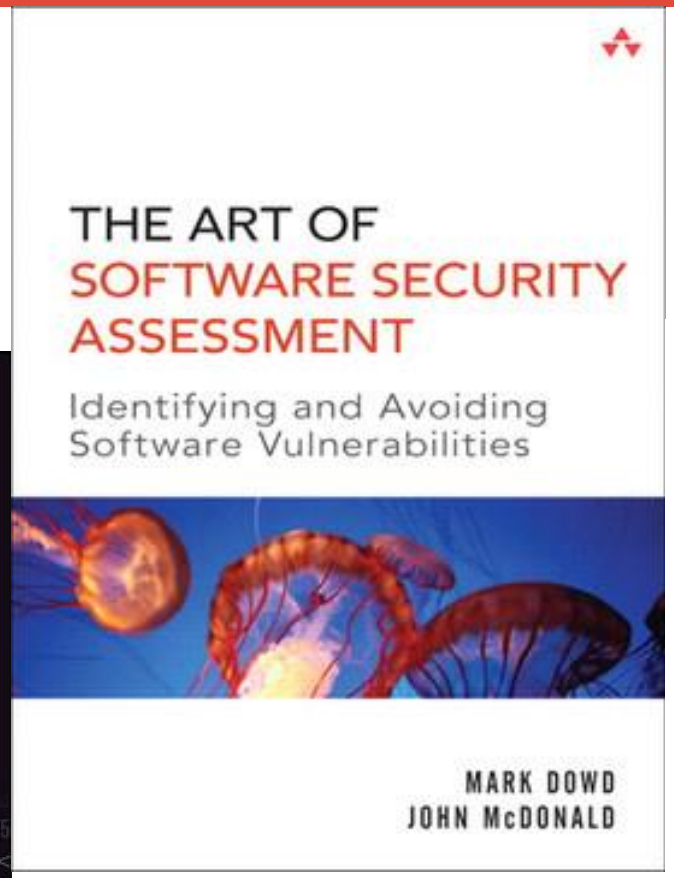
O dia que o SDLC foi para o espaço.

Hackers acessaram código-fonte da Microsoft em ataque à SolarWinds

Ataque à SolarWinds afetou milhares de empresas, incluindo a Microsoft, que confirmou acesso a repositórios de codigo-fonte

Leituras interessantes.





OWASP/**www-project-developer-guide**

OWASP Project Developer Guide - Document and Project Web pages

4 Contributors · 7 Issues · 3 Discussions · 10 Stars · 1 Fork

Possíveis áreas de atuação

- Application Security Engineer;
- DevSec;
- Pentester

Como dizia minha ex:

“TERMINAMOS”