

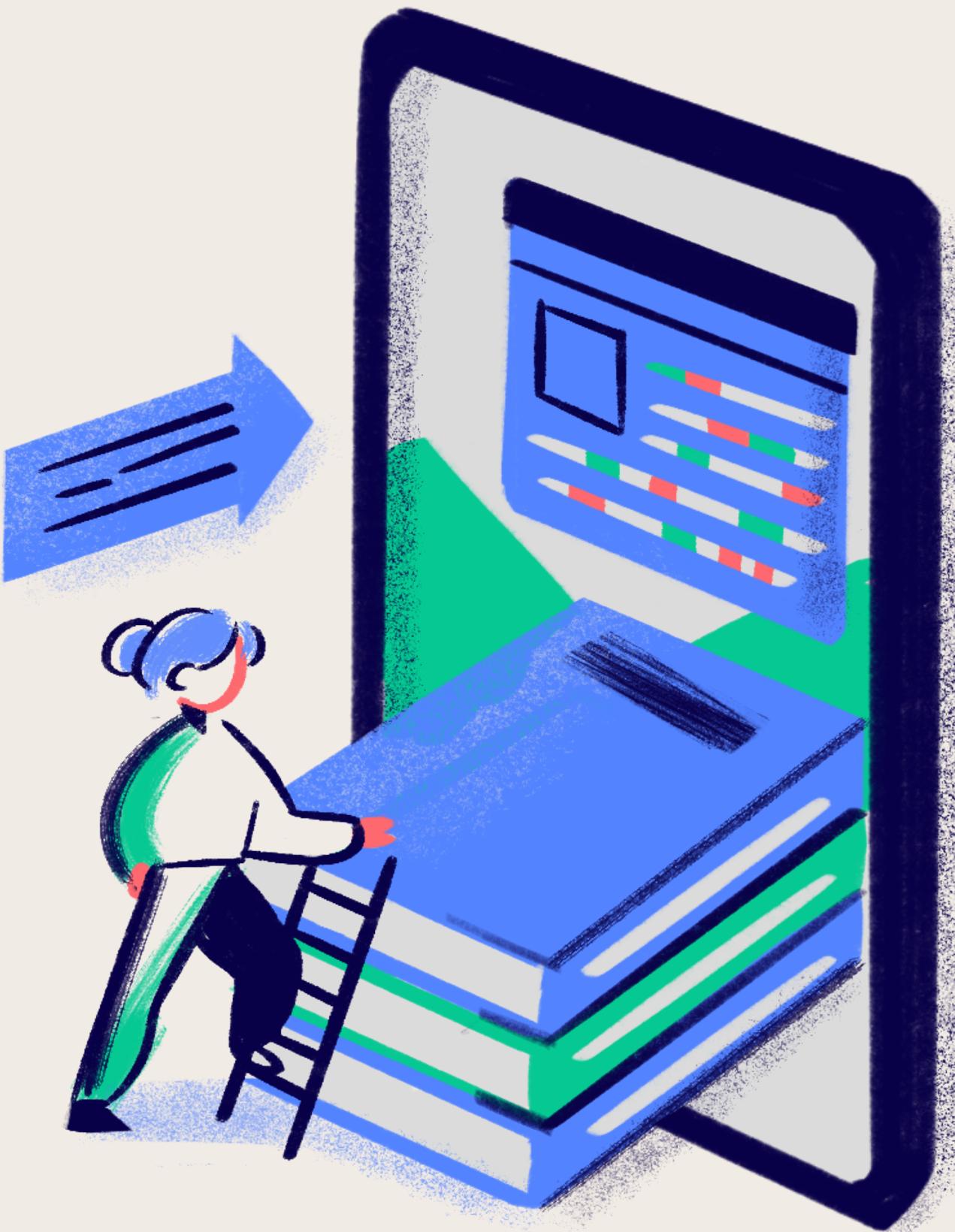
A04 INSECURE DESIGN



OWASP

Open Web Application
Security Project

ISABELLA COSTA THOMAZINI
ISABELLE FERMINO CABRIOTTI
JULIANA GIROTTO LEITE
KAMILY DE SOUZA GRACIA



INSECURE DESIGN

-----INTRODUÇÃO-----

- Nova categoria de 2021;
- Falhas de design e arquitetura;
- Uso de modelagem de ameaças;
- Padrões de design seguros;
- Arquiteturas de referência;



INSECURE DESIGN

-----DESCRIÇÃO-----

É uma categoria ampla que representa diferentes pontos fracos, expressos como "design de controle ausente ou ineficaz", mas não é a fonte de todas as outras 10 categorias de risco de segurança.

Um dos fatores que contribuem para um design inseguro é a falha em determinar o nível de design de segurança necessário.

Há uma diferença entre design inseguro e implementação insegura, pois têm diferentes causas raízes e remediação.

Um design seguro ainda pode ter defeitos de implementação que levam a vulnerabilidades que podem ser exploradas.

Um design inseguro não pode ser corrigido por uma implementação perfeita, pois os controles de segurança necessários nunca foram criados para a defesa contra ataques específicos.

SECURE DESIGN

----- DESCRIÇÃO -----

- Avaliar constantemente as ameaças ;
- Evitar métodos de ataque conhecidos;
- Determinar o fluxo correto e os estados de falha;
- Analisar suposições e condições para fluxos esperados e de falha, assegure-se de que eles ainda sejam precisos e desejáveis;
- O design seguro não uma ferramenta que você pode adicionar ao software.



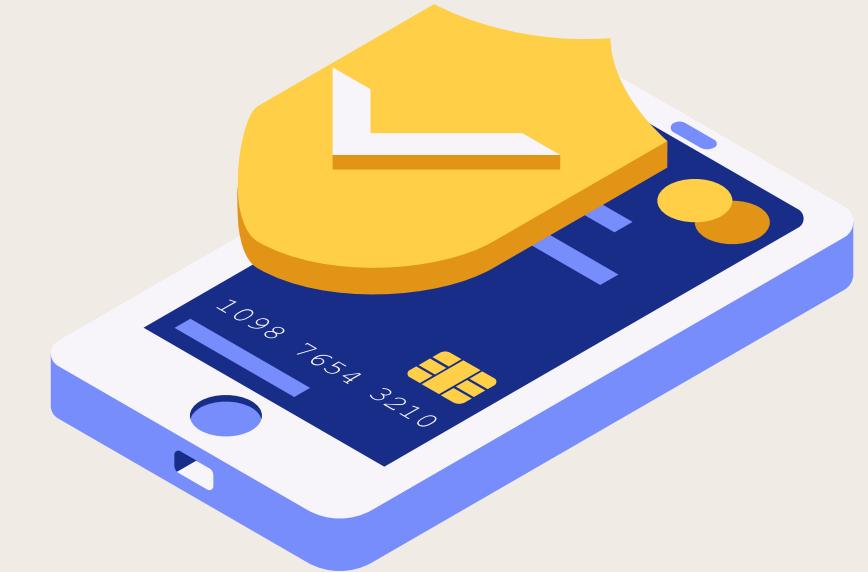
FORMAS DE PREVENÇÃO INSECURE DESIGN

REALIZAR ANÁLISES DE AMEAÇAS

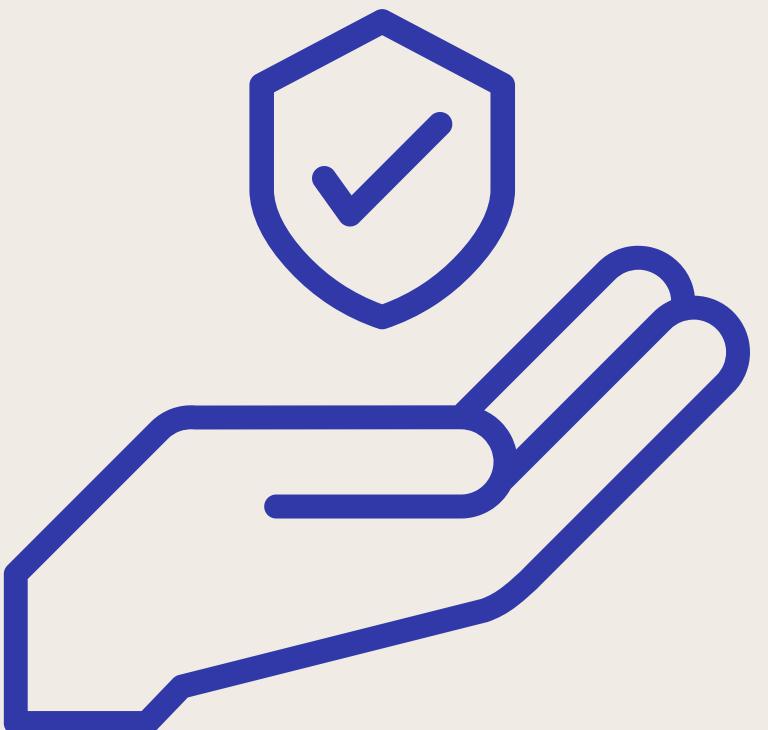
**MANTER A SEGURANÇA EM TODO
O CICLO DE VIDA DO SOFTWARE**

TESTAR DESIGNS DE SEGURANÇA

FALHAS MAIS NOTÁVEIS



- CWE-209: Geração de mensagem de erro contendo informações confidenciais;
- CWE-256: Armazenamento desprotegido de credenciais;
- CWE-501: Violação de limite de confiança;
- CWE-522: Credenciais insuficientemente protegidas.



CWE 209

GERAÇÃO DE MENSAGEM DE ERRO CONTENDO INFORMAÇÕES CONFIDENCIAIS

- Escopo: confidencialidade;
- Probabilidade de exploração: alta;



PREVENÇÃO⁵

CWE 209

GERAÇÃO DE MENSAGEM DE ERRO CONTENDO INFORMAÇÕES CONFIDENCIAIS

- Certifique-se de que as mensagens de erro contenham apenas detalhes mínimos que sejam úteis para o público-alvo e mais ninguém;
- Se os erros precisarem ser capturados com algum detalhe, registre-os em mensagens de log;
- Evite mensagens inconsistentes que possam alertar acidentalmente um invasor sobre o estado interno, como se uma conta de usuário existe ou não;
- Trate exceções internamente e não exiba erros contendo informações potencialmente confidenciais para um usuário;
- As informações de depuração não devem chegar a uma versão de produção;
- Desative exibição de erros detalhados em produção e use mensagens de erro padrão

REFERÊNCIAS

- OWASP TOP 10:2021. Disponível em:
https://owasp.org/Top10/A04_2021-Insecure_Design/
- CWE Common Weakness Enumeration. Disponível em:
<https://cwe.mitre.org/data/definitions/209.html>

**MUITO
OBRIGADA!**

