



A04:2021 – Insecure Design



Présentation d'une fiche

A04:2021 - *Insecure Design*

Factors

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit
40	24.19%	3.00%	6.46

Overview

A new category for 2021 focuses on risks related to design. To make more use of threat modeling, secure design patterns, and related tools, in the developer community we need to move beyond "shift-left" in the coding process. This is critical for the principles of Secure by Design. Notable CWEs in this category include CWE 200: Generation of Error Messages Containing Sensitive Information, CWE 201: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection), and CWE 202: Improper Neutralization of Special Elements used in a Web Browser (Cross-Site Scripting).

Sommaire



Présentation de la fiche A04	1
Contexte	2
Cas concret	3
Solutions à mettre en place	4





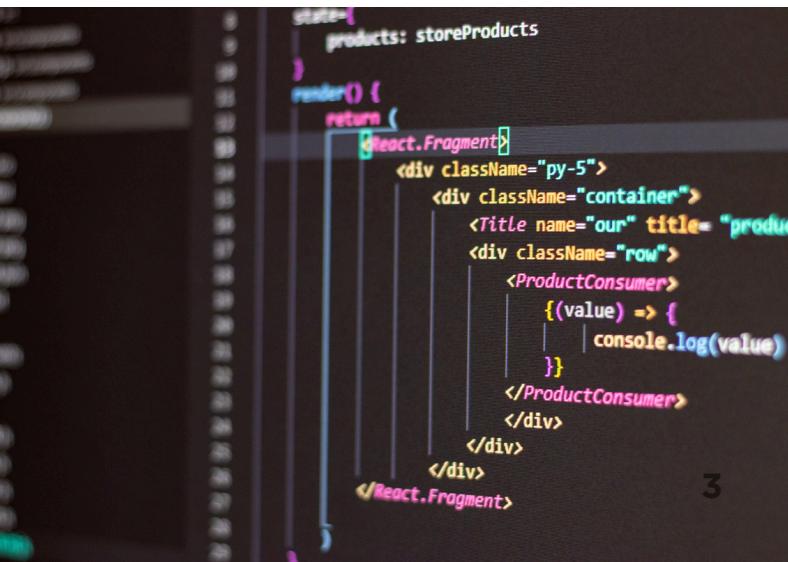
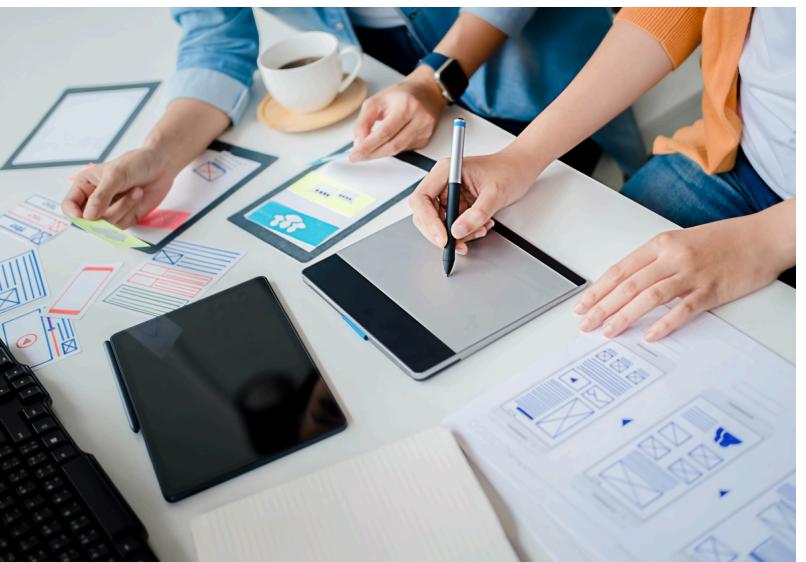
I. Présentation de la fiche A04

Créée en 2021, cette nouvelle catégorie se concentre sur les risques liés à la **conception et aux défauts architecturaux**, avec un appel en faveur d'une plus grande utilisation de la modélisation de la menace, de modèles de conception sécurisés et d'architectures de référence.

“

Il y a une différence entre la conception non sécurisée et l'implémentation peu sûre. Nous faisons la distinction entre les défauts de conception et les défauts de mise en œuvre pour une raison, ils ont des causes profondes et des mesures correctives différentes.

The screenshot shows the OWASP Top 10:2021 website with the A04:2021 – Insecure Design page selected. The page includes sections for Factors, Overview, and Description, along with a sidebar containing links to other categories like A01 Broken Access Control and A02 Cryptographic Failures.





2. Contexte

L'un des facteurs qui contribuent à l'insécurité de la conception est **l'absence de profilage des risques commerciaux inhérent au logiciel** ou au système en cours de développement, et donc à la non-détermination du niveau de conception de la sécurité requise.



Identifier

Déterminer les états de flux et de défaillance corrects, s'assurer qu'ils sont bien compris et convenus par les parties responsables et touchées.

Analyser

Analyser les hypothèses et les conditions des flux attendus et des flux de défaillance, veiller à ce qu'elles soient toujours exactes et souhaitables.

Assurer

Déterminer comment valider les hypothèses et imposer les conditions nécessaires à des comportements appropriés.

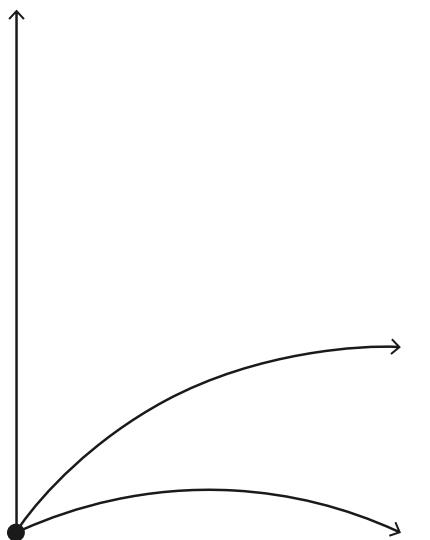
Documenter

S'assurer que les résultats sont documentés dans l'histoire de l'utilisateur.



3. Cas concret

La **conception sécurisée** est une culture et une méthodologie qui évalue en permanence les menaces et garantit que le code est solidement conçu et testé pour prévenir les méthodes d'attaque connues. La **modélisation des menaces** devrait être intégrée dans les sessions de perfectionnement (ou activités similaires); rechercher les changements dans les flux de données et le contrôle de l'accès ou d'autres contrôles de sécurité.



- **Scénario no 2 :** Une chaîne de cinéma permet des rabais de réservation de groupe et dispose d'un maximum de quinze participants. Les attaquants pourraient simuler ce flux et tester s'ils pouvaient réserver six cents sièges et tous les cinémas en même temps sur quelques demandes, entraînant une perte massive de revenus.





4. Solutions à mettre en place

Recours et négociation des exigences commerciales pour une application avec l'entreprise, y compris les exigences de protection concernant la confidentialité, l'intégrité, la disponibilité et l'authenticité de tous les actifs de données et la logique commerciale attendue.

Tenez compte de la visibilité de votre demande et si vous avez besoin d'une séparation des locataires (en plus du contrôle d'accès).

Compiler les prescriptions techniques, y compris les exigences fonctionnelles et non fonctionnelles en matière de sécurité.

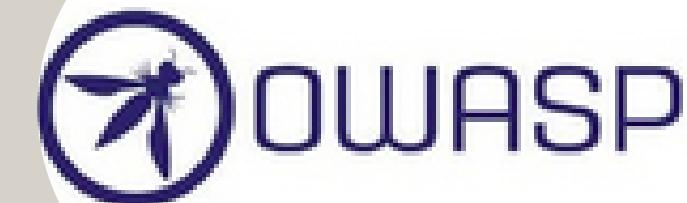


Planifier et négocier le budget couvrant l'ensemble de la conception, de la construction, des essais et de l'exploitation, y compris les activités de sécurité.



MAZ&MAR
PRÉSENTE

O W A S P A 0 4 I N S E C U R E D E S I G N



TOP10

A04:2021

Insecure Design