Menaces et risques applicatifs

[sommaire]

1. **Objectifs**

- Savoir protéger les pages web

- **Types d’attaques**

  - Le **WASC** établie dans son rapport "WASC Threat Classification" une liste exhaustive des menaces qui pèsent sur la sécurité des applications Web. Elles sont regroupées dans six catégories définies dans la version 2004 de ce rapport.

1. La catégorie **`"authentification"`** regroupe les attaques de sites Web dont la cible est le système de validation de l’identité d’un utilisateur, d’un service ou d’une application.
2. La catégorie **`"autorisation"`** couvre l’ensemble des attaques de sites Web dont la cible est le système de vérification des droits d’un utilisateur, d’un service ou d’une application pour effectuer une action dans l’application.
3. La catégorie **`"attaques côté client"`** rassemble les attaques visant l’utilisateur pendant qu’il utilise l’application.
4. La catégorie **`"exécution de commandes"`** englobe toutes les attaques qui permettent d’exécuter des commandes sur un des composants de l’architecture du site Web.
5. La catégorie **`"révélation d’informations"`** définit l’ensemble des attaques permettant de découvrir des informations ou des fonctionnalités cachées.
6. La catégorie **`"attaques logiques"`** caractérise les attaques qui utilisent les processus applicatifs (système de changement de mot de passe, système de création de compte, …) à des fins hostiles.

- **Risques de sécurité**

  - Contrairement au **WASC** qui décrit toutes les attaques possibles sur une application Web, l’OWASP ne traite que les dix plus grands risques de sécurité.
  - Le rapport "OWASP Top 10" permet ainsi à l’équipe projet de se focaliser sur la protection de l’application Web face aux menaces les plus importantes, ce qui est moins couteux et plus facilement réalisable que d’essayer de se protéger de tous les dangers. L’OWASP établit le classement 2010 ci-dessous, dont chacune des failles est développée dans les chapitres

apcpedagogie.com

suivants :

- Une faille d’injection se produit quand une donnée non fiable est envoyée à un interpréteur en tant qu'élément d'une commande ou d'une requête. Les données hostiles de l'attaquant peuvent duper l'interpréteur afin de l'amener à exécuter des commandes inhabituelles ou accéder à des données non autorisées.
- Les failles de Cross-Site Scripting (XSS) se produisent chaque fois qu'une application prend des données non fiables et les envoie à un navigateur Web sans validation. XSS permet à des attaquants d'exécuter du script dans le navigateur de la victime afin de détourner des sessions utilisateur, défigurer des sites web, ou rediriger l'utilisateur vers des sites malveillants.
- Les failles de violation de gestion d'authentification et de session se produisent quand les fonctions correspondantes ne sont pas mises en œuvre correctement, permettant aux attaquants de compromettre les mots de passe, clés, jetons de session, ou d'exploiter d'autres failles d'implémentation pour s'approprier les identités d'autres utilisateurs. Une faille de référence directe à un objet se produit quand un développeur expose une référence à une variable interne, tel un nom de fichier, de dossier, un enregistrement de base de données, ou une clé de base de données. Sans un contrôle d'accès ou autre protection, les attaquants peuvent manipuler ces références pour accéder à des données non autorisées.
- Une attaque par falsification de requête inter-sites (CSRF) force le navigateur d'une victime authentifiée à envoyer une requête http, comprenant le cookie de session de la victime ainsi que toute autre information automatiquement inclue, à une application web vulnérable. Ceci permet à l'attaquant de forcer le navigateur de la victime à générer des requêtes, l'application vulnérable considérant alors qu'elles émanent légitimement de la victime.
- Une faille due à une mauvaise configuration de sécurité se produit quand les serveurs d'application, serveurs web, serveur de base de données, et la plate-forme n’ont pas de configuration sécurisée correctement établie et déployée. Tous ces paramètres doivent être définis, mis en œuvre, et maintenu. Ceci implique de maintenir tous les logiciels à jour, notamment toutes les bibliothèques de code employées par l'application.
- Une faille de stockage de données non sécurisées se produit quand une application Web ne protège pas correctement les données sensibles, telles que les numéros de cartes de crédit, de sécurité sociale, les informations d'authentification, avec un algorithme de chiffrement ou de hash approprié. Les pirates peuvent voler ou modifier ces données faiblement protégées pour perpétrer un vol d'identité et d'autres crimes, tels que la fraude à la carte de crédit.

apcpedagogie.com

- La défaillance dans la restriction des accès à une URL se produit quand une application web ne protège pas l'accès aux URL. Les applications doivent effectuer des contrôles d'accès similaires chaque fois que ces pages sont accédées, sinon les attaquants seront en mesure de forger des URL pour accéder à ces pages cachées.
- La faille de protection de la couche transport se produit quand les applications ne peuvent pas chiffrer et protéger la confidentialité et l'intégrité du trafic réseau sensible. De plus, quand elles le font, elles supportent parfois des algorithmes faibles, utilisent des certificats expirés ou invalides, ou ne les emploient pas correctement.
- Une faille de redirection et renvoie non validés se produit quand une application Web réoriente les utilisateurs vers d'autres pages et sites web, et utilise des données non fiables pour déterminer les pages de destination. Sans validation appropriée, les attaquants peuvent rediriger les victimes vers des sites de phishing ou de logiciel malveillant, ou utiliser les renvois pour accéder à des pages non autorisées.

Correspondances entre les définitions de l'OWASP et du WASC

Risques identifiés par l'OWASP en 2010	Attaques identifiées par le WASC en 2010	Catégories
Injection	SQL Injection (WASC-19) XML Injection (WASC-23) Null Byte Injection (WASC-28) LDAP Injection (WASC-29) Mail Command Injection (WASC-30) OS Commanding (WASC-31) XPath Injection (WASC-39) XQuery Injection (WASC-46)	Exécution de commandes
Cross-Site Scripting	Cross-Site Scripting (WASC-08)	Attaques côté client
Violation de Gestion d'Authentification et de Session	Insufficient Authentication (WASC-01) Brute Force (WASC-11) Credential/Session Prediction (WASC-18) Session Fixation (WASC-37) Insufficient Session Expiration (WASC-47)	Autorisation,Authentification
Référence directe à un objet non sécurisée	Insufficient Authentication (WASC-01) Insufficient Authorization (WASC-02) Path Traversal (WASC-33) Predictable Location (WASC-34)	Autorisation,Authentification,Révélation d'informations

Risques identifiés par l'OWASP en 2010	Attaques identifiées par le WASC en 2010	Catégories
Falsification de requêtes inter-sites	Cross-Site Request Forgery (WASC-09)	Attaques logiques
Gestion de configuration non sécurisée	Server Misconfiguration (WASC-14) Application Misconfiguration(WASC-15)	Révélation d'informations
Stockage de données non sécurisé	Insufficient Data Protection (WASC-50)	Révélation d'informations
Défaillance de restriction d'accès à une URL	Insufficient Authorization (WASC-02) Denial of Service (WASC-10) Brute Force (WASC-11) Insufficient Anti-automation (WASC-21) Predictable Location (WASC-34)	Autorisation, Authentification, Révélation d'informations
Communications non sécurisées	Insufficient Transport Layer Protection (WASC-04)	Révélation d'informations
Redirection et renvoi non validés	URL Redirector Abuse (WASC-38)	Attaques logiques

Source : https://apcpedagogie.com/menaces-et-risques-applicatifs · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com