



Home

About

Content

Others

OWASP





Qu'est ce qu'OWASP

L'Open Web Application Security Project (OWASP) est une organisation à but non lucratif fondée en 2001, dont l'objectif est d'aider les propriétaires de sites web et les experts en sécurité à protéger les applications web contre les cyberattaques.



```
"container">
  <div class="row">
    <div class="col-md-6 col-lg-8"> <!--
      <nav id="nav" role="navigation">
        <ul>
          <li><a href="index.html">Home</a>
          <li><a href="home-events.html">Home Events</a>
          <li><a href="multi-col-menu.html">Multi Col Menu</a>
          <li class="has-children"> <a href="#">More Options</a>
            <ul>
              <li><a href="tall-button-height.html">Tall Button Height</a>
              <li><a href="image-logo.html">Image Logo</a>
              <li class="active"><a href="#">Active Item</a>
            </ul>
          </li>
          <li class="has-children"> <a href="#">More Options</a>
            <ul>
              <li><a href="variable-width.html">Variable Width</a>
              <li><a href="list-item.html">List Item</a>
            </ul>
          </li>
        </ul>
      </nav>
    </div>
  </div>
</div>
```



OWASP TOP 10

Les contrôles d'accès ne sont pas correctement appliqués, permettant à un utilisateur d'accéder à des ressources ou actions qui ne devraient pas être autorisées.

⚠ Exemple d'attaque

- Un utilisateur “user” accède à /admin en modifiant son URL.
- Une API renvoie les données d'un autre utilisateur.


🛡 Défenses

- Vérifier systématiquement les rôles (RBAC).
- Filtrer les accès côté serveur (pas uniquement côté front).
- Retourner 403 Forbidden lorsqu'un accès est refusé.

Broken Access Control

Mauvaises pratiques cryptographiques ou absence de chiffrement, exposant les données sensibles.

Cryptographic Failures

⚠ Exemple d'attaque

- Mots de passe stockés en clair.
- Formulaire envoyé en HTTP → interception réseau.

🛡 Défenses

- Utiliser HTTPS partout.
- Hasher les mots de passe avec bcrypt ou Argon2.
- Chiffrer les données sensibles en base (numéro de carte...).



L'attaquant insère du code malveillant dans une requête (SQL, NoSQL, LDAP, OS...).

Injection

⚠ Exemple d'attaque

- SQL Injection :
- ' OR 1=1 --



Défenses

- Utiliser des requêtes préparées / ORM.
- Valider et nettoyer les entrées.
- Ne jamais concaténer des chaînes dans une requête SQL.

Le système n'a pas été conçu avec la sécurité dès le départ : absence de règles, protections ou validations structurelles.

⚠ Exemple d'attaque

- Formulaire critique sans validation prévue au niveau du modèle.
- API qui accepte tout type de payload par défaut.



🛡 Défenses

- Modèle de données robuste + validation obligatoire.
- Threat Modeling (analyser les risques avant de coder).
- Patterns sécurisés dès la conception du projet.

Insecure Design

Les contrôles d'accès ne sont pas correctement appliqués, permettant à un utilisateur d'accéder à des ressources ou actions qui ne devraient pas être autorisées.

⚠ Exemple d'attaque

- Page d'erreur détaillée en production.
- Port sensible laissé ouvert.
- Admin panel accessible sans IP filtering.



🛡 Défenses

- Désactiver le debug en production.
- Mettre des permissions minimales.
- Vérifier régulièrement la configuration (CIS Benchmarks).

Security Misconfiguration

L'utilisation de dépendances (librairies, frameworks, packages) vulnérables.

Vulnerable and Outdated Components

⚠ Exemple d'attaque

- Version de Log4j vulnérable (Log4Shell 2021).
- Dépendances non mises à jour depuis plusieurs années.



🛡 Défenses

- Faire des audits : npm audit, pip-audit, composer audit.
- Mettre à jour régulièrement (patching).
- Éviter les dépendances non maintenues.

Mauvaises implémentations de l'authentification : mots de passe faibles, sessions mal sécurisées, brute-force possible.

⚠ Exemple d'attaque

- Un attaquant teste 1000 mots de passe par minute.
- Cookie de session sans HttpOnly / Secure.



🛡 Défenses

- Verrouillage après X tentatives.
- Cookies sécurisés : HttpOnly + Secure + SameSite.
- Timeout de session

Identification and Authentication Failures

Absence de vérification d'intégrité lors du chargement de dépendances, mises à jour, plugins ou scripts externes.

⚠ Exemple d'attaque

- CDN compromis → script modifié pour voler les données.
- Mise à jour automatique d'un package malveillant.



Software Integrity Failures



Défenses

- Utiliser SRI : integrity="sha256-..."
- Signer les mises à jour.
- Télécharger les dépendances depuis des sources fiables.

Absence de logs, logs incomplets, ou absence de surveillance permettant de détecter les attaques.

⚠ Exemple d'attaque

- Tentatives de login illimitées non enregistrées.
- Aucune alerte lors d'un comportement anormal.



🛡 Défenses

- Logs horodatés des actions importantes.
- Monitoring + alertes.
- Aucun mot de passe ou token dans les logs.

Security Logging & Monitoring Failures

L'attaquant force le serveur à faire une requête HTTP vers une adresse non prévue.

⚠ Exemple d'attaque

- L'attaquant envoie :
`http://localhost:8080/admin`
- Le serveur appelle une URL interne sensible.



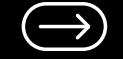
🛡 Défenses

- Limiter les URL autorisées (whitelists).
- Désactiver la possibilité de fournir une URL externe si non nécessaire.
- Filtrer les adresses IP internes.



DEMONSTRATION





CONCLUSION



THANK YOU