**Compte-Rendu de Réunion Projet OWASP 2021 vulnerabilités WEB**

**Date de la réunion :** 07/11/2024

**Participants :** **Christophe Kiennert, Gregory Blanc, Antoine Pennamen, Salma El Bougrini**

**Restitution sur le Top 10 OWASP :**

1. **Injections**
   * Dans le cadre des injections (xss) : Détourner le but de l’application web (ne renvoie plus seulement des pages mais exécute du code).
   * htmlspecialchars : vérifier si seulement 5 caractères sont échappés (< > «  ‘ &). Possible de contourner cette fonction en utilisant un autre moyen que les caractères qui sont échappés ?
2. **CSRF et Broken Access Control :**
   * Examiner la vulnérabilité CSRF dans le contexte de Broken Access Control.
3. **Vulnérable and Outdated Components**
   * La mise à jour n’est pas toujours possible, dans ce cas agir sur le code ou ajouter des filtres utilisateurs et firewall.
4. **Software and Data Integrity Failures**
   * Étudier le cas de ssl strip, MITM
   * Injection de librairies != de la vulnérabilité 6 de l’OWASP ou la librairie ne serait pas mise à jour.
5. **SSRF**
   * Type d’injection coté client dans lequel on va utiliser les privilèges de l’application web pour accéder à un service interne tiers. Donc détournement de l’utilisation de l’application.
   * Faire les labs SSRF sur PortSwigger pour mieux comprendre la vulnérabilité.
6. **Cryptographic Failures** 
   * Étudier le cas d’un détournement de certificat <https://security.stackexchange.com/questions/71208/can-any-website-secured-using-tls-can-be-impersonated-using-a-rogue-certificate>

**Prochaines Étapes :**

* + Continuer l’étude des vulnérabilités
  + Choisir les exemples à implémenter sur notre application
  + Définir des scénarios d’enchainement de l’exploitation des vulnérabilités
* **Prochaine Réunion :** Mercredi 27 novembre 2024 à 15:00 (visio)