**Thème(s):**

Quelles sont les failles de sécurité les plus courantes dans le web ?

**BONUS:**

https://www.root-me.org/

Rootme est un superbe outil afin de sensibiliser aux failles de sécurité, avec plusieurs catégories dédiées au dev web.

**I. Informations et contexte:**

**Articles utilisés**:

* https://www.clubic.com/antivirus-securite-informatique/actualite-414600-les-5-types-de-vulnerabilites-les-plus-courants-selon-trend-micro.html
* https://www.lemagit.fr/conseil/Cinq-vulnerabilites-communes-dans-les-applis-Web-et-comment-y-remedier

**Date**: 03/2022

**Mots clés**: cybersécurité, web, vulnérabilité, attaque

**II. Synthèse:**

Dans cet article, Trend Micro, un fournisseur de solutions de sécurité informatique, énumère les 5 types de vulnérabilités les plus courantes dans les systèmes informatiques. Les vulnérabilités sont des failles de sécurité qui peuvent être exploitées par des pirates informatiques pour accéder aux systèmes informatiques.

Les 5 types de vulnérabilités les plus courantes sont : les failles de sécurité de la chaîne d'approvisionnement, les vulnérabilités liées à l'exécution de code arbitraire, les vulnérabilités de l'interface web, les failles de sécurité des protocoles de communication et les vulnérabilités de la configuration des systèmes.

L'article explique chacune de ces vulnérabilités en détail, ainsi que les mesures à prendre pour les éviter ou les corriger.

Article 2:

Cet article aborde les cinq vulnérabilités les plus courantes dans les applications web et propose des mesures pour les corriger. Les vulnérabilités courantes incluent les attaques par injection SQL, les vulnérabilités XSS (Cross-site scripting), les problèmes d'authentification et d'autorisation, les vulnérabilités liées à la gestion des fichiers et les vulnérabilités CSRF (Cross-site request forgery).

L'article explique chacune de ces vulnérabilités en détail, ainsi que les mesures à prendre pour les éviter ou les corriger. Les mesures de prévention comprennent la validation des entrées utilisateur, l'utilisation de paramètres de sécurité pour la gestion des sessions, l'application de politiques de mots de passe solides et l'utilisation de mécanismes de protection contre les attaques CSRF.

En fin de compte, la prévention et la gestion des vulnérabilités dans les applications web sont cruciales pour protéger les données et les systèmes contre les cyberattaques et les failles de sécurité.

**III. Qu’en retenir ?:**

La cybersécurité est un domaine VITAL dont tout développeur devrait avoir des bases. Ces articles permettent de se rendre compte des tenants et aboutissants de ce milieu ainsi que d'apporter des réflexes simples afin de protéger ses applications des pirates.