



CYBERPHILES
Cyber Security

Intro. sécurité des réseaux - Séance 5.1

Table des matières

Sujet.....	3
Objectif	3
Consignes	3

Sujet

Objectif

L'objectif de ce projet est de développer un script automatisé permettant d'évaluer l'état de sécurité d'un site WordPress en vérifiant la version des composants (WordPress, PHP, Nginx, base de données) et en identifiant les vulnérabilités associées (CVEs). Un rapport détaillé sera affiché sur une interface web et envoyé par email à l'administrateur du site.

Consignes

Dans ce projet, les étudiants devront concevoir un script capable **d'analyser la sécurité d'un site WordPress** en se basant sur plusieurs critères. Tout d'abord, le programme devra accepter en entrée un **nom de domaine** ou une **URL** et vérifier si le site fourni fonctionne sous WordPress. S'il ne s'agit pas d'un site WordPress, un message d'erreur devra être affiché. Si aucun site n'est spécifié en entrée, le script devra demander une saisie à l'utilisateur. Ensuite, une analyse approfondie du site sera effectuée afin d'extraire **la version de WordPress installée ainsi que les versions des principaux composants du serveur, notamment PHP, Nginx et la base de données si possible**. Ces versions seront comparées avec les dernières mises à jour disponibles afin de déterminer si des mises à jour sont nécessaires.

Une fois ces informations collectées, le script recherchera les vulnérabilités connues (CVEs) associées aux versions détectées en s'appuyant sur une base de données de sécurité, telle que **WPScan ou une API de CVE publique**. Les failles de sécurité identifiées seront ensuite affichées sous forme d'un tableau récapitulatif sur une interface web. Ce tableau devra indiquer clairement les composants obsolètes et les actions recommandées pour améliorer la sécurité du site. Une fois l'audit complété, **un rapport détaillé sera généré, résumant les résultats de l'analyse ainsi que les recommandations de mise à jour**. Ce rapport devra être automatiquement **envoyé par email** à l'administrateur du site pour lui permettre de prendre les mesures nécessaires.

Enfin, pour aller plus loin, une fonctionnalité d'automatisation pourra être ajoutée en **permettant au script d'exécuter l'audit périodiquement grâce à une tâche planifiée via un cron job**. Cela permettra d'assurer un suivi régulier de la sécurité du site sans intervention manuelle. Ce projet offrira ainsi aux étudiants une expérience pratique sur l'analyse de sécurité des sites web, l'automatisation et la gestion des vulnérabilités dans un environnement réel.