Cours **Auditez la sécurité d'un système d'exploitation**

Corrigé de l'activité : **Effectuez l'audit de la configuration du serveur de base de données MariaDB sur la machine**

Pour valider la compétence, l'étudiant doit au moins avoir inclus dans son livrable

- **les 4 recommandations suivantes exécutées par le script**

Recommandation	**Type**	**Principe associé**	**Commande associée**
Vérifier la force du mot de passe de l'utilisateur SQL **root** disposant de tous les droits sur toutes les bases de données	CRITICAL	Défense en profondeur	mysqladmin password UnPasswordTresLongEtTresComplique
Vérifier que les comptes anonymes ne peuvent pas se connecter sur la base	CRITICAL	Moindre privilège	use mysql;drop user “”@”localhost”;flush privileges;
Désactiver les connexions distantes de l'utilisateur **root**	CRITICAL	Défense en profondeur	DELETE FROM mysql.user WHERE User='root' AND Host NOT IN ('localhost', '127.0.0.1', '::1');FLUSH PRIVILEGES;
Supprimer la base **test** installée par défaut	CRITICAL	Minimisation	DELETE FROM mysql.db WHERE Db LIKE 'test%'; FLUSH PRIVILEGES;

- **2 recommandations supplémentaires parmi les suivantes dont une concernant phpMyAdmin (mises en couleur dans le tableau)**

Recommandation	**Type**	**Principe associé**	**Commande associée**

Vérifier qu'il existe bien un compte SQL applicatif dédié au schéma de base de données de l'application fichesproduits	CRITICAL	Défense en profondeur	use mysql;select * from user;
Vérifier que le compte SQL applicatif dédié au schéma de base de données de l'application fichesproduits dispose des droits minimums et nécessaires sur le schéma	WARNING	Moindre privilège	*use mysql;grant select,insert,update,delete privileges on mydb.* to fichesproduits@"localhost" identified by 'motDePasseDuCompteFichesProduits';
Vérifier que le service est disponible uniquement pour les connexions locales	CRITICAL	Défense en profondeur	echo "bind-address = 127.0.0.1" >> /etc/my.cnf"
Changer le port d'écoute par défaut du service	WARNING	Défense en profondeur	echo "Port = 6033" >> /etc/my.cnf
Vérifier la gestion des fichiers de traces du service	WARNING	Minimisation	echo "log=/var/log/mysql.log" >> /etc/my.cnf
Changer l'url d'accès par défaut à phpMyAdmin	CRITICAL	Défense en profondeur	Modifier le fichier /etc/httpd/conf.d/phpMyAdmin.conf et notamment les lignes suivantes : console Alias /phpMyAdmin /usr/share/phpMyAdmin Alias /phpmyadmin /usr/share/phpMyAdmin

Désactiver la connexion du compte SQL **root** sur phpMyAdmin	CRITICAL	Moindre privilège	Modifier le fichier **/etc/phpMyAdmin/config.inc.php** et notamment la ligne suivante :
			``console
			$cfg['Servers'][$i]['AllowRoot'] = TRUE; // whether to allow root login

			``