

DOSSIER DE DOCUMENTATION TECHNIQUE & FONCTIONNELLE

Plateforme d'Entraînement et de Validation : Cyberskills

Version du document : 2.0

Statut : Livré / Conforme

Date de publication : Juin 2026

Auteur : Melvin Mage, Apprenti Administrateur Systèmes et Réseaux

1. INTRODUCTION ET VISION STRATÉGIQUE

1.1 Contexte du Projet

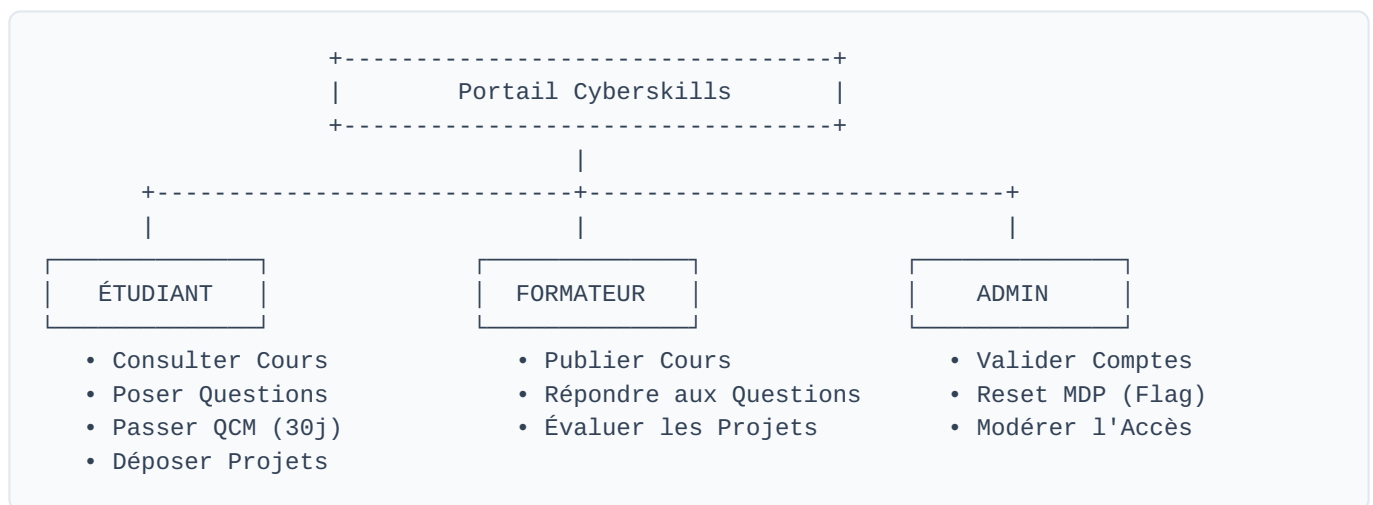
Dans un paysage technologique où les menaces informatiques évoluent de manière exponentielle, la formation pratique des futurs administrateurs et techniciens en sécurité est devenue une priorité critique. La plateforme **Cyberskills** a été conçue pour répondre à ce besoin spécifique. Il s'agit d'une application web dynamique de gestion, d'apprentissage et d'évaluation des compétences, modélisée pour s'intégrer au sein d'un cursus académique ou d'une structure de formation professionnelle en sécurité des systèmes d'information.

1.2 Objectifs RSE et Rôle de l'Application

L'application ne se contente pas de centraliser des supports de cours ; elle structure un parcours complet de validation théorique et pratique à travers un mécanisme strict d'évaluation par les pairs et par les formateurs. Elle vise à autonomiser l'apprenant tout en offrant aux équipes pédagogiques des outils de pilotage précis pour suivre l'acquisition des compétences clés du référentiel.

2. SPÉCIFICATIONS FONCTIONNELLES DÉTAILLÉES

La plateforme Cyberskills s'articule autour d'un modèle d'accès basé sur les rôles (RBAC). Chaque profil utilisateur dispose d'un périmètre d'action hermétique.



2.1 Périmètre de l'Apprenant (Rôle : Étudiant)

- **Authentification et Sécurisation** : Accès à un espace personnel après validation stricte du compte par un administrateur.
- **Consultation du Référentiel Pédagogique** : Visualisation des formations disponibles sous forme de fichiers PDF. L'étudiant dispose d'un système de filtrage dynamique lui permettant de trier les cours en fonction d'une compétence ciblée.
- **Espace d'Interaction Synchrone** : Directement sous le support de cours, l'étudiant peut soumettre une question technique contextuelle au formateur responsable du module. Il accède également à l'historique complet de ses échanges triés par ordre chronologique inversé.
- **Évaluation Théorique (QCM)** : Accès à des questionnaires d'évaluation. Le système calcule instantanément le score. En cas d'échec, un verrou informatique interdit toute nouvelle tentative sur le même module avant un délai strict de 30 jours.
- **Validation Pratique (Dépôt de Projet)** : Téléversement de livrables (rapports d'audit, scripts, livrables techniques) au format compressé ou PDF, associés à une compétence spécifique du référentiel.

2.2 Périmètre Pédagogique (Rôle : Formateur)

- **Tableau de Bord Holistique** : Vue d'ensemble des actions requises (projets en attente de correction, questions étudiantes sans réponse).
- **Gestion du Contenu (Publishing)** : Formulaire dédié permettant l'injection de nouvelles formations. Le formateur téléverse le document PDF, définit le titre et associe le module aux compétences correspondantes.
- **Modération et Support** : Interface de traitement des questions étudiantes avec un historique clair, permettant d'apporter une réponse technique qui sera immédiatement publiée sur l'espace de l'étudiant concerné.
- **Évaluation des Travaux Pratiques** : Outil de téléchargement des livrables étudiants, couplé à un système de notation binaire (Valider / Rejeter) qui met à jour le statut de la compétence de l'apprenant.

2.3 Périmètre de Contrôle (Rôle : Administrateur)

- **Gestion des Inscriptions (Gatekeeping)** : Interface de modération affichant les comptes en attente d'approbation. L'administrateur a le pouvoir exclusif de valider l'accès ou de supprimer la demande d'inscription.
- **Cycle de Vie des Comptes et Secours** : En cas de perte d'accès, l'administrateur peut déclencher une procédure de réinitialisation forcée du mot de passe, générant un jeton d'accès temporaire unique.

3. ARCHITECTURE TECHNIQUE ET SÉCURITÉ

3.1 Pile Technologique (Stack Technique)

L'application a été développée dans l'optique d'un déploiement standardisé, limitant les dépendances externes pour garantir une portabilité maximale (notamment compatible avec les environnements d'hébergement universitaires de type `public_html`).

- **Serveur Web** : Apache 2.4+ (gestion des répertoires, réécriture d'URL si nécessaire).
- **Langage Serveur** : PHP 8.x (programmation procédurale structurée, utilisation stricte de l'extension PDO pour MySQL).
- **Base de Données** : MySQL 8.0 / MariaDB 10.x.
- **Interface Graphique** : HTML5, CSS3 natif (Design System moderne basé sur le *Glassmorphism*, opacité contrôlée, filtres de flou d'arrière-plan et accents néon cyan).

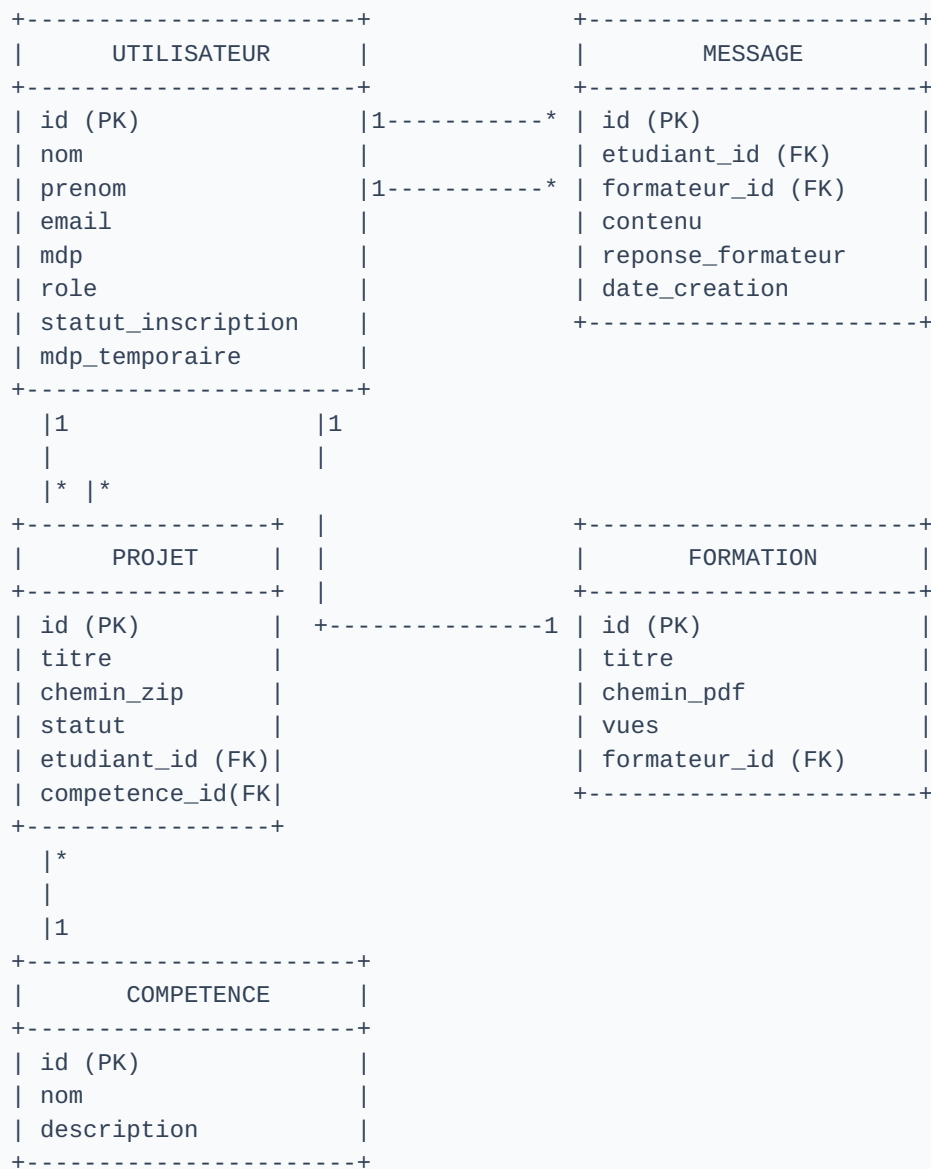
3.2 Implémentation de la Sécurité (Sécurité par Conception)

1. **Injections SQL** : Élimination totale des risques d'injection via l'utilisation systématique de requêtes préparées avec typage des paramètres (`$pdo->prepare()`), interdisant l'interprétation de code malveillant au sein des requêtes transactionnelles.

2. **Hachage Cryptographique** : Les mots de passe utilisateurs ne transitent jamais en clair et ne sont pas lisibles en base de données. Ils sont traités via l'algorithme robuste de dérivation de clé bcrypt grâce aux fonctions natives `password_hash()` et `password_verify()`.
3. **Sécurisation des Téléversements (File Upload)** : Pour éviter l'exécution de scripts malveillants (ex: webshell PHP), les fichiers téléversés par les étudiants et les formateurs subissent un traitement strict :
 - Renommage complet et aléatoire via la fonction `uniqid()`.
 - Stockage en dehors des répertoires d'exécution directe ou contrôle strict des extensions acceptées (PDF, ZIP).
4. **Cinématique du Flag de Mot de Passe Temporaire** : Lorsqu'un administrateur réinitialise un compte, le système injecte un mot de passe de secours et passe l'attribut `mdp_temporaire` à 1 en base de données. Lors de la tentative de connexion, le script `login.php` détecte ce drapeau, bloque l'accès aux fonctionnalités globales et applique une redirection logicielle stricte vers `changer_mdp.php`. L'utilisateur est contraint de soumettre un mot de passe fort d'au moins 8 caractères pour lever le drapeau (remise à 0) et accéder à son tableau de bord.

4. ARCHITECTURE DE LA BASE DE DONNÉES (SCHÉMA RELATIONNEL)

Le modèle physique des données est hautement normalisé afin de garantir l'intégrité référentielle et d'éviter toute redondance d'information.



Script d'Initialisation SQL Structurel

```

-- Création de la structure de la base de données Cyberskills
SET FOREIGN_KEY_CHECKS = 0;
DROP TABLE IF EXISTS message;
DROP TABLE IF EXISTS projet;
DROP TABLE IF EXISTS formation;
DROP TABLE IF EXISTS competence;
DROP TABLE IF EXISTS utilisateur;
SET FOREIGN_KEY_CHECKS = 1;

-- 1. Table Utilisateur
CREATE TABLE utilisateur (
    id INT AUTO_INCREMENT PRIMARY KEY,
    nom VARCHAR(50) NOT NULL,
    prenom VARCHAR(50) NOT NULL,
    email VARCHAR(100) UNIQUE NOT NULL,

```

```

    mdp VARCHAR(255) NOT NULL,
    role ENUM('etudiant', 'formateur', 'admin') NOT NULL,
    statut_inscription ENUM('en_attente', 'valide') DEFAULT 'en_attente',
    mdp_temporaire TINYINT(1) NOT NULL DEFAULT 0
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;

-- 2. Table Competence
CREATE TABLE competence (
    id INT AUTO_INCREMENT PRIMARY KEY,
    nom VARCHAR(100) NOT NULL,
    description TEXT
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;

-- 3. Table Projet
CREATE TABLE projet (
    id INT AUTO_INCREMENT PRIMARY KEY,
    titre VARCHAR(150) NOT NULL,
    chemin_zip VARCHAR(255) NOT NULL,
    statut ENUM('en_attente', 'valide', 'rejete') DEFAULT 'en_attente',
    etudiant_id INT,
    competence_id INT,
    CONSTRAINT fk_projet_etudiant FOREIGN KEY (etudiant_id) REFERENCES utilisateur(id) ON DELETE CASCADE,
    CONSTRAINT fk_projet_competence FOREIGN KEY (competence_id) REFERENCES competence(id) ON DELETE CASCADE
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;

-- 4. Table Formation
CREATE TABLE formation (
    id INT AUTO_INCREMENT PRIMARY KEY,
    titre VARCHAR(150) NOT NULL,
    chemin_pdf VARCHAR(255) NOT NULL,
    vues INT DEFAULT 0,
    formateur_id INT,
    CONSTRAINT fk_formation_formateur FOREIGN KEY (formateur_id) REFERENCES utilisateur(id) ON DELETE SET NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;

-- 5. Table Message
CREATE TABLE message (
    id INT AUTO_INCREMENT PRIMARY KEY,
    etudiant_id INT,
    formateur_id INT,
    contenu TEXT NOT NULL,
    reponse_formateur TEXT,
    date_creation DATETIME NOT NULL,
    CONSTRAINT fk_message_etudiant FOREIGN KEY (etudiant_id) REFERENCES utilisateur(id) ON DELETE CASCADE,
    CONSTRAINT fk_message_formateur FOREIGN KEY (formateur_id) REFERENCES utilisateur(id) ON DELETE CASCADE
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;

```

5. REPERTOIRE DE CODE (STRUCTURE DES PAGES CLÉS)

5.1 Fichier : `config/database.php`

Ce script établit la connexion persistante avec l'instance de base de données en appliquant des directives de sécurité strictes (activation des exceptions et désactivation de l'émulation des requêtes préparées).

```

<?php
// config/database.php

define('DB_HOST', 'localhost');
define('DB_NAME', 'cyberskills_db');
define('DB_USER', 'cyberskills_user');
define('DB_PASS', 'M0tD3P4ss3S3cur1s3!');

try {
    $options = [
        PDO::ATTR_ERRMODE            => PDO::ERRMODE_EXCEPTION,
        PDO::ATTR_DEFAULT_FETCH_MODE => PDO::FETCH_ASSOC,
        PDO::ATTR_EMULATE_PREPARES   => false,
    ];
    $pdo = new PDO("mysql:host=" . DB_HOST . ";dbname=" . DB_NAME . ";charset=utf8mb4", DB_USER, DB_PASS, $options);
} catch (PDOException $e) {
    // En production, ne jamais afficher le message brut de l'erreur (risque de fuite d'informations)
    error_log($e->getMessage());
    die("Erreur critique d'infrastructure réseau. Veuillez contacter l'administrateur.");
}

```

5.2 Fichier : pages/changer_mdp.php

Ce composant gère l'isolement et la mise à jour obligatoire des profils basculés en mode "Mot de passe temporaire".

```

<?php
// pages/changer_mdp.php

require_once '../includes/auth.php';

if (!isset($_SESSION['user_id'])) {
    header('Location: login.php');
    exit;
}

if (!isset($_SESSION['doit_changer_mdp']) || $_SESSION['doit_changer_mdp'] !== true) {
    header('Location: dashboard.php');
    exit;
}

require_once '../config/database.php';
$erreur = '';

if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $nouveau_mdp = $_POST['nouveau_mdp'] ?? '';
    $confirmation = $_POST['confirmation'] ?? '';

    if (strlen($nouveau_mdp) < 8) {
        $erreur = "Le mot de passe doit contenir au moins 8 caractères.";
    } elseif ($nouveau_mdp !== $confirmation) {
        $erreur = "Les configurations de mots de passe ne correspondent pas.";
    } else {
        $mdp_hash = password_hash($nouveau_mdp, PASSWORD_DEFAULT);
    }
}

```

```

$user_id = $_SESSION['user_id'];

$stmt = $pdo->prepare("UPDATE utilisateur SET mdp = ?, mdp_temporaire = 0 WHERE id = ?");
if ($stmt->execute([$mdp_hash, $user_id])) {
    unset($_SESSION['doit_changer_mdp']);
    header('Location: dashboard.php?msg=success_verification');
    exit;
} else {
    $erreur = "Une erreur système interne est survenue.";
}
}
}
?>
<!DOCTYPE html>
<html lang="fr">
<head>
    <meta charset="UTF-8">
    <title>Sécurisation Obligatoire - Cyberskills</title>
    <style>
        body { background-color: #0d0d15; color: #f9fafb; font-family: 'Inter', sans-serif; display: flex; align-items: center; justify-content: center; min-height: 100vh; }
        .glass-panel { background: rgba(255, 255, 255, 0.02); backdrop-filter: blur(12px); -webkit-backdrop-filter: blur(12px); border: 1px solid #f9fafb; border-radius: 10px; padding: 20px; width: 100%; }
        .input-group-reg { display: flex; align-items: center; background: rgba(255, 255, 255, 0.05); border: 1px solid #f9fafb; border-radius: 5px; margin-bottom: 10px; }
        .input-group-reg input { flex: 1; height: 100%; background: transparent; border: none; color: #f9fafb; padding: 0 10px; }
        .btn-submit { width: 100%; background: linear-gradient(135deg, #f59e0b, #d97706); padding: 10px; border: none; border-radius: 5px; color: white; font-weight: bold; }
        .btn-submit:hover { opacity: 0.9; }
    </style>
</head>
<body>
    <div class="glass-panel">
        <h2 style="color: #f59e0b; margin-top: 0;"> Mise à niveau de sécurité</h2>
        <p style="color: #9ca3af; font-size: 0.9rem; margin-bottom: 20px;"> Votre compte utilise actuellement un mot de passe faible. Nous vous recommandons de le mettre à jour pour améliorer la sécurité de votre compte. </p>

        <?php if ($erreur): ?>
            <div style="background: rgba(239, 68, 68, 0.15); border: 1px solid #ef4444; color: #fca5a5; padding: 10px; margin-bottom: 20px;">
                <strong>Erreur système</strong>: <span style="color: #fca5a5;"> <?php echo $erreur; ?>
            </div>
        <?php endif; ?>

        <form method="POST" action="">
            <input type="password" name="nouveau_mdp" required placeholder="Nouveau mot de passe (8 caractères min.)" />
            <input type="password" name="confirmation" required placeholder="Confirmez votre mot de passe" class="input-group-reg" />
            <button type="submit" class="btn-submit"> Appliquer les modifications</button>
        </form>
    </div>
</body>
</html>

```

6. MANUEL DE DÉPLOIEMENT ET D'EXPLOITATION (GUIDE TECHNIQUE)

Cette section décrit point par point les manipulations requises pour initialiser l'infrastructure de la plateforme sur un serveur de production ou de test dénué de configuration préalable.

6.1 Prérequis Système Obligatoires

Serveur Web : Apache HTTP Server 2.4.x avec le module `mod_rewrite` activé.

Moteur de Base de Données : MySQL Server 8.0+ ou MariaDB 10.4+.

Interpréteur : PHP 8.1 minimum, incluant les extensions obligatoires suivantes : `php-pdo`, `php-mysql`, `php-json`, et `php-mbstring`.

6.2 Processus d'Installation Étape par Étape

Étape 1 : Déploiement des Sources Logicielles

- Positionnez-vous dans le répertoire racine de la distribution de votre serveur web (généralement `/var/www/html/` sur Linux ou dans votre répertoire `public_html`).
- Transférez-y le dossier compressé du projet, puis extrayez-le. Le dossier racine doit être nommé explicitement `cyberskills`.

Étape 2 : Configuration des Permissions Système (Système de Fichiers)

Pour permettre aux scripts PHP de stocker de manière dynamique les documents PDF de formation et les livrables d'évaluation compressés soumis par les étudiants, les processus du serveur web doivent disposer des droits d'écriture sur les répertoires d'uploads.

```
# Attribution de la propriété des fichiers à l'utilisateur du serveur web (ex: www-data)
chown -R www-data:www-data /var/www/html/cyberskills/

# Attribution des droits d'écriture sur les répertoires de stockage
chmod -R 755 /var/www/html/cyberskills/
chmod -R 775 /var/www/html/cyberskills/uploads/projets/
chmod -R 775 /var/www/html/cyberskills/uploads/formations/
```

Étape 3 : Initialisation de l'Instance de Base de Données

- Connectez-vous à votre interface d'administration MySQL (via CLI ou PhpMyAdmin).
- Exécutez les requêtes de provisionnement suivantes pour instancier la structure de données et isoler les privilèges :

```
-- Création de l'espace de stockage logique
CREATE DATABASE cyberskills_db CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;

-- Création de l'utilisateur applicatif dédié (Moindre Privilège)
CREATE USER 'cyberskills_user'@'localhost' IDENTIFIED BY 'M0tD3P4ss3S3cur1s3!';

-- Attribution exclusive des privilèges DML et DDL sur la base de données
```

```
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP ON cyberskills_db.* TO 'cyberskills_user'@'localhost';  
FLUSH PRIVILEGES;
```

Sélectionnez la base de données nouvellement créée (USE cyberskills_db;) et importez le script d'initialisation structurel fourni à la **Section 4** du présent document.

Étape 4 : Alignement du Fichier de Configuration

Ouvrez le fichier /var/www/html/cyberskills/config/database.php et vérifiez que les constantes d'accès (DB_HOST, DB_NAME, DB_USER, DB_PASS) correspondent scrupuleusement aux identifiants configurés lors de l'étape précédente.

Étape 5 : Validation Initiale du Système

Ouvrez un navigateur internet et saisissez l'adresse URL de ciblage (ex: <http://localhost/cyberskills/index.php> ou http://server_ip/~user/cyberskills/). L'interface de la Landing Page doit s'afficher sans aucune alerte PHP ou erreur de connexion à la base de données. Vous pouvez dès lors procéder à l'inscription du premier compte de test afin de valider la cinématique globale.