



OWASP - *Secure Coding* - Rendu de projet

« MediaTek »

Livrable attendu

La *MediaTek* dans son état d'avancement, incluant, au minimum :

1. L'intégralité des éléments attendus tels que décrits dans les fiches de TP fournies durant les cours (parties « *bonus* » **non requises**) :
 - 01 - OWASP - *Secure Coding* - Entrées _ Sorties.pdf
 - 02 - OWASP - *Secure Coding* - Contrôle d'accès - Authentification.pdf
 - 03 - OWASP - *Secure Coding* - Contrôle d'accès - Autorisations.pdf
2. En complément (**obligatoire**) :
 - La fonctionnalité de suppression sur les entités **book**, **illustration**, et **user**.
 - Le remplacement de la validation et de la *sanitization* des saisies utilisateurs par la fonction **filter_input()**, sur la fonctionnalité de création d'un livre (scripts **admin/book_new_form.php** et **admin/book_new.php**), voir [PHP: Filter - Manual](#).
 - La mise en place d'une protection contre les attaques de type CSRF, sur la fonctionnalité de création d'un livre (mêmes scripts).
 - La gestion de l'ensemble des erreurs liées à MySQL via le mécanisme natif des exceptions de PHP, sur la fonctionnalité de création d'un livre (mêmes scripts), voir [PHP: Les exceptions - Manual](#).
 - La journalisation des erreurs « *techniques* » dans un fichier **var/log/error.log**, sur la fonctionnalité de création d'un livre (mêmes scripts), voir [PHP: Gestion des erreurs - Manual](#).
 - La journalisation des tentatives d'accès non autorisées dans un fichier **var/log/access.log**, sur la fonctionnalité de création d'un livre (mêmes scripts), voir [PHP: Gestion des erreurs - Manual](#).

3. IMPORTANT :

- Un fichier `README.md`, situé à la racine de votre projet, détaillant (voir [template](#) ci-dessous) :
 - L'état d'avancement de votre projet *MediaTek*.
 - Les difficultés rencontrées et les solutions appliquées.
 - Le bilan en termes d'acquis.
 - Toute remarque complémentaire qui vous semble pertinente.
- Un export de la base de données (structure et données comprises) au format `.sql`, à enregistrer dans le dossier `stuff/db/` et nommé `mediatek_eval.sql`.

Modalités de rendu

- Mise à disposition d'un lien vers un dépôt Git public¹ (GitHub, Bitbucket, ou autre) : compléter le tableau ci-dessous dans la partie [Rendus](#).
- Pour le **mercredi 9 avril 2025 23:59:59** au plus tard.

¹ Ou privé, à condition de m'inviter à rejoindre le projet (n.brousse@gmail.com).

Rendus

Étudiant	E-mail	Lien vers le dépôt Git
CAILLAUD Elie	elie.caillaud@efrei.net	
CHEBBI-VIGNEAU Maël	mael.chebbi--vigneau@efrei.net	
FARE-BREDIN Ahuarii	ahuarii.fare-bredin@efrei.net	
FERNANDEZ PUENTE Nathan	nathan.fernandez-puente@efrei.net	
GAMIN Mathis	mathis.gamin@efrei.net	
GARNERO NGUYEN Clément	clement.garnero-nguyen@efrei.net	
GILLOT Robin	robin.gillot@efrei.net	
LAFON William	william.lafon@efrei.net	
LESTAGE Yann	yann.lestage@efrei.net	
PRUNET--BOUTRIN Kevin	kevin.prUNET--boutrin@efrei.net	
ROSMANINHO HENRIQUES Ricardo	ricardo.rosmaninho-henriques@efrei.net	
ROZE Loan	loan.roze@efrei.net	
RUSSIAS Esteban	esteban.russias@efrei.net	
ZANATTA Raphaël	raphael.zanatta@efrei.net	

Template README.md

```
# Projet « MediaTek »

## État d'avancement

- TPs 01 à 03
  - [ ] CR(U)D `Book` avec validation / *sanitization*
  - [ ] CR(U)D `Illustration` avec validation / *sanitization*
  - [ ] CR(U)D `User` avec validation / *sanitization*
  - [ ] Authentification standard
  - [ ] MFA simple (au moyen de la fonction `fakeMailSend()` )
  - [ ] *Refactoring*
  - [ ] Script `env.php` protégé
  - [ ] Script `utils/db_connect.php`
  - [ ] Gestion des autorisations côté *front*
  - [ ] Gestion des autorisations côté *back*
- Complément (**obligatoire**)
  - [ ] Validation et *sanitization* via la fonction `filter_input()`
  - [ ] Protection CSRF
  - [ ] Gestion des exceptions liées à MySQL
  - [ ] Journalisation des erreurs *« techniques »*
  - [ ] Journalisation des accès non autorisés
- Autres
  - [ ] À compléter, si besoin

## Difficultés rencontrées et solutions

À compléter

## Bilan des acquis

- À compléter
- À compléter
- À compléter
- Etc.

## Remarques complémentaires
```

À compléter, si besoin.

Contact

Si besoin, ne pas hésiter à me contacter :

- Par mail : n.brousse@gmail.com
- Via Discord : [_el.profesor_](#)