Syllabus projet

Année : **2025-2026**

Enseignant(s)	Email(s)
DETROY Kevin	kdetroy1@myges.fr

Projet Final

1 Matières, formations et groupes

Matière liée au projet :

Formations : -

Nombre d'étudiant par groupe : **1 à 3**

Règles de constitution des groupes: **Libre**

Charge de travail estimée par étudiant : **20,00 h**

2 Sujet(s) du projet

Type de sujet : **Imposé**

Créez un pipeline CI/CD complet avec une simple application Python. Réaliser des challenges de sécurité Web offensive.

Partie 1 > réaliser la partie CI/CD via les instructions du fichier "Consignes CI-CD" et la base "Resources".

Créez un pipeline CI/CD complet pour une application Python simple à l'aide de GitHub Actions.

Votre pipeline doit :

Exécuter des tests sur plusieurs versions de Python.

Exécuter une analyse de vulnérabilité Trivy.

Créer et pousser une image Docker vers Docker Hub.

Je vous fournirai un répertoire contenant un code Python simple. Vous pouvez réaliser votre projet à partir de celui-ci, mais vous n'obtiendrez pas la meilleure notation.

Pour obtenir plus de points, n'hésitez pas à prendre un autre code d'application web vulnérable ou le vôtre (implémentation d'une SQLi, Path Traversal, etc.), y exécuter les tests, le CI/CD et à mettre en œuvre les mesures de sécurité liées à ce que Trivy a détecté.

Partie 2 > réaliser les challenges suivants:

https://portswigger.net/web-security/file-path-traversal/lab-validate-file-extension-null-byte-bypass

~~https://www.root-me.org/fr/Challenges/Web-Serveur/PHP-Filters~~

~~https://www.root-me.org/fr/Challenges/Web-Client/CSRF-contournement-de-jeton~~

~~https://portswigger.net/web-security/csrf/bypassing-token-validation/lab-token-not-tied-to-user-session~~

~~https://portswigger.net/web-security/csrf/bypassing-referer-based-defenses/lab-referer-validation-depends-on-header-being-present~~

~~https://www.root-me.org/fr/Challenges/Web-Serveur/JWT-Jeton-revoque~~

https://www.root-me.org/fr/Challenges/Web-Serveur/SQL-injection-Error

https://www.root-me.org/fr/Challenges/Web-Serveur/Injection-de-commande-Contournement-de-filtre

https://www.root-me.org/fr/Challenges/Web-Client/XSS-Stockee-2

https://portswigger.net/web-security/server-side-template-injection/exploiting/lab-server-side-template-injection-in-an-unknown-language-with-a-documented-exploit

https://www.root-me.org/fr/Challenges/Web-Serveur/API-Mass-Assignment

Un fichier .md attendu pour les challenges.
Pour chaque challenges:
- Le nom/l'URL
- Les étapes de découvertes de la vulnérabilité
- Le payload utilisé + un screenshot
- Les recommandations pour sécuriser cette vulnérabilité et une référence (un lien) d'où vous avez trouvé ces recommandations

Lors de la soutenance vous présenterez sous forme d'un PPT votre CI-CD et je vous interrogerai sur différents challs en live.

3 Détails du projet

Objectif du projet (à la fin du projet les étudiants sauront réaliser un...)

> Créez un pipeline CI/CD complet avec une application Python simple.
> Réaliser des challenges de sécurité Web offensive.

Descriptif détaillé

Ouvrages de référence (livres, articles, revues, sites web...)

Outils informatiques à installer

4 Livrables et étapes de suivi

5 Soutenance

Durée de présentation par groupe : **12 min** Audience : **A huis clos**

Type de présentation : **Présentation / PowerPoint**

Précisions :