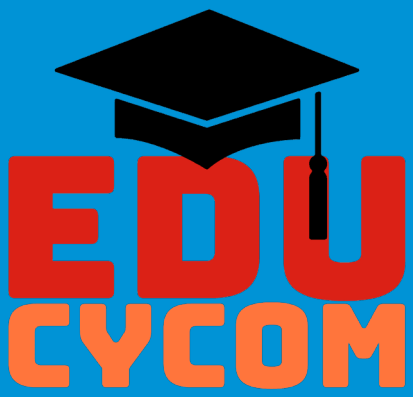
{EPITECH}

HACKATON EDUCYCOM 2025

BUG BOUNTY “ADISTA”



HACKATON EDUCYCOM 2025

Objectif

L'objectif du Hackathon est de **développer un outil d'audit et de détection de vulnérabilités, intégrant une brique d'IA pour l'analyse et/ou le reporting**.

Pour tester la qualité de l'outil développé, notre partenaire Adista met à disposition *ses propres serveurs de production*, sur le domaine suivant : `adista.fr` (les sous-domaines peuvent bien entendu être considérés).

L'objectif est que l'outil développé permette de scanner ces serveurs, et fournisse un rapport d'audit qualitatif à l'utilisateur.

Les meilleurs d'entre vous trouveront peut-être même des vulnérabilités !

Il y a donc 3 éléments évalués dans ce Hackaton :

- ✓ La capacité à réaliser manuellement un audit de sécurité sur un serveur de production, et éventuellement détecter des vulnérabilités ;
- ✓ La capacité à développer un outil permettant d'automatiser ce processus ;
- ✓ La capacité à utiliser une brique d'IA dans l'outil développé, pour augmenter les étapes d'analyse ou de reporting.

Modalités

Les étudiants devront s'organiser en groupes de 4 à 5 personnes pour relever ce défi.

- ✓ **Horaires du Hackathon** : 11h00 -> 17h00, soit **6h**
- ✓ **Évaluation par le jury** : 17h00 - 17h30
- ✓ **Annonce des résultats** : 17h45

Critères d'évaluation

Le jury évaluera les projets sur les critères suivants :

- ✓ **Qualité du rapport d'audit** : clarté, précision et exhaustivité du rapport.
- ✓ **Criticité des vulnérabilités trouvées** : importance et impact des vulnérabilités identifiées.
- ✓ **Pertinence de l'utilisation de l'IA dans la solution**.

Utilisation de l'IA

Pour faciliter l'intégration de la brique d'IA dans votre outil, une clé *OpenAPI* sera mise à disposition pour la durée de l'événement. Cette clé sera remise à chaque chef de groupe au début du Hackathon. Nous vous demandons d'utiliser cette ressource de manière raisonnable.

Recommandations et Conseils

Utilisation d'outils existants

Les participants sont bien entendu encouragés à réutiliser et s'appuyer sur des logiciels et outils existants.

Serveurs de tests en local

Compte tenu de la nature des serveurs mis à disposition (en production, donc potentiellement bien protégés), les participants sont encouragés à développer et tester leur outil en premier lieu sur des applications volontairement non sécurisées, utilisables localement.

En voici quelques exemples :

- ✓ **Google Gruyère** : `https://google-gruyere.appspot.com/`
- ✓ **Juice Shop** : `https://hub.docker.com/r/bkimminich/juice-shop`

Pour vous faciliter la tâche, vous trouverez dans ce dépot des scripts permettant de lancer localement ces applications (prérequis : système Ubuntu et Docker).

À noter que *Google Gruyère* peut également être instancié en ligne directement depuis le site (vous aurez alors une instance de l'application dédiée en ligne sans besoin d'installation locale).

Resources documentaires

Il existe de nombreuses resources sur Internet couvrant un large panel de pratiques offensives.

À titre d'exemple :

- ✓ `https://github.com/swisskyrepo/PayloadsAllTheThings/`
  - Plus particulièrement, la section *XSS Injection*

Méthodologie de travail

Pour optimiser le travail, nous recommandons aux groupes de diviser leur équipe en 3 sous-équipes :

- ✓ 2 étudiants sur l'analyse manuelle des vulnérabilités trouvées sur les serveurs de production d'Adista.
- ✓ 1 - 2 étudiants sur le prototypage d'outil, en utilisant les applications non sécurisées en local dans un premier temps, puis sur les serveurs d'Adista lorsque la première sous-équipe a déja pu faire un premier état des lieux (cf. que chercher ? où chercher ? etc.).
- ✓ 1 - 2 étudiant sur l'intégration de l'IA.

Une communication efficace entre ces 3 sous-équipes est essentielle pour réussir !

C'est parti !

Nous vous souhaitons à tous un excellent Hackathon ! Que les meilleurs gagnent, et surtout, que cette expérience soit enrichissante et formatrice pour chacun d'entre vous.

v1