Comment faire du Hack éthique avec ChatGPT

Hacking automatisé assisté par IA

Dans cette vidéo, nous allons vous montrer comment j’ai réussi à trouver une faille dans un centre hospitalier en utilisant l’IA pour m’aider.

Qu’est-ce que le hacking assisté par IA ?

Le hacking assisté par IA est une technique qui consiste à utiliser l’IA pour comprendre le code et trouver des failles plus facilement. Il y a tellement de langages différents, de frameworks et de bibliothèques que ce n’est pas possible d’être expert immédiatement dans tous les domaines. Il est donc important de savoir comment optimiser sa productivité en donnant à l’IA les bribes de code pour qu’elle nous explique en anglais le code.

Comment j’ai utilisé l’IA pour trouver une faille

J’ai installé un plugin public sur WordPress pour un site d’un centre hospitalier et je suis allé directement voir le code. J’ai demandé à l’IA de m’expliquer le code en PHP de WordPress. L’IA m’a alors généré une explication détaillée sur le fonctionnement du code, ce qui m’a permis de comprendre les différentes fonctions et de trouver des failles

d’autorisation, d’injection et de peinture dans le code.

Par exemple, l’IA m’a expliqué qu’il y avait un paramètre Q dans la requête qui pouvait être modifié par l’utilisateur, ce qui pouvait entraîner une injection SQL. L’IA m’a même écrit que c’était peut-être possible, sans que je le lui demande. J’ai alors demandé à l’IA de m’écrire la requête SQL que je devrais faire pour vérifier s’il y avait une faille et c’était la bonne requête pour identifier une injection.

Rapport de bug Bounty

Une fois que j’ai constaté la faille de sécurité, j’ai demandé à l’IA de générer un rapport de bug Bounty. Le rapport était très proche de ce que nous envoyons habituellement. Il est important de savoir que ce type de faille est très basique et qu’il serait possible de trouver des failles plus difficiles en utilisant cette technique.

En conclusion, le hacking assisté par IA peut être très utile pour trouver des failles dans le code. En utilisant l’IA pour comprendre le code, nous pouvons optimiser notre productivité et trouver des failles plus facilement.