Comment gagner 42 000$ avec ChatGPT ?

Cette vidéo YouTube intitulée “Comment gagner 42 000$ avec ChatGPT ?” est une excellente façon de découvrir comment gagner de l’argent en ligne. Elle explique comment utiliser un service appelé ChatGPT pour générer des revenus en ligne. La vidéo donne des conseils sur la façon dont vous pouvez gagner des revenus en ligne et sur les différentes façons dont vous pouvez le faire. Elle explique également comment vous pouvez utiliser le service ChatGPT pour gagner de l’argent et comment vous pouvez le faire facilement et efficacement. Si vous êtes à la recherche d’une façon de gagner de l’argent en ligne, cette vidéo est un excellent moyen de commencer.

Ce transcription décrit une démonstration d’un outil d’IA appelé “Open Air” qui aide les chercheurs en cybersécurité à trouver des failles de sécurité dans le code. L’outil aide à identifier les failles d’autorisation d’injection et de peinture et peut même générer des rapports de bug bounty. Il est montré que l’outil a été utilisé pour trouver une faille dans un centre hospitalier et une faille sur Facebook qui a valu 42 000 dollars à un chercheur. Le conseil à appliquer lors de l’utilisation de l’outil est de donner un contexte clair à l’IA et de lui expliquer ce que l’on veut accomplir.

Source : UCWedHS9qKebauVIK2J7383g | Date : 2023-01-16 19:56:39 | Durée : 00:11:56

➡ Accéder à CHAT GPT en cliquant dessus

Voici la transcription de cette vidéo :

On va vous montrer très concrètement comment j'ai pété 3 a réussi plus ou moins à trouver une faille dans un centre hospitalier Ronnie c'est grâce à toi qu'on peut montrer tout ça puisque donc tu es accurétique juste avant qu'on parle du coup de ce hacking automatisé
Est-ce que tu peux nous expliquer à quoi ça ressemble très concrètement du hacking assisté par Ia en fait un truc qu'on adore faire quand on est en bug Bounty c'est de passer en boîte blanche directement ça veut dire que au lieu de faire des tests à distance on va aller

Lire le code pour mieux comprendre ce qui se passe dans le code et finalement pouvoir trouver des failles plus facilement le truc c'est qu'il y a tellement de langages différents de framework de librairie que on peut pas être expert tout de suite sur tous les langages il faut avoir vraiment pas mal

D'expérience il faut connaître tout ça et je me suis dit est-ce que je peux optimiser ma productivité en donnant le les bribes de code à open air et je lui laisse m'expliquer en anglais le code et du coup là je lui dis bon bah explique-moi du code en PHP d'un

WordPress ils ont des plugins sur WordPress qui totalement public j'ai installé le plugin et je suis directement allé voir le code et du coup là c'est vraiment le site d'un centre hospitalier et je lui ai dit bah tu es un pentastur tu dois m'assister dessus et il m'a généré du coup ce magnifique

Pavé et du coup il m'explique que ça sert à chercher des noms d'utilisateurs dans une base de données en SQL après ce que je

lui ai demandé c’est est-ce que tu peux m’expliquer si le code interprète une action d’un utilisateur en fait c’est hyper important parce que

On a ce concept qui est de source et de Sync donc en fait on va essayer de voir le code comme un entonnoir c’est à dire qu’est-ce que l’utilisateur peut faire qu’est-ce qu’on lui donne accès et cet accès où est-ce qu’il va dans le code et

Dans quelle fonction il est en train de rentrer et en fait par rapport aux accès qu’on a en train de donner à l’utilisateur ben on va pouvoir manipuler le code et trouver des failles d’autorisation d’injection et de peinture comme ça et effectivement bah comme on le voit à l’écran il me dit bah

Oui il y a un paramètre Q qui est dans la roquette que l’utilisateur peut modifier et ce paramètre va après dans une fonction qui s’appelle stripslash et stripstash tout ce qui est fait c’est enlève les backslash de la chaîne de caractères du texte et ce qu’il faut savoir c’est

Qu’il m’a même écrit que il y avait peut-être possibilité qui est une injection SQL ça veut dire que on peut éditer la requête SQL pour demander ce qu’on veut à la base de données on a fait tout seul si il y a même pas demandé si c’était possible qu’il me l’avait

Déjà écrit il y a peut-être moyen que ce soit possible du coup je lui ai dit ok écris-moi la requête SQL que je devrais faire et c’est exactement la bonne requête pour identifier une injection actuelle et du coup à partir de ce moment là j’ai pu vérifier moi en

Tant que cumin que voilà je constate il y a une faille de sécurité et je lui ai dit bon bah maintenant génère moins un beau rapport de bug Bounty comme ça j’ai vraiment mais rien à faire et voilà imaginera un rapport qui est très proche de nous ce qu’on envoie ce qu’il faut

Savoir c’est que ça c’est vraiment faille hyper hyper basique est-ce que ça marcherait pour des failles dures ou qui valent beaucoup entre guillemets et bah c’est exactement la question que que je me suis posée pour cette chronique et du coup j’ai voulu retrouver une faille sur Facebook que un chercheur qui s’appelle

Youssef Saouda que j’adore je l’ai rencontré il est génial il est trop bon techniquement il a trouvé une faille sur Facebook qui lui a valu 42000 dollars parce que clairement l’impact de cette faille c’est il a réussi à prendre contrôle de n’importe quel compte facebook si tu cliques sur son lien ok

Pas donc concrètement le gaz c’est vraiment il est trop fort et il a expliqué dans dans un article voilà comment j’ai réussi à hacker Facebook je veux savoir c’est que ce gars il a pas une fois Facebook il est premier du top leader bar du bug Bounty de Facebook je

Crois que il a mis un tweet très récemment il a trouvé 4 fail l’année dernière il a fait 450 000 dollars donc voilà le gars c’est un turbocrac et du coup dans son article il montre un code javascript donc le code qui a vraiment dans ton navigateur de Facebook et ça

Ressemble à ce pavé là concrètement c’est du code qu’on appelle minifier donc en gros le le développeur n’a pas du tout écrit ça c’est un système une moulinette qui a tout réduit condensé réduit les variables etc c’est ça mais du coup à lire c’est un femme du coup je

Me suis dit est-ce que au penaille pourra m’aider à trouver la faille dans ce code et du coup je lui ai dit vas-y explique-moi le code et très surprenant il m’a dit exactement ce qu’il faisait exactement ce qui est décrit d’ailleurs dans l’article et j’ai trouvé ça inside

Parce que concrètement là j’ai plus besoin de lire du code minifié ça veut dire de vraiment mettre un des bugger

comprendre que ok là c'est telle variable qui rentre dans tel truc tout ça qui peut être hyper soporifique là je me suis enlevé une heure à deux heures

De de mon temps et derrière je lui ai dit bon bah simplifie moi le code pour que je peux puisse lire humainement et imaginez un code qui est vraiment très très proche de la réalité ou en tout cas c'est la même algorithmie derrière et du coup la faille je vais pas rentrer dans

Les détails mais en gros c'était vérifier l'origine d'une requête pour savoir s'il y a tel domaine avait le droit de faire une roquette sur un autre domaine et je lui ai dit maintenant est-ce que tu peux me générer le code malveillant qui aurait pu exploiter la faille de sécurité et effectivement il

M'a généré quelque chose qui est très très très proche de ce qui est dans l'article là ça veut dire que j'ai pété avec le même bout de code que ce chercheur de malade mental a réussi à produire le code malveillant pour exploiter une faille qui vaut 42 dollars

Mais du coup j'ai parlé à Youssef sur Twitter de cette faille et il m'a dit en effet il y a pas il a pas tout le contexte de comment Facebook fonctionne tout le truc interne tout ça et peut-être qu'avec plus de discussion on aurait pu arriver à un résultat plus

Probant mais par contre un truc qu'on a réussi à noter et c'est un peu notre conclusion c'est super bien juste pour déblayer tous les trucs chiants que nous on veut pas faire j'ai l'impression qu'il y a un peu ce truc avec chat GPT ou il y a des formulations des choses

Comme ça qui vont vous donner beaucoup de résultats et d'autres non est-ce que vous avez un exemple de conseil à appliquer quand on utilise le chat j'ai pété [Rires] on en a plein là récemment j'ai vu un gars sur Twitter que j'ai heurté

parce que c’était insane où il l’a expliqué en

Fait plein de de petits points ou par exemple tu expliques l’objectif dès le début de ce que tu veux faire tu dis toi tu es un pentasteur toi tu es un cuisinier Top Chef tout ça et je veux que tu me fasses une recette gastronomique trop bonne et en fait il

Faut que tu lui donnes un contexte de qui il est effectivement tu as fait ça sur un des captures d’écran tu dis ça tu es un assistant qui m’aide à faire de la cybersécurité c’est comme ça l’huile comprend c’est quoi son objectif parce que si je lui dis juste explique-moi ce

Code et après je lui dis trouve la faille de sécurité bah déjà son truc éthique il va me dire bah non c’est mort et deux après peut-être qu’il va essayer de te trouver un truc même s’il existe pas et du coup il est généraliste un peu

Et là tu es spécialise dans son objectif nous je pense qu’aujourd’hui on a l’habitude de faire des requêtes qui sont assez simplifiées où on va direct droit gros but alors qu’en fait avec lia il faut lui donner du contexte mais il faut aussi préciser un peu comment tu

Veux qu’elle formule sa réponse et tu peux même moduler le vocabulaire qu’elle va utiliser ou ou le niveau de d’expertise par exemple de vulgarisation que tu veux genre par exemple moi si je veux écrire un truc ultra technique sur une techno comme comme tu disais tu vas

Introduire avec une phrase du style tu es expert en ça mais après tu peux lister comment tu veux caractériser ta réponse par exemple tu peux tu peux lui dire fais-le dans le ton d’un article d’accord ou fais-le comme si t’écrivais un rapport d’expertise et en fait ça

Modifie son style ça modifie les mots qui l’emploi enfin je trouve ça ultra incroyable vous entendez par exemple dire que

il fallait pas trop lui demander 5 exemples de quelque chose il faut que je dise quoi alors si on veut un peu comprendre le truc c’est que

Chaque mot va être égal à des points et ces points là il va les mettre dans une dimension et en gros il va essayer de trouver le chemin de probabilité dans ces points là par rapport au point il va te dire bah lui ce qui est ce qui me

Demande dans la dimension que j’ai créée c’est on sait pas trop comment il fait pour chercher là dedans c’est pas pourquoi il arrive à ce résultat mais il arrive à ce résultat là et en gros quand tu lui dis je veux que tu me fasses 5

Points bah tu vas lui créer plus de points alors que si tu lui dis juste je veux que tu brainstorm il a la capacité de comprendre ce qui est un brainstorm et du coup il va peut-être en générer 10 et toi tu prends juste ce que je préfère

En gros tu as réussi à simplifier ta demande pour GPT et finalement il va avoir des résultats beaucoup plus pertinents que si il s’auto bride a déjà comprendre le concept de devoir se limiter à 5 tu vois c’est facile à comprendre mais pas très facile c’est

Très Astrid je valide il y a aussi que de base on va tous poser plus ou moins les mêmes questions tu vois par exemple si tu dis à 10 personnes dans une pièce bah chercher des idées pour faire un gâteau de Noël par exemple et ben les

Gens plus ou moins tous formulé la question pareil et du coup tu vas avoir des réponses qui sont très mainstream comme tu disais tu vois c’est pas satisfaisant très novatrices c’est toujours des avis consensuels tu vois il y a une notion de ok bon alors tu vas aimer le prochain tricks

Alors que tu peux le pousser tu vois en fait tu peux lui dire propose-moi une recette de gâteau de Noël mais original enfin tu vois ou alors tu lui dis tous les trucs que tu veux pas

genre fais quelque chose de d’original ou alors c’est quelque chose que personne n’a

Jamais encore proposé quelque chose comme ça et là il va sortir de comme tu disais de son nuage probabilité de réponse possible et il va essayer de proposer de nous des nouvelles choses et en fait c’est comme ça que tu peux essayer d’enrichir ton échange et il y a

Aussi un autre truc que j’ai remarqué c’est quand tu poses une question et que la réponse ne te satisfait pas souvent à des gens ils fraîche le pompe et il recommence depuis le début non en fait c’est mieux que tu le corriges ok pendant la conversation et lui du

Coup il va s’inspirer de ton contexte en fait de la croissance que vous avez eu avant et tu dis non non tu m’as proposé ça mais en fait je veux pas que tu me le proposes comme ça je veux que ce soit plutôt comme ça tu vois ah il est

Meilleur si tu as donné un exemple négatif avant en fait tu peux le corriger au fur et à mesure faites lui tu vas le pointer en fait vers ce que tu veux et du coup il va plus ou moins ignorer d’autres endroits de l’espace où il pourrait te proposer des choses mais

Il comprend que c’est pas ce que tu veux mais tu vois moi un truc qui me frustre énormément c’est quand par exemple je lui demande d’écrire des rapports des mails ou des trucs comme ça il me gère toujours avoir un style d’écriture qui est lambda je sais pas corpo chien par

Contre il y a une machine il y a c’est très bien il y a une technique de dingue plus que juste dire il faut que ça soit fan il faut que ça soit ça tu donnes un texte que toi tu as déjà écrit et tu dis analyse moi ce texte et dis-moi quels

Sont les styles d’écriture de ce texte et après tu lui dis écris-moi cette phrase là dans ce style d’écriture et du coup

ce qui moi je vais créer un script de vidéo actuellement il me ferait un truc ennuyeux à mourir sur un ton très corporate je pourrais lui dire analyse

Moi du coup un extrait de vidéo que j'ai déjà écrit et décris-moi dans quel style il est exactement lui me gênait un pavé et ça après ça me sert de réflexion et je peux lui redonner toutes les prochaines fois pour avoir le style d'écriture par exemple un truc qui est recommandé

Par l'équipe de PNL dans leur documentation c'est si tu veux lui faire générer des listes ou des trucs comme ça qui ont un algo un peu spécial par exemple ordonne-moi cette liste de telle manière bah d'abord donne-lui un exemple et un résultat et tu dis ça c'est les

Résultats attendus et après donne-lui un autre jeu de données et en fait il va automatiquement chercher le raisonnement entre le premier jeu de données et le résultat pour refaire l'expérience expliquer par l'exemple et en fait c'est bien plus simple pour une niaque si toi humain tu essaies de t'expliquer

Exactement ce que tu veux quoi très très stylé ronik que vous avez entendu dans cette vidéo à une fâcheuse réputation auprès de grandes marques comme Epic Games tout simplement parce que il passe son temps à trouver des failles dans leur système il nous avait raconté tout ça c'était hyper intéressant dans cette vidéo