+--------------------+
| CYBERGUARD |
| CONSULTING |
+--------------------+

Adresse : 123 Avenue de la Sécurité, 75000 Paris, France
Téléphone : +33 1 23 45 67 89
Email : contact@cyberguard-consulting.fr

MISSION : CADRAGE DU PENTEST

Scénario fictif : vous avez fait une réunion avec un client (Monsieur KOXI Jean de la société KOXIELEC), qui vous a expliqué son activité. Vous avez ainsi extrait de la discussion au format audio.

Votre mission, si toutefois vous l'acceptez, est de préparer le pentest en ciblant son cadre et périmètre. Pour cela, vous devez vous baser sur le fichier audio pour remplir les points suivants qui seront repris sur le contrat et/ou le rapport final. BONUS : manque-t-il des éléments ?

1. Contexte et Objectifs

Client :
Société KOXIELEC – Monsieur KOXI Jean

Secteur d'activité :
TPE locale spécialisée dans le dépannage et les travaux de maintenance en électricité.

Contexte :

- Le site web a été créé par un membre de la famille (non expert en développement web) et n'a pas encore vocation à accueillir un trafic important.
- Des inquiétudes ont été exprimées concernant la sécurité des données et la conformité du site aux standards actuels de sécurité informatique.

Objectifs du Pentest :

- Évaluer la sécurité du site web du point de vue d'un attaquant externe.
- Identifier les éventuelles vulnérabilités et proposer des recommandations pour corriger les failles détectées.
- Vérifier la conformité du site avec l'état de l'art en matière de sécurité.

Cadre de réalisation :

- **Type de test :** Pentest en mode « boîte noire » (simulation d'attaque externe sans connaissance préalable détaillée du système).
- **Mode de réalisation :** À distance.
- **Période d'exécution :** Du 1er au 7 octobre.

2. Ciblage des Besoins et de l’Approche

Besoins exprimés :

- Vérifier que le site est protégé contre les attaques extérieures.
- Obtenir un diagnostic de la sécurité pour mettre en œuvre les corrections nécessaires et renforcer la conformité aux bonnes pratiques.

Approche proposée :

- Test d’intrusion en mode externe (boîte noire) pour simuler le comportement d’un attaquant externe.
- Analyse de la surface d’attaque du site, incluant les points d’entrée accessibles publiquement.
- Vérification complémentaire des composants tiers, notamment en ce qui concerne le WiX Toolset, afin d’identifier d’éventuelles vulnérabilités connues (CVE-2024-29188, CVE-2024-29187, CVE-2024-24810, CVE-2023-39021, CVE-2020-18169, CVE-2019-16511) pouvant impacter la sécurité globale.

Modalités de communication et planning :

- Rapport de pentest à remettre dans un délai à définir après la prestation (7 jours après la fin des tests).
- Modalités précises (budget, interlocuteurs, points de contact) à finaliser avec le client.

3. Cartographie Technique du Système

Cibles à tester :

- **Nom du site :** electriciteabc.com
- **Adresse IP hébergeant le site :** 172.20.30.40

Technologies et outils utilisés :

- Le site a été développé via la solution Wix, connue comme une plateforme de publication de sites (offrant des versions gratuites et payantes).
- Hébergement : L'hébergeur « yonas » a donné son autorisation pour la réalisation du test.

Environnement :

- Il est présumé que le site est en production, bien qu'il ne soit pas encore exposé à un trafic significatif.

Interlocuteur technique :

- Pour l'instant, le point de contact principal reste Monsieur KOXI Jean. Il est recommandé de désigner un responsable technique ou un contact en cas d'incident afin de faciliter la coordination pendant le test.

4. Points Complémentaires et Informations Manquantes

Informations complémentaires à obtenir :

- **Budget et Modalités Financières :**
    - Le budget alloué pour la prestation n'a pas été précisé. Il est important de définir un plafond et les modalités de facturation.
- **Détails sur l'Infrastructure et la Stack Technique :**
    - Précisions sur le CMS et/ou les technologies (langages, frameworks, plugins, éventuels modules de sécurité) utilisés dans la création du site.
    - Existence d'autres composants (bases de données, services tiers, API) qui pourraient être dans le périmètre du test ou à exclure.
- **Interlocuteurs et Procédures en Cas d'Incident :**
    - Désignation d'un responsable technique ou d'un contact dédié en cas d'incident durant le pentest, peut-être le fils de Mr KOXI.
- **Contraintes et Limitations de l'Intervention :**
    - Horaires spécifiques d'exécution (en dehors des heures critiques, par exemple).
    - Exclusions éventuelles de certains systèmes ou sous-domaines non concernés par le test.
- **Documentation et Autorisations :**
    - Confirmation écrite (lettre de consentement) de l'hébergeur « yonas » pour réaliser le test.
    - Existence de documents ou procédures internes (PAS, PAQ, PSI) relatifs à la sécurité ou à l'hébergement.