**Document de cadrage**

[Réalisez un test d’intrusion web]

# Modalités de prestation

Les informations contenues dans ce document sont strictement confidentielles et à destination unique du personnel de <CLIENT> dûment habilité.

## **Périmètre de la prestation**

Le présent document vise à encadrer les différentes activités qui seront réalisées dans le cadre des tests d’intrusion sur **l’application <APPLICATION>** de <CLIENT>.

Les infrastructures et applications suivantes seront auditées :

* <liste des adresses IP>
* <liste des URL>
* <Description du périmètre si impossible de lister les IP/URL en amont>

**Activités**

Les tests d’intrusion seront conduits en **boîte noire** et en **boîte grise** sur l’ensemble du périmètre.

**Qualification de la prestation**

La présente prestation n’est **pas qualifiée** PASSI.

**Livrables**

Les livrables de la prestation seront les suivants :

* Un **rapport d’audit détaillé**, contenant :
* une synthèse managériale ;
* une analyse de risques ;
* le détail des vulnérabilités et des recommandations ;
* le détail complet des tests réalisés.
* Un **support de présentation** de la réunion de restitution.
* Un **plan d’action**.

**Communication entre les parties**

1. **Contacts**

Le contact privilégié pour cette prestation chez <CLIENT> est le responsable d’audit dont les coordonnées sont les suivantes :

| Prénom | NOM | Mail | Téléphone |
| --- | --- | --- | --- |
|  |  |  |  |

Les auditeurs seront joignables pendant toute la durée de l’audit aux coordonnées suivantes :

| Prénom | NOM | Mail | Téléphone |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

À la demande du responsable d’audit, les auditeurs collaboreront avec les différentes équipes et personnes indiquées. Notamment, dans le cadre de la gestion d’un incident de sécurité, les auditeurs pourront être sollicités afin de déterminer si le test d’intrusion en cours en est la cause.

1. **Modalités d’échange**

Tous les documents échangés dans le cadre de la prestation sont confidentiels et seront communiqués entre <CLIENT> et <PRESTATAIRE> de manière chiffrée, avec le mot de passe échangé suite à la réunion de lancement.

1. **Langue des livrables**

Les livrables ainsi que les présentations seront rédigés en **français**.

**Prérequis**

Dans le cadre de l’audit, pour le bon déroulé de la prestation les prérequis suivants ont été identifiés :

* 2 comptes utilisateurs standard sur l’application <APPLICATION>, avec des périmètres différents ;
* 1 compte administrateur ;
* …

**Exclusion du périmètre**

Sauf autorisation expresse du responsable d’audit, les activités suivantes ne seront pas effectuées lors de l’audit :

* Attaques de type déni de service par surcharge du trafic réseau.
* XXX
* XXX

Cependant, la réalisation de tests d’intrusion comporte toujours un risque d’altération du service, la découverte ou la confirmation d’une vulnérabilité étant très souvent liée à son exploitation. Auquel cas, le traitement de l’incident sera effectué conjointement entre le responsable d’audit et les auditeurs.

Dans le cas où les auditeurs parviendraient à accéder à <données ou fonctionnalité>, aucun traitement postérieur ne pourra être effectué / tout traitement postérieur doit faire l’objet d’une autorisation expresse du responsable d’audit.

**Responsabilités**

Les tests et plus globalement l’ensemble de la prestation ne commenceront qu’après la signature du présent document. Si <PRESTATAIRE> venait à manquer à un des éléments du présent document, notamment au niveau du périmètre ou de la confidentialité des données, <PRESTATAIRE> s’engage à informer <CLIENT> du manquement dans les plus brefs délais.

<PRESTATAIRE> s’engage à ce que les actions réalisées dans le cadre de la prestation restent strictement en adéquation avec les objectifs de la prestation. Si le périmètre de l’audit venait à évoluer, une mise à jour du présent document et la signature de la mise à jour seraient nécessaires.

Le commanditaire garantit disposer de l’ensemble des droits de propriété et d’accès sur le périmètre de la prestation (systèmes d’information, supports matériels, etc.) ou d’avoir recueilli l’accord des éventuels tiers, et notamment de ses prestataires ou de ses partenaires, dont les systèmes d’information entreraient dans le périmètre. Notamment, il s’engage à avoir obtenu l’accord de l’hébergeur dans le cadre d’un test d’intrusion hébergé en externe, si la politique de l’hébergeur par rapport aux tests de sécurité implique une déclaration ou le recueil de son accord.

Le commanditaire autorise provisoirement le prestataire, pour la durée de l’audit et aux seules fins de réaliser la prestation, d’accéder et de se maintenir dans tout ou partie du périmètre et d’effectuer des traitements sur les données hébergées, quelle que soit la nature de ces données.

Le commanditaire autorise provisoirement le prestataire à reproduire, collecter et analyser, pour la durée de l’audit et aux seules fins de réaliser la prestation, des données appartenant au périmètre du système d’information cible.

Le commanditaire et le prestataire remplissent toutes les obligations légales et réglementaires nécessaires aux activités d’audit. En outre, les auditeurs sélectionnés pour la mission ont tous une relation contractuelle avec <PRESTATAIRE> et n’ont pas de passé de *cracker.*

<PRESTATAIRE> dispose d’une assurance professionnelle couvrant les éventuels dommages causés lors de la réalisation des activités d’audit à hauteur de <MONTANT> €.

**Confidentialité**

L’ensemble des données et informations récupérées ou traitées dans le cadre de l’audit sont strictement confidentielles et ne doivent pas être communiquées à des tiers, hors autorisation écrite du responsable d’audit. De fait, les seules personnes autorisées chez <PRESTATAIRE> à accéder aux données sont les personnes participant à l’audit. Chez <CLIENT>, les personnes autorisées à accéder aux données sont à la discrétion du responsable d’audit, qui relaiera alors l’information à ces personnes.

Sauf refus formel et explicite du commanditaire, le <PRESTATAIRE> ne conservera à l'issue de la mission que les livrables de la mission, ainsi que certaines données anonymisées à des fins de traitement automatisés. Les livrables ne seront accessibles qu’aux personnes ayant participé à la prestation. Toutes les autres données d’audit, notamment les preuves, fichiers récupérés et traces d’audit, seront supprimées de manière sécurisée.

**Validation de la convention de service**

Je soussigné \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ en qualité de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ autorise \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ à réaliser la prestation décrite ci-dessus.

Fait à le .

Signature