Audit informatique et libertés

6ix Secured E-commerce

REFERENCE: 2012/DOC/INT/006/v1.0

DIFFUSION : PUBLIQUE

ETAT DES VALIDATIONS		
Fonction	**Rédacteur**	**Vérificateur/Approbateur**
Signé par	Karim Slamani	Karim Slamani
Fonction	Consultant SSI	Consultant SSI
Date	30/10/2012	30/10/2012

SUIVI DE VERSION			
Version	**Date**	**Nature des modifications**	**Page et section**
1.0	30/10/2012	Création du document	*

DIFFUSION		
Entité	**Nom**	**Coordonnées**
6ix IT	Karim Slamani	karim.slamani@6ix-it.com

1. DESCRIPTION

1.1. Contexte

La sécurité n'a jamais été aussi recherchée et les entreprises font aujourd'hui face à une recrudescence du piratage.
On peut régulièrement lire dans la presse que des données personnelles sont dans la nature. A titre d'exemple, la fuite des données de l'UMP en juillet 2012 ou encore la compromission du site pearl.fr, site e-Commerce à très forte audience.

Ce sont des milliers de données personnelles qui ont été compromises. Nom, prénom, date de naissance, adresse, numéro de carte bancaire, autant de donnée personnelles dans la nature.

Sur internet, les labels et certificats rassurent (les clients) et assurent (des ventes) : ils sont des **garanties de sécurité**, paiement, livraison, qualité des produits pour vous et pour vos clients.

1.2. La societé 6ix iT

Société de conseil à forte valeur ajoutée dans le domaine de la sécurité des systèmes d'information, **6ix IT** bénéficie d'un large retour d'expérience dans les secteurs hautement sensibles de l'industrie, du jeu en ligne, du milieu bancaire et de l'Administration française.
Parce que chaque entreprise doit devenir une place forte afin de protéger son savoir-faire, **6ix IT** offre une démarche complète pour la sécurisation des systèmes d'information et vous **accompagne** dans la mise en œuvre de votre sécurité, de son organisation aux audits de sécurité, en passant par l'élaboration de mesures de protection et la sensibilisation des personnels.

Positionné en tant que société indépendante, 6ix IT intervient plus spécifiquement sur 4 grands types de missions :

- Mission d'assistance auprès des responsables sécurité de Grands comptes, ainsi que les maîtrises d'ouvrage : Elaboration de Politique de sécurité, analyse de risque, rédaction de dossier de sécurité…. Ces prestations sont réalisées par des experts sécurité, disposant d'au moins 10 ans d'expérience.
- Mission d'audits de sécurité et audit intrusifs, boite noire ou boite blanche ;
- Assistance à l'obtention de certification ARJEL ;
- Formations spécifiques à la sécurité.

Société au capital fermé entièrement détenu par des personnes physiques, **6ix IT** est totalement indépendante de tout éditeur ou constructeur qui pourrait influer sur ses activités, ce qui constitue une garantie de l'impartialité des prestations fournies.

1.3. Labels et certificats : explications.

Les acheteurs sont à l'affût des **signes de qualité** et surtout de sécurité avant de passer commande. Les labels et certificats sont une garantie de mise en confiance des clients qui parcourront votre boutique en ligne et qui seront alors plus enclins à acheter vos produits.

Il existe de très nombreux labels, plus ou moins connus. Tous fonctionnent sur le même principe, ils évoquent au premier coup d'œil une **marque de qualité** pour les clients.

Concrètement les labels apparaissent distinctement sur les sites.

Fia-net et L@belsite sont les deux labels les plus connus et les plus utilisés par les boutiques en ligne mais ne concernent que les prestations de paiement en ligne.

Fia-net est un courtier d'assurance et L@belSite est édité par la FEVAD, la Fédération des entreprises de vente à distance.

Pour le premier, il s'agit de souscrire auprès de Fia-net un contrat d'assurance pour les paiements en ligne.
Le label Fia-net est une sécurité à la fois pour le site e-Commerce et ses clients. Il garantit une protection contre les fraudes et que le système de paiement est sécurisé.

Pour le second, il suffit de s'adresser à la FEVAD pour en faire la demande. Au niveau du client, c'est la garantie de l'authenticité du marchand mais également que le site soit en conformité avec la réglementation et la déontologie de la vente à distance.

1.4. Mission

Sensibiliser les responsables informatiques à la sécurité de leur système d'information en proposant un service de certification aboutissant à la délivrance d'un label : Le label 6ix Secured.

Un audit de sécurité est donc réalisé sur l'applicatif interagissant avec les données personnelles gérées par le marchand en ligne. L'intérêt est donc double :

- L'e-commerçant bénéficie d'un audit de sécurité accessible (car réduit à un périmètre spécifique) ainsi que d'un interlocuteur pour toute les questions liées à la sécurité. Cela lui permet alors de bénéficier de garanties à présenter à ses clients : Le taux de conversion est amélioré.

- Le label affiché sur le site e-commerce est une garantie de sécurité pour l'internaute. Il sait que le site e-commerce sur lequel il se trouve a fait des **démarches visant à protéger** ses données personnelles.

2. EN QUOI CONSISTE UN AUDIT 6IX SECURED

2.1. Une déclaration sur l'honneur de l'audité

L'audité s'engage à déclarer au moins tout les 4 mois, **quelles sont les données personnelles** qui transitent par son SI et quelles sont les **mesures mises en place** pour en **assurer la sécurité**.
Un formulaire, à télécharger sur le site du projet 6ixSecured, guide l'audité et lui permet de quantifier et qualifier quelles sont les données sensibles qui devront faire l'objet d'une attention particulière.

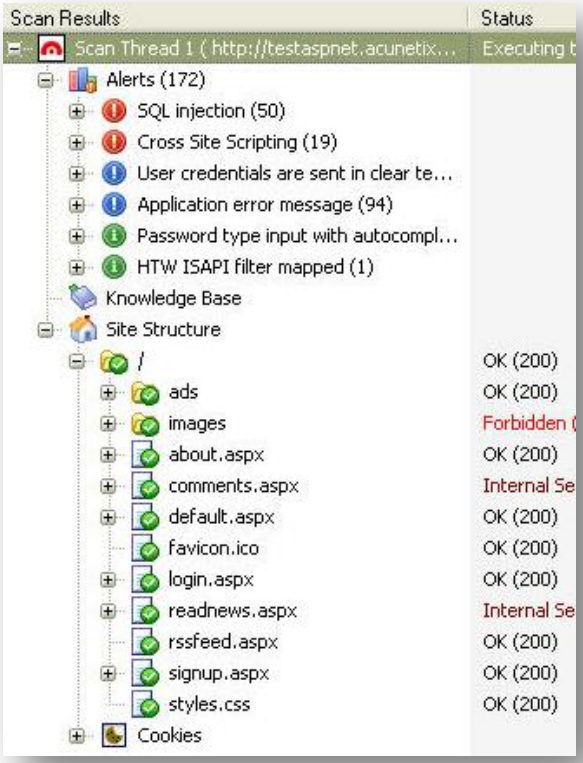
Email, nom, prénom, adresse IP, historiques des commandes font bien entendu partis des informations entrant dans le périmètre de cette prestation.

2.2. Un contrôle technique

Le contrôle réalisé porte sur les mécanismes de sécurité mis en place par l'audité, qui visent à protéger les données personnelles qu'il stocke.
Deux méthodes de contrôle sont préconisées.

Le Test d'intrusion

L'objectif de ce contrôle est de détecter des vulnérabilités ou incohérence accessible par un utilisateur malveillant positionné sur Internet.



La démarche de tests consiste en un:

- Parcours (crawler) exhaustif de l'ensemble des ressources du site : pages de contenu, pages d'erreur, scripts, feuilles de style, etc.
- Relevé des versions des logiciels : serveur web, base de données, Webservices.
- Relevé d'informations sensibles : table de base de données, mots de passe éventuels, etc.
- Relevé de l'ensemble des paramètres passés aux différentes fonctions : formulaires, références, etc.

D'après les informations relevées précédemment :

- Tentative d'Injection de script,
- Tentative d'Injection de code,
- Tentative d'Injection SQL (en mode « aveugle » si aucune information n'a été trouvée précédemment),
- Sortie d'arborescence,
- Etc…

Les tests menés porteront sur l'application et l'infrastructure.

Un rapport sera émis et pourra être téléchargé par le client 24H après les tests.

L'Audit de code source.

L'objectif de l'analyse du code source est de détecter des erreurs de conception et/ ou de développement qui causeraient des vulnérabilités potentiellement exploitables par un attaquant.

La méthodologie, issue de la démarche CVSS, est la suivante :

- Vérifier la **complétude** des codes sources en s'assurant que son **fonctionnement soit correct**.

- Naviguer dans les sources afin de comprendre l'architecture de l'application et la façon dont les mécanismes dédiés et **touchant à la sécurité** sont implémentés.
- Identifier les variables et fonctions sensibles et en déterminer les modes **d'utilisation critiques**.
- Examiner les dépendances entre les éléments de données pour rechercher des **dépendances indésirables**.
- Réaliser des études du **comportement des objets** (variables, fonctions) à travers le déroulement du programme.
- Rechercher dans le code source des **fonctions illicites** ou non documentées, c'est-à-dire ne correspondant à aucun élément spécifié dans la conception détaillée (si fournie)

2.3. Un contrôle organisationnel

En complément de l'audit technique, un audit organisationnel est conduit. L'objectif est de s'assurer que les informations sensibles soient traitées conformément à l'état de l'art en matière de protection des données personnelles.

- Exigences relatives à l'identification des procédures internes
- Exigences relatives à l'identification des traitements
- Exigences relatives à l'appréciation de la licéité des traitements
- Exigences relatives à l'étude des personnes accédants aux données
- Exigences relatives à l'analyse des durées de conversation
- Exigences relatives à l'étude du respect des droits des personnes
- Exigences relatives à l'étude du respect des traitements particuliers

Un plan d'audit est remis en début de mission. Il récapitule tout les points qui seront abordés :

- Objectif
- Critères
- Document de référence
- Périmètre de l'audit
- Dates, lieux et horaires
- Rôles et responsabilité de chacune des parties
- Un récapitulatif des ressources mobilisées par le marchand.

Ces contrôles sont réalisés par échantillonnage et sont définis après la réunion d'initialisation.

2.4. Un sceau de confiance 6ix Secured.

Le Sceau de Confiance 6ix Secured est un sceau de transparence sur la sensibilité de l'audité à la sécurité de son système d'information vis à vis des données personnelles dont il a la responsabilité.
Son but est d'aider à distinguer les sites les plus **fiables en termes de sécurité**, en affichant leurs performances, obtenues à l'issue des tests de sécurité réalisés.

Nos prestations sont bien entendu limitées aux seuls sites auxquels nous avons délivré notre logo.
La certification d'un site n'est valable que si celui-ci dispose du sceau de confiance 6ix Secured et que celui-ci existe dans les références présentées sur le site 6ix IT.

Les références sont organisées par catégories sur le site de 6ix-it.com et recense l'ensemble des sites ayant obtenu le label 6ix IT.

Exemple d'organisation des références.

Dans chacune des catégories, une image ainsi que le descriptif du site labellisé est disponible.
Aucune note ne sera visible.
La présence dans l'index des références sera gage de la robustesse du système d'information.

<SCEAU_ICI>

3. TARIFS

CA Annuel	Cotisation annuelle HT
De 0 à 100 000€	500€
De 100 000 à 250 000€	1 000€
De 250 000 à 500 000€	2 000€
De 500 000 à 1 000 000€	4 500€
De 1 000 000 à 3 000 000€	12 000€
A partir de 3 000 000 €	25 000€

Un devis gratuit et personnalisé peut être obtenu en fonction de l'architecture technique déployée par le marchand en ligne ainsi que du type de données personnelles transitant par son système d'information.
La certification 6ix Secured représente un investissement faible à la vue des bénéfices associés à la prestation :

- Influence sur l'image de marque,
- Protection du patrimoine intellectuel de l'entreprise vis-à-vis de la concurrence,
- Influence positive sur les internautes,
- Interlocuteur privilégié sur les questions de sécurité des systèmes d'informations

4. CONTACT

Pour toute question, merci de contacter la personne suivante :

Karim Slamani - **6ix IT** - **IT Security Expert**
Tél: +33 (0)6 10 92 18 03
karim.slamani@6ix-it.com
http://www.6ix-it.com
12 rue de la fontaine de lattes, 34000 Montpellier.