AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Règlement de l'appel à candidature éditeurs

Tests d'intrusion cyber sécurité dans le cadre de la vague 2 du Ségur du numérique en santé

Statut : En cours | *Classification : Restreinte* | *Version : v0.1*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Destinataires

Prénom / Nom	Entité / Direction

Documents de référence

Historique du document

Version	Rédigé par		Vérifié par		Validé par	
0.1	A.MARTEAU-E.CLOUT	Le 31/08/2022	E.CLOUT	Le 02/09/2022	P.NOM	Le JJ/MM/AA
	Motif et nature de la modification : **Création du document + Ajustements**					
	A.MARTEAU	Le 05/09/2022	V.CROISILLE			
	Motif et nature de la modification : Prise en compte des remarques, modification du document					
	A. MARTEAU	Le 15/09/2022				
	Motif et nature de la modification : Ajout des tests Applications Mobile + précision sur la sélection des éditeurs					
	Motif et nature de la modification :					
	Motif et nature de la modification :					
	Motif et nature de la modification :					
	Motif et nature de la modification :					
	Motif et nature de la modification :					

SOMMAIRE

1. CONTEXTE : VAGUE 2 SEGUR DU NUMERIQUE EN SANTE

Notre ambition : généraliser le partage fluide et sécurisé de données de santé entre professionnels et usagers pour mieux soigner et accompagner.

Le Ségur du numérique en santé, c'est :

- Un investissement inédit de 2 milliards d'euros pour soutenir le développement massif et cohérent du numérique en santé en France ;
- Des objectifs ambitieux pour accélérer la feuille de route du numérique en santé.

Un programme co-construit avec tous les acteurs de l'écosystème

Le Ségur a été porté par les professionnels de santé, fournisseurs des solutions logicielles, patients et pouvoirs publics.
Il alimentera Mon espace santé, qui permet à chaque citoyen de disposer d'une vision consolidée de son parcours de soins afin d'être acteur de sa santé.
Comme annoncé lors du COSUI du 12 juin, une vague 2 est prévue pour un lancement fin 2022 / début 2023 comme annoncé.

2. PRIORITE A LA SECURITE ET EXIGENCES SECURITE

Exigences SSI dans le cadre de la vague 2 du Ségur du numérique en santé

Dans le cadre du Ségur du numérique en santé, l'Etat met en place un mécanisme d'achat pour compte au bénéfice des acteurs de l'offre de soins, sous la forme d'un système ouvert et non sélectif (SONS) de référencement et de financement.

Plus d'informations sur ce dispositif.

Le référencement des solutions logicielles par les éditeurs est un prérequis à l'obtention d'un financement. Les éditeurs candidats au référencement doivent pour cela suivre un processus qui permet de s'assurer que leurs solutions respectent l'ensemble des exigences techniques et fonctionnelles décrites dans un référentiel d'exigences minimales (REM) qui est mis à leur disposition.

La sécurité des données de santé est aujourd'hui au cœur des préoccupations. Il est par conséquent essentiel que les solutions logicielles proposées par les éditeurs permettent un partage sécurisé des données de santé entre professionnels et usagers. Elles doivent notamment pouvoir s'interfacer de façon sécurisée avec les services numériques en santé tels que le Dossier Médical Partagé ou encore Mon espace santé. En conséquence des exigences de sécurité ont été élaborées en vue d'intégrer les référentiels d'exigences minimales dans le cadre de la vague 2 du programme SONS, en tenant compte des résultats des questionnaires sécurité complétés dans le cadre de la vague 1.

3. TEST D'INTRUSION

Condition de réalisation du Test d'intrusion

Pour la vague 2 du Ségur des exigences SSI réalistes et ambitieuses, permettront de faire progresser la maturité des éditeurs sur les thématiques de sécurité des SI et seront imposées aux candidats.

Dans ce contexte, des tests d'intrusion doivent s'effectuer sur une durée globale d'une semaine (2,5 à 3 jours pour la prestation opérationnelle et 1-2 jours pour la rédaction du rapport) et se réaliser en boite grise avec des compléments en boite noire.

En boite noire: l'auditeur ne dispose d'aucune information sur l'application hormis celle-ci;

En boite grise: l'éditeur transmet des informations d'identification (compte utilisateur, compte à privilège, compte administrateur) à l'auditeur afin d'orienter le travail sur l'analyse au sein du système.

Le test d'intrusion vise à valider la mise en œuvre des bonnes pratiques de sécurité et l'absence de vulnérabilité sur un certain nombre de thématiques telles que l'authentification à l'application, le chiffrement des données et des flux sensibles, le contrôle des accès aux ressources, la gestion des sessions et le traitement des paramètres.

Le périmètre du test d'intrusion est encadré pour limiter les impacts sur l'application ou le système d'information de l'éditeur. Ainsi, la prestation est réalisée dans un environnement de développement / test / iso-prod. L'application testée doit se rapprocher de celle que l'on pourrait retrouver sur l'environnement de production (données similaires et niveau de sécurité suffisant) afin d'obtenir une vision réaliste de la sécurité.

Par ailleurs, l'ensemble des dispositifs de sécurité (WAF, sondes, etc.…), s'ils ne font pas partie de la solution commercialisée, doivent être désactivés pour se concentrer uniquement sur le fonctionnement de l'application telle qu'elle pourrait être installée par un client.

Les tests sont disponibles en annexe 1

Les points de contrôles comportent une partie commune puis sont spécifiques en fonction du type d'application (web ou client lourd)

4. PILOTE DES TESTS D'INTRUSION

Pour estimer la charge pour l'éditeur, s'assurer que les éditeurs seront bien en capacité de réaliser ces tests d'intrusion dans les délais de référencement de la vague 2, d'évaluer les impacts pour les éditeurs candidats, de s'assurer du bon niveau des tests d'intrusion et de leur faisabilité, l'ANS propose d'organiser un pilote des tests d'intrusion décrits en annexe 1.

Période de réalisation des pentests :

Trois sessions de tests d'intrusion pilote seront réalisées avec des éditeurs candidats potentiels à la vague 2 :

Un logiciel Web, une application client lourd et une application mobile.

5. MODALITES DE CANDIDATURES AU PILOTE

Types d'éditeurs pouvant candidater au pilote : LGC, DPI, RIS, SGL, DUI

Le formulaire de candidature sera disponible sur le portail ANS des industriels : https://industriels.esante.gouv.fr/ et sera actif du 22/09/2022 au 29/09/2022

Critères de sélection :

> Chaque type d'application devra être représenté (WEB, client lourd, application mobile). Les premiers candidats qui manifesteront leur intérêt seront retenus avec la contrainte d'avoir une diversité des types de logiciel (LGC, DPI, RIS, SGL, DUI) et des types d'application (WEB, client lourd, application mobile)

Les entrants sont attendus à la fin du mois de septembre au plus tard.

Annexe 1 : les points de contrôle du test d'intrusion à réaliser

Attention, les points de contrôles sont évolutifs avec la concertation en cours.

Base Commune :

ID	Périmètre	Nom court	Règles de sécurité
C-1	Gestion de l'authentification	Autocomplétion	Aucun des champs de mot de passe n'affiche ce dernier lorsqu'il est saisi et l'auto-complétion est bien désactivée sur l'intégrité des champs
C-2	Gestion de l'authentification	Authentification côté serveur	Tous les contrôles d'authentification sont effectués du côté serveur.
C-3	Gestion de l'authentification	Complexité MDP	La complexité de chaque mot de passe d'authentification répond à la PGSSI-S et doit être vérifiée côté client avant de l'envoyer côté serveur (entropie de 50 bits au minimum si le mot de passe peut être utilisé comme unique facteur d'authentification).
C-4	Gestion de l'authentification	Blocage compte	Une mesure de restriction d'accès parmi les suivantes, conformes à la PGSSI-S est appliquée en cas de tentatives multiples d'authentification : - Une temporisation d'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement dans le temps ; il est recommandé que cette durée soit supérieure à 1 minute après 5 tentatives échouées, et permette de réaliser au maximum 25 tentatives infructueuses par 24 heures ; - Un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (p. ex. : « captcha ») ; - Un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 10.
C-5	Gestion de l'authentification	Changement MDP	Le changement de mot de passe doit respecter la politique initiale en terme de complexité.
C-6	Gestion de l'authentification	Ré-authentification	Une nouvelle authentification ou un moyen d'identification de l'utilisateur doit être exigé avant de permettre toute opération sensible
C-7	Gestion des sessions	Invalidation à la déconnexion	La session est invalidée quand l'utilisateur se déconnecte.
C-8	Gestion des sessions	Invalidation après inactivité	La session est invalidée après une période d'inactivité. Cette durée doit être au maximum de 20mn.
C-9	Gestion des sessions	Invalidation sessions	Les sessions sont invalidées après un temps maximum configurable indépendant de l'activité (4h : durée de timeout absolue).

C-10	Gestion des sessions	changement ID session	L'identifiant de session est changé à chaque nouvelle connexion sans avoir de lien avec la précédente
C-11	Contrôle d'accès aux ressources	Directory traversal	La navigation dans les répertoires est désactivée
C-12	Contrôle d'accès aux ressources	Moindre privilège - fonctions	Les utilisateurs ou applications clientes ne peuvent avoir accès qu'aux fonctionnalités protégées pour lesquelles ils ont des autorisations spécifiques.
C-13	Contrôle d'accès aux ressources	Contrôles côté serveur	Tout usage/modification d'une référence directe à une ressource (clé de base de données, nom de fichier, ressource web, etc.) par le client fait nécessairement l'objet d'une vérification d'habilitation côté serveur ou envoie une notification à l'éditeur qui doit être en attente de validation
C-14	Comptes génériques	Exposition des comptes génériques	Les comptes génériques doivent être restreints, ou disposent d'autorisations prédéfinies et fixes
C-15	Gestion des traces et événements de sécurité	Journalisation authentifications	Toutes les tentatives d'authentification sont journalisées (y compris les contrôles de session) et un timestamp émanant d'une source de confiance est associé à chaque évènement.
C-16	Gestion des traces et événements de sécurité	Journalisation données sensibles	Aucune donnée sensible n'est journalisée.
C-17	Gestion des traces et événements de sécurité	Composition des Journaux	Chaque événement de journalisation est géré côté serveur et inclut : * un timestamp provenant d'une source de confiance (au moins hors poste client) ; * un niveau de gravité de l'évènement (optionnel) * une indication du fait que c'est un événement lié à la sécurité (optionnel) ; * l'identifiant de l'utilisateur à l'origine de l'évènement (s'il y a un utilisateur lié à l'évènement) (optionnel); * l'adresse IP source de la requête associée à l'évènement ; * si l'évènement a réussi ou échoué ; * une description de l'évènement
C-18	Gestion des traces et événements de sécurité	Journalisation des echecs	Les échecs de validation des entrées sont journalisés.
C-19	Composant vulnérable	Obsolescence	Lors d'un scan, l'application doit être consituée d'éléments à jour
C-20	Antivirus	Virus	Les dépôts de fichiers ne doivent pas pouvoir accepter le téléchargement de virus ou autres malwares

C-21	Antivirus	Virus	Toutes les pièces jointes doivent interdire les formats exectutables (SVG, exe, msi, jar…), ou qui intègre du code et restreindre les extensions à ce qui est strictement nécessaire
C-22	Protection des données en transport et chiffrement	Cryptographie	Les données sensibles doivent être chiffrées avec des algorithmes cryptographiques à l'état de l'art (https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf). De plus une version de TLS 1.2 ou + doit être utilisée à minima pour tout type de connexion

Application Web :

ID	Périmètre	Nom court	Règles de sécurité
W-1	Gestion de l'authentification	Authentification des pages	Toutes les pages et ressources exigent une authentification exceptées celles qui sont spécialement prévues pour être publiques.
W-2	Gestion de l'authentification	Déconnexion	Toutes les pages qui requièrent une authentification pour y accéder possèdent un lien de déconnexion
W-3	Gestion de l'authentification	Authentification utilisateur	L'application doit avoir une mire de réinitialisation des mots de passe sécurisés afin de prévenir les énumérations d'utilisateur
W-4	Gestion des sessions	ID session	L'identifiant de session n'est jamais communiqué autrement que par l'en-tête de cookie ou l'en-tête Authorization (et particulièrement dans l'URL, les messages d'erreur et les journaux).
W-5	Gestion des sessions	domaine cookies	Dans le cas de l'utilisation de cookies, ceux qui contiennent les identifiants de session ont leur domaine et chemin définis sur une valeur suffisamment restrictive
W-6	Gestion des sessions	Secure Attribute	Le drapeau de sécurité (*secure attribute*) est utilisé sur tous les cookies qui contiennent des données sensibles, y compris le cookie de session.
W-7	Gestion des sessions	CSRF	Des protections contre les CSRF doivent être mis en œuvre
W-8	Contrôle d'accès aux ressources	Moindre privilège	Les utilisateurs ont des restrictions d'accès pour les données auquelles ils n'ont pas accès.
W-9	Gestion des entrées	Input encoding	Un type d'encodage des caractères, tel que l'UTF-8, est indiqué pour toutes les sources d'entrées.
W-10	Gestion des entrées	Type de requêtes	L'application n'accepte qu'un nombre défini de types de requêtes HTTP et interdit la méthode TRACE
W-11	Gestion des entrées	Whitelist input	Un motif de validation par liste blanche est défini et appliqué à toutes les entrées (listes déroulantes, et contrôles de syntaxe tels que la longueur, le typage, la cohérence et la syntaxe)

W-12	Gestion des entrées	sanitization failures	Tous les échecs de validation d'entrée entraînent un rejet de l'entrée ou son assainissement.
W-13	Gestion des entrées	XSS Injection	Les entrées incluant des injections XSS, XSS stockées et DOM XSS doivent être interdites
W-14	Gestion des entrées	SQL Injection / Prepared statement	Les entrées incluant des injections SQL doivent être interdites. Toutes les données non sûres qui doivent être envoyées à un interpréteur SQL utilisent une interface paramétrée, une déclaration préparée (prepared statements) ou sont correctement neutralisées.
W-15	Gestion des entrées	redirection control	Les redirections ne transmettent pas de données non validées.
W-16	Gestion des sorties	output sanitization - server	Tous les contrôles d'encodage/échappement des sorties sont implémentés coté serveur.
W-17	Gestion des sorties	output sanitization	Toutes les données non fiables qui doivent sortir sous forme HTML (y compris les éléments, attributs, données Javascript, blocks CSS et attributs d'URLs) sont correctement neutralisées en fonction du contexte.
W-18	Gestion des sorties	XML sanitization	Afin d'éviter une XXE (XML eXternal Entity attack), toutes les données non sûres qui sont envoyées en sortie vers du XML utilisent une interface paramétrée ou sont correctement neutralisées.
W-19	Gestion des sorties	LDAP sanitization	Toutes les données non sûres qui sont utilisées dans des requêtes LDAP sont correctement neutralisées.
W-20	Gestion des sorties	Output encoding	Chaque réponse HTTP contient un en-tête Content-Type indiquant un type d'encodage de caractères sûr (par exemple UTF-8).
W-21	Gestion des sorties	HTTPOnly	Le drapeau *HTTPOnly* est utilisé par défaut sur tous les cookies
W-22	Gestion des sorties	Data Leak	Des contrôles de la verbosité des erreurs (try, catch…) sont mis en place
W-23	Gestion des sorties	Entête HTTP	Les entêtes HTTP verbeux doivent être maitrisées afin de ne pas retourner des informations sensibles (version du serveur,etc.)
W-24	Gestion de l'exposition	Contrôle de l'exposition	Les services du serveur doivent être limités (ports ouverts, services accessibles….)
W-25	Gestion de l'exposition	Durcissement du serveur	Des entêtes HTTP de sécurité doivent être utilisées (Content-Security-Policy, X-XSS-Protection, X-Frame-Options et X-Content-Type-Options)
W-26	Gestion de l'exposition	Connexion au serveur	L'IP du serveur ne doit pas être directement accessible et des mécanismes de sécurité protègent ce dernier (utilisation d'un reverse proxy)
W-27	Gestion de l'exposition	Ressources externes	Si l'application utilise le CDN, un contrôle de l'intégrité des scripts via l'attribut HTML integrity ainsi que des contrôles d'utilisation HTTPS sont nécessaires. Le cas echéant, des scripts locaux doivent être priviligiés

Client Lourd :

ID	Périmètre	Nom court	Règles de sécurité
T-1	Analyse Statique	Code Source	Le code source de l'application ne doit pas être accessible par un décompilateur et tous les programmes non compilés doivent être obfusqués
T-2	Analyse Statique	Stockage des données	Le client lourd ne stocke aucune donnée sensible côté client (dans les binaires, les fichiers cachés, etc….) et communique avec le serveur pour les obtenir
T-3	Analyse dynamique	buffer overflow	L'environnement d'exécution n'est pas sujet aux débordements de tampons ou que les contrôles de sécurité préviennent les débordements de tampons.
T-4	Analyse dynamique	Injection de commande	Les entrées incluant des injections de commandes doivent être interdites et les entrées côtés clients doivent être nettoyées
T-5	Analyse dynamique	Connexion au serveur	L'IP du serveur ne doit pas être directement accessible et des mécanismes de sécurité protègent ce dernier (utilisation d'un reverse proxy)
T-6	Analyse dynamique	Graphical User Interface	Les contrôles GUI de l'application ne permettent pas d'activer des fonctions ou options supplémentaires pour l'utilisateur (objet caché, mot de passe masqué, injection, élévation de privilège…)
T-7	Analyse dynamique	Analyse de la RAM	Dans le cadre d'un poste partagé, lorsque l'application est en cours d'execution, la RAM ne contient aucune information sensible en clair
T-8	Analyse dynamique	Dépendence de l'application	Les dépendances de l'application doivent être limitées afin d'éviter de potentielles erreurs de configuration
T-9	Contrôle d'accès aux ressources	Détournement de DLL	L'utilisation de DLL doit être sécurisée afin de se protéger contre tout détournement.
T-10	Contrôle d'accès aux ressources	ASLR/DEP	Les .dll doivent être compilées avec ASLR et DEP afin de rendre la corruption de mémoire difficile

Application Mobile :

ID	Périmètre	Nom court	Règles de sécurité
M-1	Analyse Statique	Autorisation de l'application	L'application ne demande qu'une série minimum de permissions nécessaires
M-2	Analyse Statique	Version non sécurisée de l'OS	L'installation de l'application doit s'effectuer sur un système d'exploitation sécurisé et non obsolète

M-3	Stockage des données	Stockage sécurisé	Aucune donnée sensible n'est stockée hors du conteneur de l'application ou des fonctions de stockage sécurisées sont proposées par le système.
M-4	Stockage des données	Keyboard Press Caching	Le cache du clavier est désactivé sur les champs d'entrée textuels qui traitent de données sensibles.
M-5	Stockage des données	Application Backgrounding	L'application enlève les données sensibles lors de son passage en arrière-plan.
M-6	Stockage des données	Stockage donnée sensible	L'application ne garde pas les données sensibles en mémoire plus longtemps que nécessaire et la mémoire est explicitement nettoyée après son utilisation
M-7	Stockage des données	Information de connexion	Les informations de connexion doivent être stockées de manière sécurisée sur le téléphone (stockage d'un jeton tel un cookie de session, jeton Oauth, SAML…)
M-8	Analyse Dynamique	Sécurité de l'appareil	L'application ne peut pas s'exécuter lorsque le verrouillage par PIN ou Pattern n'est pas activé.
M-9	Analyse Dynamique	Divulgation d'information	Le journal de l'application "Logcat/Apple System Log (ASL)" ne doit pas transmettre d'informations sensibles
M-10	Analyse Dynamique	XML sanitization	Afin d'éviter une XXE (XML eXternal Entity attack), toutes les données non sûres qui sont envoyées en sortie vers du XML doivent utiliser une interface paramétrée ou doivent être correctement neutralisées.
M-11	Analyse Dynamique	Local File Inclusion & WebViews	Les entrées soumises par l'utilisateur ne doivent pas être transmises aux systèmes de fichier ou Framework des API
M-12	Analyse Dynamique	WebView & XSS	L'usage de javascript dans les Webview doit être interdite
M-13	Analyse Dynamique	Validation entrée côté serveur	Le format d'une entrée doit être aussi vérifié au niveau du serveur distant
M-14	Analyse Dynamique	Certificate Pinning	L'ensemble des requêtes vers le backend doivent se baser sur une méthode sécurisée validant le certificat du serveur distant
M-15	Analyse Dynamique	Rooted et Jaibreak	L'application détecte et réagit à la présence d'appareils rootés ou jailbreakés soit en alertant l'utilisateur ou en mettant fin à l'application.
M-16	Contrôle d'accès aux ressources	Configuration des réponses	La réponse du serveur ne doit laisser transparaitre aucune information (Traitement des erreurs, bannière de réponse HTTP)

M-17	Contrôle d'accès aux ressources	SQL Injection	Les entrées incluant des injections SQL doivent être interdites. Toutes les données non sûres qui doivent être envoyées à un interpréteur SQL utilisent une interface paramétrée ou sont correctement neutralisées.
M-18	Gestion des sessions	domaine cookies	Dans le cas de l'utilisation de cookies, ces derniers qui contiennent les identifiants de session ont leur domaine et chemin définis sur une valeur suffisamment restrictive
M-19	Gestion des sessions	Secure Attribute	Le drapeau de sécurité (*secure attribute*) est utilisé sur tous les cookies qui contiennent des données sensibles, y compris le cookie de session.
M-20	Gestion des sorties	HTTPOnly	Le drapeau HTTPOnly est utilisé par défaut sur tous les cookies
M-21	Analyse Statique	Structure de l'application	Les secrets ne doivent pas être "hardcodés" dans l'application
M-22	Android	Mode de développement	Les modes Back-up et débug sont désactivés
M-23	Android	Exposition de l'application	Les ressources de l'application ne doivent pas être exportées en dehors de l'application (en particulier les content providers)