Considérations de sécurité relatives au développement et à la gestion de votre site Web

NOVEMBRE 2021 | ITSAP.60.005

Votre site Web est une composante essentielle de votre entreprise, car il donne accès à vos services et produits. Cependant, les cybermenaces peuvent compromettre la sécurité de votre site Web et ainsi nuire aux fonctions, aux revenus et à la réputation de votre entreprise. Pour réduire le risque d'être la cible de cybermenaces et atténuer les répercussions en découlant, vous devez considérer la sécurité dans le cadre du développement et de la maintenance de votre site Web. Vous trouverez ci-dessous quelques mesures de sécurité et de protection de la vie privée dont vous devriez tenir compte d'entrée de jeu. Vous trouverez également plus de renseignements dans l'ITSM.60.005, *Facteurs à considérer en matière de cybersécurité pour votre site Web*. Pour d'autres conseils et pratiques exemplaires en matière de cybersécurité, consultez notre site Web cyber.gc.ca.

EXEMPLES DE CYBERMENACES

La liste ci-dessous énumère les cybermenaces les plus courantes à considérer lors du développement et de la maintenance d'un site Web.

- **Attaques par injection** : Terme générique désignant toute exploitation perpétrée par un auteur de menace au moyen de données d'entrée non fiables (p. ex., injection de code malveillant) dans un système afin d'en modifier les opérations ou les données.
- **Attaques par script intersites :** Un auteur de menace utilise un script intersites (XSS pour *Cross-site Scripting)* pour compromettre un serveur Web et injecter du code malveillant dans des sites Web fiables. Lorsqu'un utilisateur visite le site Web, son navigateur exécute le script, ce qui pose un risque pour les témoins (*cookies*), les jetons de session et l'information sensible. L'attaque par script intersites exploite la confiance d'un utilisateur à l'égard d'un site Web.
- **Attaque par falsification de requête intersites :** Attaque qui vise à inciter l'utilisateur à faire des actions non souhaitables dans son navigateur, comme une fermeture de session, un téléchargement de renseignements sur le compte ou un téléversement des témoins d'un site. L'attaque par falsification de requête intersites (CSRF pour *Cross-site Request Forgery)* exploite le niveau de fiabilité qu'un site Web confère au navigateur d'un utilisateur.

Si votre site Web est compromis, ce n'est pas seulement votre organisation qui est à risque : les auteurs de menace peuvent également cibler votre chaîne d'approvisionnement, des organisations affiliées et vos clients.

Votre site Web fait le pont entre l'Internet et votre organisation. Les auteurs de menace peuvent exploiter les vulnérabilités et les erreurs de configuration pour voler, modifier ou supprimer des données sensibles (p. ex., les portails des fournisseurs, les données des clients, les clients potentiels, de même que les renseignements opérationnels et financiers). Gardez une longueur d'avance en examinant les aspects suivants de votre site Web. Si vous utilisez un service d'hébergement, vous devriez discuter de chacun des sujets ci-dessous avec votre fournisseur de services.

ARCHITECTURE DE SÉCURITÉ

Assurez-vous que l'architecture de votre site Web est sécurisée, c'est-à-dire ses éléments, les liens, les composants sélectionnés et les principes de conception. Vous devriez appliquer, entre autres, les principes de séparation et de redondance.

Séparez vos composants de service Web. Si un composant est compromis, les autres seront protégés parce qu'ils ont été séparés. Vous devez également séparer votre serveur d'applications et votre base de données pour protéger les données sensibles.

Vous devriez concevoir votre site Web de façon à ajouter des redondances dans vos composants de service Web (c.-à-d. les reproduire). La redondance vous permettra d'assurer la continuité de vos opérations en cas de défaillance d'un composant.

Vous devez utiliser le protocole HTTPS par défaut sur votre site Web pour vous assurer que les données sensibles, comme les données d'authentification et l'information confidentielle, sont chiffrées pendant le transit. Le protocole HTTPS s'appuie sur le protocole de sécurité de la couche transport (TLS pour *Transport Layer Security*) pour chiffrer et authentifier les visites des pages Web.

AUTHENTIFICATION

L'authentification désigne les mécanismes qui valident l'identité d'un utilisateur.

Mettez en œuvre une politique de mot de passe fort qui comprend l'authentification multifacteur (MFA pour *Multi-Factor Authentication*) pour renforcer la sécurité. N'envoyez jamais des mots de passe en texte brut sur Internet. Faites plutôt appel à des condensés et au chiffrement.

Si le seuil de tentatives d'ouverture de session infructueuses est atteint, verrouillez les comptes et retardez les ouvertures de session. Mettez en place un processus sécurisé de récupération de compte.

CONTRÔLE DE L'ACCÈS

Les contrôles d'accès déterminent qui peut accéder à quelles ressources sur votre site Web et ils limitent l'information que ces personnes peuvent voir et utiliser. Définissez des contrôles d'accès précis et mettez en pratique le principe du droit d'accès minimal afin de vous assurer que les utilisateurs ne disposent que des accès dont ils ont besoin pour accomplir les fonctions qui leur ont été confiées.

Tenez compte de toutes les couches de contrôle d'accès aux applications Web (p. ex., couche de présentation d'application, couche de données) et des types d'autorisations suivants : basée sur un URL, système de fichiers et serveur, logique applicative (c.-à-d., ce que l'utilisateur peut faire). Relevez les couches de contrôle d'accès incluses dans vos normes de codage et testez-les rigoureusement avant de déployer vos services Web.

FOURNISSEURS DE SERVICES

Si vous avez recours à un fournisseur de services, il se peut que vous n'ayez pas accès à l'infrastructure ou ne puissiez pas contrôler les fonctions de sécurité connexes. Toutefois, même lorsque vous faites appel à un fournisseur de services, votre organisation est toujours légalement responsable d'assurer la confidentialité et l'intégrité de vos données.

Avant de passer un contrat avec un fournisseur de services, examinez ses capacités et ses politiques en matière de sécurité des données et de protection des renseignements personnels. Définissez clairement les rôles et les responsabilités de votre organisation et de votre fournisseur de services en ce qui concerne la sécurité. Vous pouvez utiliser les sections de ce document pour guider les discussions que vous aurez avec un fournisseur de services au sujet de ses capacités en matière de sécurité.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

VALIDATION DES ENTRÉES

La validation des entrées est un processus qui permet de vérifier que les utilisateurs et les applications ne puissent entrer que des données correctement formées, notamment dans les champs, les formulaires et les requêtes.

Toutes les données d'entrée de votre site Web doivent être considérées comme non fiables. Validez les données d'entrée de vos services Web, y compris celles associées aux navigateurs des clients, aux pare-feu d'applications Web, aux serveurs Web, aux bases de données et à la logique applicative. Vous devriez valider les données d'entrée le plus tôt possible dans le cadre du processus de traitement pour réduire les contraintes que doivent subir vos serveurs. Mettez à l'essai la validation des données d'entrée pendant le processus de développement.

Les données d'entrée doivent également être contrôlées. Validez la longueur des données d'entrée pour éliminer les valeurs non valides et limiter la saisie de données en forme libre afin de minimiser le risque d'injection de scripts. Veillez à ce que les utilisateurs finaux ne puissent pas consulter les messages d'erreur du langage Structured Query Language (SQL), car ces derniers contiennent des informations précieuses sur votre base de données.

CONFIGURATION SÉCURISÉE

Bien que les configurations de sécurité recommandées par le fournisseur constituent généralement un bon point de départ, ces configurations par défaut peuvent ne pas fournir le niveau de sécurité nécessaire pour protéger vos systèmes et vos données contre les cybermenaces. Assurez-vous d'examiner les configurations pour identifier les vulnérabilités (p. ex., ports ou services inutilisés, fichiers ou répertoires non protégés).

Vous devriez désactiver l'exploration des répertoires, car cette fonction donne un aperçu de la structure de votre site Web. Supprimez tous les fichiers d'opérations Web inutiles (p. ex., les fichiers de code source ou de sauvegarde qui pourraient contenir des mots de passe). Désactivez le cache des informations d'identification du navigateur. Bien que la mise en cache des justificatifs d'identité soit pratique pour les utilisateurs, elle peut poser un risque pour les renseignements sensibles.

La mise en œuvre de la gestion de la configuration vous favorisera un codage sécurisé et facilitera le maintien des bases de référence dans l'ensemble de votre organisation.

GESTION DE SESSION

Une session est basée sur un échange d'information entre au moins deux entités, comme deux dispositifs ou un utilisateur et un serveur Web. La gestion de session est un processus qui permet d'amorcer des échanges, de les contrôler, de les maintenir et d'y mettre fin. Si les sessions ne sont pas gérées de façon sûre, les auteurs de menace peuvent les interrompre ou s'en approprier pour intercepter les données ou se faire passer pour des utilisateurs authentifiés.

Randomisez vos identifiants de session pour empêcher les auteurs de menace de déduire les séquences employées. Les identifiants de session doivent avoir une longueur minimale acceptable pour offrir une protection contre les attaques de force brute.

Stockez les données de suivi de session sensibles sur les serveurs de services Web avec une période de conservation appropriée et détruisez-les à la date d'expiration. Mettez un terme aux données de session lorsqu'un utilisateur se déconnecte ou est inactif pendant une durée déterminée.

Les témoins volatiles, aussi appelés « témoins en mémoire », permettent aux utilisateurs d'être reconnus lorsqu'ils naviguent sur le site Web (p. ex., les articles restent dans leur panier d'achat). Utilisez l'attribut de témoin sécurisé pour empêcher l'envoi de témoins par l'entremise d'un canal non chiffré.

SÉCURISER LES OPÉRATIONS

Une fois que votre site Web en ligne, vous devez prévenir les cybermenaces et les incidents, les détecter et intervenir en conséquence. Vous devez surveiller continuellement les activités du site Web pour déceler les comportements anormaux, comme les tentatives répétées d'ouverture de session ou les tentatives d'injection. Par exemple, dans le cas d'une attaque par bourrage d'identifiants, les auteurs de menace utilisent des justificatifs d'identité qui ont été divulgués ou volés et les « bourrent » dans les pages d'ouverture de session d'autres sites Web jusqu'à ce que des correspondances soient trouvées.

Afin de promouvoir la sécurité et la fonctionnalité continues de vos services Web, mettez en œuvre un processus de gestion des correctifs pour acquérir, tester et installer des correctifs et des mises à jour sur vos systèmes et appareils. Assurez-vous de corriger les systèmes sous-jacents, les systèmes de gestion du contenu, les applications Web et les modules d'extension.

Vous devriez également promouvoir la sécurité au sein de votre organisation et auprès de vos clients. Une plus grande transparence des mesures que vous prenez pour protéger les données vous aidera à établir un lien de confiance avec vos organisations partenaires, votre chaîne d'approvisionnement et vos clients.

SIGNALER UN INCIDENT

Si votre organisation est victime de fraude, communiquez avec le service de police le plus près de chez vous et signez l'incident en ligne au moyen du système de signalement de cas de fraude du Centre antifraude du Canada.

POUR EN SAVOIR PLUS

Le projet de sécurité des applications Web de sources ouvertes (OWASP pour *Open Source Web Application Security Project*) dresse la liste des dix plus importants risques en matière de sécurité des applications Web.

Pour la liste complète des documents d'orientation, consultez le site cyber.gc.ca. Voici certaines publications connexes :

- *Défiguration de site Web* (ITSAP.00.060)
- *Gestion et contrôle des privilèges administratifs* (ITSAP.10.094)
- *Sécurisez vos comptes avec une authentification multifacteur* (ITSAP.30.030)
- *Protéger son organisation contre les attaques par déni de service* (ITSAP.80.100)

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

 No de cat.D97-1/60-005-2021F-PDF | ISBN 978-0-660-40249-9