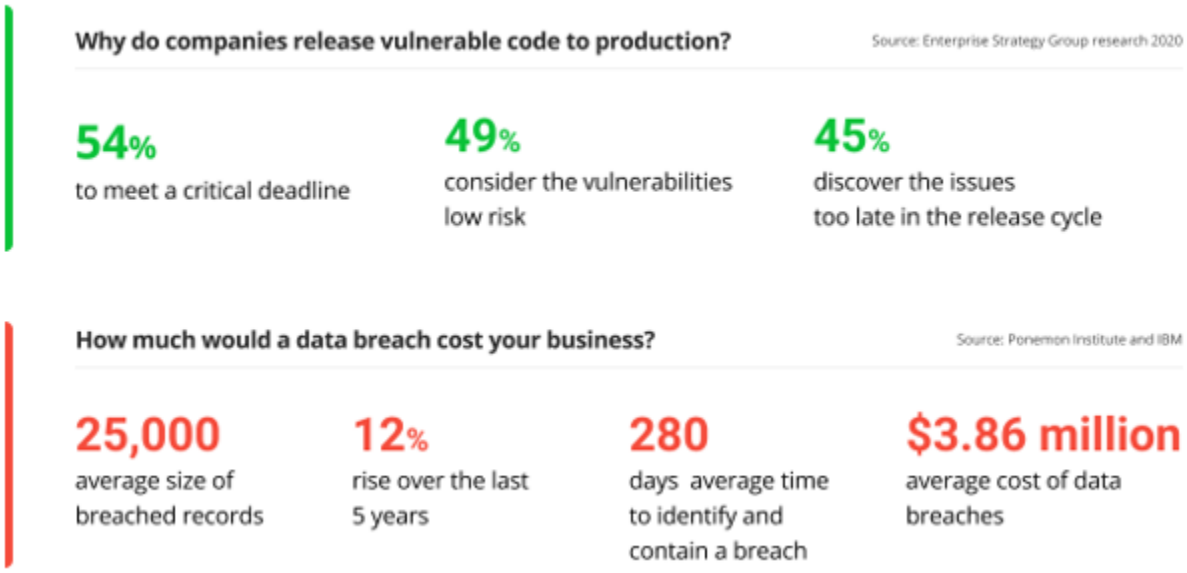
Comment sécuriser les applications Web contre les vulnérabilités couramment connues en 2021

Pour de nombreuses entreprises, 2020 consistait à passer au travail à distance dans des systèmes d'entreprise basés sur le cloud, et les équipes de sécurité des applications ont dû s'adapter à un changement d'usage et à un nombre croissant de défis.

Les vulnérabilités des applications Web étaient à l'origine de 43 % des violations de données en 2019, selon The 2020 Verizon Data Breach Investigations Report. Étonnamment, 79 % des organisations ont intentionnellement poussé du code vulnérable à la production, tout en considérant que leur propre niveau de sécurité des applications est supérieur à 7 sur 10, selon une étude de l'Enterprise Strategy Group.



Le coût moyen des violations de données étant de 3,86 millions de dollars , la sécurité des applications n'est certainement pas quelque chose que les entreprises peuvent ignorer. Les chiffres ne cessent d'augmenter, de 12 % au cours des cinq dernières années.

Par rapport à d'autres actifs informatiques, les applications Web sont particulièrement vulnérables aux attaques, car elles sont exposées à Internet. De nombreux vecteurs d'attaque contre les applications Web se concentrent sur la manipulation des entrées utilisateur via des formulaires Web et des entrées machine via des API.

Dans cet article, nous discuterons des vulnérabilités des applications Web et des meilleures pratiques pour protéger les applications Web contre les attaques malveillantes et les dommages accidentels. Vous pouvez télécharger la **liste** de **contrôle des exigences** de sécurité des applications Web pour sécuriser votre application Web sous tous les angles.

Vulnérabilités des applications Web

Les vulnérabilités des applications Web sont des faiblesses de sécurité qui permettent aux acteurs malveillants de manipuler le code source, d'obtenir un accès non autorisé, de voler des données ou d'interférer de quelque manière que ce soit avec le fonctionnement normal de l'application.

Le document OWASP Top 10 répertorie les risques de sécurité les plus critiques pour les applications Web. Passons en revue quelques vecteurs d'attaque connus :

- Injection SQL : se produit lorsque les attaquants utilisent du code SQL malveillant pour manipuler les bases de données principales. Le résultat peut inclure une liste de données non autorisée, une suppression (suppression) de tables et un accès administratif non autorisé.
- Cross-Site Scripting (XSS) : une attaque ciblant les utilisateurs d'une application. Il peut être utilisé pour accéder aux comptes d'utilisateurs, injecter des chevaux de Troie ou modifier le contenu de la page pour tromper les utilisateurs ou dégrader un site Web. Une autre variante, plus dangereuse, est le XSS stocké, lorsqu'un code malveillant est injecté de manière persistante dans l'application. Le XSS reflété se produit lorsque des scripts malveillants sont reflétés de l'application vers le navigateur de l'utilisateur.

- Inclusion de fichiers à distance (RFI) : injection à distance de fichiers dans un serveur d'applications Web. Cela peut entraîner l'exécution de scripts et de codes malveillants dans les applications, la compromission du serveur Web et le vol de données.
- Cross-Site Request Forgery (CSRF) : une attaque qui peut entraîner des transferts de fonds indésirables, des modifications de mot de passe ou le vol de données. Implique un attaquant exploitant la session ouverte d'un utilisateur, ce qui amène le navigateur de l'utilisateur à effectuer sans le savoir des actions sur un site auquel l'utilisateur est connecté.

L'assainissement des entrées et des sorties des applications et l'adoption de pratiques de codage sécurisées peuvent protéger les applications contre la plupart des vulnérabilités. Ce n'est pas sufisant. Les applications Web sont en développement constant et des tests de sécurité doivent être intégrés à chaque étape du cycle de vie du développement, afin d'identifier et de corriger le code vulnérable dès le début.

De plus, la plupart des applications Web utilisent des composants open source tiers, qui peuvent eux-mêmes être vulnérables et doivent être analysés en permanence.

Conseils d'experts

La plupart des frameworks Web modernes fournissent des techniques de sécurité prêtes à l'emploi pour empêcher les vulnérabilités courantes telles que SQL Injection, XSS, CSRF.

Techniques et outils de sécurité des applications Web

La technique de sécurité la plus puissante dans le développement Web consiste à penser à la sécurité dans tous les détails, même les plus petits. La sécurité des applications Web ne concerne pas seulement la base de code, mais aussi les processus de projet, le stockage des données, les politiques de l'entreprise, etc. En fin de compte, peu importe la qualité et la protection de votre code, si votre documentation API est accessible au public ou le mot de passe super administrateur écrit sur un tableau blanc au bureau.

Donc, tout d'abord, la sécurité des applications vient de la sécurité du projet lui-même. Mais lorsque tous les processus sont parfaits, quelle est la prochaine étape ?

Pour obtenir des informations sur la sécurité des applications Web, il existe généralement deux approches principales. Nous parlons de tests de sécurité statiques et dynamiques. Ils ne s'excluent pas mais doivent au contraire se compléter.

Voici quelques technologies que vous pouvez utiliser pour protéger vos applications Web contre les vulnérabilités, ainsi que pour répondre aux attaques si elles se produisent.

SAST

Les solutions SAST (Static Application Security Testing) analysent votre code source à la recherche de vulnérabilités et de risques de sécurité. De nombreuses applications Web intègre l'analyse de code à plusieurs étapes de développement, principalement lors de la validation du nouveau code dans la base de code et lors d'une construction.

SAST est généralement basé sur des règles et les résultats de l'analyse incluent généralement des faux positifs. Vous devrez donc analyser et filtrer soigneusement les résultats pour identifier les vrais problèmes de sécurité.

Conseils d'experts

Nous utilisons l'outil d'analyse statique SonarQube pour surveiller les problèmes de sécurité qui peuvent être introduits pendant le développement. Il est recommandé de l'intégrer au pipeline CI/CD afin qu'il analyse chaque commit/merge commit. SonarQube a une bonne représentation visuelle et vérifie non seulement les aspects de sécurité, mais également la maintenabilité et la fiabilité de la base de code. Il prend en charge plus de 20 langages de programmation différents, il fonctionne donc pour la plupart des frameworks frontend et backend.

DAST

Les tests dynamiques de sécurité des applications (DAST) consistent à tester le code déployé ou à exécuter pour détecter les vulnérabilités. Il peut être effectué à la fois manuellement et automatiquement, à l'aide d'outils spéciaux.
Les tests manuels s'articulent autour de l'utilisation de l'API d'application avec des outils tels que la suite Burp, Fiddler, Postman.

Les outils DAST d'automatisation envoient un grand nombre de requêtes au code d'application, y compris des entrées inattendues et malveillantes, à la recherche de vulnérabilités. Il analyse les résultats et identifie les failles de sécurité.

Conseils d'experts

Après une analyse de sécurité manuelle réfléchie, nous utilisons OwaspZap, un scanner de sécurité d'applications Web open source, pour accélérer les tests de régression. Les scanners ne peuvent pas remplacer les humains en termes de créativité, d'analyse des causes profondes ou de capacité à sortir des sentiers battus, mais ils peuvent gérer les tâches de routine à un rythme et un volume beaucoup plus rapide.

TESTS DE PÉNÉTRATION

Les tests d'intrusion sont une technique de sécurité qui combine des outils d'analyse dynamique et une expertise en sécurité humaine pour détecter les failles dans la posture de sécurité d'une application Web.

Les pentesters agissent comme de véritables acteurs de la menace : ils exploitent les vulnérabilités, obtiennent des accès non autorisés, volent des données et perturbent les services. Cependant, ils le font sous contrat avec le propriétaire de l'application Web, dans un périmètre convenu, et sans causer de dommages réels à l'organisation.

Par rapport au SAST et au DAST, cette technique est plus complexe à mettre en œuvre, mais permet d'identifier des risques supplémentaires que les outils automatisés peuvent ignorer.

XDR

Les solutions de détection et de réponse étendues (XDR) sont une nouvelle génération de plates-formes de sécurité qui offrent aux équipes de sécurité une interface leur permettant de détecter et de répondre aux menaces partout où elles existent dans l'environnement informatique.

XDR collecte les données de sécurité de toutes les couches de la pile de sécurité, y compris les applications Web, les réseaux, les clouds privés et publics et les points de terminaison. Il applique des analyses et une automatisation avancée pour analyser, trier et détecter les menaces connues et inconnues. Plus important encore, il s'intègre directement aux outils de sécurité et peut répondre automatiquement aux menaces en temps réel.

Références :

https://mobidev.biz/blog/