TOP 10 OWASP 2017

A1 : 2017 – FAILLE D’INJECTION

Les failles d’injection telles que les injections SQL, NoSQL, OS et LDAP sont fréquentes dans les applications Web. L'injection se produit quand des données provenant de l'utilisateur sont envoyées à un interpréteur en tant qu'élément faisant partie d'une commande ou d'une requête. Les données hostiles de l'attaquant dupent l'interpréteur afin de l'amener à exécuter des commandes fortuites, à changer des données, etc.

HubSO

TOP 10 OWASP 2017

A2 : 2017 – VIOLATION DE GESTION D’AUTHENTIFICATION

Les fonctions applicatives relatives à l'authentification et la gestion de session ne sont souvent pas mises en œuvre correctement, permettant aux attaquants de compromettre les mots de passe, clés, jetons de session, ou d'exploiter d'autres failles d'implémentation pour s'approprier les identités d'autres utilisateurs.

HubSO

TOP 10 OWASP 2017

A3 : 2017 – EXPOSITION DE DONNEES SENSIBLES

L'exposition de données sensibles peut se produire lorsque des fonctions de sécurité adéquates ne sont pas appliquées sur les données ou sont appliquées de façon incorrecte permettant ainsi aux attaquants de dérober des informations sensibles telles que des mots de passe, des informations de paiement, des adresses ou toute autre information pouvant être d'une certaine valeur pour l'attaquant. Les données sensibles doivent être bien protégées à la fois au stockage et durant leur transport et des précautions particulières doivent être prises lorsqu'elles sont échangées avec un navigateur Web.

HubSO

TOP 10 OWASP 2017

A4 : 2017 – ATTAQUE XXE

Une attaque XXE est un type d'attaque contre un analyseur syntaxique XML. Cette attaque se produit lorsqu'un fichier XML contenant une référence à une entité externe est traité par un analyseur XML mal configuré. Les attaquants peuvent facilement exploiter les vulnérabilités dans ces analyseurs XML, en leur donnant des fichiers XML malveillants qui peuvent contenir du code indésirable. Cette attaque peut mener à la divulgation de données confidentielles, au déni de service, à la falsification des requêtes côté serveur, à l'analyse des ports du point de vue de la machine où se trouve l'analyseur et à d'autres impacts.

HubSO

TOP 10 OWASP 2017

A5 : 2017 – VIOLATION DE CONTRÔLE D’ACCES

Le contrôle d’accès permet de spécifier ce qu’il est permis aux utilisateurs authentifiés de faire sur une application. Pour mettre en place un contrôle d’accès adéquat, il faut s’assurer que de bonnes vérifications d’autorisation et une bonne authentification permettant de dire ce qu’un tel utilisateur peut faire sur l’application soient en place.

Les restrictions sur ce que les utilisateurs authentifiés sont autorisés à faire ne sont souvent pas correctement appliquées. Les attaquants peuvent exploiter ces failles pour accéder à des fonctionnalités et/ou données non autorisées, telles que l'accès aux comptes d'autres utilisateurs, l'affichage de fichiers sensibles, la modification des données d'autres utilisateurs, la modification des droits d'accès, etc.

HubSO

TOP 10 OWASP 2017

A6 : 2017 – MAUVAISE CONFIGURATION DE SECURITE

La sécurité d'une application Web ne concerne pas seulement le code. D'après l'Owasp, la mauvaise configuration de sécurité est le problème le plus souvent rencontré. Ceci est généralement le résultat de configurations par défaut non sécurisées, de configurations incomplètes, d'un stockage cloud ouvert, d'en-têtes HTTP mal configurés, de messages d'erreur détaillés contenant des informations sensibles, entre autres. Une sécurité renforcée nécessite un ensemble de configurations correctes et sécurisées déployées pour les applications, les frameworks, les serveurs, les bases de données et le code. De même, toutes ces configurations doivent être maintenues à jour.

HubSO

TOP 10 OWASP 2017

A7 : 2017 – CROSS-SITE SCRIPTING (XSS)

Les failles XSS se produisent lorsqu'une application accepte des données non fiables et les envoie à un browser web sans validation appropriée. XSS permet à des attaquants d'exécuter du script dans le navigateur de la victime afin de détourner des sessions utilisateur, défigurer des sites web, insérer du contenu hostile, effectuer des attaques par phishing, et prendre le contrôle du navigateur de l'utilisateur en utilisant un script malicieux. Le script malicieux est habituellement écrit en JavaScript, mais n'importe quel langage de programmation supporté par le navigateur de la victime est un moyen d'exécution de cette attaque.

HubSO

TOP 10 OWASP 2017

A8 : 2017 – DESERIALISATION NON SECURISEE

La sérialisation est le processus consistant à transformer un objet en un format pouvant être restauré plus tard. Les objets sont le plus souvent sérialisés afin d'être sauvegardés ou d'être transmis dans le cadre d'une communication. La désérialisation est le processus inverse, c'est-à-dire le fait de prendre des données structurées à partir d'un certain format et de les reconstruire en un objet. Une désérialisation non sécurisée conduit souvent à l'exécution de code distant, et même si les failles de désérialisation n'aboutissent pas à l'exécution de code distant, elles peuvent être utilisées pour effectuer des attaques, y compris des attaques d'injection et d'escalade de privilèges.

A9 : 2017 – UTILISATION DE COMPOSANTS VULNERABLES

Les composants logiciels, bibliothèques et frameworks utilisés dans les applications Web proviennent le plus souvent de la communauté open source et doivent être utilisés avec prudence au cas où des vulnérabilités s'y cacheraient. En effet certaines versions d'un composant peuvent être sujettes à diverses vulnérabilités qui pourraient avoir été corrigées dans les versions les plus récentes. Une fois qu'une vulnérabilité est révélée, les failles sont rendues publiques. Ces failles peuvent ensuite être utilisées pour compromettre avec succès la version vulnérable d'un composant et par le même biais, les applications l'utilisant.

HubSO

TOP 10 OWASP 2017

A10 : 2017 – LOGGING ET MONITORING INSUFFISANTS

Les événements tels que les tentatives de connexion réussies et infructueuses, l'adresse IP des connexions entrantes, les événements importants tels que les transactions de grande valeur doivent être enregistrés et surveillés régulièrement. Ce faisant, l'on peut comprendre tout ce qui se passe sur l'application et être prêt à réagir en cas d'attaque. Autrement, il peut être très difficile de répondre à une attaque ou de connaître l'origine d'une certaine faille.

HubSO

TOP 10 OWASP 2017