Securing Web Application Technologies [SWAT] Checklist

https://www.sans.org/cloud-security/securing-web-application-technologies/?msc=cloud-security-lp

Gestion des erreurs et des journaux

Bonne pratique	
Afficher des messages d'erreur génériques	
Aucune exception non gérée	
Supprimer les erreurs générées par le framework	
Consigner toutes les activités d'authentification	
Consigner toutes les modifications de privilèges	
Journaliser les activités administratives	
Journaliser les accès aux données sensibles	
Ne pas journaliser de données inappropriées	
Stockez les journaux en toute sécurité	

Protection des données

Bonne pratique	
Utilisez HTTPS partout	
Désactiver l'accès HTTP pour toutes les ressources protégées	
Utiliser l'en-tête Strict-Transport-Security	
Stockez les mots de passe des utilisateurs à l'aide d'un hachage fort, itératif et salé	
Échangez vos clés de chiffrement dans un mode sécurisé	
Mettre en oeuvre des processus sécurisés de gestion des clés	
Utiliser des certificats HTTPS valides d'une autorité de certification réputée	
Désactiver la mise en cache des données et la saisie semi-automatique	
Limiter l'utilisation et le stockage des données sensibles	

Configuration et mise en œuvre

Bonne pratique	
Automatisez le déploiement des applications	
Établir un processus rigoureux de gestion du changement	
Définir les exigences de sécurité	
Effectuer une revue de conception	
Effectuer des revues de code	
Effectuer des tests de sécurité	
Renforcez l'infrastructure	
Définir un plan de traitement des incidents	
Former l'équipe à la sécurité	

Authentification

Bonne pratique	
Ne codez pas les informations d'identification en dur	
Développer un système de réinitialisation de mot de passe fort	
Mettre en œuvre une politique de mots de passe forts	
Mettre en œuvre le verrouillage de compte contre les attaques par force brute	
Ne divulguez pas trop d'informations dans les messages d'erreur	
Stockez les informations d'identification de la base de données	
Les applications et le middleware doivent fonctionner avec des privilèges minimaux	

Gestion des sessions

Bonne pratique	
Assurez-vous que les identifiants de session sont suffisamment aléatoires	
Régénérer les jetons de session	
Implémenter un délai d'expiration de session inactive	
Implémenter un délai d'expiration de session absolu	
Détruire les sessions à tout signe de falsification	
Invalider la session après la déconnexion	
Placez un bouton de déconnexion sur chaque page	
Utiliser les attributs de cookies sécurisés (HttpOnly, Secure et SameSite Flags)	
Définir correctement le domaine et le chemin des cookies	
Définir l'heure d'expiration des cookies	

Gestion des entrées et sorties

Bonne pratique	
Préférez les listes d'autorisation aux listes de blocage	
Utiliser des requêtes SQL paramétrées	
Utiliser des jetons pour empêcher les demandes falsifiées	
Définir l'encodage de votre application	
Valider les fichiers téléchargés	
Utiliser l'en-tête Nosniff pour le contenu téléchargé	
Valider la source d'entrée	
Utiliser l'en-tête X-Frame-Options	
Utiliser des en-têtes de réponse HTTP sécurisés	
Désérialiser les données non fiables en integrant des contrôles appropriés	

Contrôle d’accès

Bonne pratique	
Appliquer les vérifications des contrôles d'accès de manière cohérente	
Appliquer le principe du moindre privilège	
N'utilisez pas de transferts ou de redirections non validés	