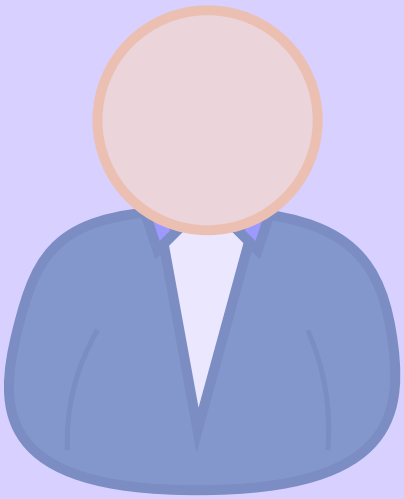
UVSQ
université PARIS-SACLAY

IUT de Vélizy-Rambouillet
CAMPUS DE VÉLIZY-VILLACOUBLAY

CYBERSECURITE



Yannis BOUTTIER

Présentation des attaques

Injection SQL

Description: **L'injection SQL** est une attaque visant à exploiter les failles de **sécurité** dans le traitement des **requêtes SQL** par une application. Les attaquants insèrent du **code SQL** malveillant dans les champs de saisie, les **paramètres d'URL** ou d'autres zones où des données utilisateur sont incluses. Cela peut permettre aux **attaquants** de manipuler la **base de données**, d'exécuter des commandes non autorisées ou de récupérer des données sensibles.

Méthode: Les attaquants utilisent souvent des requêtes **SQL** malicieuses comme **UNION SELECT**, **DROP TABLE**, ou **OR 1=1** dans les champs de formulaire pour exploiter des vulnérabilités.

Exemple réel: En 2013, Adobe a été victime d'une attaque par injection SQL. Les attaquants ont exploité une faille dans le logiciel de gestion des utilisateurs d'Adobe, permettant l'accès non autorisé à des données sensibles, y compris des millions d'identifiants et de mots de passe cryptés.

RFI

Description: L'inclusion de fichiers à distance se produit lorsque des attaquants parviennent à **inclure** des fichiers distants dans le **code source** d'une **application**. Cela peut conduire à l'exécution de **scripts malveillants** hébergés sur des serveurs **externes**.

Méthode: Les attaquants exploitent des vulnérabilités permettant **l'inclusion dynamique** de fichiers (par exemple, avec des fonctions include() ou require() en **PHP**) en fournissant des **URL malicieuses**.

Exemple réel: En 2012, le site Web de la Chambre des représentants des États-Unis a été victime d'une attaque RFI. Les attaquants ont exploité une vulnérabilité pour inclure un fichier malveillant, compromettant la sécurité du site.

CSRF

Description: Le **CSRF** force un utilisateur authentifié à effectuer involontairement des actions sur un site où il est connecté. L'attaquant exploite la confiance que le site a envers l'utilisateur.

Méthode: Les attaquants créent des **liens** ou des **formulaires malveillants** et incitent les utilisateurs à les **ouvrir** alors qu'ils sont déjà **authentifiés** sur un autre site.

Exemple réel: En 2013, Facebook a été victime d'une attaque CSRF. Des liens malveillants ont été partagés, incitant les utilisateurs à aimer involontairement des pages ou à ajouter des amis.

XSS

Description : Le **cross-site scripting** permet à un attaquant d'injecter du code JavaScript malveillant dans des pages web consultées par d'autres utilisateurs. Cela peut être utilisé pour voler des informations, rediriger les utilisateurs vers des sites malveillants, ou effectuer des actions au nom de la victime.

Méthode: Les attaquants injectent généralement du code **JavaScript** dans des champs de formulaire, des zones de **commentaire**, ou des paramètres **d'URL**. Lorsque d'autres utilisateurs visitent la page, le code s'exécute dans leur navigateur.

Exemple réel: En 2010, le réseau social Twitter a été victime d'une attaque XSS. Des tweets contenant du code JavaScript malveillant ont été postés, affectant les utilisateurs qui consultent ces tweets.

Tendances actuelles

Les tendances en matière de sécurité web évoluent constamment pour faire face aux nouvelles menaces et aux avancées technologiques.

Protection contre les attaques de supply chain

Les attaques visant la chaîne d'approvisionnement, telles que **l'injection de code malveillant** dans des bibliothèques **tierces** ou des composants **logiciels**, sont en **hausse**. Les organisations renforcent la **sécurité** de leur chaîne d'approvisionnement pour minimiser ces **risques**.

Intelligence Artificielle et Machine Learning en sécurité

Les technologies **d'intelligence artificielle** et de **machine learning** sont de plus en plus utilisées pour détecter les anomalies, identifier les comportements suspects et automatiser les réponses aux incidents de sécurité.

Zero Trust Security

La tendance **Zero Trust** repose sur le principe de ne faire confiance à personne, même à l'intérieur du périmètre de sécurité. Les entreprises adoptent des approches de sécurité qui vérifient l'identité et l'autorisation à chaque étape, plutôt que de simplement faire confiance aux utilisateurs ou aux périphériques une fois qu'ils ont franchi la frontière du réseau.

Protection de la confidentialité des données

Avec l'accent accru sur la confidentialité des données, les entreprises cherchent à mettre en œuvre des politiques et des technologies qui garantissent la protection des données sensibles conformément aux réglementations telles que le **RGPD**.

DevSecOps

L'intégration de la sécurité dans les pratiques **DevOps**, appelée **DevSecOps**, est devenue une norme. Les équipes de développement, d'exploitation et de sécurité collaborent dès le début du processus de développement pour intégrer des mesures de sécurité de manière continue.

Prévisions pour l'Avenir

Quantum-Safe Cryptography

Avec le développement potentiel de l'informatique quantique, l'industrie se penche sur des techniques de chiffrement appelées **cryptographie quantum-safe**.

Blockchain en Sécurité

La technologie **blockchain** est explorée pour renforcer la **sécurité**, notamment dans la gestion des **identités**, la **traçabilité** des **transactions** et la **protection** contre les **attaques**.

Automatisation et Orchestration de la Sécurité

L'automatisation et **l'orchestration** deviendront encore plus essentielles pour gérer la complexité **croissante** des environnements de sécurité et répondre rapidement aux **menaces**.

Amélioration de la Détectabilité des Menaces

Les efforts pour améliorer la détection précoce des menaces, notamment à l'aide de l'**IA**, se poursuivront pour réduire les délais de **détection** et de **réponse**.

Importance Sécurité Web

La sécurité web est d'une importance cruciale dans le contexte actuel de la cybersécurité en raison de plusieurs facteurs qui rendent internet dynamique et complexe

Augmentation des Menaces en Ligne

Les cybermenaces sont de plus en plus sophistiquées et variées, allant des attaques par **phishing** aux **ransomwares** en passant par les attaques de type **zero-day**. Les applications web, étant souvent accessibles en ligne, sont des cibles privilégiées pour les attaquants.

Protection des Données Sensibles

Les applications web traitent fréquemment des informations sensibles telles que les données **personnelles**, les informations **financières** et les **identifiants** de **connexion**. La **sécurité web** est essentielle pour protéger ces données contre les accès non **autorisés**, les **fuites** ou encore les **manipulations**.

Conformité Réglementaire

Les réglementations sur la protection des données, comme le **RGPD**, imposent des exigences strictes en matière de sécurité des données. Les organisations doivent garantir la conformité de ces **réglementations** afin d'éviter une **mauvaise réputation**.

Confiance des Utilisateur

La **confiance** des utilisateurs est un élément **clé** de la **réussite** des applications web car ils s'attendent à ce que leurs données soient **sécurisées**. Dans le cas contraire, les **évènements** peuvent entraîner une **perte** de confiance, des conséquences **financières** et des **pertes** de clientèle.

Complexité des Applications Web

Les applications web modernes sont souvent complexes. Elles utilisent des technologies variées telles que les **API**, les **bases de données** et les **frameworks**.

Attaques Ciblées

Les attaques ciblées contre des organisations spécifiques sont de plus en plus courantes. Les attaquants exploitent souvent des **vulnérabilités** dans les applications web pour accéder à des systèmes **sensibles** ou voler des **informations confidentielle**

Évolution des Technologies

L'évolution rapide des technologies, telles que le **IoT** et **l'intelligence artificielle**, introduit de nouveaux fonctionnement en matière de **sécurité** web. Les organisations doivent constamment s'adapter pour **protéger** leurs **infrastructures**

Conclusion

La **sécurité web** est un **pilier fondamental** de la **cybersécurité globale**, elle a pour mission de **protéger** les applications et les données. Les **investissements** dans la **sécurité web** sont essentiels pour garantir la **sécurité** des **utilisateurs** et des **entreprises**.

Lien de mon site

https://yannis.bouttier.mmi-velizy.fr/cybersecurite/

Bibliographie

- https://www.01net.com/actualites/adobe-pirate-2-9-millions-de-comptes-clients-compromis-604762.html
- https://www.journaldunet.com/solutions/dsi/1069577-pourquoi-la-nouvelle-menace-des-url-raccourcies-interesse-les-plus-grands-editeurs/
- https://www.lepoint.fr/high-tech-internet/facebook-cible-d-une-cyberattaque-16-02-2013-1628084_47.php#11
- https://openclassrooms.com/fr/courses/7727176-realisez-un-test-dintrusion-web/7917166-attaquez-la-base-de-donnees-avec-les-injections-sql
- https://fr.eitca.org/la-cyber-s%C3%A9curit%C3%A9/eitc-est-les-fondamentaux-de-la-s%C3%A9curit%C3%A9-des-applications-Web-de-wasf/script-intersite/d%C3%A9fenses-contre-les-scripts-intersites/examen-examen-d%C3%A9fenses-contre-le-cross-site-scripting/quelles-sont-les-d%C3%A9fenses-courantes-contre-les-attaques-XSS/
- https://www.ionos.fr/digitalguide/serveur/securite/cross-site-request-forgery/
- https://www.rejoindre-plus-que-pro.fr/en-savoir-plus/transformation-numerique/tendances-cles-enjeux-cybersecurite/
- https://www.itforbusiness.fr/15-predictions-cybersecurite-pour-2024-et-au-dela-70009
- https://www.europarl.europa.eu/news/fr/headlines/society/20211008STO14521/pourquoi-la-cybersecurite-est-elle-importante-pour-l-ue
- https://www.onelogin.com/fr-fr/learn/what-is-cyber-security
- https://weblog.wemanity.com/fr/la-cybersecurite-pilier-dune-transformation-digitale-reussie/