|  |  |
| --- | --- |
| A1 - Cross Site Scripting  (XSS) | Les failles XSS se produisent à chaque fois qu'une application prend des données écrites par l'utilisateur et les envoie à un browser web sans avoir au préalable validé ou codé ce contenu. 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, potentiellement introduire des vers, etc.  Les failles XSS se produisent à chaque fois qu'une application prend des données écrites par l'utilisateur et les envoie à un browser web sans en avoir au préalable validé ou codé le contenu.  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 (Malware Scripting). Le script malicieux est habituellement écrit en Javascript, mais n'importe quel langage de programmation supporté par le navigateur de la victime est une cible potentielle pour cette attaque. |
| A2 - Faille d’Injection | Les failles d'injection, en particulier l'injection SQL, sont communes dans les applications web. L'injection se produit quand des données écrites par 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 ou changer des données.  Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. |
| A3 - Exécution de Fichier  Malicieux | Un code vulnérable à l'inclusion de fichier à distance (RFI - Remote File Inclusion) permet à des attaquants d'inclure du code et des données hostiles, ayant pour résultat des attaques dévastatrices, telle la compromission totale d'un serveur. Les attaques par exécution de fichier malveillant affectent PHP, XML et toute structure qui accepte des noms de fichiers ou des fichiers des utilisateurs. |
| A4 - Référence directe non sécurisée à un Objet | Une référence directe à un objet se produit quand un développeur expose une référence à un objet d'exécution interne, tel qu'un fichier, un dossier, un enregistrement de base de données, ou une clef, comme paramètre d'URL ou de formulaire. Les attaquants peuvent manipuler ces références pour avoir accès à d'autres objets sans autorisation. |
| A5 - Falsification de requête inter-site (CSRF) | Une attaque CSRF (Cross Site Request Forgery) force le navigateur d'une victime authentifiée à envoyer une demande pré-authentifiée à une application web vulnérable, qui force alors le navigateur de la victime d'exécuter une action hostile à l'avantage de l'attaquant.  CSRF peut être aussi puissant que l'application web qu'il attaque. |
| A6 - Fuite d’Information et Traitement d’Erreur  Incorrect | Les applications peuvent involontairement divulguer des informations sur leur configuration, fonctionnements internes, ou violer la vie privée à travers toute une variété de problèmes applicatifs. Les attaquants utilisent cette faiblesse pour subtiliser des données sensibles ou effectuer des attaques plus sérieuses. |
| A7 - Violation de Gestion d’Authentification et de Session | Les droits d'accès aux comptes et les jetons de session sont souvent incorrectement protégés. Les attaquants compromettent les mots de |
|  | passe, les clefs, ou les jetons d'authentification identités pour s'approprier les identités d'autres utilisateurs. |
| A8 - Stockage  Cryptographique non  Sécurisé | Les applications web utilisent rarement correctement les fonctions cryptographiques pour protéger les données et les droits d'accès. Les attaquants utilisent des données faiblement protégées pour perpétrer un vol d'identité et d'autres crimes, tels que la fraude à la carte de crédit. |
| A9 - Communications non  Sécurisées | La plupart du temps, les applications ne chiffrent pas le trafic réseau quand il est nécessaire de protéger des communications sensibles. |
| A10 - Manque de  Restriction d’Accès URL | Fréquemment, une application protège seulement la fonctionnalité sensible en empêchant l'affichage des liens ou des URLs aux utilisateurs non autorisés. Les attaquants peuvent utiliser cette faiblesse pour accéder et effectuer des opérations non autorisées en accédant à ces URL directement. |