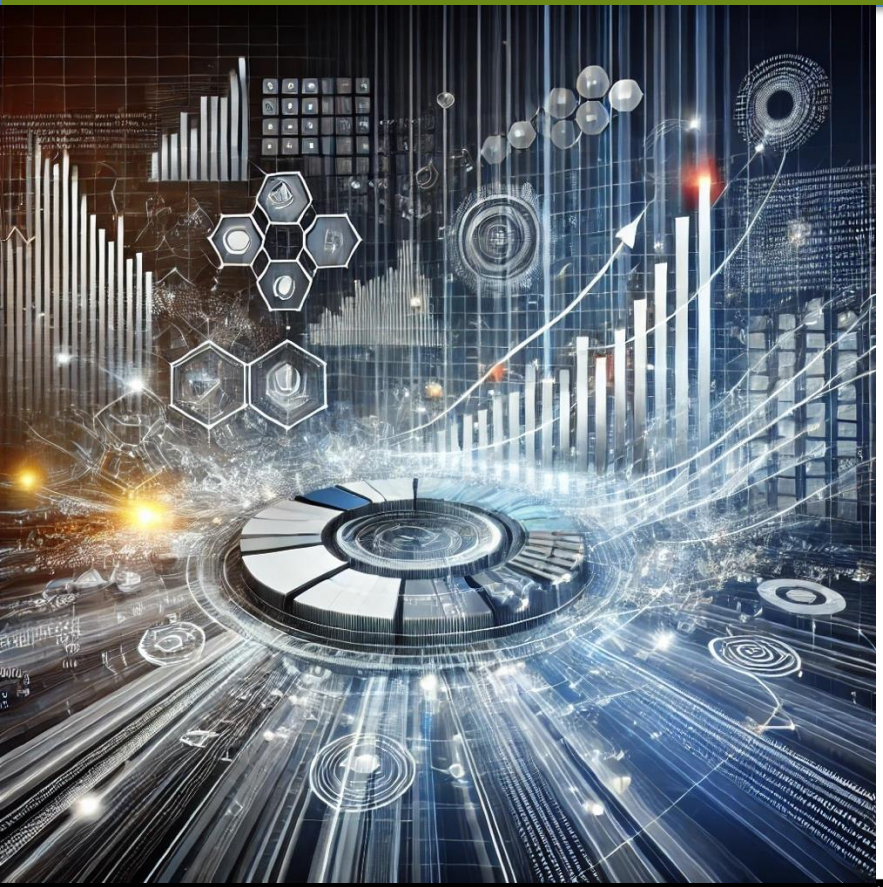
Sécurité et gouvernance des données



- **Cyberattaques**

1. ATTAQUES BASÉES SUR DES MALWARES RANSOMWARES, CHEVAUX DE TROIE, ETC

- **Malware** désigne un « logiciel malveillant » conçu pour perturber ou voler des données d'un réseau informatique ou d'un serveur.
- **Ransomware** : ce type de malware crypte les fichiers de votre système et bloque l'accès jusqu'à ce que vous payiez une « rançon » (généralement en cryptomonnaie).
- **Logiciel espion** : comme son nom l'indique, ce type de logiciel malveillant espionne vos activités et renvoie des données au pirate. Il peut s'agir de vos coordonnées bancaires, de vos identifiants et de vos mots de passe.
- **Keyloggers** : les keyloggers sont similaires aux logiciels espions, à la différence qu'ils suivent vos activités. Tout ce que vous saisissez est envoyé au pirate et peut être utilisé à des fins de chantage ou de vol d'identité.
- **Trojans** : cheval de Troie, ces types de malwares se « cachent » dans un logiciel légitime.
  - Par exemple, vous pouvez télécharger ce que vous *pensez* être un logiciel antivirus, mais votre appareil est infecté.

1. ATTAQUES BASÉES SUR DES MALWARES RANSOMWARES, CHEVAUX DE TROIE, ETC

- **Virus** : les virus se fixent sur les programmes et les fichiers et se déclenchent lorsque vous les ouvrez. Une fois actif, un virus peut se répliquer à votre insu et ralentir votre appareil ou détruire des données.
- **Vers** sont des virus qui se déplacent sur votre réseau d'un ordinateur infecté à un autre, donnant aux pirates un accès à distance à l'ensemble de votre système.

- Les attaques de logiciels malveillants peuvent toucher des particuliers via des liens dans email de phishing.
- Mais elles sont également utilisées pour attaquer des entreprises et des organisations.

- En mai 2021, JBS USA, le plus grand fournisseur mondial de viande, a été victime d'une attaque de Ransomware
  - a entraîné l'arrêt de la production dans de nombreuses de ses usines.
  - L'entreprise a fini par payer une rançon de 11 millions de dollars en Bitcoin pour éviter de nouveaux dommages

2. ATTAQUES DE PHISHING (SPEAR PHISHING, WHALING…)

- Une attaque de phishing se produit lorsqu'un cybercriminel vous envoie un e-mail, un SMS (appelé « smishing») ou un appel téléphonique (appelé « vishing ») frauduleux.
- Ces messages semblent provenir d'une autorité officielle ou d'une personne ou entreprise en laquelle vous avez confiance, comme votre banque, le FBI ou une entreprise comme Microsoft, Apple ou Netflix .
- En réalité, ces messages sont envoyés par des imposteurs. Si vous répondez avec des informations sensibles telles que votre mot de passe, ils peuvent les utiliser pour prendre le contrôle de vos comptes.
- Les messages de phishing et de **smishing** peuvent également vous demander de cliquer sur un lien ou d'ouvrir une pièce jointe à un e-mail qui téléchargera un logiciel malveillant sur votre appareil ou vous enverra vers un site de phishing conçu pour voler vos informations.
  - Dans de nombreux cas, les attaques de phishing sont très larges et ne ciblent pas des individus spécifiques (ce qui les rend plus faciles à identifier).
  - Cependant, il existe quelques nouvelles cyberattaques de phishing plus ciblées et plus difficiles à repérer.

2. ATTAQUES DE PHISHING (SPEAR PHISHING, WHALING…)

- **Attaques de spear phishing** : ces attaques sont généralement envoyées par courrier électronique et ciblent une personne spécifique. Le pirate utilisera vos informations personnelles qu'il a achetées sur le Dark Web (ou trouvées dans votre empreinte digitale et sur les réseaux sociaux) pour rendre le tout plus crédible et vous inciter à cliquer sur le lien.
- **Whaling** : une attaque de phishing (hameçonnage) se produit lorsqu'un pirate cible des personnes de haut rang, comme des PDG et des cadres. L'objectif est de voler leurs identifiants et d'obtenir un accès par porte dérobée au réseau de leur entreprise.
  - La fraude au PDG représente désormais 26 milliards de dollars par an
- **Attaques de phishing de type Angler** : est un nouveau type d'escroquerie par phishing dans lequel un pirate « appâte » les utilisateurs sur les réseaux sociaux en se faisant passer pour le compte du service client d'une entreprise bien connue.
  - Les escrocs créent des comptes comme « @AmazonHelp$ » et répondent ensuite automatiquement aux messages pertinents en vous fournissant un lien pour parler à un « représentant ». Mais en réalité, il s'agit d'une escroquerie conçue pour voler vos informations.
  - Les escrocs recourent à des attaques de phishing de plus en plus sophistiquées, ce qui rend plus difficile l'identification de votre cible.

3. MAN-IN-THE-MIDDLE ATTACK

- se produit lorsque des attaquants interceptent des données ou compromettent votre réseau pour vous « espionner ».
  - Ces attaques sont particulièrement courantes lors de l'utilisation de réseaux Wi-Fi publics , qui peuvent facilement être piratés.
- Les attaques MitM peuvent également être utilisées pour « usurper » des conversations. Les pirates s'immiscent dans votre conversation et se font passer pour la personne à laquelle vous pensez parler.
  - Dans un exemple extrême, un pirate informatique a intercepté les communications entre un investisseur chinois et le fondateur d'une startup et les a amenés à modifier la destination d'un virement bancaire d'un million de dollars

4. DÉNI DE SERVICE (DOS) ET DÉNI DE SERVICE DISTRIBUÉ (DDOS)

- De nombreuses cyberattaques visent à surcharger les serveurs, forçant ainsi les services à s'arrêter.
- Une attaque par déni de service (**DOS**) se produit lorsque des pirates informatiques utilisent de fausses requêtes et du trafic pour submerger un système et le fermer.
- Une attaque par déni de service distribué (**DDoS**) est du même type, sauf que le pirate utilise plusieurs appareils compromis en même temps.
- L'objectif de ces cyberattaques n'est généralement pas de voler des données, mais d'interrompre, voire de fermer, des activités commerciales.
- Les attaques **DDoS** ont entraîné la fermeture de sites comme Twitter, SoundCloud et Spotify, et ont même gravement endommagé AWS d'Amazon.

ATTAQUES PAR INJECTION SQL

- La plupart des sites Web utilisent des bases de données SQL pour stocker des informations sensibles telles que les identifiants, les mots de passe et les informations de compte. Les pirates informatiques utilisent une attaque par injection SQL pour « tromper » la base de données et lui faire divulguer ces informations.
- Ces attaques sont un peu techniques, mais elles consistent pour un pirate à saisir des commandes SQL prédéfinies dans une zone de saisie de données (comme un champ de connexion ou de mot de passe).
  - Ces commandes peuvent lire des données sensibles, modifier des données de base de données ou même déclencher des fonctions exécutives (comme l'arrêt du système).

5. CAS D'INJECTION SQL

- Imaginez une application d'achat qui affiche des produits dans différentes catégories. Lorsque l'utilisateur clique sur la catégorie Cadeaux, son navigateur demande l'URL :
- https://insecure-website.com/products?category=Gifts
- L'application effectue alors une requête SQL pour récupérer les détails des produits pertinents à partir de la base de données :
- **SELECT * FROM products WHERE category = 'Gifts' AND released = 1**
- Cette requête SQL demande à la base de données de renvoyer :

  Tous les détails (*) à partir du tableau des produits où la **category** est **Gift** et **released** est 1.
- https://insecure-website.com/products?category=Gifts'-- Cela entraîne la requête SQL:
- **SELECT * FROM products WHERE category = 'Gifts'--' AND released =** 1Il est important de noter que -- est un indicateur de commentaire en SQL. Cela signifie que le reste de la requête est interprété comme un commentaire, ce qui la supprime de fait. Dans cet exemple, cela signifie que la requête n'inclut plus AND released = 1. De ce fait, tous les produits sont affichés, y compris ceux qui ne sont pas encore sortis.

6. TUNNELLISATION DNS

- Le **tunneling DNS** est un type de cyberattaque utilisé par les pirates informatiques pour contourner les systèmes de sécurité traditionnels tels que les pare-feu afin d'accéder aux systèmes et aux réseaux.
- Les pirates informatiques codent des programmes malveillants dans les requêtes et réponses DNS (que la plupart des programmes de sécurité ignorent).
- Une fois le programme à l'intérieur, il se verrouille sur le serveur cible, donnant aux pirates un accès à distance.
- Les attaques par tunneling DNS sont particulièrement dangereuses, car elles passent souvent inaperçues pendant des jours, des semaines ou des mois.
  - Pendant ce temps, les cybercriminels peuvent voler des données sensibles, modifier du code, installer de nouveaux points d'accès et même installer des logiciels malveillants.
  - Dans un exemple, des cybercriminels ont utilisé le tunneling DNS pour attaquer Air India et d'autres compagnies aériennes et voler des informations de passeport et des numéros de carte de crédit. La « porte dérobée » est restée ouverte pendant plus de deux mois

7. QU'EST-CE QU'UNE VULNÉRABILITÉ/EXPLOIT ZERO-DAY ?

- Une **vulnérabilité zero-day** est une faille de sécurité dans un logiciel, un système d'exploitation ou un matériel qui est inconnue des développeurs ou des fournisseurs du produit concerné.
  - Cela signifie qu'il n'existe aucun correctif ou mise à jour de sécurité pour contrer cette vulnérabilité au moment où elle est découverte ou exploitée.
- **Zero-Day** : Ce terme fait référence au fait que les développeurs ont eu "zéro jour" pour corriger la faille, car elle n'a pas encore été découverte par eux ou signalée publiquement.
- Un **exploit zero-day** est un programme malveillant ou un code utilisé par les attaquants pour exploiter une vulnérabilité zero-day. Les cybercriminels conçoivent ces exploits pour tirer parti de la faille de sécurité avant que les utilisateurs ou les entreprises ne puissent se protéger.
- **Exploiter la vulnérabilité** : Les exploits zero-day peuvent permettre à un attaquant de voler des informations, de prendre le contrôle d'un système, d'installer des malwares ou d'endommager des données en profitant de la faille avant que les développeurs ne la corrigent.

POURQUOI LES ATTAQUES ZERO-DAY SONT-ELLES SI DANGEREUSES ?

- **Aucune Protection Immédiate :** Les utilisateurs et les entreprises ne disposent d'aucune protection immédiate contre une vulnérabilité zero-day puisque le problème est encore inconnu ou non corrigé.
- **Large Portée :** Une attaque zero-day peut toucher un grand nombre de victimes rapidement si la vulnérabilité concerne des logiciels ou des systèmes largement utilisés (par exemple, les systèmes d'exploitation Windows ou les navigateurs comme Chrome).
- **Difficulté de Détection :** Les systèmes de sécurité traditionnels, comme les antivirus, ne sont pas efficaces contre les exploits zero-day puisqu'ils ne connaissent pas encore la menace. Les attaquants peuvent ainsi pénétrer dans les systèmes sans être détectés.

EXEMPLES D'ATTAQUES ZERO-DAY

- **Attaque Zero-Day sur Windows (Stuxnet - 2010)**
- Stuxnet est un célèbre ver informatique qui a utilisé plusieurs vulnérabilités zero-day pour infecter des systèmes de contrôle industriel, notamment ceux de centrales nucléaires en Iran. Ce malware a été conçu pour cibler spécifiquement les systèmes SCADA utilisés dans les infrastructures critiques, et a détruit physiquement des centrifugeuses en modifiant leur fonctionnement.
- Impact : C'est l'un des exemples les plus célèbres d'utilisation d'exploits zero-day à des fins de sabotage, démontrant que ces attaques peuvent avoir des impacts numériques et physiques.
- **Attaque Zero-Day sur Internet Explorer (Aurora - 2009)**
- L'attaque **Aurora**, menée par un groupe de hackers chinois, a exploité une vulnérabilité zero-day dans Internet Explorer pour accéder aux systèmes de plusieurs entreprises, y compris Google. L'attaque a permis aux hackers de voler des informations sensibles.
- ***Impact*** : Cette attaque a révélé l'importance de sécuriser les navigateurs web, car ces applications sont couramment utilisées comme vecteurs d'attaque.
- **Vulnérabilité Zero-Day dans Zoom (2020)**
- Zoom, a été exposée à plusieurs vulnérabilités zero-day qui permettaient aux attaquants d'espionner les appels vidéo des utilisateurs ou d'accéder à leurs appareils.

8. ATTAQUES PAR MOT DE PASSE

- Les **attaques par mot de passe** sont des tentatives malveillantes pour accéder à des comptes, des systèmes ou des réseaux protégés par des mots de passe.
- Elles exploitent la faiblesse des mots de passe ou utilisent des méthodes pour voler ou deviner les mots de passe des utilisateurs.
  1. Attaque par Force Brute
  2. Attaque par Dictionnaire
  3. Attaque par Rejeu (Pass-the-Hash)
  4. Attaque par Phishing
  5. Attaque par Rainbow Table
  6. Attaque par Keylogger
  7. Attaque par Credential Stuffing

9. ATTAQUES PAR TÉLÉCHARGEMENT FURTIF (DRIVE-BY DOWNLOAD ATTACKS)

- sont des cyberattaques dans lesquelles des logiciels malveillants sont installés sur l'ordinateur ou l'appareil d'un utilisateur sans qu'il en soit conscient. .
- **Comment Fonctionnent les Attaques par Téléchargement Furtif ?**
  - **a) Exploitation des Vulnérabilités**
    - Les attaques par téléchargement furtif exploitent généralement des vulnérabilités présentes dans les navigateurs web, les plug-ins (comme Flash, Java, ou Silverlight), ou les systèmes d'exploitation. Lorsque l'utilisateur visite un site web infecté ou malveillant, le site détecte les vulnérabilités présentes dans le système de l'utilisateur et injecte un code malveillant qui télécharge automatiquement le malware sur l'appareil.
  - **b) Redirection Vers des Sites Malveillants**
    - Dans certains cas, un utilisateur est redirigé sans le savoir vers un site web malveillant via des liens, des publicités compromises (malvertising), ou des scripts injectés dans des pages web légitimes. Ce site malveillant initie alors l'attaque en téléchargeant et exécutant un malware.
  - **c) Absence d'Interaction de l'Utilisateur**
    - Le téléchargement furtif ne nécessite aucune action active de l'utilisateur. Contrairement aux attaques par phishing où l'utilisateur doit cliquer sur un lien ou télécharger un fichier, dans une attaque par téléchargement furtif, le simple fait de visiter une page web compromise suffit pour déclencher l'attaque.

TYPES DE MALWARES DÉPLOYÉS PAR TÉLÉCHARGEMENT FURTIF

- Les attaquants utilisent les attaques par téléchargement furtif pour installer divers types de logiciels malveillants sur les appareils des victimes.
  - **Ransomware**
  - **Trojans (Chevaux de Troie)**
  - **Keyloggers**
  - **Spyware et Adware**
    - Les **spywares** collectent secrètement des informations sur l'utilisateur, telles que les frappes au clavier ou les données de navigation, tandis que les **adwares** affichent des publicités non sollicitées sur l'appareil de la victime.
  - **Botnets**
  - Les attaquants peuvent infecter l'ordinateur de la victime avec un **bot** qui fait partie d'un **botnet**. Les ordinateurs infectés sont ensuite contrôlés à distance pour mener d'autres attaques, comme des attaques DDoS (Déni de service distribué).

10. ATTAQUES DE TYPE CROSS-SITE SCRIPTING

- sont des cyberattaques qui exploitent les vulnérabilités des applications web pour injecter du code malveillant (généralement sous forme de scripts) dans des pages web vues par d'autres utilisateurs.
- Cela permet à un attaquant d'exécuter des scripts sur le navigateur des victimes, souvent à leur insu, et d'accéder à des informations sensibles ou d'effectuer des actions malveillantes.
- Les attaques XSS sont particulièrement dangereuses car elles exploitent la confiance des utilisateurs envers des sites web légitimes et peuvent compromettre des sessions, voler des informations d'identification, et rediriger les utilisateurs vers des sites malveillants.
- Trois types
  - **XSS Réfléchi (Non Persistant)**
  - **XSS Persistant (Stocké)**
  - **XSS Basé sur le DOM**

XSS RÉFLÉCHI (NON PERSISTANT)

- L'attaque XSS réfléchie se produit lorsque le script malveillant est injecté dans une requête HTTP (souvent via une URL ou un champ de formulaire) et renvoyé immédiatement dans la réponse de l'application web sans être stocké sur le serveur.
- **Mode d'Opération** : L'attaquant envoie un lien malveillant à la victime. Lorsque la victime clique sur ce lien, le script injecté est "réfléchi" par le serveur et exécuté dans le navigateur de la victime. Cela peut permettre à l'attaquant de voler des cookies, des identifiants de session, ou d’exécuter des actions au nom de l'utilisateur.
- **Exemple** : Un attaquant envoie un e-mail contenant un lien vers un site web légitime, mais avec un script malveillant ajouté dans l'URL. Lorsque la victime visite le lien, le script est exécuté dans le navigateur.

XSS PERSISTANT (STOCKÉ)

- le code malveillant est stocké de manière permanente sur le serveur, par exemple dans une base de données. Il est ensuite exécuté chaque fois que les utilisateurs accèdent à la page contenant ce contenu.
- **Mode d'Opération** : L'attaquant injecte du code malveillant dans un champ de saisie sur une page web (comme un champ de commentaire ou un forum). Le script est ensuite stocké sur le serveur et exécuté chaque fois qu'un utilisateur visite la page, affectant potentiellement de nombreux utilisateurs.
- **Exemple** : Un attaquant publie un commentaire malveillant sur un site web qui est stocké dans une base de données. Tous les utilisateurs qui visitent cette page déclenchent l'exécution du script malveillant, ce qui permet à l'attaquant de voler des informations de session.

XSS BASÉ SUR LE DOM

- Dans les attaques **DOM-based XSS**, l'injection malveillante se produit directement dans le **Document Object Model (DOM)** du navigateur sans impliquer de communication avec le serveur. Le script malveillant est exécuté par le navigateur lorsque la structure DOM est modifiée dynamiquement par JavaScript.
- **Mode d'Opération** : L'attaquant modifie directement les éléments de la page web dans le navigateur de l'utilisateur en utilisant JavaScript malveillant, généralement en exploitant des vulnérabilités dans le code front-end. Cela peut permettre à l'attaquant d'exécuter des actions non désirées ou de voler des données.
- **Exemple** : Un utilisateur saisit une URL contenant un script malveillant dans le navigateur. Le code JavaScript malveillant interagit directement avec le DOM et peut manipuler les données ou rediriger l'utilisateur sans jamais impliquer le serveur.

11. ROOTKIT

- Un **rootkit** est un type de logiciel malveillant conçu pour permettre à un attaquant d'obtenir un accès non autorisé et prolongé à un ordinateur ou à un réseau, tout en restant caché du propriétaire légitime et des systèmes de sécurité.
  - Le rootkit se dissimule profondément dans le système d'exploitation, permettant à l'attaquant de contrôler à distance le système infecté sans être détecté.
- **Rootkits de Noyau (Kernel-Level Rootkits)**
- **Rootkits en Mode Utilisateur (User-Mode Rootkits)**
- **Rootkits de Bootloader (Bootkits)**
- **Rootkits de Mémoire (Memory Rootkits)**
- **Rootkits Virtuels (Virtual Rootkits)**

12. USURPATION OU EMPOISONNEMENT DU DNS (DNS SPOOFING OU DNS CACHE POISONING)

- L'**empoisonnement DNS** survient lorsque des informations DNS incorrectes sont insérées dans la mémoire cache d'un serveur DNS, redirigeant les utilisateurs vers des adresses IP malveillantes. L'attaque modifie les enregistrements DNS afin que, lorsqu'un utilisateur tente d'accéder à un site web légitime, il soit dirigé vers un faux site web contrôlé par l'attaquant.
- Par exemple, au lieu de diriger l'utilisateur vers **192.0.2.1** pour **www.example.com**, le serveur DNS empoisonné pourrait lui fournir une fausse adresse IP, comme **203.0.113.5**, qui héberge un site malveillant.
- **Méthodes Utilisées pour l'Empoisonnement du DNS**
- a) DNS Cache Poisoning
- b) Spoofing des Réponses DNS
- c) Compromission d'un Serveur DNS

13. ATTAQUES CONTRE L'INTERNET DES OBJETS (IOT)

- L'**Internet des Objets (IoT)** désigne un réseau d'appareils physiques interconnectés, capables de collecter et d'échanger des données via Internet.
  - Ces objets peuvent inclure des appareils domestiques intelligents (caméras de surveillance, thermostats, assistants vocaux), des dispositifs industriels, des capteurs médicaux, des véhicules connectés, et bien plus encore.
- Les **attaques contre l'IoT** ciblent ces appareils.
- **Pourquoi les Appareils IoT sont-ils Vulnérables ?**
  - Sécurité Faible ou Inexistante
  - Mise à Jour Infréquente
  - Accès Non Sécurisé à Internet
- **Types d'attaques contre les Appareils IoT**
  - a) Attaques par Botnet (Botnets IoT)
  - b) Attaques par Forçage de Mot de Passe (Credential Stuffing)
  - c) Attaques DDoS (Déni de Service Distribué)
  - d) Attaques par Écoute (Eavesdropping)
  - e) Ransomware IoT
  - f) Attaques de Mise à Jour Malveillante (Firmware Hijacking)

14. DÉTOURNEMENT DE SESSION

- Le **détournement de session**, également appelé **Session Hijacking**, est une attaque informatique dans laquelle un attaquant intercepte ou prend le contrôle d'une session utilisateur active pour accéder à des systèmes ou des informations sensibles.
- Une session est une période de communication active entre un utilisateur et un serveur, souvent authentifiée par des identifiants de session (comme des cookies ou des tokens). Si un attaquant parvient à voler ces identifiants, il peut se faire passer pour l'utilisateur légitime et agir en son nom.
- Le détournement de session peut être utilisé pour accéder à des comptes personnels, voler des données, effectuer des transactions non autorisées ou compromettre des systèmes.
- **Session ID** : Chaque session est associée à un **identifiant de session** unique (souvent stocké dans un cookie ou un token) qui permet au serveur d'associer les requêtes de l'utilisateur à sa session active.
- **Cookies de Session** : Les **cookies** sont souvent utilisés pour stocker ces identifiants de session sur le navigateur de l'utilisateur. Le serveur utilise le cookie pour authentifier les requêtes et maintenir la connexion.

MÉTHODES DE DÉTOURNEMENT DE SESSION

- **Vol de Cookies (Cookie Hijacking)**
- Les attaquants peuvent voler les **cookies de session** d'un utilisateur pour usurper son identité. Au moyen de:
  - **Attaques XSS (Cross-Site Scripting)** : Si une application web est vulnérable à une attaque XSS, un attaquant peut injecter du code malveillant qui vole les cookies de session des visiteurs.
  - **Sniffing des Réseaux Non Sécurisés** : Sur des réseaux non chiffrés (Wi-Fi publics), les attaquants peuvent capturer les cookies de session en interceptant le trafic réseau entre l'utilisateur et le serveur.
- **Fixation de Session (Session Fixation)**
  - Dans une attaque par **fixation de session**, l'attaquant force une victime à utiliser un identifiant de session connu par l'attaquant. Une fois la victime authentifiée, l'attaquant peut prendre le contrôle de la session.
  - **Mode d'opération** : L'attaquant crée une session sur le serveur, obtient l'ID de session et incite la victime à se connecter en utilisant cet identifiant de session (par exemple, en envoyant un lien spécialement conçu). Une fois l'utilisateur authentifié, l'attaquant peut utiliser le même identifiant de session pour accéder à son compte.
- **Attaque par Rejeu (Replay Attack)**
  - Dans une **attaque par rejeu**, l'attaquant intercepte les communications réseau et réutilise des informations valides envoyées par l'utilisateur, comme un token ou un cookie de session, pour accéder au système sans avoir besoin d'authentification supplémentaire.
  - **Exemple** : L'attaquant intercepte un cookie de session valide et le renvoie au serveur pour se faire passer pour l'utilisateur légitime.
- **Détournement Actif de Session (Man-in-the-Middle)**

15. MANIPULATION D'URL

- La **manipulation d'URL** est une technique utilisée par des attaquants pour modifier les paramètres ou les composants d'une URL afin d'exploiter les failles de sécurité d'une application web. L'objectif de ces attaques peut être varié : accéder à des informations non autorisées, contourner des mécanismes d'authentification, manipuler des données, ou même compromettre le serveur web.

```
https://www.example.com/products?product_id=123
```

`user_id=124`

```
https://www.example.com/products?product_id=123;DROP%20TABLE%20users;
```

```
https://www.example.com/search?q=<script>alert('XSS');</script>
```

16. MENACES INTERNES

- Les **menaces internes** font référence aux risques de sécurité posés par des personnes au sein d'une organisation, telles que les employés, les sous-traitants, ou d'autres personnes ayant accès aux systèmes, aux réseaux ou aux informations sensibles de l'entreprise.
  - Contrairement aux menaces externes, qui proviennent de hackers ou de cybercriminels hors de l'organisation, les menaces internes sont perpétrées par des individus ayant déjà un accès légitime aux ressources internes.
- Ces menaces peuvent être intentionnelles (lorsqu'une personne commet un acte malveillant) ou involontaires (lorsqu'une personne cause un incident de sécurité par erreur ou négligence).
- Les menaces internes peuvent avoir des conséquences graves, notamment le vol de données sensibles, la perturbation des activités, ou la compromission des systèmes critiques.