

# Securite Applicative

# Sommaire

1. Introduction à la sécurité informatique
2. Principes fondamentaux de la sécurité informatique
3. Importance de la sécurité des applications
4. Introduction aux menaces et vulnérabilités
5. Évaluation des Vulnérabilités
6. Les différents types de menaces et leurs traitements

# Introduction à la sécurité informatique

# Introduction à la sécurité informatique

## Définition de la sécurité informatique

La sécurité informatique (abréviation de sécurité des technologies de l'information ou **IT**) consiste à protéger les actifs informatiques d'une organisation, à savoir les systèmes informatiques, les réseaux, les appareils numériques et les données, contre les accès non autorisés, les violations de données, les cyberattaques et autres activités malveillantes.

# Introduction à la sécurité informatique

## Définition de la sécurité informatique

- La **sécurité informatique** est souvent confondue avec la cybersécurité, une discipline plus étroite qui est techniquement un sous-ensemble de la sécurité informatique.
- Alors que la cybersécurité se concentre principalement sur la protection des organisations contre les attaques numériques, telles que les ransomwares, les logiciels malveillants et les escroqueries par hameçonnage, la sécurité informatique concerne l'ensemble de l'infrastructure technique d'une organisation.

# Introduction à la sécurité informatique

## Les Types de sécurité informatique

- Sécurité cloud
- Sécurité au nœud final
- Sécurité des réseaux
- Sécurité des applications
- Sécurité Internet
- Sécurité IdO et OT

# Introduction à la sécurité informatique

## Les Types de sécurité informatique

### 1. Sécurité cloud

La sécurité du cloud concerne les cybermenaces externes et internes qui pèsent sur l'infrastructure, les applications et les données d'une organisation basées sur le cloud.

### 2. Sécurité au nœud final

La sécurité des terminaux protège les utilisateurs finaux et les terminaux, tels que les ordinateurs de bureau, les ordinateurs portables, les téléphones mobiles et les serveurs, contre les cyberattaques.

# Introduction à la sécurité informatique

## Les Types de sécurité informatique

### 3. Sécurité des réseaux

Elle s'articule autour de trois objectifs principaux : empêcher l'accès non autorisé aux ressources du réseau, détecter et neutraliser les cyberattaques et les violations de sécurité en temps réel, et veiller à ce que les utilisateurs autorisés puissent accéder en toute sécurité aux ressources du réseau dont ils ont besoin, au moment où ils en ont besoin.



# Introduction à la sécurité informatique

## Les Types de sécurité informatique

### 4. Sécurité des applications

La sécurité des applications fait référence aux mesures prises par les développeurs lors de la création d'une application afin de remédier aux vulnérabilités potentielles et de protéger les données des clients et leur propre code contre le vol, les fuites ou la compromission.

# Introduction à la sécurité informatique

## Les Types de sécurité informatique

### 5. Sécurité Internet

La sécurité Internet protège les données et les informations sensibles transmises, stockées ou traitées par les navigateurs ou les applications. Elle implique une série de pratiques et de technologies de sécurité qui contrôlent le trafic Internet entrant pour y détecter les logiciels malveillants et autres contenus malveillants.

# Introduction à la sécurité informatique

## Les Types de sécurité informatique

### 6. Sécurité IdO et OT

La sécurité de l'Internet des objets (IoT) vise à empêcher les capteurs et les appareils connectés à l'Internet, par exemple, les caméras installées sur les sonnettes, les appareils intelligents, les automobiles modernes, d'être contrôlés par des pirates ou d'être utilisés par des pirates pour s'infiltrer dans le réseau d'une organisation.

# Introduction à la sécurité informatique

## Les menaces liées à la sécurité informatique

- Logiciels malveillants : ransomware, Cheal de Troie, logiciels espions, ver, etc.
- Attaques d'ingénierie sociale : harponnage, Whaling, e-mails
- Attaques par déni de service (DoS).
- Exploits zero day
- Menaces internes
- Attaques de l'homme du milieu (MITM)

# Introduction à la sécurité informatique

## Les menaces liées à la sécurité informatique

- Logiciels malveillants : ransomware, Cheal de Troie, logiciels espions, ver, etc.
- Attaques d'ingénierie sociale : harponnage, Whaling, e-mails
- Attaques par déni de service (DoS).
- Exploits zero day
- Menaces internes
- Attaques de l'homme du milieu (MITM)

# Introduction à la sécurité informatique

## Bonnes pratiques



# Principes fondamentaux de la sécurité informatique

# Principes fondamentaux de la sécurité informatique

Les principes fondamentaux de la sécurité informatique forment la base des meilleures pratiques pour protéger les systèmes informatiques et les données contre les menaces et les vulnérabilités



# Principes fondamentaux de la sécurité informatique

## Les principes

### 1. Confidentialité (Confidentiality).

- Assurer que les informations sont accessibles uniquement aux personnes autorisées.
- La confidentialité est souvent garantie par des mécanismes comme le chiffrement, les contrôles d'accès, et les politiques de gestion des identités.

# Principes fondamentaux de la sécurité informatique

## Les principes

### 2. Intégrité (Integrity).

- Garantir que les données ne sont ni altérées ni détruites de manière non autorisée.
- L'intégrité implique des mesures comme les sommes de contrôle (checksums), les hachages cryptographiques, et les signatures numériques pour vérifier que les données n'ont pas été modifiées.

# Principes fondamentaux de la sécurité informatique

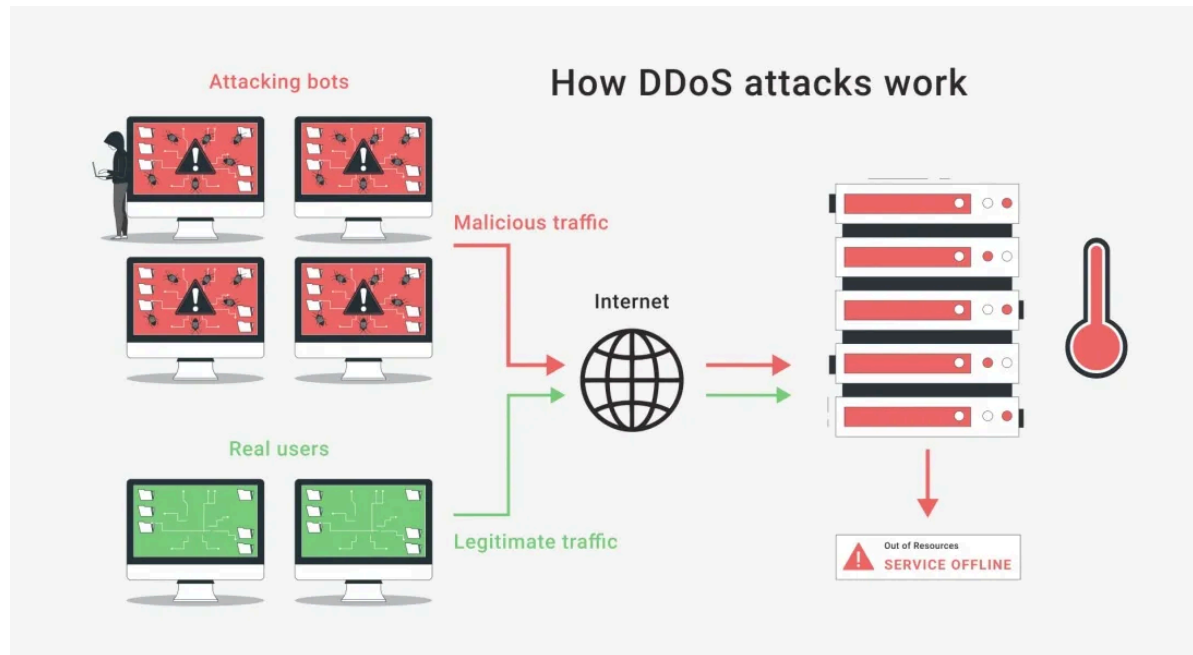
## Les principes

### 3. Disponibilité (Availability)

- S'assurer que les informations et les systèmes sont disponibles pour les utilisateurs autorisés lorsqu'ils en ont besoin.
- Cela peut inclure des stratégies de sauvegarde, des plans de reprise après sinistre, et la protection contre les attaques de déni de service (DoS).

# Principes fondamentaux de la sécurité informatique

## 3. Disponibilité (Availability).



# Principes fondamentaux de la sécurité informatique

## Les principes

### 4. Authentification (Authentication).

- Vérifier l'identité des utilisateurs, systèmes, ou entités avant d'accorder l'accès aux ressources.
- Les méthodes courantes d'authentification comprennent les mots de passe, les cartes à puce, les jetons de sécurité, et les données biométriques.

# Principes fondamentaux de la sécurité informatique

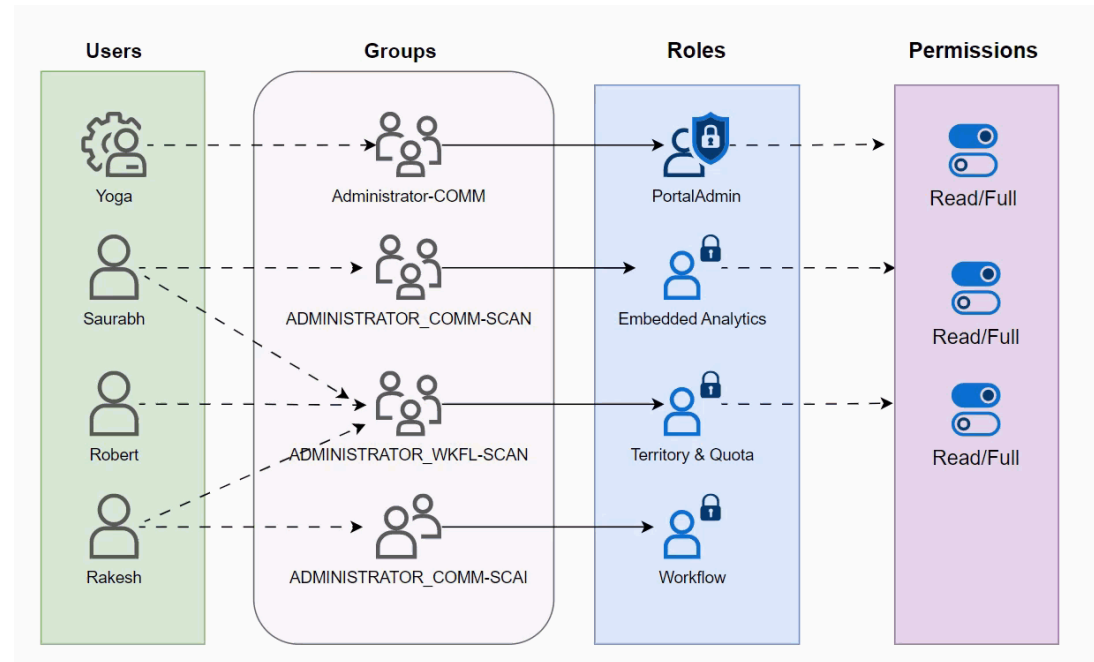
## Les principes

### 5. Autorisation (Authorization)

- Déterminer les niveaux d'accès et les permissions accordés aux utilisateurs authentifiés.
- Les systèmes de gestion des accès basés sur les rôles (RBAC) et les politiques de contrôle d'accès (ACL) sont souvent utilisés pour gérer l'autorisation.

# Principes fondamentaux de la sécurité informatique

## 5. Autorisation (Authorization)



# Principes fondamentaux de la sécurité informatique

## Les principes

### 7. Contrôle des accès (Access Control)

- Restreindre l'accès aux ressources et aux informations en fonction des besoins d'emploi et des niveaux d'autorisation.
- Les modèles de contrôle d'accès incluent les listes de contrôle d'accès (ACL), les modèles de sécurité discrétionnaire (DAC), et les modèles de sécurité obligatoires (MAC).



# Principes fondamentaux de la sécurité informatique

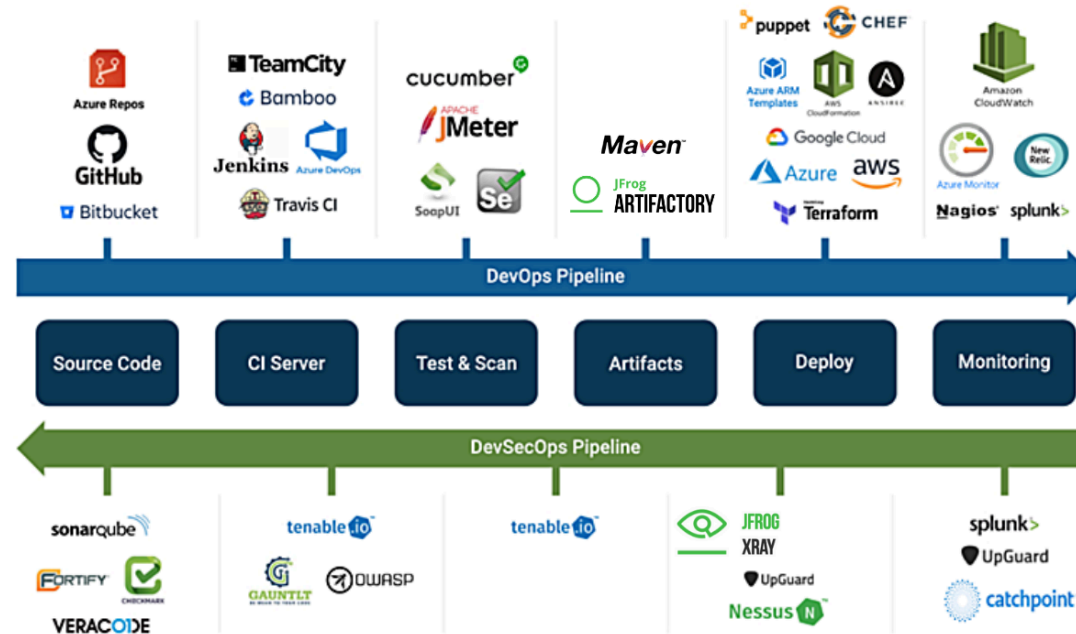
## Les principes

### 8. Sécurité par conception (Security by Design).

- Intégrer des mesures de sécurité dès le début du cycle de développement des systèmes et des logiciels.
- Cela inclut des pratiques comme le développement sécurisé, les revues de code, et les tests de sécurité tout au long du processus de développement.

# Principes fondamentaux de la sécurité informatique

## 8. Sécurité par conception (Security by Design).



# Principes fondamentaux de la sécurité informatique

## Les principes

### 9. Principes de moindre privilège (Principle of Least Privilege).

- Limiter les privilèges accordés aux utilisateurs et aux systèmes au strict minimum nécessaire pour accomplir leurs tâches.
- Cela réduit les risques d'exploitation des privilèges en cas de compromission.

# Principes fondamentaux de la sécurité informatique

## Les principes

### 10. Défense en profondeur (Defense in Depth)

- Utiliser plusieurs couches de sécurité pour protéger les systèmes et les données.
- Si une couche de défense échoue, d'autres couches restent en place pour continuer à protéger contre les attaques.

# Principes fondamentaux de la sécurité informatique

## Les principes

### 11. Audits et Surveillance (Audits and Monitoring)

- Utiliser plusieurs couches de sécurité pour protéger les systèmes et les données.
- Si une couche de défense échoue, d'autres couches restent en place pour continuer à protéger contre les attaques.

# Principes fondamentaux de la sécurité informatique


## Les principes

### 12. Gestion des vulnérabilités (Vulnerability Management)

- Identifier, évaluer, et corriger les vulnérabilités dans les systèmes et les applications.
- Cela inclut des pratiques comme les scans de vulnérabilité, les mises à jour de sécurité, et les correctifs logiciels.

# Principes fondamentaux de la sécurité informatique


## 12. Gestion des vulnérabilités (Vulnerability Management)



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or CNASGP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

[Sponsor](#)

Project:  archiver:0.0.1-SNAPSHOT

Scan Information ([show all](#)):

- dependency-check version: 7.1.1
- Report Generated On: Tue, 5 Jul 2022 09:56:30 GMT
- Dependencies Scanned: 162 (137 unique)
- Vulnerable Dependencies: 3
- Vulnerabilities Found: 3
- Vulnerabilities Suppressed: 0
- ...

Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
<a href="#">log4j-api-2.17.2.jar</a>	<a href="#">cpe:2.3:a:apache:log4j:2.17.2:*****</a>	<a href="#">org.apache.logging.log4j/log4j-api@2.17.2</a>	HIGH	1	Highest	46
<a href="#">spring-security-crypto-5.7.2.jar</a>	<a href="#">cpe:2.3:a:pivotal:software:spring_security:5.7.2:*****</a> <a href="#">cpe:2.3:a:vmware:spring_security:5.7.2:*****</a>	<a href="#">org.springframework.security/spring-security-crypto@5.7.2</a>	MEDIUM	1	Highest	38
<a href="#">tomcat-embed-core-9.0.64.jar</a>	<a href="#">cpe:2.3:a:apache:tomcat:9.0.64:*****</a> <a href="#">cpe:2.3:a:apache:tomcat:apache_tomcat:9.0.64:*****</a>	<a href="#">org.apache.tomcat.embed/tomcat-embed-core@9.0.64</a>	MEDIUM	1	Highest	71

# Importance de la sécurité des applications



# Importance de la sécurité des applications

## Définition de la sécurité des applications

- La **sécurité des applications** est un domaine de la **sécurité informatique** qui se concentre sur la protection des applications logicielles contre les menaces et les vulnérabilités.
- Elle comprend l'ensemble des mesures, des pratiques et des processus visant à empêcher les attaques malveillantes, à réduire les risques de failles de sécurité et à garantir l'intégrité, la confidentialité et la disponibilité des données et des services fournis par les applications.

# Importance de la sécurité des applications

## Les Eléments clés de la sécurité des applications

### 1. Détection et correction des vulnérabilités :

- **Analyse statique du code** : Examen du code source pour identifier des vulnérabilités potentielles sans exécuter l'application.
- **Analyse dynamique** : Test de l'application en cours d'exécution pour découvrir des failles de sécurité en simulant des attaques.
- **Test de pénétration** : Évaluation de la sécurité en essayant de compromettre activement l'application de manière contrôlée.

# Importance de la sécurité des applications

## Les Eléments clés de la sécurité des applications

### 2. Authentification et gestion des identités :

- Assurer que seuls les utilisateurs autorisés peuvent accéder à l'application.
- Utilisation de mécanismes solides tels que l'authentification multifactorielle (MFA).

# Importance de la sécurité des applications

## Les Eléments clés de la sécurité des applications

### 3. Contrôle des accès :

- Gestion fine des permissions et des rôles pour limiter l'accès aux ressources et fonctionnalités de l'application en fonction des droits des utilisateurs.

### 4. Chiffrement :

- Protection des données en transit et au repos par des techniques de chiffrement pour garantir leur confidentialité et leur intégrité.

# Importance de la sécurité des applications

## Les Eléments clés de la sécurité des applications

### 5. Sécurisation du développement :

- Adoption de méthodologies de développement sécurisées comme le DevSecOps, intégrant des pratiques de sécurité tout au long du cycle de vie du développement logiciel (SDLC).

### 6. Gestion des mises à jour et des correctifs :

- Maintien de l'application à jour avec les dernières corrections de sécurité pour combler les vulnérabilités découvertes.

# Importance de la sécurité des applications

## Les Eléments clés de la sécurité des applications

### 7. Surveillance et détection des intrusions :

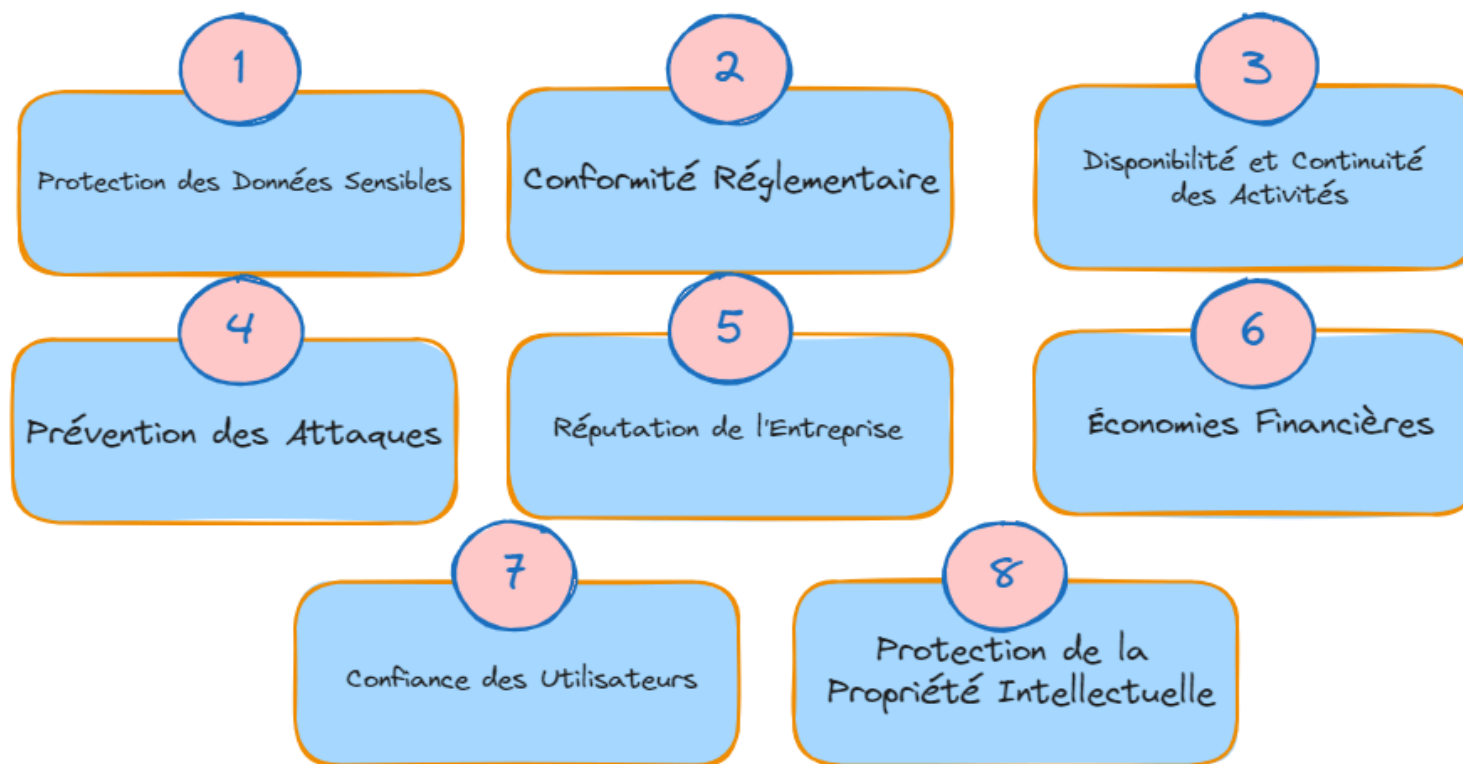
- Mise en place de systèmes de surveillance pour détecter et réagir rapidement aux tentatives d'intrusion et aux comportements anormaux.

### 8. Formation et sensibilisation :

- Éducation des développeurs et des utilisateurs sur les bonnes pratiques de sécurité pour réduire les risques liés à l'erreur humaine.

# Importance de la sécurité des applications

## Les principaux points qui soulignent son importance



# Introduction aux menaces et vulnérabilités



# Introduction aux menaces et vulnérabilités

## Définitions

### Menaces

- Les menaces sont des acteurs ou des événements potentiels qui peuvent causer un dommage à un système ou à une organisation.
- Elles peuvent être de nature intentionnelle (comme les attaques cybernétiques) ou non intentionnelle (comme les catastrophes naturelles).

### Vulnérabilités

- Les vulnérabilités sont des failles ou des faiblesses dans un système, un réseau ou une application qui peuvent être exploitées par des menaces pour causer des dommages ou des perturbations.

# Introduction aux menaces et vulnérabilités

## Types de Menaces

### 1. Menaces Internes

- ***Employés Mécontents*** : Employés qui abusent de leurs accès pour endommager l'organisation.
- ***Erreur Humaine*** : Erreurs non intentionnelles commises par les employés, comme la configuration incorrecte de systèmes.

# Introduction aux menaces et vulnérabilités

## Types de Menaces

### 2. Menaces Externes

- **Hackers** : Individus ou groupes qui cherchent à exploiter les failles pour des gains financiers, politiques ou personnels.
- **Malware** : Logiciels malveillants conçus pour endommager ou infiltrer des systèmes, comme les virus, les vers, les chevaux de Troie, les ransomwares.
- **Phishing** : Techniques d'ingénierie sociale utilisées pour tromper les utilisateurs et obtenir des informations sensibles.
- **Attaques DDoS (Distributed Denial of Service)** : Attaques visant à rendre un service indisponible en le submergeant de trafic.

### 3. Catastrophes Naturelles

- **Incendies, Inondations, Tremblements de Terre** : Événements naturels qui peuvent endommager l'infrastructure physique.

# Introduction aux menaces et vulnérabilités

## Types de Vulnérabilités

### 1. Vulnérabilités Logicielles

- ***Bugs et Failles de Code*** : Erreurs dans le code source qui peuvent être exploitées.
- ***Injections SQL*** : Failles permettant d'injecter des commandes SQL malveillantes.
- ***Scripts Inter-Sites (XSS)*** : Failles permettant l'injection de scripts malveillants dans des pages web.

# Introduction aux menaces et vulnérabilités

## Types de Vulnérabilités

### 2. Vulnérabilités Réseau

- ***Configuration Inappropriée*** : Réseaux mal configurés qui exposent des points d'entrée non sécurisés.
- ***Manque de Chiffrement*** : Absence de chiffrement des données sensibles transmises sur le réseau

# Introduction aux menaces et vulnérabilités

## Types de Vulnérabilités

### 3. Vulnérabilités Physiques

- ***Accès Non Autorisé*** : Accès physique non contrôlé aux serveurs et aux infrastructures critiques.
- ***Manque de Redondance*** : Absence de systèmes de secours ou de sauvegarde pour les infrastructures critiques.

# Introduction aux menaces et vulnérabilités

## Types de Vulnérabilités

### 4. Vulnérabilités Humaines

- ***Manque de Formation*** : Employés non formés aux bonnes pratiques de sécurité.
- ***Utilisation de Mots de Passe Faibles*** : Utilisation de mots de passe facilement devinables ou réutilisés.

# Évaluation des Vulnérabilités



# Évaluation des Vulnérabilités

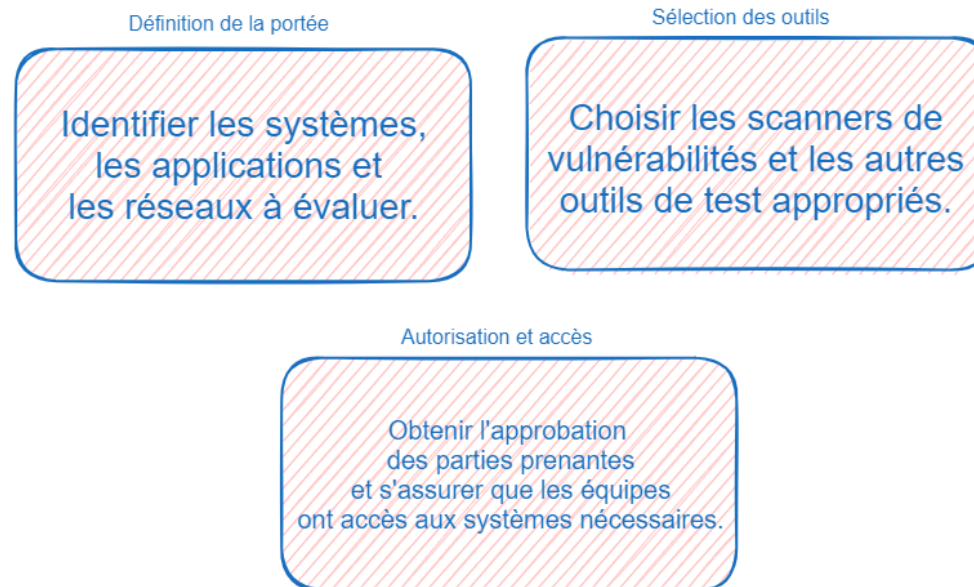
## Definition

- L'évaluation des vulnérabilités est un processus crucial pour identifier, quantifier et hiérarchiser les faiblesses de sécurité dans un système d'information.
- Cette évaluation permet de prendre des mesures correctives pour prévenir les cyberattaques et minimiser les risques

# Évaluation des Vulnérabilités

## 1. Préparation

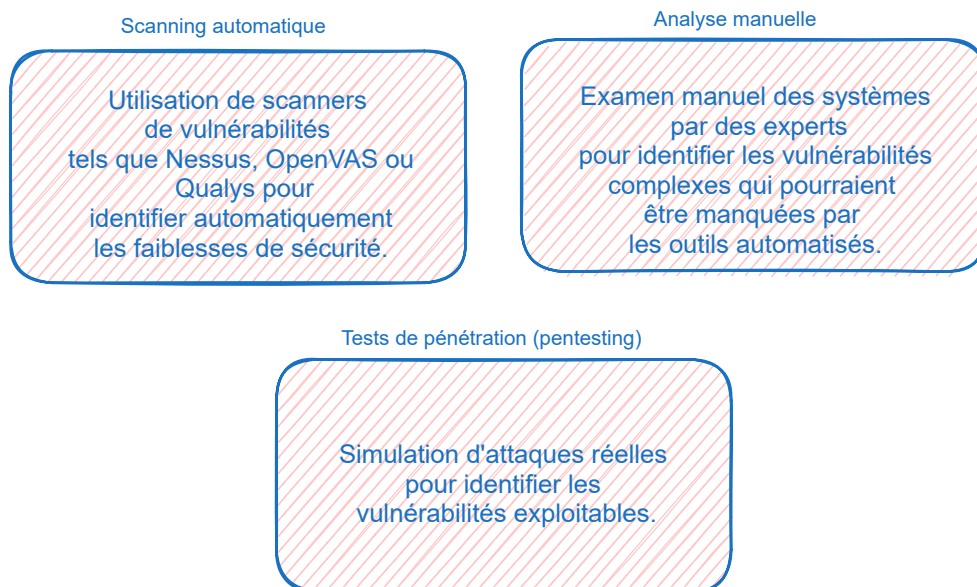
La phase de préparation consiste à définir les objectifs de l'évaluation, à sélectionner les outils et les méthodologies appropriés et à obtenir l'autorisation des parties prenantes.



# Évaluation des Vulnérabilités

## 2. Identification des vulnérabilités

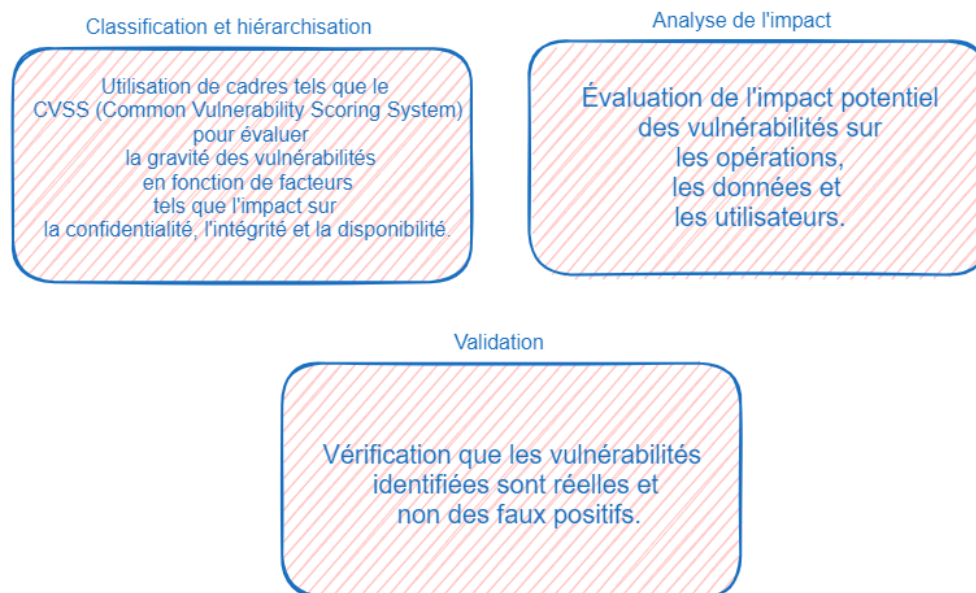
Cette phase consiste à découvrir les vulnérabilités présentes dans les systèmes, les applications et les réseaux. Les méthodes incluent :



# Évaluation des Vulnérabilités

## 3. Analyse des vulnérabilités

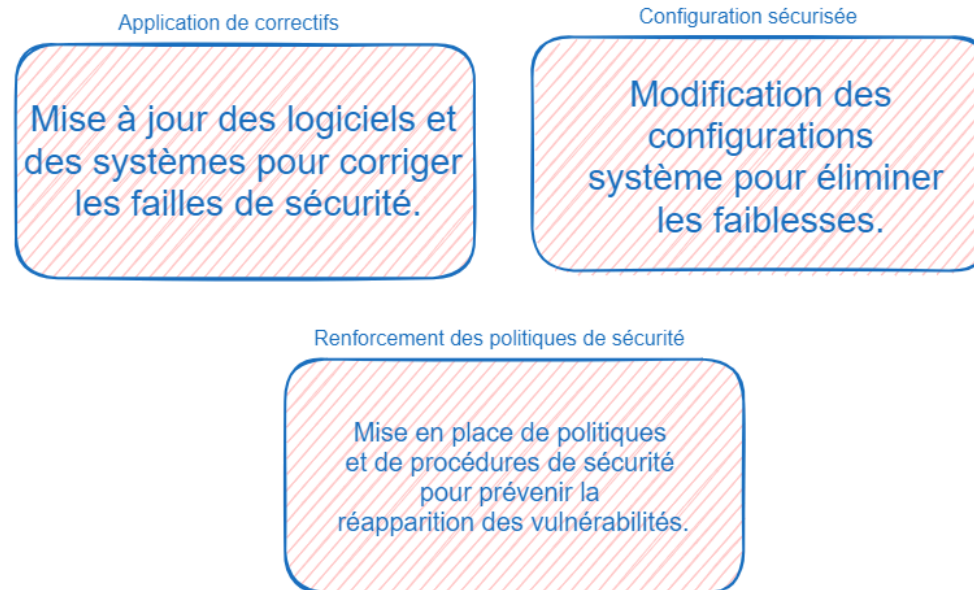
Une fois les vulnérabilités identifiées, elles doivent être analysées pour comprendre leur impact potentiel et leur exploitabilité. Les étapes incluent :



# Évaluation des Vulnérabilités

## 4. Remédiation

La phase de remédiation consiste à corriger les vulnérabilités identifiées pour réduire les risques.  
Les actions incluent :



# Évaluation des Vulnérabilités

## 5. Rapport et suivi

La phase de remédiation consiste à corriger les vulnérabilités identifiées pour réduire les risques.  
Les actions incluent :



# Évaluation des Vulnérabilités

## CVE, c'est quoi ?

**CVE**, qui signifie "Common Vulnerabilities and Exposures" (Vulnérabilités et Expositions Communes), est un programme qui identifie et catalogue les vulnérabilités de sécurité connues dans les logiciels et les systèmes. Il est maintenu par le MITRE Corporation et est soutenu par l'Agence de sécurité nationale des États-Unis (NSA) et le Département de la Sécurité intérieure des États-Unis (DHS).

# Évaluation des Vulnérabilités

## CVE, les éléments clés :

1. **Identification Unique** : Chaque vulnérabilité répertoriée dans la base de données CVE reçoit un identifiant unique appelé CVE ID. Par exemple, CVE-2021-34527.
2. **Catalogue Centralisé** : Le CVE fournit un catalogue centralisé de vulnérabilités de sécurité, permettant aux organisations de rechercher des informations sur des vulnérabilités spécifiques.
3. **Interopérabilité** : En utilisant des identifiants CVE standardisés, différents outils et services de sécurité peuvent échanger et corréler des informations sur les vulnérabilités plus efficacement.



# Évaluation des Vulnérabilités

## CVE, les éléments clés :

4. **Accès Public** : Les informations dans la base de données CVE sont accessibles publiquement, ce qui permet aux administrateurs système, aux chercheurs en sécurité, et aux développeurs de logiciels de rester informés des vulnérabilités actuelles.
5. **Processus de Validation** : Avant d'être incluses dans la base de données CVE, les vulnérabilités doivent être validées et approuvées par le comité de rédaction CVE.

# Évaluation des Vulnérabilités

## Types de vulnérabilités (OWASP Top 10)

- L'**OWASP** (**O**pen **W**eb **A**pplication **S**ecurity **P**roject) est une organisation mondiale à but non lucratif qui se consacre à la sécurité des applications logicielles.
- Depuis sa création en 2001, l'**OWASP** se concentre sur l'amélioration de la sécurité des logiciels grâce à des projets collaboratifs, des outils gratuits, des documents de formation, des forums et des conférences.

# Évaluation des Vulnérabilités

## Types de vulnérabilités (OWASP Top 10)

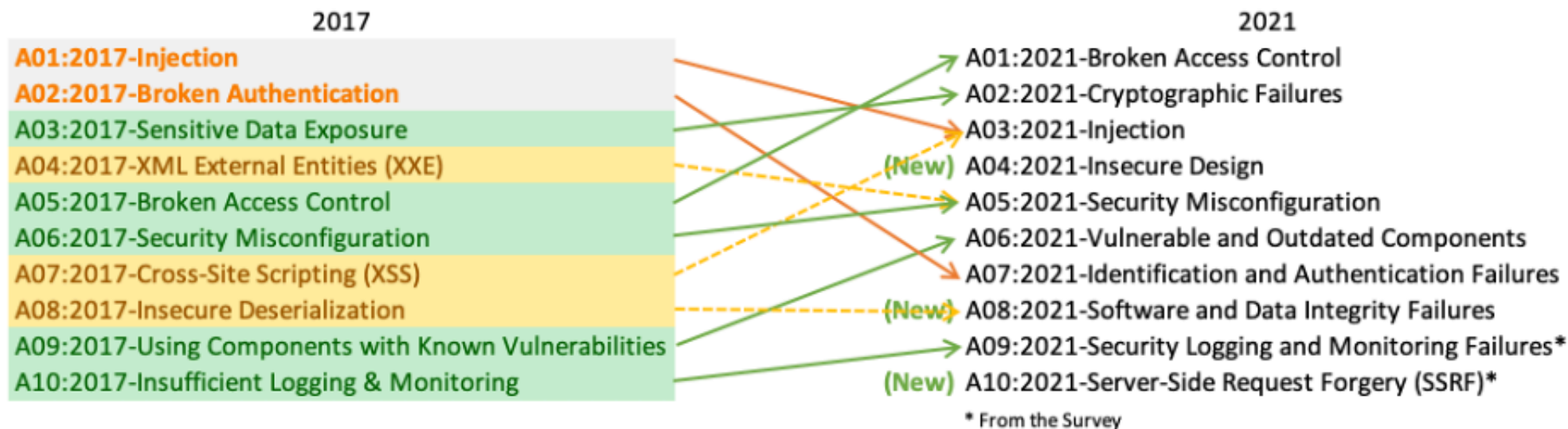
L'OWASP développe une multitude de projets visant à améliorer la sécurité des applications. Les plus connus incluent :

- **OWASP Top Ten** : Une liste des dix vulnérabilités les plus critiques dans les applications web. Elle est mise à jour régulièrement pour refléter les menaces actuelles et est largement utilisée par les développeurs et les professionnels de la sécurité pour orienter leurs efforts de sécurisation.
- **OWASP SAMM (Software Assurance Maturity Model)** : Un cadre permettant aux organisations de formuler et de mettre en œuvre une stratégie de sécurité logicielle adaptée à leurs risques spécifiques.
- **OWASP ASVS (Application Security Verification Standard)** : Un cadre de vérification de la sécurité des applications qui fournit un guide pour tester la sécurité des applications web.
- **OWASP ZAP (Zed Attack Proxy)** : Un outil de test de sécurité des applications web, très utilisé pour identifier les vulnérabilités dans les applications.

# Évaluation des Vulnérabilités

## Types de vulnérabilités (OWASP Top 10)

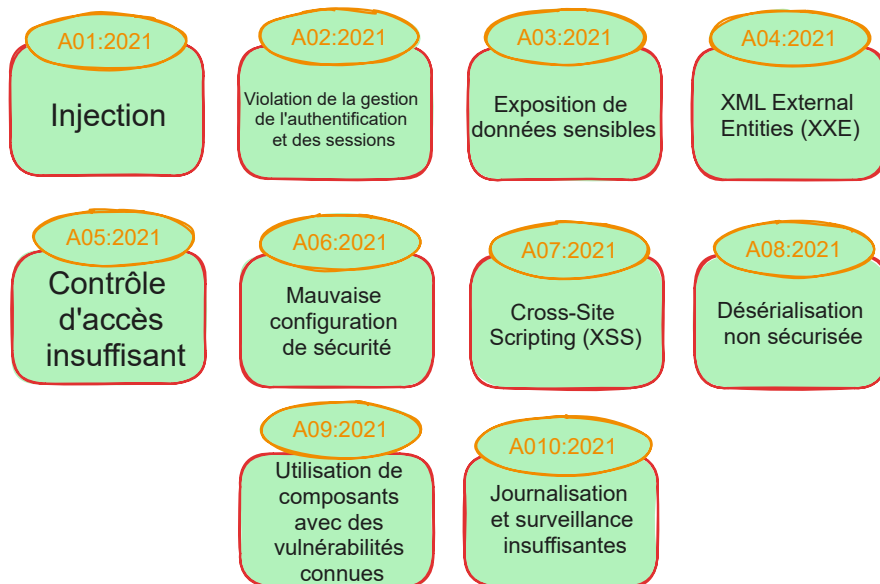
L'OWASP Top Ten est l'un des documents les plus influents et les plus consultés. Voici les catégories de vulnérabilités qui sont souvent présentes dans le Top Ten :



# Évaluation des Vulnérabilités

## Types de vulnérabilités (OWASP Top 10)

L'OWASP Top Ten est l'un des documents les plus influents et les plus consultés. Voici les catégories de vulnérabilités qui sont souvent présentes dans le Top Ten :



# Évaluation des Vulnérabilités

## A01:2021-Broken Access Control

- **A01:2021 de l'OWASP Top Ten** est intitulé "Broken Access Control", c'est-à-dire "Contrôle d'accès insuffisant" en français. C'est la vulnérabilité la plus critique identifiée dans le rapport OWASP Top Ten 2021
- Les contrôles d'accès sont des politiques et des règles qui déterminent les actions que les utilisateurs authentifiés et non authentifiés peuvent effectuer dans une application.
- Les contrôles d'accès défaillants surviennent lorsque les restrictions sur ce que les utilisateurs peuvent faire ne sont pas correctement appliquées.
- Les attaquants peuvent exploiter ces faiblesses pour accéder à des fonctionnalités et à des données non autorisées, comme accéder à des comptes d'autres utilisateurs, voir des fichiers sensibles, modifier des données d'autres utilisateurs, modifier des rôles d'accès, etc.

# Évaluation des Vulnérabilités

## A01:2021-Broken Access Control

### Principales Causes

- Contrôles d'accès manquants ou incorrectement implémentés.
- Absence de vérification des autorisations après l'authentification initiale.
- Utilisation de l'identifiant d'objet (comme l'ID utilisateur) dans les URL sans validation.
- Exposition excessive de services API sans contrôles d'accès appropriés.
- Mauvaise configuration de la gestion des sessions et des rôles.

# Évaluation des Vulnérabilités

## A01:2021-Broken Access Control

### Mesures de Prévention

- Implémenter des contrôles d'accès partout : Appliquer des vérifications de contrôle d'accès sur chaque fonction et chaque niveau de données.
- Utiliser des contrôles d'accès basés sur des rôles (RBAC) : Limiter les permissions en fonction des rôles définis.
- Ne jamais autoriser la modification directe des données sensibles via les entrées utilisateur : Utiliser des contrôles d'accès sur le serveur plutôt que de faire confiance aux données fournies par l'utilisateur.



# Évaluation des Vulnérabilités

## A01:2021-Broken Access Control

### Mesures de Prévention

- Limiter l'exposition des points d'accès : Restreindre l'accès aux API et aux services uniquement aux utilisateurs et aux systèmes autorisés.
- Tester régulièrement : Effectuer des tests d'intrusion et des audits de sécurité pour identifier et corriger les faiblesses dans les contrôles d'accès.
- Enregistrer et surveiller les accès : Utiliser la journalisation et la surveillance pour détecter les tentatives d'accès non autorisées.

# Évaluation des Vulnérabilités

## A01:2021-Broken Access Control

### Score de Gravité

- Le "**Broken Access Control**" est considéré comme très critique en raison de son potentiel à exposer des données sensibles et à permettre des actions non autorisées dans les applications.
- Il est souvent noté avec un score **CVSS** (Common Vulnerability Scoring System) élevé en raison de son impact sur la confidentialité, l'intégrité et la disponibilité des systèmes.

# Évaluation des Vulnérabilités

## A01:2021-Broken Access Control

### Exemples de Scénarios d'Attaque

#### 1. Bypass d'authentification :

- Un attaquant accède à une API non authentifiée qui permet d'obtenir les informations d'un utilisateur en utilisant simplement l'ID utilisateur dans l'URL.
- URL : <https://example.com/api/user/12345> permet à l'attaquant d'accéder aux informations de l'utilisateur avec l'ID 12345.

# Évaluation des Vulnérabilités

## A01:2021-Broken Access Control

### Exemples de Scénarios d'Attaque

#### 2. Escalade de privilèges :

- Un utilisateur normal modifie un paramètre de rôle dans une requête pour obtenir des privilèges administratifs.
- URL : <https://example.com/admin/settings> peut être accessible en modifiant simplement son rôle dans le paramètre de requête.

# Évaluation des Vulnérabilités

## A01:2021-Broken Access Control

### Exemples de Scénarios d'Attaque

3. Accès à des données non autorisées :

- Un utilisateur change l'ID d'un fichier dans l'URL pour accéder à des fichiers appartenant à d'autres utilisateurs.
- URL : <https://example.com/download?file=confidential.pdf> en modifiant le nom du fichier peut donner accès à des documents sensibles.

# Évaluation des Vulnérabilités

## A02:2021 - Cryptographic Failures

- Les échecs cryptographiques font référence à des problèmes liés à l'utilisation incorrecte ou inadéquate de la cryptographie.
- Ces problèmes peuvent inclure des algorithmes de chiffrement faibles, une gestion incorrecte des clés, des protocoles de chiffrement mal implémentés, et des données sensibles transmises ou stockées sans protection adéquate.

# Évaluation des Vulnérabilités

## A02:2021 - Cryptographic Failures

### Raisons de vulnérabilité

- Utilisation d'algorithmes de chiffrement obsolètes ou cassés.
- Clés cryptographiques mal gérées ou exposées.
- Protocole de chiffrement mal configuré ou implémenté.
- Absence de chiffrement pour des données sensibles en transit ou au repos.
- Utilisation de bibliothèques cryptographiques non sécurisées ou mal implémentées.

# Évaluation des Vulnérabilités

## A02:2021 - Cryptographic Failures

### Prévention et Atténuation

1. **Utilisation de normes cryptographiques robustes** : Utiliser des algorithmes de chiffrement et des protocoles reconnus et recommandés par des organisations de sécurité, tels que AES pour le chiffrement, RSA pour les échanges de clés, et TLS pour les communications sécurisées.
2. **Gestion sécurisée des clés** : Mettre en œuvre une gestion rigoureuse des clés, y compris la rotation régulière des clés, le stockage sécurisé des clés, et l'utilisation de HSM (Hardware Security Modules) si nécessaire.



# Évaluation des Vulnérabilités

## A02:2021 - Cryptographic Failures

### Prévention et Atténuation

3. **Chiffrement des données sensibles** : Chiffrer toutes les données sensibles en transit (par exemple, via HTTPS/TLS) et au repos (par exemple, via AES).
4. **Tests de sécurité** : Intégrer des tests de sécurité automatisés pour vérifier les configurations de chiffrement et détecter les faiblesses.
5. **Formation et bonnes pratiques** : Former les développeurs sur les bonnes pratiques en matière de cryptographie et les sensibiliser aux risques associés à une mauvaise implémentation.

# Évaluation des Vulnérabilités

## A02:2021 - Cryptographic Failures

### Outils et Ressources

- **OWASP Cryptographic Storage Cheat Sheet** : Guide pour une gestion sécurisée du stockage cryptographique.
- **SSL Labs** : Un outil pour tester les configurations TLS des serveurs web.
- **OpenSSL** : Une bibliothèque populaire pour implémenter les protocoles SSL et TLS.

# Évaluation des Vulnérabilités

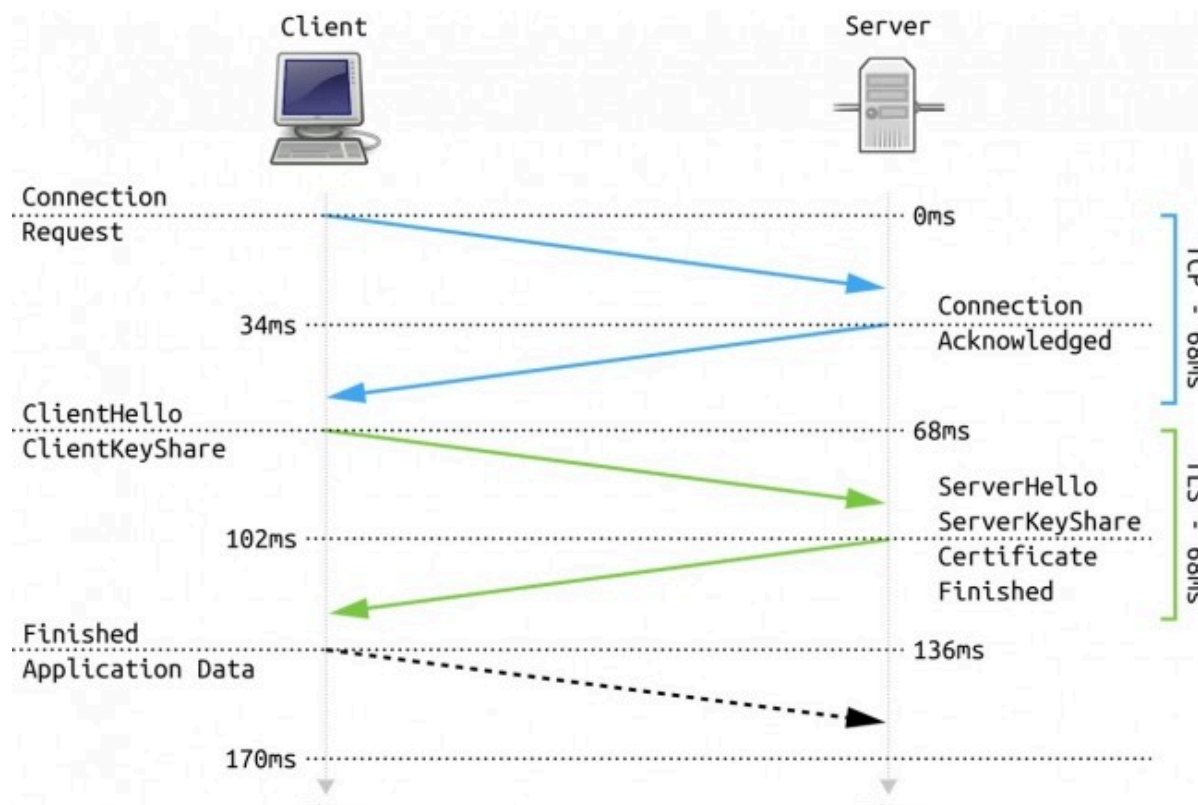
## A02:2021 - Cryptographic Failures

### Exemple

- Une application web utilise le protocole HTTPS, mais avec une configuration TLS obsolète qui permet l'utilisation de suites de chiffrement faibles comme RC4.
- Un attaquant pourrait exploiter cette faiblesse pour déchiffrer les communications entre l'utilisateur et le serveur, exposant ainsi des données sensibles telles que des informations de connexion ou des numéros de carte de crédit.

# Évaluation des Vulnérabilités

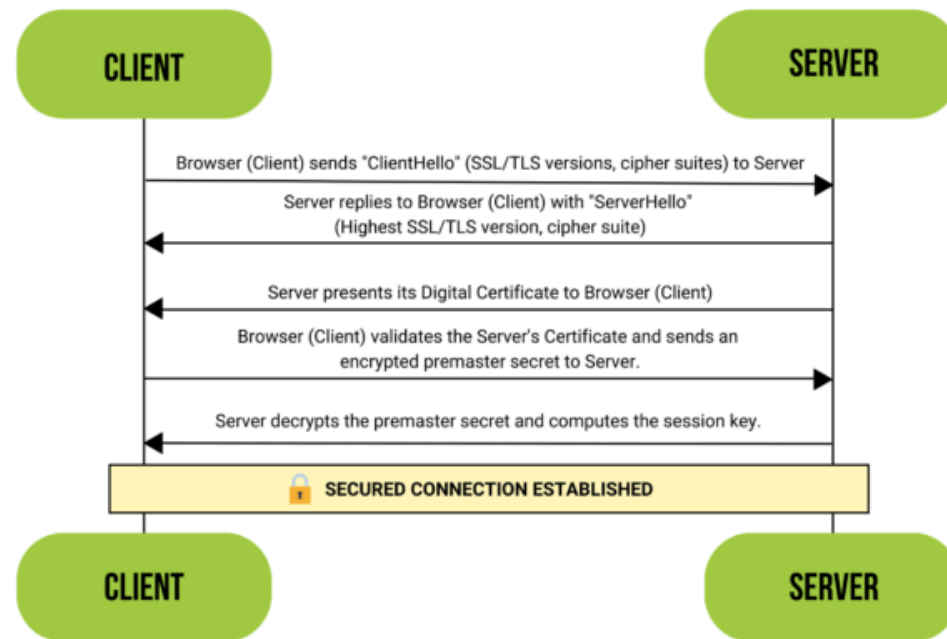
## A02:2021 - Cryptographic Failures



# Évaluation des Vulnérabilités

## A02:2021 - Cryptographic Failures

### SSL/TLS HANDSHAKE



# Évaluation des Vulnérabilités

## A03:2021 - Injection

- L'entrée A03:2021 dans le OWASP Top 10 est **Injection**.
- Cette catégorie englobe diverses formes d'attaques par injection où des données non fiables sont envoyées à un interpréteur comme partie d'une commande ou d'une requête
- Ces injections peuvent se produire dans divers contextes tels que SQL, NoSQL, OS et LDAP.

# Évaluation des Vulnérabilités

## A03:2021 - Injection

### Formes Communes :

- **Injection SQL** : Où du code SQL malveillant est inséré dans une requête.
- **Injection NoSQL** : Similaire à l'injection SQL, mais cible les bases de données NoSQL.
- **Injection de Commandes OS** : Où un attaquant peut exécuter des commandes arbitraires sur le système d'exploitation hôte.
- **Injection LDAP** : Implique l'insertion de déclarations LDAP malveillantes.

# Évaluation des Vulnérabilités

## A03:2021 - Injection

### Risques :

- **Violation de Données** : Accès non autorisé à des données sensibles.
- **Perte/Manipulation de Données** : Modification ou suppression de données.
- **Compromission du Système** : Contrôle potentiel total sur le système.



# Évaluation des Vulnérabilités

## A03:2021 - Injection

### Mesures Préventives :

- **Validation des Entrées** : Valider et nettoyer toutes les entrées.
- **Requêtes Paramétrées/Instructions Préparées** : Utilisez-les pour empêcher l'insertion directe de l'entrée utilisateur dans les requêtes.
- **Utiliser des ORM (Object-Relational Mapping)** : Les frameworks ORM comme Hibernate, Entity Framework ou Django ORM fournissent une abstraction au-dessus des requêtes SQL, ce qui réduit le risque d'injection SQL.

# Évaluation des Vulnérabilités

## A03:2021 - Injection

### Mesures Préventives :

- **Procédures Stockées** : Utilisez-les au lieu des requêtes dynamiques.
- **Échappement** : Échapper correctement les caractères spéciaux dans les entrées.
- **Principe du Moindre Privilège** : Assurez-vous que l'application dispose des permissions minimales nécessaires.

# Évaluation des Vulnérabilités

## A03:2021 - Injection

Exemple requêtes préparées :

```
String query = "SELECT * FROM users WHERE username = ? AND password = ?";
PreparedStatement stmt = connection.prepareStatement(query);
stmt.setString(1, username);
stmt.setString(2, password);
ResultSet rs = stmt.executeQuery();
```

# Évaluation des Vulnérabilités

## A04:2021 - Insecure Design

- L'entrée A04:2021 dans le OWASP Top 10 est **Conception sécurisée**.
- Cette catégorie met l'accent sur l'importance de l'intégration des pratiques de sécurité dès le début du cycle de développement des applications, afin de prévenir les vulnérabilités avant qu'elles ne surviennent.

# Évaluation des Vulnérabilités

## A04:2021 - Insecure Design

### Principes de Conception Sécurisée :

- **Sécurité par Conception** : Incorporer des mécanismes de sécurité dès la phase de conception.
- **Sécurité par Défaut** : Configurer les systèmes pour qu'ils soient sécurisés par défaut, avec des options permettant de renforcer la sécurité.
- **Modélisation des Menaces** : Identifier et analyser les menaces potentielles dès le début.
- **Principe du Moindre Privilège** : Restreindre les permissions et l'accès aux ressources au minimum nécessaire.

# Évaluation des Vulnérabilités

## A05:2021 - Security Misconfiguration

### Exemples de Mauvaise Configuration

- **Configurations Par Défaut** : Utilisation de paramètres par défaut qui peuvent être facilement devinés ou exploités.
- **Messages d'Erreur Verbeux** : Messages d'erreur détaillés qui divulguent des informations sensibles.
- **Serveurs Non Sécurisés** : Serveurs avec des ports ouverts ou des services non nécessaires activés.
- **Permissions Excessives** : Comptes et services disposant de permissions plus élevées que nécessaire.

# Évaluation des Vulnérabilités

## A05:2021 - Security Misconfiguration

### Risques :

- **Exposition de Données Sensibles** : Informations sensibles accessibles à des utilisateurs non autorisés.
- **Compromission de Systèmes** : Les systèmes peuvent être compromis en raison de paramètres non sécurisés.
- **Exploitation des Failles** : Les configurations incorrectes peuvent être exploitées pour lancer des attaques plus complexes.

# Évaluation des Vulnérabilités

## A05:2021 - Security Misconfiguration

### Mesures Préventives :

- **Revue de Sécurité** : Effectuer des revues régulières des configurations de sécurité.
- **Automatisation** : Utiliser des outils d'automatisation pour gérer et vérifier les configurations.
- **Principes du Moindre Privilège** : Limiter les permissions des comptes et des services.
- **Hardening** : Renforcer les serveurs et les applications en désactivant les fonctionnalités inutiles et en appliquant des configurations sécurisées.



# Évaluation des Vulnérabilités

## A05:2021 - Security Misconfiguration

### Scénario d'Exemple :

- **Exemple de Base de Données :**

Une base de données pourrait être laissée avec son mot de passe administrateur par défaut, tel que "admin" ou "password". Un attaquant pourrait facilement deviner ce mot de passe et accéder à la base de données, volant ainsi des informations sensibles ou modifiant des données critiques.

# Évaluation des Vulnérabilités

## A05:2021 - Security Misconfiguration

### Bonnes Pratiques :

- **Gestion des Patches** : Maintenir tous les systèmes à jour avec les dernières mises à jour de sécurité.
- **Tests de Pénétration** : Effectuer des tests de pénétration pour identifier et corriger les configurations non sécurisées.
- **Surveillance** : Mettre en place une surveillance continue pour détecter les configurations vulnérables et les corriger rapidement.

# Évaluation des Vulnérabilités

## A06:2021 - Vulnerable and Outdated Components

L'entrée A06:2021 dans le OWASP Top 10 est **Composants vulnérables et obsolètes**. Cette catégorie met en lumière les risques liés à l'utilisation de composants logiciels qui présentent des vulnérabilités connues ou qui ne sont plus maintenus par leurs développeurs.

# Évaluation des Vulnérabilités

## A06:2021 - Vulnerable and Outdated Components

### Sources de Vulnérabilités :

- **Librairies et Frameworks** : Utilisation de librairies et frameworks contenant des failles de sécurité connues.
- **Composants Non Mis à Jour** : Composants logiciels qui ne sont pas mis à jour avec les derniers patches de sécurité.
- **Composants Obsolètes** : Utilisation de composants qui ne sont plus supportés par les développeurs et pour lesquels il n'y a plus de mises à jour de sécurité.

# Évaluation des Vulnérabilités

## A06:2021 - Vulnerable and Outdated Components

### Risques :

- **Compromission du Système** : Les vulnérabilités dans les composants peuvent être exploitées pour prendre le contrôle du système.
- **Exposition des Données** : Accès non autorisé à des données sensibles via des composants vulnérables.
- **Propagation des Vulnérabilités** : Une faille dans un composant peut entraîner une cascade de vulnérabilités dans l'ensemble du système.

# Évaluation des Vulnérabilités

## A06:2021 - Vulnerable and Outdated Components

### Mesures Préventives :

- **Gestion des Dépendances** : Maintenir une liste à jour de toutes les dépendances et de leurs versions.
- **Mises à Jour Régulières** : Appliquer régulièrement les mises à jour et patches de sécurité pour tous les composants utilisés.
- **Scanner de Vulnérabilités** : Utiliser des outils de scan de vulnérabilités pour identifier les composants à risque.
- **Politique de Sécurité des Composants** : Adopter des politiques strictes pour l'utilisation de composants externes, y compris la vérification de leur sécurité et de leur support.

# Évaluation des Vulnérabilités

## A06:2021 - Vulnerable and Outdated Components

### Scénario d'Exemple :

- **Exemple de Librairie JavaScript :**

Une application web utilise une librairie JavaScript populaire mais obsolète, connue pour avoir une faille de sécurité critique. Un attaquant peut exploiter cette faille pour injecter du code malveillant, compromettant ainsi la sécurité de l'application et de ses utilisateurs.

# Évaluation des Vulnérabilités

## A06:2021 - Vulnerable and Outdated Components

### Bonnes Pratiques :

- **Inventaire des Composants** : Maintenir un inventaire détaillé de tous les composants et leurs versions.
- **Surveillance des Annonces de Sécurité** : Suivre les annonces de sécurité des fournisseurs de composants pour être informé des nouvelles vulnérabilités.
- **Tests de Sécurité** : Intégrer des tests de sécurité dans le cycle de développement pour détecter les composants vulnérables avant le déploiement.



