# Cours
# Sécurité et cryptographie

## Chapitre 4:
## Analyse de risques

# Plan

- Définitions et objectifs
- Méthodes d’analyse de risques
- Méthode Méhari
- Méthode du NIST 8000-30
- Méthode OWASP
- Conclusion

# Définitions

- Vulnérabilité:
  - Défaut ou faiblesse
- Menace:
  - La possibilité qu'une vulnérabilité soit exploitée
- Vraisemblance de la menace:
  - La probabilité qu'une vulnérabilité soit exploitée
- Attaques:
  - Action malveillante exploitant des vulnérabilités
- Risque:
  - **Impact** sur la mission de l'entreprise

# Objectifs

- Prendre de meilleures décisions basées sur des faits tangibles et mesurables.
  - Investissement en équipement, personnel, formation,

➔ Avoir une meilleure protection des systèmes d'information

# Méthodes d'analyse de risques

- MEHARI (janvier 2010: nouvelle version )
  - ***ME****thode* ***H****armonisée d'****A****nalyse des* ***RI****sques*
- NIST 800-30 (juillet 2002)
  - *Risk Management Guide for Information Technology Systems*
- MARION (1983)
  - *Méthode d'analyse de risques informatiques optimisée par niveau 1983*
- OCTAVE (1999)
  - *Operationally Critical Threat, Asset and Vulnerability Evaluation*
- EBIOS
  - *Expression des Besoins et Identification des Objectifs de Sécurité*
- OWASP
  - *Open Web Application Security Project*

# MEHARI

- L’analyse couvre:
  - L’identification des situations susceptibles de remettre en cause un des résultats attendus de l’organisation
    - Destruction de matériel, altération de données, perte de fichiers….
  - L'évaluation :
    - de la probabilité de telles situations ➔ potentialité
    - de leurs conséquences possibles➔ impact
    - de leur caractère acceptable ou non ➔ gravité
  - La détermination des mesures susceptibles de ramener chaque risque à un niveau acceptable

# MEHARI

- Impact (I)
  - l'ampleur des conséquences d'un événement possible : de1 (faible) à 4 (grave).
- Potentialité (P)
  - la probabilité qu'un événement survienne effectivement: de 0 (nulle) à 4 (forte)
- Gravité (G)
  - G= F( I, P). Sa valeur s'obtient en utilisant une grille (table), qui doit être **personnalisée** par l'entreprise qui applique la méthode.

Impact

| | | | | | |
|---|---|---|---|---|---|
| **4** | 0 | **3** | **4** | **4** | **4** |
| **3** | 0 | **2** | **3** | **3** | **3** |
| **2** | 0 | 1 | 1 | **2** | **2** |
| **1** | 0 | 0 | 0 | 1 | **1** |
| | **0** | **1** | **2** | **3** | **4** |

Potentialité

Gravité = *f* (I,P)

4 = Risques insupportables
3 = Risques inadmissibles
2 = Risques tolérés

# NIST (800-30 ): objectif

- Décrire une méthodologie permettant de réaliser une analyse de risques pour des systèmes tenant compte de leur cycle de développement.
  - Initiation
  - Acquisition et le développement
  - Implémentation
  - Opération et maintenance
  - Élimination

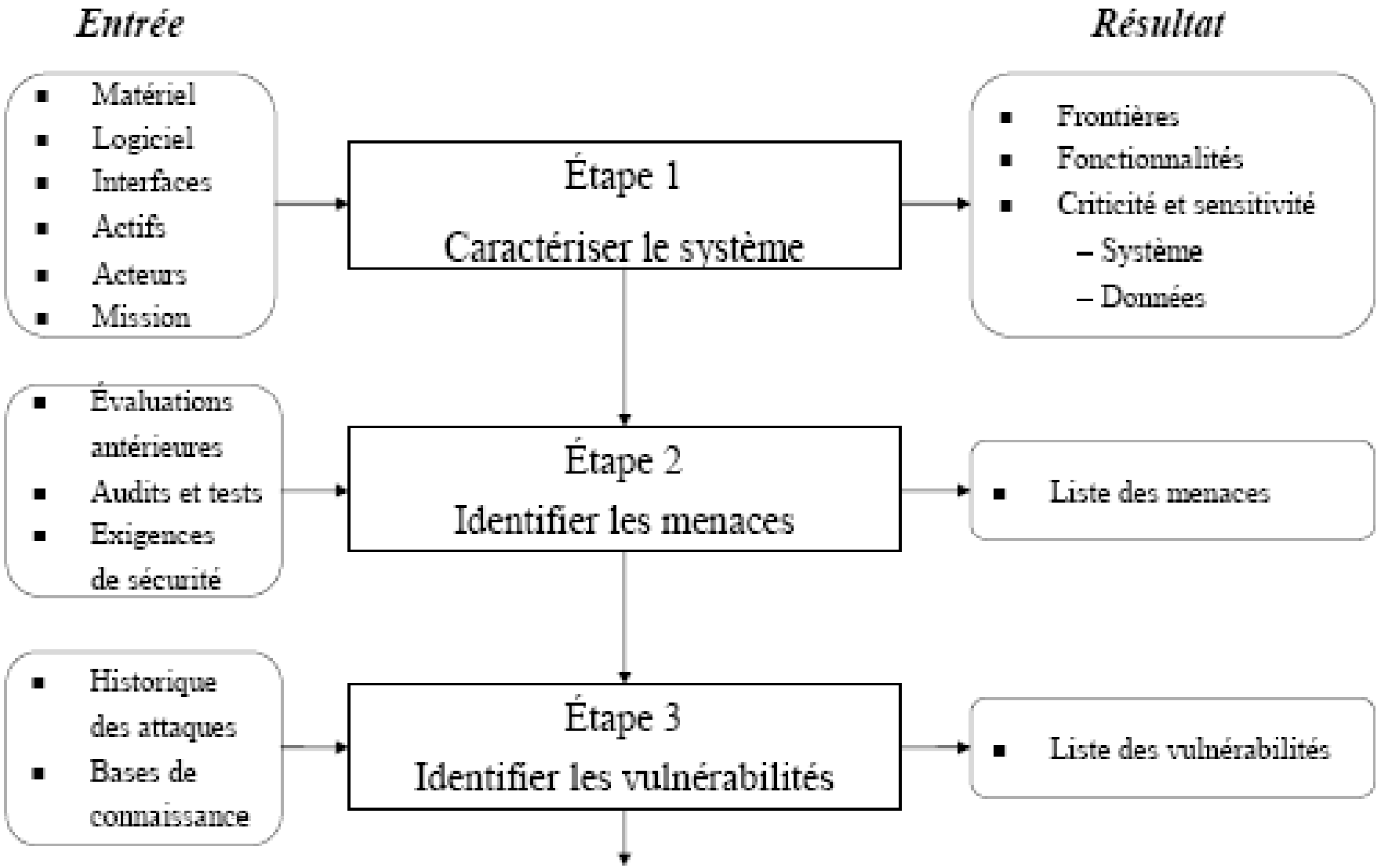
# NIST (800-30 ): trois étapes générales

- Évaluation des risques
  - Indentification et évaluation des risques et de leurs impacts
  - Détermination des priorités de ces risques
  - Recommandation de contre-mesures
- Atténuation des risques
  - Classement par ordre de priorité des contre-mesures
  - Implémentation et maintenance des contre-mesures
- Évolution et évaluation
  - Évaluation continue du système au cours de son évolution

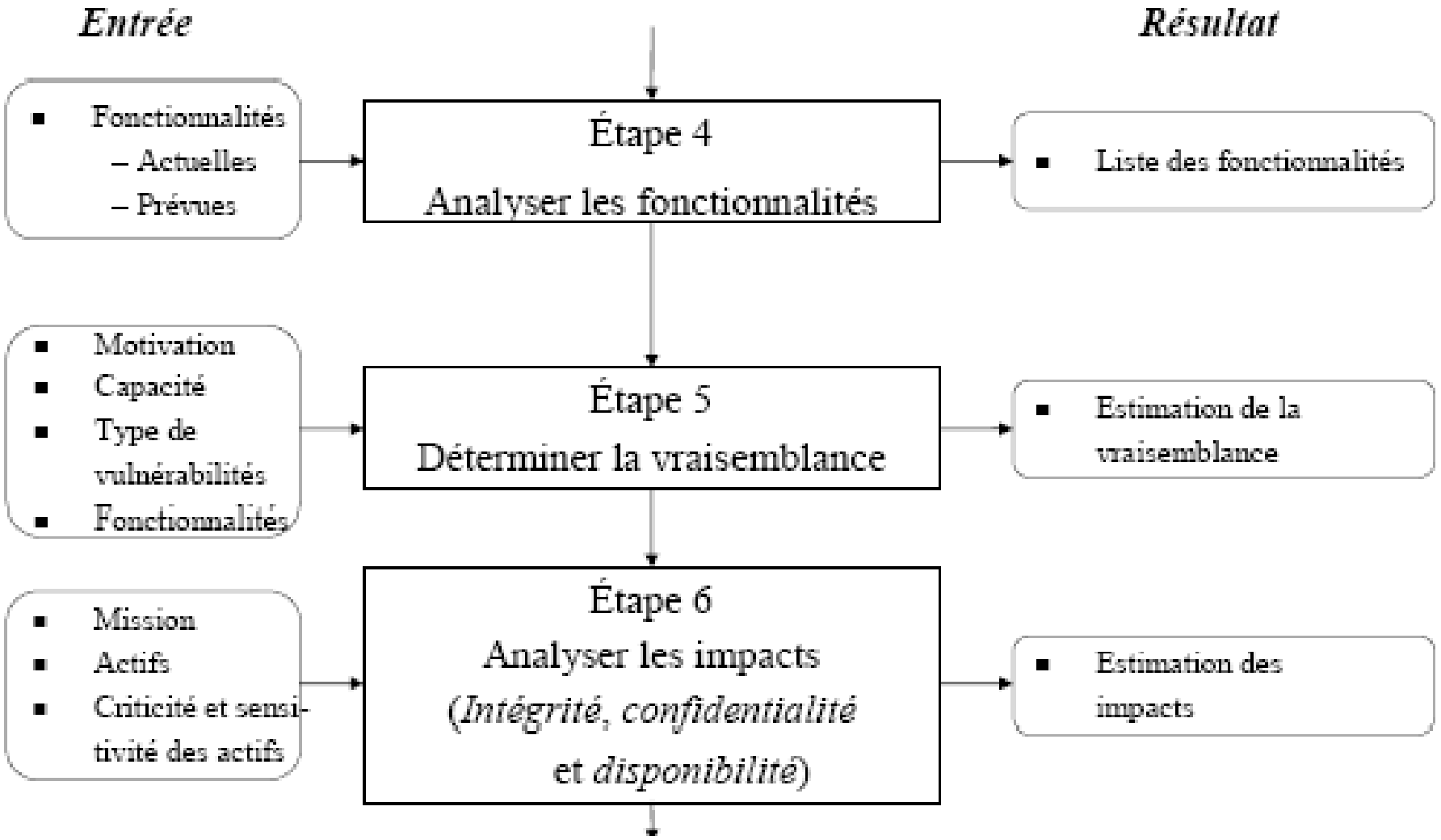
# NIST (800-30 ): 9 étapes spécifiques

- Neuf étapes
  - Caractérisation du système
  - Identification des menaces
  - Identification des vulnérabilités
  - Analyse des fonctionnalités de sécurité
  - Détermination de la vraisemblance
  - Analyse des impacts
  - Détermination des risques
  - Recommandation des contre-mesures
  - Documentation

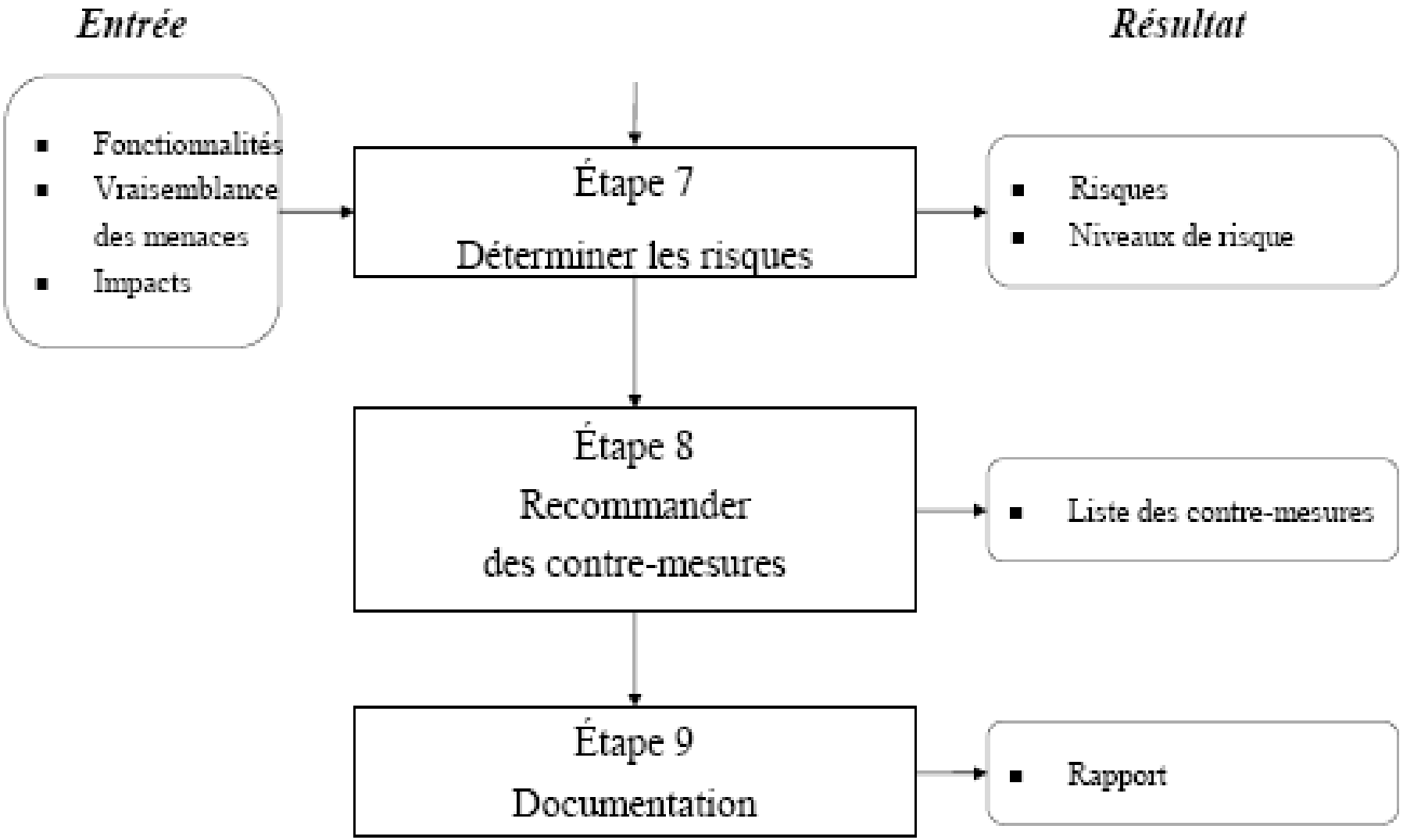
# NIST (800-30 ): 9 étapes spécifiques



# NIST (800-30 ): 9 étapes spécifiques



# NIST (800-30 ): 9 étapes spécifiques



# Etape 1: caractérisation du système

- En utilisant des:
  - Questionnaires, Entrevues, Revue de la documentation , Outils automatiques de balayage…etc

- Définir les limites du système à évaluer
  - Mission d'affaire
    - Acteurs – usagers, administrateurs, …
    - Actifs informationnels – criticité et sensitivité (intégrité, confidentialité et disponibilité)
    - Exigence de sécurité
  - Matériel
    - Topologie, mécanismes de protection, …
  - Logiciel
  - Flots d'information
    - Connectivité réseau
    - Interfaces de programmation (*API*)
  - Contrôle de gestion et Contrôle opérationnel

➔ *Évaluer la tâche à accomplir et les efforts requis.*

# Etape 2: identification des menaces

- (1) Identifier les **sources de menaces**:
  - Naturelle
    - Inondations, tremblements de terre, …
  - Environnementale
    - Pollution, pannes électriques prolongées, fuites d'eau, …
  - Humaine
    - Erreurs humaines non-intentionnelles
    - Actions malicieuses

- (2) Evaluer:
  - Leurs motivations : Argent, …
  - Leurs moyens: technologique, …

# Étape 2 – Identification des menaces

| Source | Motivation | Actions |
|---|---|---|
| Pirate<br>(*hacker, cracker*) | ▪Challenge<br>▪Ego<br>▪Rébellion | ▪Piratage<br>▪Ingénierie sociale |
| Criminel informatique | ▪Destruction d'information<br>▪Divulgation d'information<br>▪Altération d'information<br>▪Gain monétaire | ▪Ingénierie sociale<br>▪Interception d'information<br>▪Intrusion de système<br>▪Chantage informatique<br>▪Cambriolage<br>▪Mystification (*spoofing*) |
| Terroriste | ▪Destruction<br>▪Revanche<br>▪Idéologie | ▪Bombe / terrorisme<br>▪Guerre de l'information<br>▪Attaque de systèmes (DDoS)<br>▪Intrusion de systèmes<br>▪Subordination de systèmes (*tampering*) |

# Étape 2 – Identification des menaces

| Source | Motivation | Actions |
|---|---|---|
| Espionnage industriel | ▪Avantage compétitif<br>▪Appât du gain | ▪Ingénierie sociale<br>▪Intrusion de système<br>▪Vol d'information |
| Employé<br>▪Malfonné<br>▪Négligent<br>▪Malveillant<br>▪Malhonnête<br>▪Congédié | ▪Curiosité<br>▪Ego<br>▪Renseignement<br>▪Appât du gain<br>▪Revanche<br>▪Non-intentionnel et omission | ▪Code malveillant<br>⌞Cheval de Troie, Bombe logique<br>▪Accès à de l'information privée<br>▪Utilisation d'ordinateur abusive<br>▪Fraude et vol<br>▪Vente d'information personnel<br>▪Sabotage de système<br>▪Intrusion de système |

# Étape 3 – Identification des vulnérabilités

- Sources de vulnérabilités
  - Humain
  - Politiques de sécurité
  - Architecture
    - IT, logiciel
  - Implémentation
    - IT, logiciel
  - Déploiement
    - IT, configuration logicielle

# Étape 4 – Analyse des fonctionnalités

- Déterminer les fonctionnalités de sécurité
  - Existantes
  - Planifiées ➔ pour réduire ou éliminer la probabilité qu'une source de menaces puisse utiliser une vulnérabilité.

- Fonctionnalité de sécurité:
  - Techniques
    - Logiciel et matériel: contrôle d'accès, identification, authentification, chiffrement, …
  - Non-techniques
    - Politiques de sécurité, procédures opérationnelles, sécurité du personnel, sécurité physique, …

# Étape 4 – Analyse des fonctionnalités

- Types de contrôle
  - Prévenir les tentatives de violation de politiques de sécurité
    - Contrôle d'accès, chiffrement et authentification, IPS, …
  - Détecter les tentatives de violation de politiques de sécurité
    - IPS, IDS, …
  - Réagir aux tentatives de violation de politiques de sécurité
    - Firewall, IPS…

# Étape 5 – Détermination de la vraisemblance

- La vraisemblance
  - la **probabilité** qu'une vulnérabilité soit exploitée par une source de menaces.

- Points à considérer pour déterminer la vraisemblance:
  - Les aptitudes et la motivation d'une source de menaces
  - La nature de la vulnérabilité
  - L'existence et l'efficacité d'un moyen de contrôle

# Étape 5 – Détermination de la vraisemblance

| Vraisemblance | Définition |
|---|---|
| Haut | La source de menaces est hautement motivée et possède tous les moyens requis pour effectuer son attaque **ET** aucun moyen de contrôle efficace n'est en place. |
| Moyen | La source de menaces est motivée et possède les moyens courants **MAIS** des moyens de contrôle sont en place afin de réduire l'impact de vulnérabilité. |
| Bas | La source de menaces manque de motivation ou de moyen **OU** il existe un moyen efficace afin de prévenir l'exploitation de la vulnérabilité. |

# Étape 6 – Analyse des impacts

- L'impact dépend de:
  - La mission du système
  - La criticité du système et des données
  - La sensitivité du système et des données

- L'impact se mesure sur les propriétés des actifs
  - Intégrité
  - Confidentialité
  - Disponibilité

➔ Rapport d'analyse d'impact sur les affaires.
  - Analyser de façon **quantitative** et **qualitative** la criticité et la sensitivité des différents actifs.

# Étape 6 – Analyse des impacts

| Impacts | Définition |
|---|---|
| Haut | L'exploitation d'une vulnérabilité (1) résulte par la perte d'actifs ou de ressources de grande valeur; (2) cause un préjudice importance à l'entreprise (mission, réputation, …) |
| Moyen | L'exploitation d'une vulnérabilité (1) résulte par la perte d'actifs ou de ressources coûteuses; (2) cause une préjudice à l'entreprise (mission, réputation, …) |
| Bas | L'exploitation d'une vulnérabilité (1) résulte par la perte d'actifs ou de ressources; (2) affecte l'entreprise (mission, réputation, …) |

# Étape 7 – Détermination des risques

- Pour chaque paire menace-vulnérabilité, le risque dépend de:
  - La vraisemblance
  - L'impact
  - Les mécanismes de protection installés
  - Risque = Vraisemblance * Impact

| | **Impact** bas (10) | **Impact** moyen (50) | **Impact** haut (100) |
|---|---|---|---|
| **Vraisemblance** haute 1.0 | **BAS** 10 x 1.0 = 10 | **MOYEN** 50 x 1.0 = 50 | **HAUT** 100 x 1.0 = 100 |
| **Vraisemblance** moyenne 0.5 | **BAS** 10 x 0.5 = 5 | **MOYEN** 50 x 0.5 = 25 | **MOYEN** 100 x 0.5 = 50 |
| **Vraisemblance** basse 0.1 | **BAS** 10 x 0.1 = 1 | **BAS** 50 x 0.1 = 5 | **BAS** 100 x 0.1 = 10 |

# Étape 7 – Détermination des risques

| Risque | Description et Action |
|---|---|
| Haut | Méthodes correctives fortement requises. Un plan d'intervention doit être mis en place de façon urgente. |
| Moyen | Méthodes correctives requises. Un plan d'intervention doit être mis en place dans temps raisonnable. |
| Bas | La personne responsable du système doit déterminer si des actions correctives doivent être prises ou si le risque est acceptable. |

# Étape 8 – Recommandations

- Déterminer les **moyens de contrôle** à mettre en place afin de réduire les risques identifiés à un niveau acceptable en tenant compte des points suivant:
  - Efficacité
  - Compatibilité avec le système
  - Impact sur les opérations
  - Coûts
  - Politique organisationnelle
  - Loi et réglementation

# Étape 9 – Documentation

- Rapport décrivant
  - Les menaces et leurs sources (moyen et motivation)
  - Les vulnérabilités
  - Les risques et leur priorités
  - Les recommandations devant être mise en place

- Sommaire
  - Décrivant les principaux points – les risques élevés

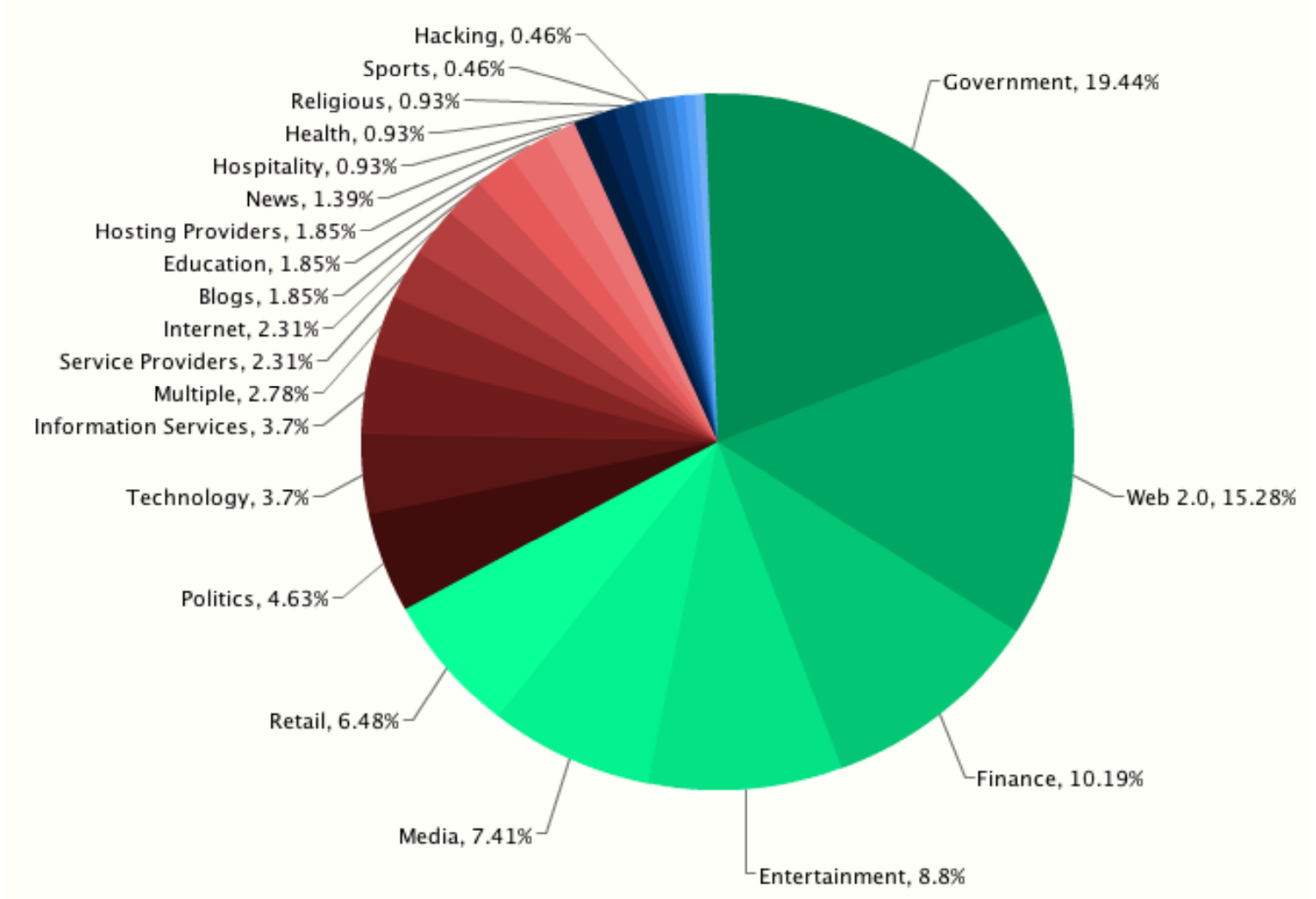
# OWASP

- Spécifique aux risques des applications Web
- Dans OWASP
  - Risque = Vraisemblance * Impact
- 5 étapes
  - Étape 1: Identification du **risque**
  - Étape 2: Estimation de la **vraisemblance**
  - Étape 3: Estimation de **l'impact**
  - Étape 4: Évaluation de la **gravité** du risque
  - Étape 5: Choix d'aspects à corriger

# OWASP

- Etape 1: identification du risque

Cibles d'attaques

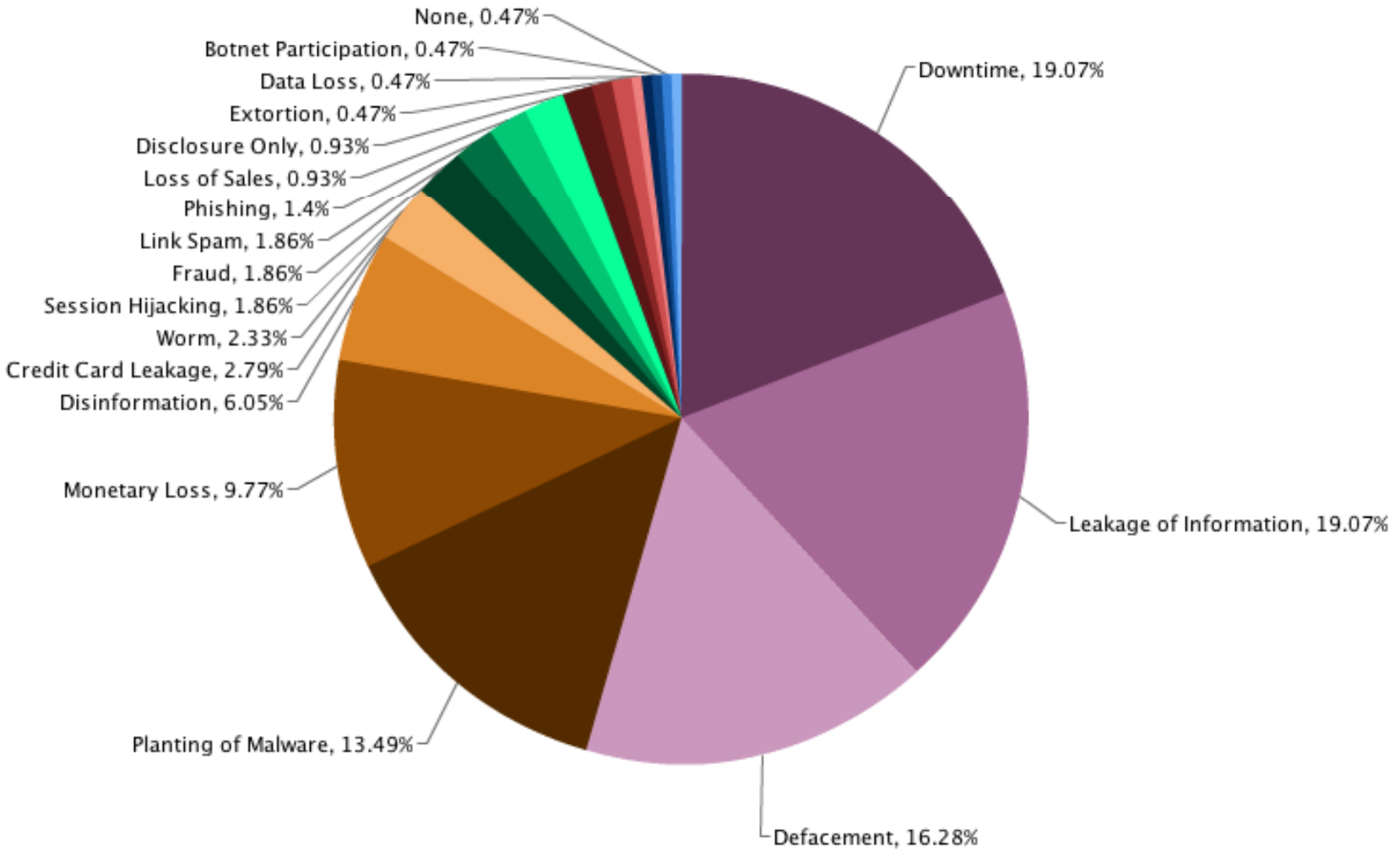



**Sourc: The Web Hacking Incident Database (WHID) Report for 2010**

# OWASP

- Etape 1: identification du risque

Objectifs d'attaques

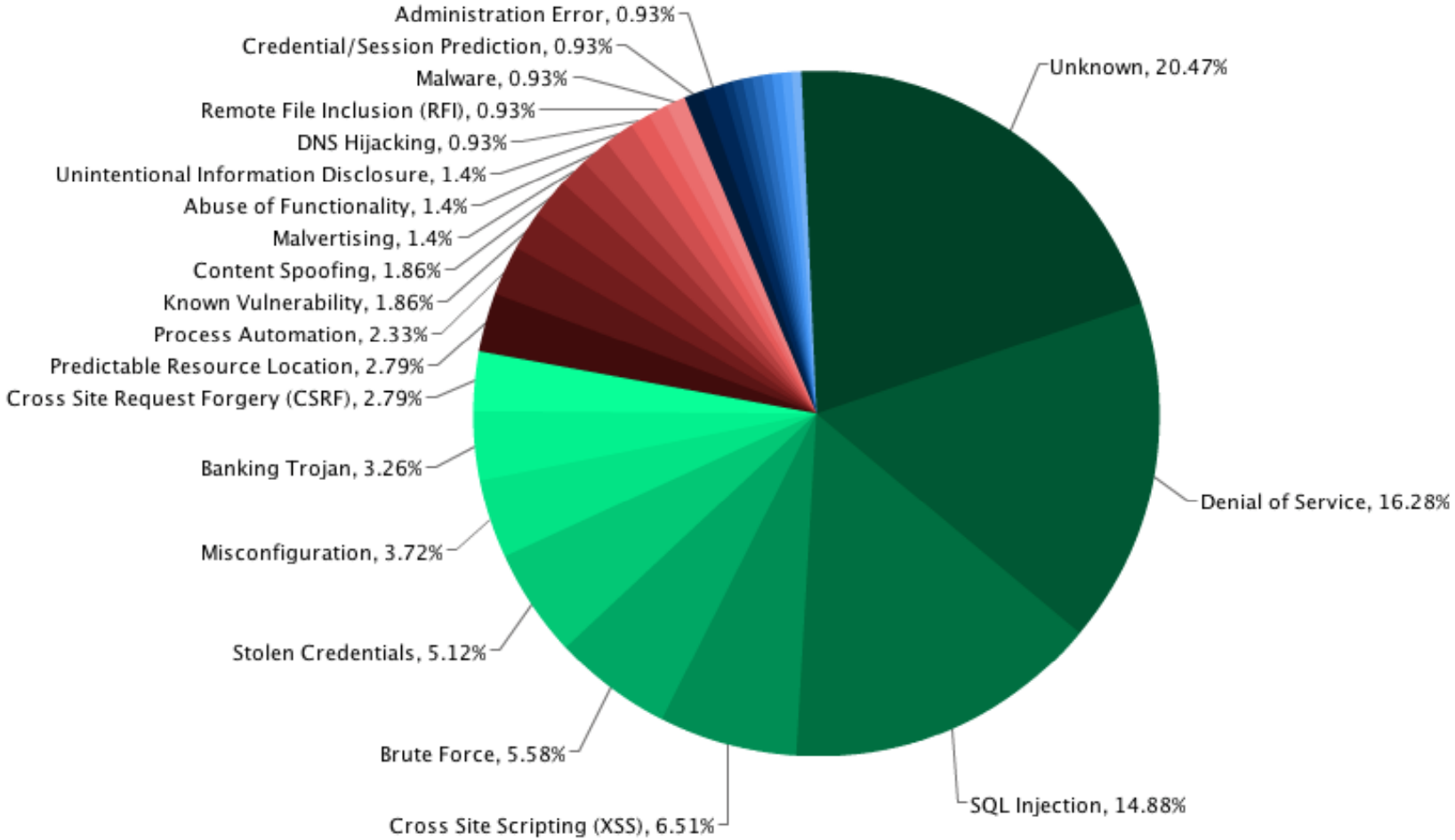



Sourc: The Web Hacking Incident Database (WHID) Report for 2010

# OWASP

- Etape 1: identification du risque

Méthodes d'attaques

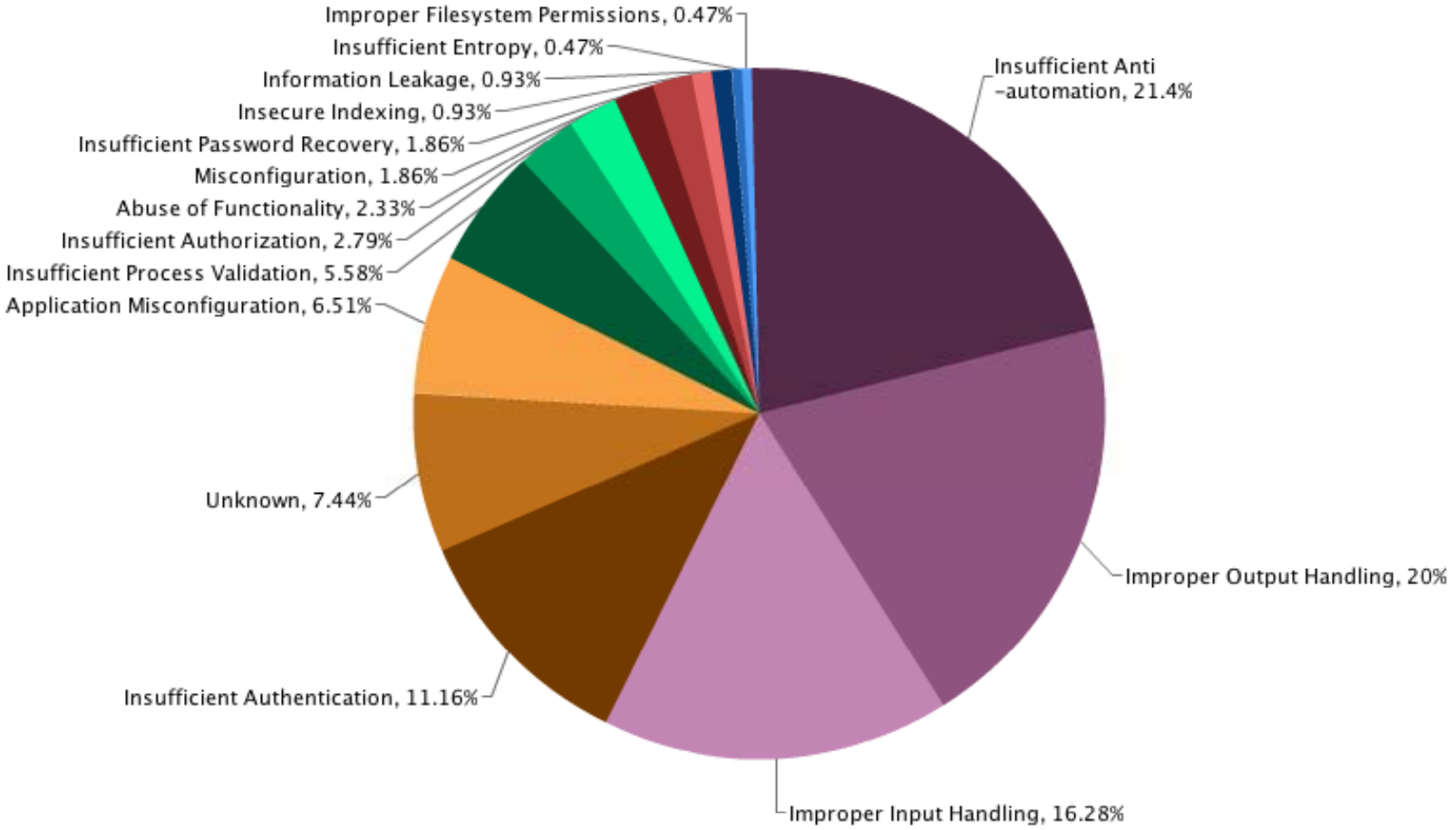



**Sourc: The Web Hacking Incident Database (WHID) Report for 2010**

# OWASP

- Etape 1: identification du risque

Vulnérabilité exploitées




Sourc: The Web Hacking Incident Database (WHID) Report for 2010

# OWASP

- Étape 2: Estimation de la **vraisemblance**

- Objectif:
  - Estimer la **probabilité** d'une attaque réussie

- Influencée par 2 types de facteurs:
  1) **Entités menaçantes**: impact de la nature de l'attaquant sur la vraisemblance d'une attaque réussie.
  2) **Vulnérabilités:** la vraisemblance d'une découverte de la vulnérabilité et son exploitation par les entités menaçantes considérées dans 1)

- Chaque facteur a un ensemble d'options notées sur 9

# OWASP

- Étape 2: Estimation de la **vraisemblance**
  - Facteurs en relation avec l'entité menaçante:

| **Niveau de compétence** | **Motivation** | **Opportunités d'exploitation nécessitant** | **Nature de la communauté menaçante** |
|---|---|---|---|
| (1) Aucune<br>(3) certaines compétences (4)utilisateurs avancés<br>(6) compétences réseaux et logiciels<br>(9) compétences de pénétration de sécurité | (1) Peu ou pas de récompenses<br>(4) récompense possible<br>(9) forte rentabilité | ( 0) accès complet ou ressources très coûteuses<br>(4) des ressources et droits d'accès spéciaux<br>(7) quelques ressources et droits d'accès<br>(9) aucun droit d'accès et aucune ressource | (2) Développeurs et administrateurs système<br>(4) utilisateurs de l'intranet<br>(5) partenaires<br>(6) utilisateurs authentifiés<br>(9) Utilisateurs Internet |

# OWASP

- Étape 2: Estimation de la **vraisemblance**
  - Facteurs en relation avec la vulnérabilité:

| **Facilité de découverte** | **Facilité d'exploitation** | **Disponibilité de l'information** | **Détection d'intrusion** |
|---|---|---|---|
| (1) pratiquement impossible<br>(3) difficile<br>(7) Facile ,<br>(9) outils automatiques disponibles | (1) Théorique<br>(3) Difficile<br>(5) facile<br>(9) des outils automatiques disponibles | (1) information inconnue<br>(4) cachée<br>(6) Évidente<br>(9) publique | (1) détection active dans l'application<br>(3) audit et révision<br>(8) audit sans révision<br>(9) absence d'audit |

# OWASP

- Étape 2: Estimation de l'impact

- Objectif:
  - estimer l'impact d'une attaque réussie lorsqu'effectuée par un groupe d'attaquant possibles.

- Influencée par 2 types de facteurs:
  - 1)Impact technique : estimer l'ampleur de l'impact sur le système si la vulnérabilité est exploitée
  - 2)Impact sur le domaine d'affaires: découle de l'impact technique, mais nécessite une compréhension approfondie des priorités de l'entreprise

- Chaque facteur a un ensemble d'options notées sur 9

# OWASP

- Étape 2: Estimation de l'impact
  - Impact technique:

| Perte de confidentialité | Perte d'intégrité | Perte de disponibilité | Perte de traçabilité |
|---|---|---|---|
| (2) peu de données non-sensibles divulguées<br>(6) peu de données critiques divulguées<br>(7) nombreuses données critiques divulguées<br>(9) toutes les données divulguées | (1) peu de données légèrement corrompues<br>(3) peu de données gravement corrompues<br>(5) nombreuses données légèrement corrompues<br>(7) nombreuses données gravement corrompues<br>(9) toutes les données complètement corrompues | (1) peu de services secondaires interrompus<br>(5) peu de services importants interrompus<br>(7) nombreux services de base interrompus<br>(9) tous les services complètement interrompus | (1) traçabilité complète<br>(7) traçabilité probable<br>(9) aucune traçabilité |

# OWASP

- Étape 2: Estimation de l'impact
  - Impact sur le domaine d'affaires:

| Préjudice financier | Atteinte à la réputation | Non-conformité | Atteinte à la vie privée |
|---|---|---|---|
| (1) moins important que le coût requis pour fixer la vulnérabilité<br>(3) effet minime sur les bénéfices annuels<br>(7) effet significatif sur les bénéfices annuels<br>(9) Faillite | (1) dommages minimes<br>(4) perte de grands comptes<br>(5) chute d'écart d'acquisition (goodwill)<br>(9) vaste dommages | (2) violation mineure<br>(5) violation flagrante<br>(7) violation de haut niveau | (3) un individu<br>(5) des centaines de personnes<br>(7) des milliers de personnes<br>(9) des millions de personnes |

# OWASP

- Étape 2: Evaluation de la gravité du risque

**Niveaux de vraisemblance et d'impact**

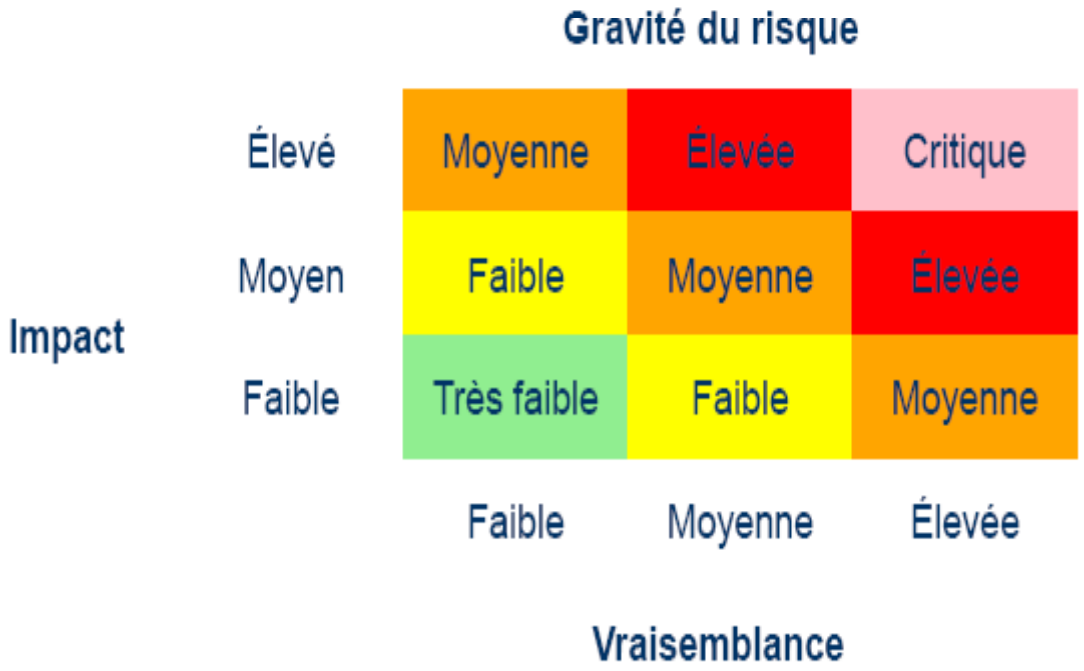
| | |
|---|---|
| 0 à <3 | Faible |
| 3 à <6 | Moyen |
| 6 à 9 | Élevé |

| Threat agent factors | | | | Vulnerability factors | | | |
|---|---|---|---|---|---|---|---|
| Skill level | Motive | Opportunity | Size | Ease of discovery | Ease of exploit | Awareness | Intrusion detection |
| 5 | 2 | 7 | 1 | 3 | 6 | 9 | 2 |
| Overall likelihood=4.375 (MEDIUM) | | | | | | | |

| Technical Impact | | | | Business Impact | | | |
|---|---|---|---|---|---|---|---|
| Loss of confidentiality | Loss of integrity | Loss of availability | Loss of accountability | Financial damage | Reputation damage | Non-compliance | Privacy violation |
| 9 | 7 | 5 | 8 | 1 | 2 | 1 | 5 |
| Overall technical impact=7.25 (HIGH) | | | | Overall business impact=2.25 (LOW) | | | |

# OWASP

- Étape 2: Evaluation de la gravité du risque




- Étape 5: Choix d'aspects à corriger

# Conclusions

- L’analyse de risque est une des plus importantes activités de la sécurité informatique.
- Elle permet de répertorier tous les risques auxquels les actifs critiques sont exposés et de les hiérarchiser.
- Cette analyse détermine ainsi quels risques devront être traitésavec priorité et quels risques seront acceptables sans aucune intervention.