Formation Sécurisation de Site Web

Ditesco
SMART TECH

Ditesco
SMART TECH

Présentation formateur

Consultant **Cybersecurity Program Manager à la BNP Paris Bas**

12 années d'expérience dont

- 4 ans en temps que **RSSI**
- 4 ans en consultant **GRC**
- 4 ans en expertise **Réseaux et Sécurité**

Sommaire

- Définition de site Web et Composant
- Quels sont les critères de sécurité d'un site Web
- Déploiement d'un site web dans un environnement de Production
- Parlons du Standard OWASP et de ses recommandations
  - OWASP
  - Top 10 OWASCP
- La Défense en profondeur
- Les outils d'évaluation de vulnérabilité
- Rédaction et analyse de rapport de vulnérabilité

Ditesco
SMART TECH

Sommaire

Qu’est qu’un site Web?

Ditesco
SMART TECH

Le site Web

- C’est est un ensemble de pages Web reliées entre elles et accessibles à partir d'une même adresse appelée URL.

Ditesco
SMART TECH

Caractéristiques

- Code
- Application
- Système d’exploitation
- Données

Ditesco
SMART TECH

Les critères de Sécurité

- **Confidentialité :** Seules les ressources autorisées ont accès à la données
- **Intégrité:** S'assurer que les données ne sont pas modifiées entre l'émetteur et le récepteur
- **Disponibilité :** Garantir l'accès à une application, un système, une donnée
- **Audit :** Toutes les informations doivent être journalisées
- **Traçabilité :** Toutes les manipulations doivent être tracées

Ditesco
SMART TECH

Les critères de Sécurité

- **Authentification :** L'authentification est une procédure, par laquelle un système informatique certifie l'identité d'une personne ou d'un ordinateur

Il existe 4 facteurs d'authentifications qui peuvent être utilisés dans le processus d'autorisation d'accès à des ressources bloquées et sécurisées

- **Ce que l'on connait (facteur mémoriel)** : une information que l'utilisateur a mémorisée et que lui seul connait (exemple : un mot de passe, un nom)
- **Ce que l'on possède (facteur matériel)** : une information que seul l'utilisateur possède et enregistrée dans un support (exemple : une clé USB).
- **Ce que l'on est (facteur corporel)** : une information qui caractérise l'utilisateur avec une empreinte qui lui est propre (exemple : voix, pupille, empreinte digitale)
- **Ce que l'on sait faire (facteur réactionnel) :** une information ou un geste que seul l'utilisateur peut produire (exemple : une signature)

Méthode 2FA et MFA

Ditesco
SMART TECH

Les critères de Sécurité

- **Autorisation :** L'autorisation est un processus qui détermine le niveau d'accès d'un utilisateur aux ressources du système telles que les données, les applications et les réseaux.

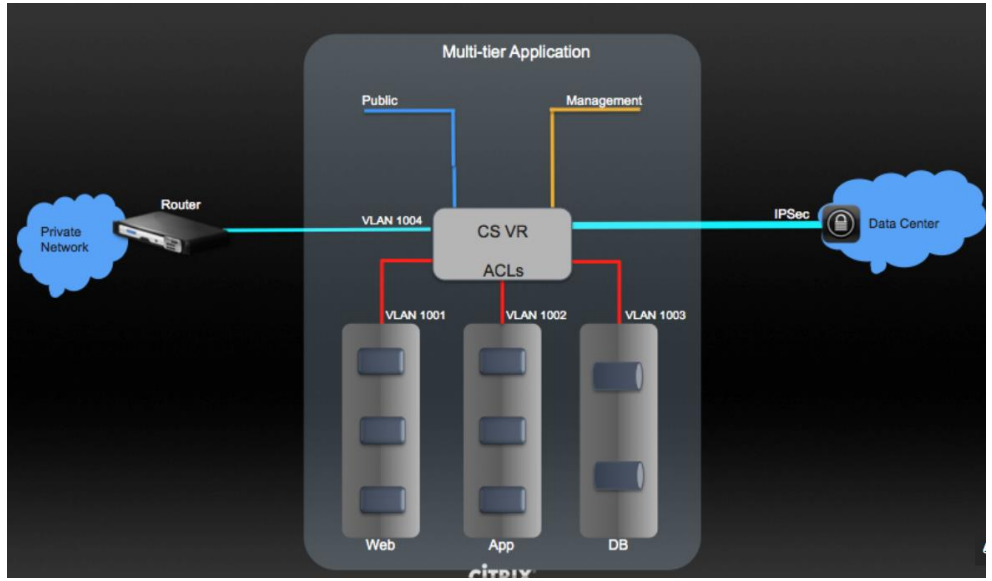
Contrôle d'accès sur les rôles (RBAC) : Il permet aux utilisateurs d'accéder à certaines ressources en fonction de leur rôle et de leurs privilèges au sein de l'organisation. Les utilisateurs se voient attribuer des rôles spécifiques au sein de l'organisation, et chaque rôle leur permet d'accéder aux ressources nécessaires à l'exercice de leur fonction.

- **Contrôle d'accès basé sur les attributs (ABAC)** : Accorde aux utilisateurs la permission d'accéder aux systèmes de l'organisation sur la base d'une série d'attributs spécifiques. L'ABAC utilise des attributs basés sur l'utilisateur, l'environnement et les ressources pour déterminer si l'utilisateur répond aux critères nécessaires pour accéder aux ressources de l'organisation.
- **Commande d'accès obligatoire (MAC)** : Impose un ensemble prédéfini d'étiquettes et de catégories de sécurité pour contrôler quels utilisateurs ou systèmes ont accès à des ressources spécifiques. Il limite l'accès en fonction de la sensibilité des données. L'organisation détermine le niveau de sensibilité des données et les personnes qui peuvent y accéder, au niveau de l'habilitation ou en deçà.
- **Commande d'accès discrétionnaire (DAC)** : le DAC attribue des privilèges basés sur l'utilisateur et son groupe d'accès. Plutôt que de laisser l'organisation déterminer l'accès, le propriétaire de la ressource peut accorder l'accès à d'autres utilisateurs en fonction des besoins.

Ditesco
SMART TECH

Production

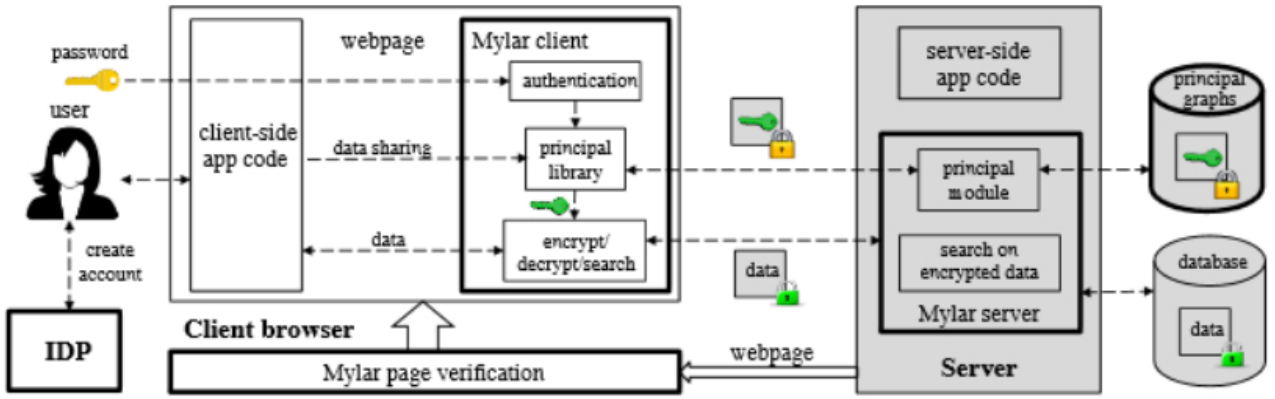
Déploiement Site Web



Ditesco
SMART TECH

Architecture de Déploiement de Site web

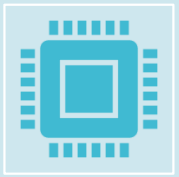
- L'architecture matérielle et logicielle du site web et de son infrastructure d'hébergement doit respecter le principe de défense en profondeur.
- Appliquer un découpage réseau
- Appliquer le filtrage par les équipements réseaux (pare feu web : WAF)
- Les composants applicatifs employés doivent être limités au strict nécessaire.
- L'accès aux mécanismes d'administration doit être restreint aux seuls postes d'administration autorisés
- Une matrice des flux précise doit être établie, tant en entrée qu'en sortie, et son respect doit être imposé par un filtrage réseau.



Ditesco
SMART TECH

Standard OWASP

https://owasp.org/



Open Web Application Security Project

Communauté en ligne pour la sécurité des sites Web

Top 10 Recommandations.

Ditesco
SMART TECH

#1
Faille de sécurité sur le contrôle des accès

Un utilisateur ne doit pas agir en dehors des droits d'accès définis ou autorisés

Risque: Divulgation non autorisée d'information

Attaque : Brute force, élévation de privilège

Solution : Bloquer par défaut les accès, Appliquer une politique de gestion d'accès, journaliser la gestion des accès, etc…

Ditesco
SMART TECH

#2 Cryptographie

Les données sensibles doivent être sécurisées en transit et au repos

Risque: Divulgation non autorisée d'information, indisponibilité, faille d'intégrité

Attaque : Brute force, plain Text attack, cipher attack

Solution : Classifier les données, Appliquer les protocoles sécurisés (TLS, Https, VPN,SHA…), certificats, Désactiver les caches,

Ditesco
SMART TECH

#3
Injection SQL

Les données fournies par l'utilisateur ne sont pas validées, filtrées ou nettoyées par l'application

Les requêtes dynamiques ou les appels non paramétrés sans échappement contextuel sont utilisés directement dans l'interpréteur

Risque: Divulgation non autorisée d'information, indisponibilité, altération

Attaque : Requête SQL injection

Solution :

Validation de nom de table sécurisée,

Redéfinir les design sur les nom d'entrées de Table et les requêtes SQL

Ditesco
SMART TECH

#4 Securisation du Design (risque)

Mettre en place une politique d'évaluation constante de la menace sur les composants de l'application

Risque: accès non autorisé, altération et indisponibilité

Attaque : Exploitation des vulnérabilités, de design

Solution : Mettre à jour les versions des agents, Assurer le cycle de vie des applications,

Ditesco
SMART TECH

#5
Faille de configuration

Mettre en place une politique d'évaluation constante de la menace sur les composants de l'application

Risque: accès non autorisé, altération et indisponibilité

Attaque : Exploitation des vulnérabilités, de design

Solution : Mettre à jour les versions des agents, Assurer le cycle de vie des applications,

Ditesco
SMART TECH

MAP SUR LE TOP 10 OWASP

Analyse Top 10 en 2017 vs Top 10 en 2021

Ditesco
SMART TECH

#6
Faille des composants non à jours et obsolètes

Les composants logiciels et matériels doivent être mise à jour et renouvelés en cas d'obsolescence et fin de vie

Risque: Divulgation non autorisée d'information, intégrité, disponibilité

Attaque : Exploitation des vulnérabilités,

Solution : Mettre à jour les composants logiciels , renouveler le cycle de vie des applications, gérer l'obsolescence.

Ditesco
SMART TECH

#7
Faille d'identification et d'Authentification

La confirmation de l'identité, de l'authentification et de la gestion des sessions de l'utilisateur est essentielle pour se protéger contre les attaques liées à l'authentification

Risque: Divulgation non autorisée d'information

Attaque : Brute force, réutilisation de mot de passe volées

Solution : Authentification multi-facteur, controller les erreurs de connexion, supprimer les accès admin par defaut, Appliquer une complexité sur les Mots de Passe

Ditesco
SMART TECH

#8
Faille Applicative et d'intégrité de données

Les défaillances d'intégrité des logiciels et des données sont liées au code et à l'infrastructure qui ne protègent pas contre les violations d'intégrité.

Risque: Divulgation non autorisée d'information, problème d'intégrité

Attaque : Tampering Attack (falsification)

Solution : Signature digitale pour vérifier les codes sources, revues de codes,

Ditesco
SMART TECH

#9
Faille sur la Sécurité des Logs et Supervision

La journalisation et la surveillance peuvent être difficiles à tester, impliquant souvent des entretiens ou la question de savoir si des attaques ont été détectées lors d'un test d'intrusion

Risque: Non Repudiation, Visibilité, Alerte et Incident

Attaque : Attaque sur les failles de sécurité (vulnérabilités)

Solution :Assurer que toutes les activités sur les login, le contrôle d'accès sont tracées et supervisées, Superviser et alerter toutes les activités suspecte, Mettre en place un plan de réponse d'incident et de restauration

Ditesco
SMART TECH

#10 Server-Side request Forgery

Les failles SSRF se produisent chaque fois qu'une application Web récupère une ressource distante sans valider l'URL fournie par l'utilisateur. Il permet à un attaquant de contraindre l'application à envoyer une requête contrefaite vers une destination inattendue, même lorsqu'elle est protégée par un pare-feu, un VPN ou un autre type de liste de contrôle d'accès réseau (ACL).

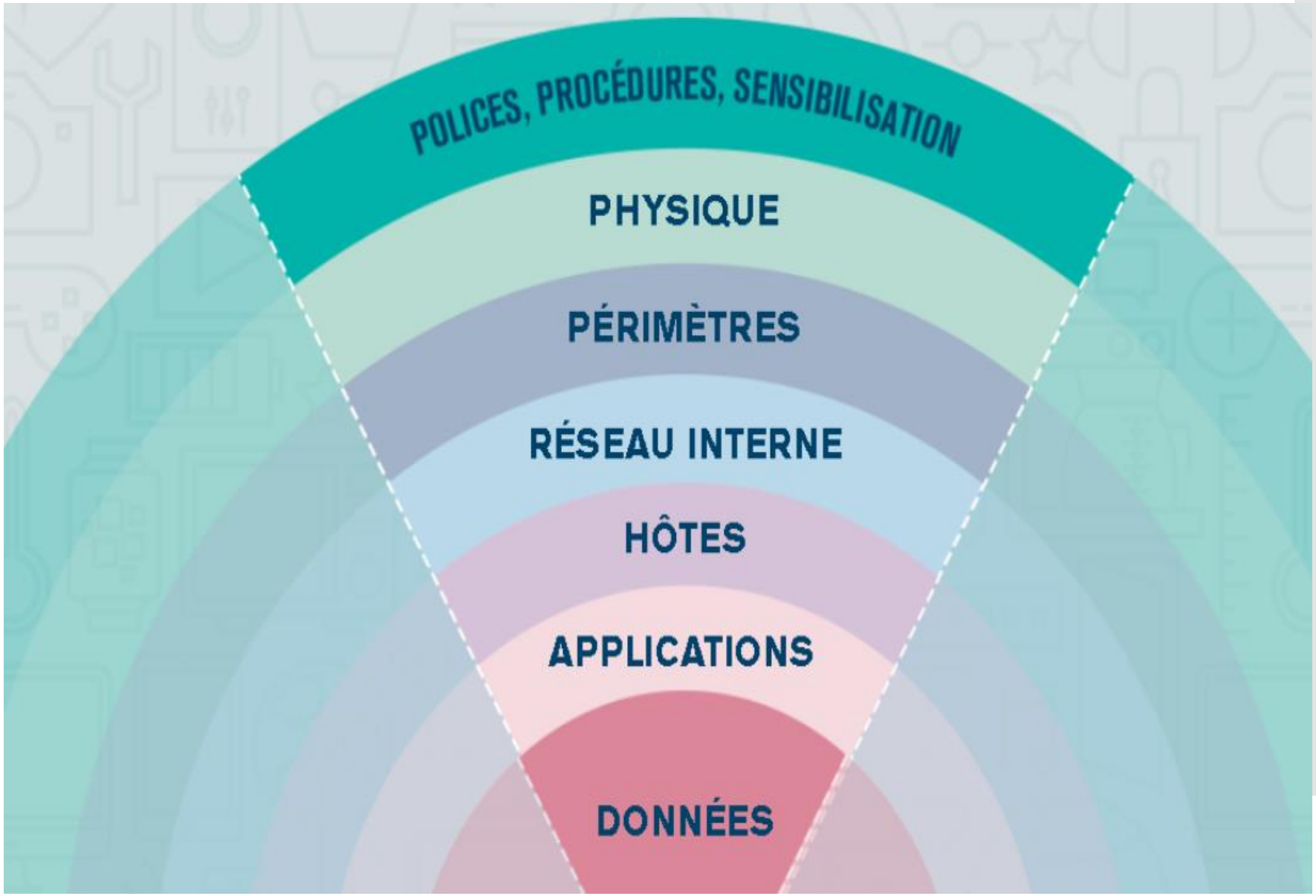
Risque: Divulgation non autorisée d'information, problème d'intégrité et de disponibilité

Attaque : Denis de Service (DDOS), Remote Code Execution

Solution : Implémenter la défense en profondeur, Mettre en place des Tunnels VPN pour les utilisateurs bien précis, Controller le Traffic Localhost

Ditesco
SMART TECH

Méthode de Sécurisation: La Défense en profondeur



Notions sur les outils de scan de vulnérabilité : Qualys, Tenable, Nexus, Bitsight, …

- Outils de détection de vulnérabilité applicative, système et réseau
- CVE : Common Vulnerability Explosure
- Rapport de scan de vulnérabilité