SÉCURITÉ

SÉCURISER UNE APP. WEB

AU PROGRAMME :

On va faire **un peu de théorie** :

- l'intérêt et les objectifs de la sécurité informatique
- la terminologie employée
- les bonnes pratiques à appliquer
- les métiers de la sécurité informatique
- les acteurs, sites et plateformes de référence
- les principes de cryptographie à connaître
- une petite intro au RGPD

POURQUOI PARLER SÉCURITÉ ?

Il y a plusieurs métiers spécialisés dans la sécurité informatique : pourquoi devrions-nous donc nous en soucier en tant que développeur ?

- **Tous les acteurs intervenants sur un projet doivent y être sensibilisés**. En tant que développeur, nous devons **faire en sorte de sécuriser au mieux notre code**.
- Certaines entreprises n'ont pas les moyens d'embaucher un expert en cybersécurité.
- Si vous envisagez de devenir Freelance, à moins de sous-traiter vous serez obligés de vous y confronter !

Et surtout ... vous devez avoir **des bases en sécurité pour votre Titre Pro DWWM** !

LA SÉCURITÉ & LE TP CDA

Comme on peut le voir dans cette capture du Référentiel Emploi Activités Compétences (REAC), vous devez **connaître et appliquer les recommandations de sécurité** sur l'ensemble des activités types.

Nous allons donc découvrir ensemble quelles sont ces recommandations, et comment les appliquer !

N° Fiche AT	Activités types	N° Fiche CP	Compétences professionnelles
1	Développer la partie front-end d'une application web ou web mobile en intégrant les recommandations de sécurité	1	Maquetter une application
		2	Réaliser une interface utilisateur web statique et adaptable
		3	Développer une interface utilisateur web dynamique
		4	Réaliser une interface utilisateur avec une solution de gestion de contenu ou e-commerce
2	Développer la partie back-end d'une application web ou web mobile en intégrant les recommandations de sécurité	5	Créer une base de données
		6	Développer les composants d'accès aux données
		7	Développer la partie back-end d'une application web ou web mobile
		8	Elaborer et mettre en œuvre des composants dans une application de gestion de contenu ou e-commerce

⚠️ Certains jurys de TP aiment bien poser des questions sur la sécurité !

INTÉRÊT, OBJECTIFS, MÉTIERS

DE LA SÉCURITÉ INFORMATIQUE

INTÉRÊT DE LA CYBERSÉCURITÉ

Dans notre société hyper-connectée, **de nombreux aspects de notre vie dépendent du bon fonctionnement de nos infrastructures informatiques**.

On passe par des applications web pour :

- déclarer nos revenus & payer nos impôts
- prendre rdv chez le médecin et faire des télé-consultations
- faire nos courses ou commander à manger
- stocker nos photos de famille
- communiquer avec nos proches
- etc.

On comprend bien que la sécurité de ces applications est très importante, personne ne souhaite voir ses données divulguées aux yeux de tous (et ce, même si “on a rien à cacher”).

Pire, les conséquences d’une attaque informatique peuvent parfois être bien plus graves qu’une fuite de données.

5 OBJECTIFS

La sécurité informatique vise en général **5 grands objectifs :**

1. **Intégrité** (garantir que les données n'aient pas été altérées)
2. **Confidentialité** (seules des personnes autorisées doivent pouvoir accéder à des données spécifiques)
3. **Authentification** (identifier avec certitude une personne)
4. **Disponibilité** (maintenir le bon fonctionnement du système d'information)
5. **Non-répudiation** (empêcher que quelqu'un puisse nier avoir effectué une transaction, garder des traces/preuves)

Pour chacun de ces objectifs nous verrons quel est notre rôle en tant que développeur d'applications.

On parle parfois de critères **DICP** ou **DICT** (Disponibilité, Intégrité, Confidentialité, Preuve ou Tracabilité), en omettant la partie authentification.

DROIT & RGPD

“On va parler de Droit & du RGPD ? Mais ce n’est pas un cours sur la sécurité ?”
Et oui, on va bien en parler !

Quand on parle de sécurité en informatique, **ce qu’on veut sécuriser en général, c’est des données**. Or, si ces données sont **à caractère personnel**, leur **collecte** et leur **traitement** nous impose de **respecter le RGPD** et la législation française !

On va donc parler un petit peu du RGPD et de la législation que l’on doit respecter quand on met en ligne un site web.

LES MÉTIERS DE LA CYBERSÉCURITÉ

Il existe de nombreux métiers dans le domaine de la cybersécurité. L'ANSSI a essayé d'en faire la liste.

Voici quelques métiers souvents rencontrés dans ce domaine (liste non-exhaustive) :

- **Cryptologue :** c'est un mathématicien spécialisé dans la cryptologie. Travail de recherche, c'est lui qui va concevoir et analyser les algorithmes et protocoles cryptographiques.
- **DSSI / RSSI (Directeur / Responsable de la Sécurité des Systèmes d'Information) :** le responsable de la sécurité du SI dans une entreprise.
- **Spécialiste en développement sécurisé :** un développeur avec une spécialisation en cybersécurité, qui va aider les équipes de développement à produire du code sécurisé.
- **Auditeur / PenTester :** il va réaliser des audits de sécurités, aussi appelés tests d'intrusion (penetration test en Anglais), afin d'identifier les vulnérabilités présentes.
- **DPO (Data Protection Officer) :** s'assure de la conformité au RGPD au sein d'une entreprise.
- **Consultant / Formateur en cybersécurité**
- etc.

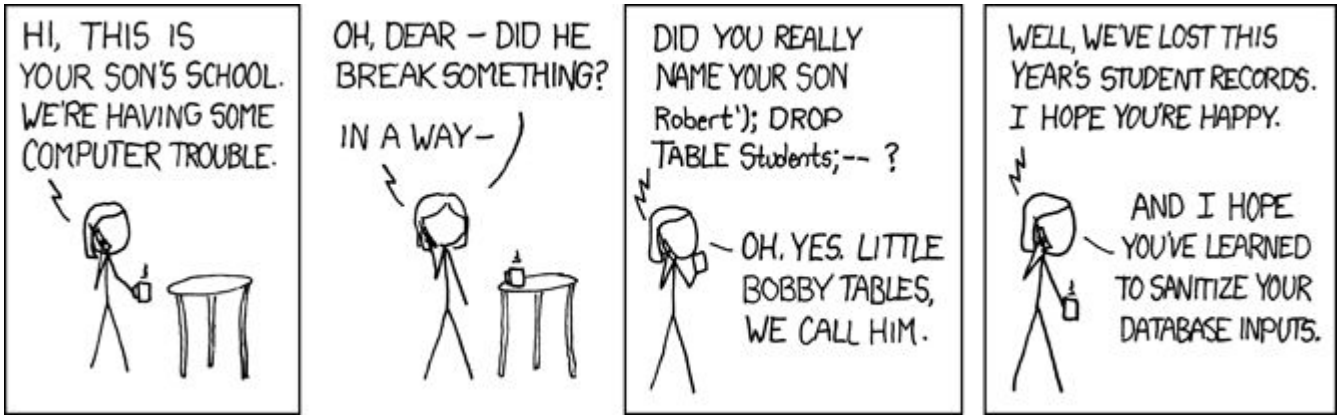
GRANDS PRINCIPES

À GARDER EN TÊTE QUAND ON PARLE DE CYBERSÉCURITÉ

MENACE #1 : L'UTILISATEUR

La plus grande menace est, et sera toujours, l'utilisateur.

Il peut être **mal-intentionné ou simplement distrait**, mais dans tous les cas : **on ne peut pas lui faire confiance !**



PRINCIPE DU PRIVILÈGE MINIMUM

Le **principe du privilège minimum** doit être appliqué : chaque service ou utilisateur doit avoir **uniquement accès à ce qui lui est strictement indispensable** pour remplir à bien ses missions.

DEFENSE IN DEPTH

Le principe de **“Defense in Depth”** (défense en profondeur) doit être appliqué : **la sécurité doit être organisée en plusieurs niveaux indépendants, en plusieurs couches**. Si un niveau est compromis, le niveau suivant devra bloquer l’attaque.

ÊTRE PARANO : C'EST BIEN

Nous devons être (un peu) **paranoïaques, suspicieux** : si quelque chose semble suspect, ou semble trop beau pour être vrai, c'est sûrement le cas (ce principe permet notamment de se protéger du social engineering).

SÉCURITÉ ABSOLUE ?

La sécurité absolue (parfaite, inviolable) **n'existe pas.**

Seule solution pour sécuriser un serveur et notre application à 100% ? Déconnecter le serveur du réseau, l'éteindre, l'enfermer dans un coffre-fort blindé, et noyer ce coffre sous 15 mètres de béton armé. Dans ce cas de figure, la plupart des pirates seront découragés. Le problème, c'est que les utilisateurs ne notre appli aussi !

On doit donc faire un **compromis** : notre mission va être d'essayer de **sécuriser au maximum notre application tout en s'assurant qu'elle reste fonctionnelle**, utilisable.

Il y aura toujours de nouvelles failles de sécurité, il faut donc **se préparer à l'échec des mesures de sécurité** que nous aurons mises en place : créez des **PRA/PCA** (Plan de Reprise/Continuité d'Activité), faites des **sauvegardes** !

LE PLUS FAIBLE DES COMPOSANTS

La sécurité d'un système est égale à la sécurité du plus faible de ses composants.
Inutile d'avoir une porte blindée si la porte de derrière ne ferme pas bien !

SECURE BY DESIGN

Comme son nom l'indique, le principe **secure by design** implique qu'une application a été **conçue pour être sécurisée**.

Plus exactement, ce principe s'oppose au fait de ne penser à la sécurité d'un projet qu'une fois celui-ci développé. Il faut au contraire **prendre en compte la sécurité dès le début du projet**.

Dès la phase de conception, on doit **prendre des décisions qui peuvent impacter la sécurité future de notre application**. Quelques exemples :

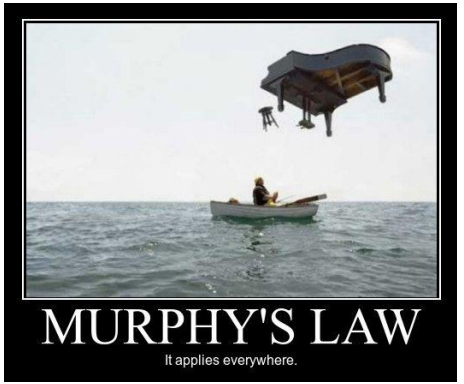
- Choisir de démarrer un nouveau projet en PHP 7.4 est une très mauvaise idée, cette version ne reçoit plus de mises à jour de sécurité depuis novembre 2022 !
- Lors de la réalisation de nos cas d'utilisation / user stories, il vaut mieux créer beaucoup de rôles pour gérer les permissions le plus finement possible (plutôt que de mettre tout le monde administrateur)

LOI DE MURPHY

Cette loi (satirique) bien connue dit que ***“tout ce qui est susceptible d’aller mal ira mal”,*** ou que ***“s'il y a plus d'une façon de faire quelque chose, et que l'une d'elles conduit à un désastre, alors il y aura quelqu'un pour le faire de cette façon”***.

En sécurité (informatique, mais pas que) **cette loi doit être érigée comme un grand principe**. Non, le pire n’est pas toujours certain, mais **par prudence, il faut concevoir notre application comme si cette loi était vraie**.

Notre application doit être à l’épreuve des erreurs ou des mauvaises manipulations les plus improbables des utilisateurs, que celles-ci soient involontaires ou au contraire préméditées, malveillantes.



LES ACTEURS

DU MONDE DE LA CYBERSÉCURITÉ

ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est un service gouvernemental Français.

Ce service, créé en 2009, est rattaché au Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) et sa mission première est d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

Mais l'ANSSI n'assiste pas que le Premier ministre : elle a un rôle d'**autorité nationale en matière de sécurité des systèmes d'information**. L'agence publie des recommandations, des livres-blancs, s'assure de la **sécurité des OIV** (Opérateurs d'Importance Vitale), gère le **CERT-FR** (voir ci-après).

💡 **à retenir :**
L'ANSSI met notamment à disposition plusieurs PDFs sur la sécurisation des applications web, que nous allons consulter.

CSIRT / CERT

Les **CSIRT** (Computer Security Incident Response Team) et **CERT** (Computer Emergency Response Team) sont des **équipes d'experts en sécurité informatique chargées de réagir en cas d'incident informatique**.

Le terme CERT est le plus utilisé, mais c'est une marque déposée qui appartient à l'université américaine Carnegie Mellon. Les CSIRT peuvent demander à utiliser cette marque.

En France, l'ANSSI opère un CSIRT qui s'appelle CERT-FR (anciennement CERTA). Son rôle est de prévenir les attaques en effectuant une **veille sur les nouvelles failles découvertes**, faire de la prévention auprès des entreprises, être un relais et centraliser la communication (avec le réseau mondial des CERT par exemple).

💡 **à retenir :**
Le CERT-FR publie notamment des **alertes de sécurité**, la liste est accessible sur son site https://www.cert.ssi.gouv.fr/.

CVE / MITRE

MITRE est une organisation à but non-lucratif américaine. Cette organisation publie le **dictionnaire CVE (Common Vulnerabilities and Exposures)**.

Une CVE est une vulnérabilité, une faille, qui peut être exploitée par des hackers et causer plus ou moins de dégâts sur un système d'information. La criticité potentielle d'une vulnérabilité est évaluée à l'aide du **CVSS (Common Vulnerability Scoring System)**.

L'identifiant CVE est une référence de la forme **CVE-YYYY-NNNN** (ou YYYY est l'année de publication et NNNN un identifiant). Pour chaque CVE, MITRE publie une description succincte de la vulnérabilité ainsi que des informations supplémentaires permettant d'en savoir plus ou de s'en prémunir.

Le dictionnaire des CVE est accessible ici : https://cve.mitre.org/.

CNIL

La **CNIL (Commission Nationale Informatique & Libertés)** est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

- *wikipédia*

💡 **à retenir :**
Son rôle est (entre autres) de **veiller au respect du RGPD et au respect de la loi Informatique et Libertés**, et de **prononcer des sanctions** (jusqu'à 20 millions d'€) à l' égard d'organismes qui ne respectent pas ces lois ou règlements.

⚠️ Avant 2018, on devait "déclarer" son site web à la CNIL, si celui-ci collectait des données personnelles. Ce n'est plus le cas !

⚠️ **En cas d'intrusion dans notre BDD** (et que certaines données personnelles ont pu être compromises)**, on doit obligatoirement notifier la CNIL et les personnes concernées.**

OWASP

OWASP (Open Web Application Security Project) est une organisation à but non lucratif spécialisée sur la sécurité des applications web.

OWASP publie des **recommandations pour la sécurisation des applications web** et propose aussi **différents outils** (pédagogiques ou techniques) liés à la sécurité sur le web.

Ses projets les plus connus :

- **Top10 :** la liste des dix risques de sécurité les plus critiques ou les plus fréquemment rencontrés sur le web.
- **ZAP (Zed Attack Proxy) :** outil de scan de failles de sécurité web.
- **Dependency Track :** une plateforme d'analyse de la SBOM (Software Bill Of Materials) - permet de gérer les versions des dépendances d'un projet.
- **WSTG (Web Security Testing Guide) :** un guide très complet à destination du pentester.
- **Cheat Sheet Series :** plein de mémos sur la sécurité des apps web.
- **ASVS (Application Security Verification Standard) :** un PDF très complet, pour aller plus loin que le Top10.

ET NOUS ?

C'EST BIEN BEAU TOUT ÇA, MAIS ON FAIT QUOI NOUS ?

NOTRE MISSION ?

La sécurité informatique s'appréhende sous **trois aspects complémentaires : la prévention, la détection et la réaction.**

En tant que Développeur, notre rôle est surtout de **prévenir les risques** ! Nous devons être capables :

- d'analyser, d'**identifier les risques**
- de **sensibiliser les utilisateurs et autres acteurs** d'un projet à ces risques
- de **définir comment s'en prémunir**, et de **mettre en place des solutions dans notre code (code défensif)**
- d'**évaluer si le risque est présent** ou non après la mise en place des mesures, ou en tout cas de **participer à cette évaluation**

DÉTECTION & RÉACTION

On ne s'occupe donc pas du tout de l'aspect détection et de l'aspect réaction ?

En tant que Développeur, ce n'est **normalement pas notre rôle**. Cela-dit, selon la taille de l'entreprise dans laquelle on travaille, **on peut aussi être amené à gérer ces aspects de la sécurité informatique**.

Quelques exemples de choses à potentiellement mettre en place :

- **Détection :**
  - mise en place de logs (enregistrement des connexions réussies & échouées)
  - alertes par mail en cas de comportement anormal détecté
- **Réaction :**
  - mise en place d'un PRA ou d'un PCA
  - création d'une politique de sauvegarde

💡 *Il faut impérativement tester les PRA, PCA et sauvegardes.*

SENSIBILISER LES ACTEURS

Les acteurs d'un projet (développeurs, administrateurs systèmes, chefs de projets, etc.) **devraient (en théorie) être déjà sensibilisés à la sécurité** informatique.

Ce ne sera par contre **probablement pas le cas pour les utilisateurs finaux** de l'application à développer. Vous aurez beau avoir développé une appli super sécurisée, si le mot de passe admin est "1234" ou est écrit sur un post-it tout ce travail sera inutile.

Il est donc important de **mettre en place des règles pour imposer des mots de passe forts**, et **sensibiliser les utilisateurs sur les risques** et bonnes pratiques à adopter.

📊 **Sondage :** parmi vous, qui utilise un gestionnaire de mot de passe ?

DÉMO : BRUTEFORCE DE MOT DE PASSE

Et si on se faisait une petite démo ?

On a dit à l'administrateur de notre appli *O'ShoppingList* qu'un mot de passe sécurisé faisait au moins 8 caractères. Il sait aussi qu'il ne faut pas le noter sur papier et donc pour s'en souvenir facilement, il utilise le mot de passe "rocknroll".

Combien de temps pensez-vous que ce mot de passe résiste ?

Logiciel utilisé : THC-Hydra.

MOTS DE PASSE : COMMENT FAIRE ?

Un mot de passe sécurisé est un mot de passe **généré aléatoirement, d'une longueur suffisante, et unique à un système** (il ne faut **surtout pas** utiliser le même mot de passe partout).

Un mot de passe ne doit pas contenir d'informations personnelles (nom d'un animal de compagnie, date de naissance/mariage, etc.), ne doit pas être uniquement composé de substitutions de caractères (exemple : `b0bm4rl3y`) ou de mots présents dans la langue anglaise/française, et il faut bien entendu éviter les mots de passe les plus souvent utilisés.

Retenir un mot de passe unique pour chaque site, généré aléatoirement, est impossible. Il faut donc **utiliser un gestionnaire de mot de passe qui stocke ces mots de passe de façon chiffrée**.

Il faut aussi, dès que c'est possible, **utiliser l'authentification à facteurs multiples** : code reçu par SMS, code TOTP (Time-based One-time Password), clé physique (type Yubikey), etc.

IDENTIFIER LES RISQUES

En tant que concepteur développeur, nous devons connaître les problèmes de sécurité les plus couramment rencontrés sur les applications web.

Quelques pistes :

- **le Top 10 OWASP**
- **Les leçons sur Hacksplaining**
- **les recommandations de l'ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information)
- **faire de la veille !** (alertes du CERT-FR, le dictionnaire des CVE, etc.)

SE PRÉMUNIR DES RISQUES

Une fois les risques identifiés, nous **devons faire en sorte que notre application soit protégée contre ces risques**.

Nous allons donc au cours des jours à venir passer en revue les failles de sécurité les plus courantes sur les applications web, et voir comment on peut s'en prémunir.

ÉVALUER LA PRÉSENCE DES RISQUES

Il n'y a qu'un seul moyen de s'assurer du bon fonctionnement des mesures de sécurité que nous avons mises en place : **les tests**.

Certains tests peuvent être automatisés, mais **dans le cas de la sécurité, les tests doivent souvent être menés par un expert**. On parle de **Pentest** (tests de pénétration, d'intrusion).

Pentester est un métier à part entière, et ce n'est pas le nôtre ! Il peut donc être judicieux de sous-traiter les tests de sécurité à un expert du domaine, surtout sur des applications "critiques". Ce n'est pas toujours possible, nous allons donc apprendre **comment tester la résistance de nos applications aux failles les plus communes.**

Je suis la loi

Attention ! Effectuer des tests d'intrusion sur un système informatique sans avoir reçu au préalable l'autorisation de le faire est **pénalement répréhensible**.