L'introduction à la sécurité

Table des matières

Objectifs

- Avoir une utilisation sécurisée des outils numériques ;
- Sécuriser ses applications ;
- Éviter les attaques les plus simples.

Contexte

Durée : 2h

Environnement de travail : Aucun

Pré-requis : Aucun

[cf. 8k5UogE5]

Le développement de l'informatique dans tous les secteurs de la société accroît le gain que peuvent tirer des malfaiteurs de l'intrusion dans les systèmes. Par ailleurs le développement de l'Internet des objets (ou IoT pour *Internet of Things*), qui sont souvent des objets peu sécurisés, augmente la facilité de mener des attaques.

Diverses formes de cybercriminalité se développent sur ces bases. En conséquence le risque qu'une de ses applications soit l'objet d'une tentative d'attaque est important.

L'objectif de ce module est de sensibiliser et de montrer des outils et méthodes qui permettent d'augmenter la sécurité des applications informatiques.

Toute application doit avoir une sécurité proportionnée à l'importance de ce qu'elle stocke. Ainsi, des applications de paiement ou traitant des données médicales nécessiteront plus d'attention qu'une application de jeu en ligne.

Mots de passe

[cf. ajXY7AH5]

Objectif

- Acquérir une bonne politique d'utilisation de mots de passe.

Mise en situation

Une date de naissance comme mot de passe bancaire ? ou un mot de passe unique pour l'ensemble de ses comptes en ligne ? Beaucoup de personnes sont conscientes que leur politique de gestion de mots de passe présente des failles, mais elles ne savent pas nécessairement comment y remédier.

Il existe quelques méthodes assez simples pour construire des mots de passe compliqués et pour vérifier que les mots de passe que l'on utilise ne sont pas trop faciles à deviner.

Par exemple la méthode *diceware* permet de créer des mots de passe à la fois longs et faciles à apprendre. La liste OWASP contient quand à elle les 10.000 mots de passe les plus fréquents, ceux qu'ils faut éviter d'utiliser donc.

Fondamental

Une application avec les plus hautes normes de sécurité reste fragile sans une bonne politique de gestion des mots de passe.

Identifier un mauvais mot de passe

Il existe plusieurs types de mauvais mots de passe et il est important de savoir les identifier pour les éviter :

- Les dates de naissance ou autre information facilement trouvable, par exemple : `DiDiEr121287`.
- Un mot de passe unique pour tous les services.
- Un mot de passe au schéma identifiable comme `FRAMATEAM123azerty` pour un compte sur le site framateam.org[1]. Un attaquant comprendra que votre mot de passe framapiaf.org[2] est FRAMAPIAF123azerty (ou quelque chose de ressemblant).
- Un mot de passe trop simple, par exemple : `mickey` (il s'agit de l'un des 10 000 mots de passe les plus courants).

Attention

Il existe des listes des mots de passe courants comme la liste maintenue par l'OWASP Foundation : 10k-worst-passwords.txt[3].

[1] https://framateam.org
[2] https://framapiaf.org
[3] https://github.com/OWASP/passfault/blob/master/wordlists/wordlists/10k-worst-passwords.txt

En haut de cette dernière sont présents des mots de passe tels que :

- `password`
- `football`
- `jennifer`

Ces listes sont très utilisées par les cybercriminels.

Les 20 premiers mots de passe de la liste OWASP *Exemple*

```
password
123456
12345678
1234
qwerty
12345
dragon
pussy
baseball
football
letmein
monkey
696969
abc123
mustang
michael
shadow
master
jennifer
111111
```

Trouver un bon mot de passe

Il existe plusieurs méthodes pour trouver un bon mot de passe :

- Méthode des premières lettres ;
- Méthode phonétique ;
- Diceware[1], ou méthode du lancer de dé ;
- Etc.

Méthode des premières lettres *Méthode*

Il s'agit de transformer une citation en mot de passe. Par exemple : *« un tiens vaut mieux que deux tu l'auras »* donnera `1tvMq2tL'a`. Il faut veiller à ne pas utiliser que des minuscules pour compliquer la tache d'un attaquant.

Ici, toutes les lettres dont la position est un multiple de 4 sont des majuscules.

Méthode phonétique *Méthode*

Il s'agit de retranscrire une phrase phonétiquement. Par exemple : *« j'ai acheté huit cd pour cent euros cet après-midi »* donnera `ght8CD%E7am`.

Les lettres en majuscule sont ici celle dont la prononciation représente le mot complet (*« E »* pour *« euro »* et *« CD »* qui est transparent).

[1] https://fr.wikipedia.org/wiki/Diceware

Diceware *Méthode*

Cette dernière méthode est très utilisée pour construire des phrases secrètes. Le mot de passe sera une phrase composée de plusieurs mots. Pour choisir chacun des mots il faut lancer 5 dés à 6 faces et mettre les résultats côte à côte. Puis il faut se munir d'une liste *diceware* qui propose 66666 mots. Dans cette liste, chaque résultat possible des 5 dés correspond à un mot.

Il en existe pour beaucoup de langues différentes, par exemple la liste de Matthieu Weber[1] référencée sur Wikipédia propose 66666 mots en français.

Si l'on souhaite un mot de passe de 6 mots et qu'on obtient les résultats suivants: 16665; 15653; 56322; 35616; 65224. En se référant à la liste ci-dessus, on obtiendra le mot de passe suivant : *« cajous bordes set juge verte »*.

Ce mot de passe n'est pas trop compliqué à retenir car il contient une liste de mots très simples mais il est pour autant très robuste.

Un bon mot de passe ne suffit pas..

Pour compléter un bon mot de passe il reste nécessaire d'avoir d'autres pratiques rigoureuses qui permettront de conserver la sécurité de votre politique de gestion de mot de passe.

Toujours changer le mot de passe initial *Conseil*

Il est absolument nécessaire de changer le mot de passe reçu initialement à la création d'un compte même si celui-ci semble aléatoire. D'une part, il arrive que certains éditeurs de matériel électronique fournisse un mot de passe identique pour chaque produit. D'autre part il est possible que le mail transmettant ce mot de passe ait été intercepté ou que ce mail soit récupéré lors d'une future fuite de données.

Une mot de passe doit rester confidentiel *Conseil*

Le propriétaire du compte doit être le seul à le posséder, même l'administrateur réseau ne doit pas le connaître (d'où la nécessité de modifier le mot de passe initial). Il est aussi préférable de ne pas enregistrer son mot de passe sur un support informatique non chiffré comme un fichier texte ou un mail brouillon.

Changement régulier de mots de passe *Conseil*

Changer régulièrement de mot de passe permet de conserver un niveau de sécurité optimal. Si un mot de passe a fuité sans qu'on le sache, un changement régulier de mot de passe pourrait vous protéger de toute attaque. À noter que cela n'est pas vrai pour des mots de passe qui ne sont pas sujet aux fuites, par exemple le mot de passe de son ordinateur personnel.

Sensibiliser ses collaborateurs *Conseil*

Il est nécessaire de veiller à ce que tous les acteurs d'un projet aient une bonne politique de gestion de mots de passe afin que le projet soit protégé. Il suffit qu'un seul des comptes soit compromis pour qu'un attaquant accède et nuise aux données de tous.

Conseil

Pour gérer ses mots de passe il est conseillé d'utiliser un gestionnaire de mot de passe, comme par exemple KeePass.

[1] http://weber.fi.eu.org/software/diceware/francais.pdf

Aller plus loin *Complément*

Note technique de l'ANSSI traitant des recommandations de sécurité relatives aux mots de passe :

ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf[1]

À retenir

- Il existe plusieurs méthodes pour trouver un mot de passe considéré comme bon. Par exemple la méthode des premières lettres, la méthode phonétique ou la méthode DiceWare.
- Un bon mot de passe ne peut être considéré comme sécurisé seulement s'il est complété de certaines bonnes pratiques : changer ses mots de passe, les conserver secret, sensibiliser ses collaborateurs.

[cf. VjS4h0e2]

[1] https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf

Exercice : Appliquer la notion

Question 1

Quel est le 42e mot de passe le plus utilisé selon la liste de l'OWASP Foundation ?

Indice :

Lien vers la liste : https://github.com/OWASP/passfault/blob/44e4062318f49c43c5c5a9edde8018206b720a68/wordlists/wordlists/10k-worst-passwords.txt[1]

Question 2

Dans la méthode Diceware, pour obtenir une phrase secrète (utilisable comme mot de passe) composée de 4 mots, combien faut-il lancer de dès ?

Question 3

Nous obtenons les résultats suivants suite à nos 20 lancers : 23161-26443-52241-65463. Quelle phrase secrète obtient-on ?

Indice :

Lien vers la liste des résultats et de leur mot correspondant : http://weber.fi.eu.org/software/diceware/francais.pdf

[1] https://github.com/OWASP/passfault/blob/master/wordlists/wordlists/10k-worst-passwords.txt

Gestionnaire de mots de passe

[cf. CSd2DTHs]

Objectif

- Connaître des outils pour faciliter la gestion de mots de passe.

Mise en situation

Les mots de passe que nous utilisons doivent être à la fois compliqués et différents pour chaque application. Or il n'est pas possible de tenir cette équation, notre cerveau ne peut pas se souvenir de dizaines de mots de passe compliqués et ne se ressemblant pas.

Les gestionnaires de mots de passe visent à répondre à ce problème. Ils permettent de réunir dans un unique fichier très sécurisé l'ensemble de nos mots de passe. Le mot de passe qui protège l'accès à ce fichier doit être lui particulièrement robuste. Mais comme on n'a plus qu'un seul mot de passe à mémoriser, ce n'est pas difficile.


Fondamental

Un mot de passe aléatoire suffisamment long et utilisant suffisamment de caractères (majuscules, minuscules, chiffres, etc.) est très robuste.

Génération aléatoire


Méthode

Pour générer un mot de passe aléatoire on peut choisir n'importe quel générateur aléatoire en lui fournissant des contraintes potentielles : présence de chiffre, de caractères spéciaux, etc. L'inconvénient de cette méthode est que le mot de passe devient impossible à retenir.

Génération aléatoire en ligne de commande


Exemple

On peut utiliser l'interface de OpenSSL, une bibliothèque de cryptographie de référence, qui génère des phrases aléatoires.

Par exemple pour générer des mots de passe de 42 caractères avec ASCII, on peut utiliser :

```
1 openssl rand -base64 32
```

On obtient la chaîne :

```
1 zVMDbYHTs9SjUJAz71ab2flFjfNc1pmrj0E3TnYxY6Q=
```


Fondamental

Lorsque la génération aléatoire est choisie, elle doit être couplée avec un gestionnaire de mots de passe qui permettra de les conserver sans avoir à les retenir par cœur tout en conservant un haut niveau de sécurité.

Le gestionnaire de mot de passe

Méthode

Pour éviter de retenir ses mots de passe, il existe des logiciels spécialisés, par exemple : KeePass.

Ce logiciel est conseillé par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Il permet de

- générer des mots de passe aléatoires
- et de stocker l'ensemble des mots de passe dans un fichier chiffré.

Pour y accéder, il suffira d'un seul mot de passe (dont on s'assurera de la robustesse).

Mot de passe maître

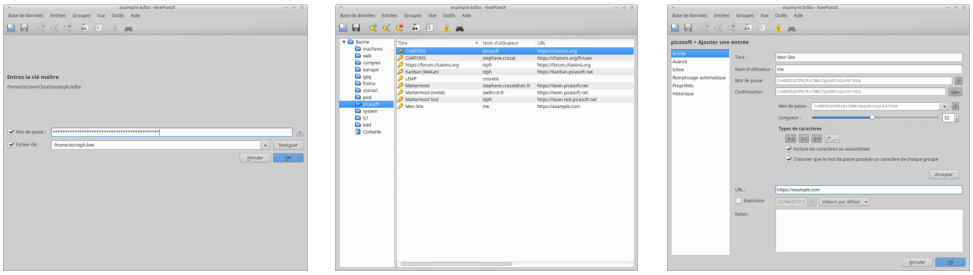
Attention

Le mot de passe maître d'un gestionnaire de mot de passe est la porte d'entrée sur tous les autres mots de passe.

Il doit donc être à la fois **très robuste** et **très secret** (mais comme il n'y a plus qu'un seul mot de passe à mémoriser, c'est facile).

KeePass

Exemple



KeePass

Aller plus loin

Méthode

- Installation de KeePass : https://keepass.info/download.html

Les plugins : des outils pour faciliter les usages

Complément

Les gestionnaires de mots de passe possèdent de nombreux *plugins* permettant de connecter son gestionnaire à divers autres logiciels type navigateur ou autre. Ces outils permettent de faciliter l'entrée des mots de passe en remplissant automatiquement les formulaires d'authentification dans un navigateur web par exemple.

https://keepass.info/plugins.html

À retenir

- Il existe des logiciels pour faciliter la gestion de ses mots de passe : génération aléatoire et stockage.
- Il existe des *plugins* pour faciliter l'intégration de ces mots de passe au quotidien.

[cf. u66dGYTA]

Exercice : Appliquer la notion

Installez le gestionnaire de mot de passe KeePass.

Gestionnaire de mots de passe *(cf. p.10)*

Question 1

Créez une base de données des mots de passe et sécurisez-la à l'aide d'un mot de passe fort.

Quelles contraintes doit respecter le mot de passe ?

Indice :

Utiliser le menu `File`, puis `New`.

Question 2

Ajoutez une entrée dans KeePass, par exemple pour votre adresse mail.

Indice :

KeePass propose des catégories par défaut : on pourra utiliser la catégorie `eMail`.

Indice :

On peut ajouter une entrée dans une catégorie avec le raccourci `Ctrl + I`.

Question 3

Comment copier le mot de passe dans votre presse-papier afin de vous connecter à votre adresse mail ?

Accès SSH aux serveurs

[cf. PkySdZL1]

Objectif

- Établir une connexion sécurisée à son serveur.

Mise en situation

Pour développer et maintenir une application, il est nécessaire de se connecter au serveur qui l'héberge. Pour cela on utilise essentiellement le protocole SSH, ainsi que le programme éponyme.

SSH repose sur le chiffrement de la communication avec le serveur, pour éviter que quelqu'un n'espionne ou ne falsifie la communication, ce qui équivaudrait à prendre le contrôle du serveur.

Le bon usage de SSH repose sur la gestion de clés qui doivent rester secrètes pour que les accès aux serveurs ne soient pas compromis.

Protocole SSH *Rappel*

Le protocole SSH permet une connexion sécurisée entre un serveur et un client SSH. Sur Linux, le client SSH est accessible nativement via la console de commandes (en utilisant la commande `ssh`). Sur Windows, il existe le client PuTTY[1].

Utiliser des mots de passe complexes

Il faut avoir un mot de passe très robuste car un attaquant pourrait nuire à l'application ou à ses données s'il réussissait à s'emparer du mot de passe.

Recours à des clés SSH *Conseil*

Il est possible d'utiliser des paires de clés SSH. Une paire est composée d'une clé publique qui sera déposée sur le serveur et d'une clé privée conservée sur l'ordinateur personnel de l'utilisateur. Pour se connecter, l'utilisateur n'aura plus à entrer son mot de passe car sa clé privée lui permettra de s'authentifier.

Cela simplifie grandement l'accès au serveur et évite de devoir taper un mot de passe compliqué à chaque connexion.

```
ssh-keygen  # Crée la paire de clés SSH
ssh-copy-id user@127.0.0.1  # Place la clé publique sur le serveur distant
[Entrer mot de passe]
ssh user@127.0.0.1
[Pas de saisie de mot de passe]
```

[1] https://www.putty.org/

Danger de l'utilisation des clés

Attention

Les clés SSH présentent un côté pratique et évitent d'avoir à retenir un mot de passe compliqué. Dans le cas où une machine personnelle est compromise, l'attaquant pourra récupérer la clé privée et l'utiliser pour accéder au serveur. Ainsi, il faudra veiller à la sécurité des ordinateurs personnels également.

Il est possible d'ajouter une phrase secrète à votre clé SSH qui empêchera un attaquant de l'utiliser. Cela ajoutera un mot de passe à retenir mais dans le cas où la clé publique est présente sur 50 serveurs, cela permet de retenir un seul mot de passe plutôt que 50.

Accès exclusif par clé aux serveurs

Méthode

Il est en général conseillé de privilégier l'accès par clé à l'accès par mot de passe en SSH. Si tous les utilisateurs autorisés ont un accès par clé, il est conseillé de désactiver, au niveau du serveur SSH, tout accès par mot de passe, ce qui supprime un risque.

À retenir

- Le mot de passe pour accéder à un serveur mérite une grande attention.
- Le recours à des clés SSH peut simplifier l'accès.
- Les clés SSH présentent tout de même des dangers dont il faut être conscient.

Dangers liés à un serveur compromis

Complément

Un utilisateur pourra considérer (par exemple en phase de développement) que son application ou ses données de test ne sont pas sensibles.

Néanmoins un attaquant pourrait prendre le contrôle du serveur et lancer des attaques sur des entreprises et des gouvernements. Dans ce cas de figure, la justice se tournera en premier lieu vers le propriétaire du serveur.

De nombreux robots essayent de se connecter aux serveurs SSH en testant divers noms d'utilisateurs et mots de passe, il est donc commun et pas du tout exceptionnel qu'un serveur soit compromis.

Il est donc conseillé de toujours protéger les accès à ses serveurs, même s'ils ne sont pas utilisés pour des projets sensibles (et même, en fait, s'il ne sont pas utilisés du tout).

[cf. G6HpHLB8]

Exercice : Appliquer la notion

Question 1

Je reçois des identifiants par mail qui permettront de se connecter à un serveur VPS. Que faire immédiatement ?

Question 2

Un collaborateur m'informe que son ordinateur personnel a été corrompu. Que faire ?

Indice :

L'attaquant pourrait utiliser ce qui se trouve sur cet ordinateur pour attaquer autre chose.

Quelques conseils de l'ANSSI

[cf. COeRfna1]

Objectifs

- Connaître l'ANSSI et son rôle ;
- Prendre connaissance de certains de ses conseils.

Mise en situation

Selon la chaîne de télévision américaine CNBC[1], qui s'appuie sur un rapport de l'entreprise de télécommunication Verizon : en 2019, 43 % des attaques informatiques sont ciblées sur des petites entreprises.

Par ailleurs, la société spécialisée en sécurité Norton[2] alerte sur l'importance et le coût des fuites de données. En moyenne, une fuite met 196 jours à être découverte et coûte 8 millions de dollars à une entreprise américaine.

En France l'ANSSI a pour objectif d'aider à lutter contre la cybercriminalité. Son activité consiste ainsi notamment à émettre des guides. Les suivre permet de mieux protéger ses infrastructures.

Qu'est-ce que l'ANSSI ?

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service français créé en 2009. Cette agence a pour rôle de protéger les intérêts numériques de l'État Français et des entreprises publiques. Ces dernières années, de nombreux grands groupes français ont demandé de l'aide à l'ANSSI lorsqu'elles subissaient des attaques d'envergures.

L'ANSSI a des relations avec la BSI (équivalent allemand) et l'ENISA (Agence européenne pour la cybersécurité).

Un rôle de sensibilisation *Fondamental*

Pour assurer la sécurité numérique de l'État français et de ses intérêts, l'ANSSI produit de nombreux documents visant à donner des conseils aux développeurs, aux administrateurs, aux utilisateurs et aux dirigeants.

5 réflexes à avoir à la réception d'un mail *Conseil*

- N'ayez pas une confiance aveugle dans le nom de l'expéditeur : son compte a pu être piraté ou son identité a pu être usurpée.
- Méfiez-vous des pièces jointes : elles peuvent contenir un virus.
- Ne répondez jamais à une demande d'informations confidentielles.

[1] https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html
[2] https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html

- Passez votre souris au-dessus des liens pour les prévisualiser, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français dans le texte ou de la langue pratiquée par votre interlocuteur.
- Paramétrez correctement votre logiciel de messagerie (mettre à jour, etc.).

Tout le monde ne doit pas avoir les droits administrateur *Conseil*

Chaque personne doit avoir son propre compte avec les droits dont il a besoin. Si un des comptes est corrompu, cela permettra de limiter les dégâts causés par l'attaque. Il faut également bien supprimer les accès lorsqu'une personne quitte l'entreprise pour que ce compte dormant ne soit pas utilisé pour une future attaque.

Sécuriser son accès Wi-Fi *Conseil*

Un accès Wi-Fi mal configuré est facile à attaquer car il est possible de récupérer le mot de passe.

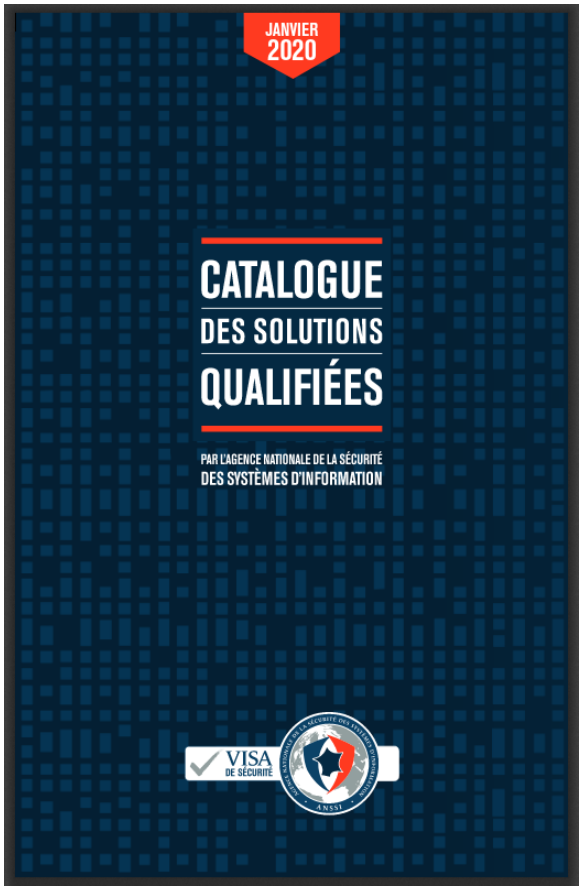
Dans sa propre entreprise, il est donc nécessaire de déployer une configuration sécurisée.

Dans un lieu public, il faut être conscient que les données sont à la merci d'un attaquant à proximité. Donc il est conseillé de ne pas accéder à des données sensibles via un accès Wi-Fi public.

Les Visas de sécurité *Complément*

L'ANSSI émet des Visas de sécurité pour des produits comme sécurisés. Il existe deux types de Visas : la qualification et la certification.

Seules les solutions certifiées ont le droit d'être utilisées par des Opérateurs d'Importance Vitale (OIV) : santé, énergie, transport, etc. Lorsqu'on cherche une solution sécurisée, cette liste est alors très pratique.



Lien vers les produits certifiés CSPN : https://www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/

Lien vers les produits qualifiés : https://www.ssi.gouv.fr/administration/visa-de-securite/visas-de-securite-le-catalogue/

Pour aller plus loin *Complément*

Le site de l'ANSSI[1] contient de très nombreux conseils et des guides dédiés à différents corps de métier.

À retenir

- L'ANSSI est une agence gouvernementale chargée de protéger la souveraineté et les intérêts numériques de la France.
- L'ANSSI émet de nombreux conseils à destination de tous les publics.
- L'ANSSI certifie et qualifie des produits qui assurent un haut niveau de sécurité.

[1] https://www.ssi.gouv.fr/

Exercice : Appliquer la notion

Question 1

Donner le lien vers la liste des produits certifiés CSPN.

Question 2

Quel produit est certifié pour servir de messagerie sécurisée ?

Question 3

Que recommande l'ANSSI en cas d'incident dont est victime une PME ?

Indice :

Regarder sur le site de l'ANSSI : https://www.ssi.gouv.fr/

Indice :

Rubrique "En cas d'incident" : https://www.ssi.gouv.fr/en-cas-dincident/

Security by Design

[cf. JZehuTKZ]

Objectifs

- Connaître l'OWASP ;
- Connaître certains principes du « Security by design ».

Mise en situation

Le travail du développeur consiste à réaliser une application qui répond à un problème posé. Mais il est également nécessaire de sécuriser cette application afin que celle-ci ne soit pas détournée par des malfaiteurs, ou encore afin qu'elle ne permettent pas de compromettre d'autres systèmes auxquels elle est connectée.

On attend ainsi d'un développeur que ses réalisations soient *secure by design*, c'est à dire sécurisés grâce à une bonne conception. Il s'agit donc de penser la sécurité dès la conception et le codage plutôt que de la reléguer à une phase marginale ou avale du projet.

OWASP Foundation (Open Web Application Security Project) *Définition*

L'OWASP Foundation est une organisation à but non lucratif qui travaille à améliorer la sécurité des logiciels et des applications. Cette organisation développe des outils, édicte des principes de développement et met en lien une grande communauté de développeurs et d'experts en sécurité.

Piliers du « Security by design » *Fondamental*

La sécurité de l'information repose sur trois piliers :

- **Confidentialité** : seuls les utilisateurs autorisés accèdent aux données.
- **Intégrité** : les données ne peuvent pas être altérées ou modifiées par des utilisateurs non autorisés.
- **Disponibilité** : les données et les services sont disponibles lorsque les utilisateurs en ont besoin.

Principes du « Security by design » *Complément*

L'OWASP a produit un wiki à destination des développeurs contenant des principes permettant développer des applications sécurisées.

https://wiki.owasp.org/index.php/Security_by_Design_Principles

Le moins de privilèges *Exemple*

Chaque application ou utilisateur doit avoir uniquement les droits dont il a besoin. Dans le cas où l'application est attaquée, les dégâts liés à l'incident seront limités.

Éviter la sécurité par l'obscurité ? *Exemple*

Une page ou une fonctionnalité n'est pas sécurisée car elle n'est visible. Par exemple, si un site ne contient pas de lien vers la page administration, cela ne l'empêchera pas d'être attaquée. Il existe des méthodes pour trouver ce type de fonctionnalités cachées.

Établir des configurations par défaut sécurisées ? *Exemple*

Par défaut, une expérience doit être sécurisée mais il est possible de laisser la liberté à l'utilisateur de désactiver certaines contraintes *a posteriori* en l'avertissant des risques encourus.

À retenir

- L'OWASP Foundation est une organisation pouvant guider un développeur souhaitant adopter des méthodes de développement assurant un maximum de sécurité.
- Le *Security by design* possède plusieurs principes concrets permettant de sécuriser ses applications, comme par exemple : minimiser les droits des utilisateurs ou éviter de cacher plutôt que de sécuriser.

Exercice : Appliquer la notion

Question

Que signifie le principe *fail securely* et pourquoi est-il important ?

Indice :

https://wiki.owasp.org/index.php/Security_by_Design_Principles#Fail_securely

Les CVE : tenir à jour ses logiciels

[cf. jLmLTS6m]

Objectifs

- Découvrir les CVE ;
- Comprendre l'importance des mises à jour logicielles.

Mise en situation

Quelques soient les efforts produits, toute application présente des vulnérabilités, et un jour ou l'autre, celles-ci émergent. L'enjeu est alors d'être au courant de ces failles devenues publiques pour appliquer au plus vite des correctifs.

Chaque jour des vulnérabilités logicielles, appelées CVE, sont découvertes et publiées sur Internet. Savoir trouver et lire des CVE est important pour maintenir les outils que l'on utilise à jour.

Qu'est-ce qu'une CVE ? ***Définition***

Common Vulnerabilities and Exposures (CVE) est un catalogue, maintenu par l'organisme MITRE, de toutes les vulnérabilités logicielles publiées. Par abus de langage, on appelle« une CVE » toute publication de vulnérabilités. Chaque CVE possède un identifiant de la forme `CVE-AAAA-NNNN` (AAAA est l'année de publication et NNNN un numéro d'identifiant).

Lien vers le catalogue : cve.mitre.org[1]

Comment déchiffrer une CVE ? ***Méthode***

Les publications sont très techniques et ne sont pas abordables par des personnes ne maîtrisant parfaitement ni la sécurité ni le logiciel concerné. Il existe des sites (dont CVE Details[2]) qui décortiquent les CVE en donnant par exemple l'impact de la vulnérabilité selon différents critères (confidentialité, intégrité, disponibilité, prise de contrôle de la machine).

Comment savoir si mon logiciel a des vulnérabilités graves publiées ? ***Méthode***

1. Il faut entrer le nom de la technologie dans la barre de recherche du catalogue des CVE.
2. Puis, pour comprendre chaque CVE, il est possible d'obtenir plus de détails en cherchant le CVE via son identifiant dans des sites comme CVE Details : https://www.cvedetails.com/.

[1] https://cve.mitre.org/index.html
[2] https://www.cvedetails.com/

CVE publiées pour la collection d'outils « Bootstrap » *Exemple*

On peut prendre un CVE de l'outil de style web Bootstrap[1] :

- En 2019, il y a eu 4 CVE, toutes de type XSS (*cross site scripting*).
- La CVE-2019-8331 stipule : *« In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute. »*

Mettre à jour ses logiciels *Fondamental*

Les CVE étant publiques, il est très fréquent que des cybercriminels les utilisent pour attaquer des cibles n'ayant pas mis à jour leur logiciel. Les éditeurs produisent des mises à jour de sécurité très fréquentes pour corriger au plus les vulnérabilités connues.

Ne pas installer des logiciels peu ou pas maintenus *Conseil*

Il est préférable d'utiliser des logiciels avec une équipe de développeurs réactifs qui se chargeront de produire régulièrement des mises à jour de sécurité. Des logiciels peu ou pas maintenus seront très sensibles à des attaques car les vulnérabilités seront rarement corrigées.

Des outils pour vous aider *Complément*

Lorsque des projets deviennent vastes, il devient compliqué d'analyse toutes les lignes à la main. Certains outils effectuent une analyse automatique de recherche de vulnérabilités dans le code.

- SonarQube[2], qui analyse la qualité du code et les vulnérabilités pour une vingtaine de langages.
- PHPCs[3], qui analyse les vulnérabilités du code PHP et de certains frameworks connus.
- FlawFinder[4], pour les langages C et C++.
- DeepDive[5], pour les langages Java et ses dérivés.
- Bandit[6], pour le langage Python.

Attention : ces outils ont leur limite et ne remplacent pas la vigilance des développeurs.

Une liste complète est disponible sur le site de l'OWASP[7].

À retenir

- Des vulnérabilités logicielles sont rendues publiques chaque jour, ce sont les CVE.
- Il est important de faire les mises à jour de sécurité dès qu'elles sont disponibles.

[cf. uR4q1rRq]

[1] https://www.cvedetails.com/product/51406/Getbootstrap-Bootstrap.html?vendor_id=19522
[2] https://www.sonarqube.org/
[3] https://github.com/FloeDesignTechnologies/phpcs-security-audit
[4] https://dwheeler.com/flawfinder/
[5] https://discotek.ca/deepdive.xhtml
[6] https://github.com/PyCQA/bandit
[7] https://owasp.org/www-community/Source_Code_Analysis_Tools

Exercice : Appliquer la notion

Question 1

Quelle est l'identifiant de la dernière CVE publiée en 2019 en lien avec PHP ? Quel système est concerné ?

Indice :

https://cve.mitre.org/cve/search_cve_list.html

Question 2

A quel logiciel est lié CVE-2019-10164 ? Quel est l'impact sur la confidentialité ?

Indice :

CVE Details[1] permet de comprendre rapidement une CVE.

[1] https://www.cvedetails.com/

Casser les mots de passe

[cf. dLEdgrxR]

Objectif

- Connaître les méthodes les plus simples pour casser un mot de passe.

Mise en situation

Savoir comment casser les mots de passe est un bon moyen de comprendre pourquoi certains mots de passe sont plus faibles que d'autres.

Savoir comment casser un mot de passe est donc un bon moyen de se protéger !

Nous présentons ici les attaques par force brute, qui consistent à essayer toutes les combinaisons possibles, et les attaques par dictionnaire qui consistent à vérifier si un mot de passe n'utilise pas des mots communs.

Attaque par dictionnaire

Cette attaque consiste à essayer chaque mot de passe contenu dans une liste. Il existe beaucoup de listes des mots de passe les plus communs comme de l'OWASP[1]. L'efficacité de l'attaque repose sur le caractère commun du mot de passe et non pas sur sa simplicité.

Attaque par force brute

Cette attaque consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver la bonne. Elle peut s'avérer très longue mais peut être optimisée si l'attaquant connaît la longueur du mot de passe ou l'absence de caractères spéciaux.

John the Ripper ***Méthode***

John the Ripper est l'outil le plus commun pour le craquage de mots de passe. Il permet à la fois des attaques par force brute et par dictionnaire. Il possède également un mode simple qui tente toutes les combinaisons dérivées du nom d'utilisateur. Par exemple, pour l'utilisateur « *toto* » : toto123, ToTo, T0to, etc.

Le logiciel est disponible sur Linux, Windows et OS X.

https://www.openwall.com/john[2]

Où et comment sont stockés les mots de passe? ***Complément***

Les mots de passe ne sont pas stockés tels quel, pour éviter qu'une compromission du système ne révèle tous les mots de passe.

[1] https://github.com/OWASP/passfault/blob/master/wordlists/wordlists/10k-worst-passwords.txt
[2] https://www.openwall.com/john/

L'astuce est d'utiliser une **fonction à sens unique**, ou fonction de hachage, qui a les propriétés suivantes :

- Chaque entrée de la fonction donne une sortie différente.
- Il est impossible de deviner l'entrée à partir de la sortie.

Les sorties de la fonction s'appellent des **hashs**, ou **condensats** : ce sont eux qui sont stockés.

Pour vérifier que l'utilisateur possède le bon mot de passe, il suffit de calculer son hash et le comparer au hash stocké. Comme la fonction est à sens unique, il est impossible de retrouver le mot de passe initial, mais possible de vérifier que l'utilisateur en est en possession.

À retenir

- Il existe des méthodes très simples pour craquer un mot de passe.
- *John the Ripper* est l'outil le plus classique pour réaliser ce type d'attaque.

[cf. sa7tTxpg]

Exercice : Appliquer la notion

Question 1

John The Ripper est un logiciel libre. Trouver un lien vers son code source

Indice :

https://fr.wikipedia.org/wiki/John_the_Ripper

Question 2

Je possède un Windows 64 bits et j'aimerais utiliser la version gratuite de John The Ripper.

Indice :

La version gratuite est par élimination la version non « Pro »

Indice :

https://www.openwall.com/john/

Question 3

Vous inspectez le contenu d'une base de données de mots de passe de votre serveur Linux dont vous êtes administrateur et que vous avez avec des amis.

Voici une des lignes de cette base :

```
charles:AZl.zWwxIh15Q
```

Enregistrez cette ligne dans un fichiez nommé `password.txt`.

Vous allez pouvoir maintenant utiliser John the Ripper. Lancez :

```
john password.txt
```

Après avoir attendu la fin de l'exécution qui prend plusieurs minutes.

Lancez :

```
john --show password.txt
```

Qu'obtenez-vous ? Qu'allez-vous dire à Charles ?

Attaquer une application Web

[cf. y8w8zcJ0]

Objectif

- Découvrir les attaques les plus simples à faire sur des applications Web.

Mise en situation

Une application web intègre des formulaires ou des appels de pages qui permettent d'interagir dynamiquement avec le serveur. Il est fondamental que ces appels soient sécurisés afin que des utilisations malveillantes ne puissent pas être menées.

L'injection de code par exemple permet de faire exécuter un programme à la place d'envoyer des données. Ce programme pourra capturer des informations sensibles et ouvrir des accès à d'autres programmes, compromettant finalement l'ensemble de l'application.

Injection SQL — *Attention*

Cette attaque très classique exploite les champs texte des formulaires. Très souvent les données envoyées via les formulaires sont utilisées pour construire des requêtes envoyées à la base de données. Ici, l'attaquant entre directement du code SQL afin d'accéder aux données qu'il souhaite.

Nettoyer les champs texte — *Conseil*

Un champ texte doit être systématiquement nettoyé afin d'éviter ce type d'attaque. Il est par exemple possible de retirer tous les apostrophes ou les point-virgules. De nombreux langages Web possèdent nativement des fonctions dédiées.

Fuzzing — *Attention*

Il ne faut pas cacher une page ou une fonctionnalité en pensant que celle-ci sera protégée des attaquants. Le *fuzzing* consiste à essayer toute une liste de mots pour trouver des URL ou des fonctionnalités cachées. Ce concept s'applique également pour trouver les noms d'utilisateur ou les mots de passe.

Le *fuzzing* est une sorte d'attaque par dictionnaire adaptée aux applications Web.

Wfuzz — *Méthode*

Wfuzz[1] est un outil très populaire et multi-plateforme car développé en Python. Pour l'installer, il faut lancer la commande :

```
1 pip install wfuzz
```

[1] https://wfuzz.readthedocs.io/en/latest/

Plusieurs listes de mots[1] sont également maintenus par les développeurs pour différents usages : injections, mots de passe, URL cachées, etc.

Prévenir le fuzzing *Conseil*

Pour prévenir ce type d'attaques, il faut d'une part changer l'architecture de son application Web car cacher des pages ne les protègent pas. Il faut également mettre en place de l'authentification lorsque cela est nécessaire. Enfin, il faut adopter une bonne politique de mots de passe car le fuzzing peut très bien toucher les mots de passe.

À retenir

- Il faut faire attention au traitement des champs texte pour ne pas subir d'injection SQL.
- Il ne faut pas adopter une sécurité par l'obscurité car le fuzzing est une méthode très efficace dans ces cas-là.

[cf. RfMJTjs1]

[1] https://github.com/xmendez/wfuzz/tree/master/wordlist

Exercice : Appliquer la notion

Je souhaite attaquer un site web possédant des pages du types : *index.php*, *a_propos.php*, *photos.php*, etc.

Exercice

Quelle méthode faut-il utiliser pour trouver des pages/fichiers potentiellement sensibles ?

- ○ Fuzzing
- ○ Injection SQL
- ○ XSS

Exercice

Selon la documentation de wfuzz[1], quelle commande faut-il lancer pour tester tous les noms de fichier les plus communs sur le site *example.com* ?

- ○ wfuzz -w wordlist/general/common.txt http://example.com/FUZZ
- ○ wfuzz -w wordlist/general/common.txt http://example.com/FUZZ.php
- ○ wfuzz -z list,nonvalid-httpwatch --basic FUZZ:FUZZ https://example.com/login.php

Exercice

Je suis un développeur PHP et je souhaite éviter les injections SQL sous MySQL.

Selon la page Wikipédia sur les injections SQL[2], quelle fonction devrait être utilisée pour prévenir de telles attaques?

- ○ mysqli_thread_safe
- ○ mysqli_real_escape_string
- ○ mysqli_data_seek

[1] https://wfuzz.readthedocs.io/en/latest/
[2] https://fr.wikipedia.org/wiki/Injection_SQL

Essentiel

[cf. mnZP3nok]

Prendre en compte la sécurité est devenu indispensable dans le domaine du développement informatique.

Une application web ou mobile, même modeste et portée par une petite entreprise, sera probablement l'objet de tentatives d'attaques. Les malfaiteurs visent la capture de données ou le contrôle de machines, ce qui leur permet de renforcer leur capacité de nuisance, y compris pour attaquer ensuite des structures plus importantes.

La sécurité est un domaine de l'informatique à part entière, qui n'a été qu'esquissé ici.

- On retiendra l'importance de la gestion des mots de passe, par exemple avec un outil comme KeePass ; et des clés de chiffrement, notamment SSH.
- On retiendra encore la nécessité de se maintenir informer des vulnérabilités publiques, les CVE ; et de suivre les conseils des agences spécialisées, comme l'ANSSI en France.
- On retiendra enfin l'intérêt qu'il y a à connaître les techniques d'attaque des cybercriminels, pour s'en prémunir ; par exemple *John the Ripper* est un outil qui sert à casser les mots de passe, tandis *Wfuzz* est un outil de fuzzing, qui sert notamment à découvrir des pages web cachées.

Exercice final

Exercice 1 : Quiz - Culture

Exercice

Qu'est-ce que l'ENISA ?

- ☐ L'équivalent de l'ANSSI pour l'Union Européenne
- ☐ L'équivalent de la BSI pour l'Union Européenne
- ☐ L'organisme qui catalogue les CVE
- ☐ Un organisme dont l'objectif est de développer des logiciels sécurisés

Exercice

Quel est le format de l'identifiant des CVE ?

- ○ CVE-AAAA-NNNN (AAAA est l'année de publication et NNNN un numéro d'identifiant)
- ○ CVE-NNNN-AAAA (AAAA est l'année de publication et NNNN un numéro d'identifiant)
- ○ CVE-JJMMAA-NNNN (JJMMAA est la date de la publication et NNNN un numéro d'identifiant)
- ○ CVE-NNNN-JJMMAA (JJMMAA est la date de la publication et NNNN un numéro d'identifiant)
- ○ CVE-MMAA-NNNN (MMAA est le mois/année de la publication et NNNN un numéro d'identifiant)

Exercice

Pourquoi le fait que toute une équipe de développeurs utilise le même compte administrateur est dangereux ?

- ☐ La confidentialité du mot de passe est mise en danger
- ☐ Le principe « Le moins de privilèges » n'est pas respecté
- ☐ En cas d'incident, il va être plus compliqué de retrouver la source
- ☐ Il est impossible d'utiliser plusieurs clés SSH

Exercice

Quels sont les trois piliers du *Security by design* ?

- ○ Confidentialité, Distribution, Disponibilité
- ○ Confidentialité, Résilience, Distribution
- ○ Résilience, Intégrité, Disponibilité
- ○ Confidentialité, Intégrité, Disponibilité

Exercice 6 : Quiz - Méthode

Exercice

Je souhaite craquer le mot de passe d'un fichier PDF. Quel logiciel peut être utilisé ?

- ☐ wfuzz
- ☐ John The Ripper
- ☐ KeePass
- ☐ Clair

Exercice

Quel mot de passe est le meilleur ?

- ○ y>AIK*3lU&G%b83Lu:hU1)3Cc (mot de passe initial)
- ○ 23091978P4ul
- ○ ItCNHKJDYckG
- ○ EokQvZJcbhzeAbXxACon

Exercice

Un collègue très peu habitué à l'informatique et utilisant très peu de services en ligne demande des conseils pour avoir un bon mot de passe. Que faudrait-il lui répondre ?

- ☐ Méthode des premières lettres
- ☐ Méthode phonétique
- ☐ Génération aléatoire
- ☐ Utilisation de KeePass

Exercice

Une amie développeuse aimerait avoir des astuces pour gérer et sécuriser ses mots de passe. Que faudrait-il lui répondre ?

- ☐ Méthode des premières lettres
- ☐ Méthode phonétique
- ☐ Génération aléatoire
- ☐ Utilisation de KeePass

Exercice

Lors du développement d'une application Web, il est nécessaire de créer un espace dédié aux administrateur.

Quelles pratiques devra-t-on observer parmi les suivants ?

- ☐ Générer le mot de passe initial aléatoirement.
- ☐ Générer le mot de passe initial différent pour chacun.
- ☐ Demander expressément à chaque administrateur de changer son mot de passe au plus vite.

- [ ] Joindre une documentation pour aider à choisir des mots de passe sécurisés.
- [ ] Vérifier automatiquement la robustesse du mot de passe lors de la modification de celui-ci.

Exercice

Quel plugin KeePass permet d'intégrer la fonctionnalité GPG ?

- [ ] KeePasser
- [ ] KeePT
- [ ] KeePassCommander

Exercice 13 : Quiz - Code

Exercice

Quel commande sert à générer une paire de clés SSH ?

- ○ ssh-keygen
- ○ ssh-copy-id
- ○ ssh-pairgen
- ○ ssh-init

Exercice

Quel commande permet d'installer l'utilitaire wfuzz ?

- ○ apt install wfuzz
- ○ install wfuzz
- ○ pip install wfuzz
- ○ python install wfuzz