Le monde de la cybersécurité

1. Les acteurs de la cybersécurité
2. Les cibles et impacts d’une attaque

Jeremy, Quentin, Benjamin, AnthonyR
GROUPE 1

Quel est le profil de ces cybercriminels qui menacent nos entreprises ?

Les 5 profils

Le "Kiddie"

Le jeune débutant qui copie/colle ou télécharge et exécute un script sans se soucier des dommages collatéraux.

Le Cracker

Celui-ci a juste pour but d’avoir du plaisir à pirater pour en démontrer les failles.

Alias Kevin Mitnick

Le hacker éthique

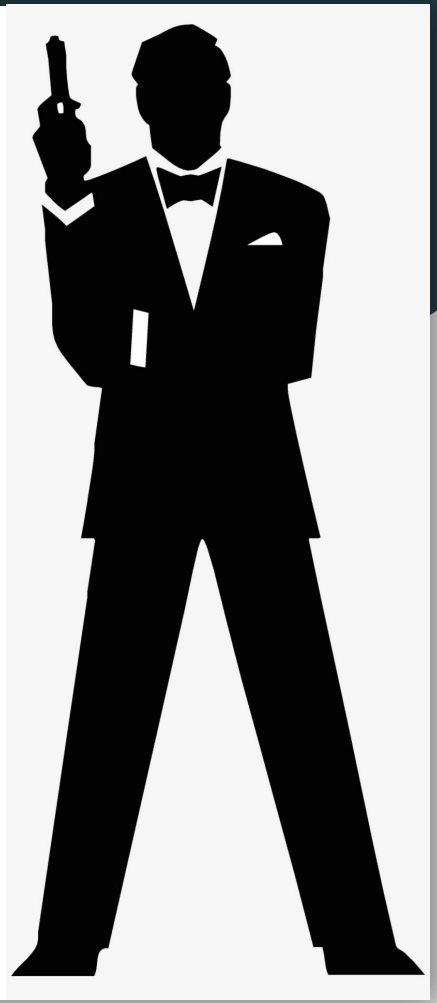
Il met à profit son expérience et apporte des solutions techniques aux entreprises sur les failles trouvées.

Les mercenaires

Ceux-ci ont des compétences techniques variées et les utilisent pour des organisations mafieuses en échange d'argent.

Le cyber espion

Il est le James Bond des temps modernes, il met son savoir-faire et son expérience dans le vol de données et de l’ingénierie sociale.



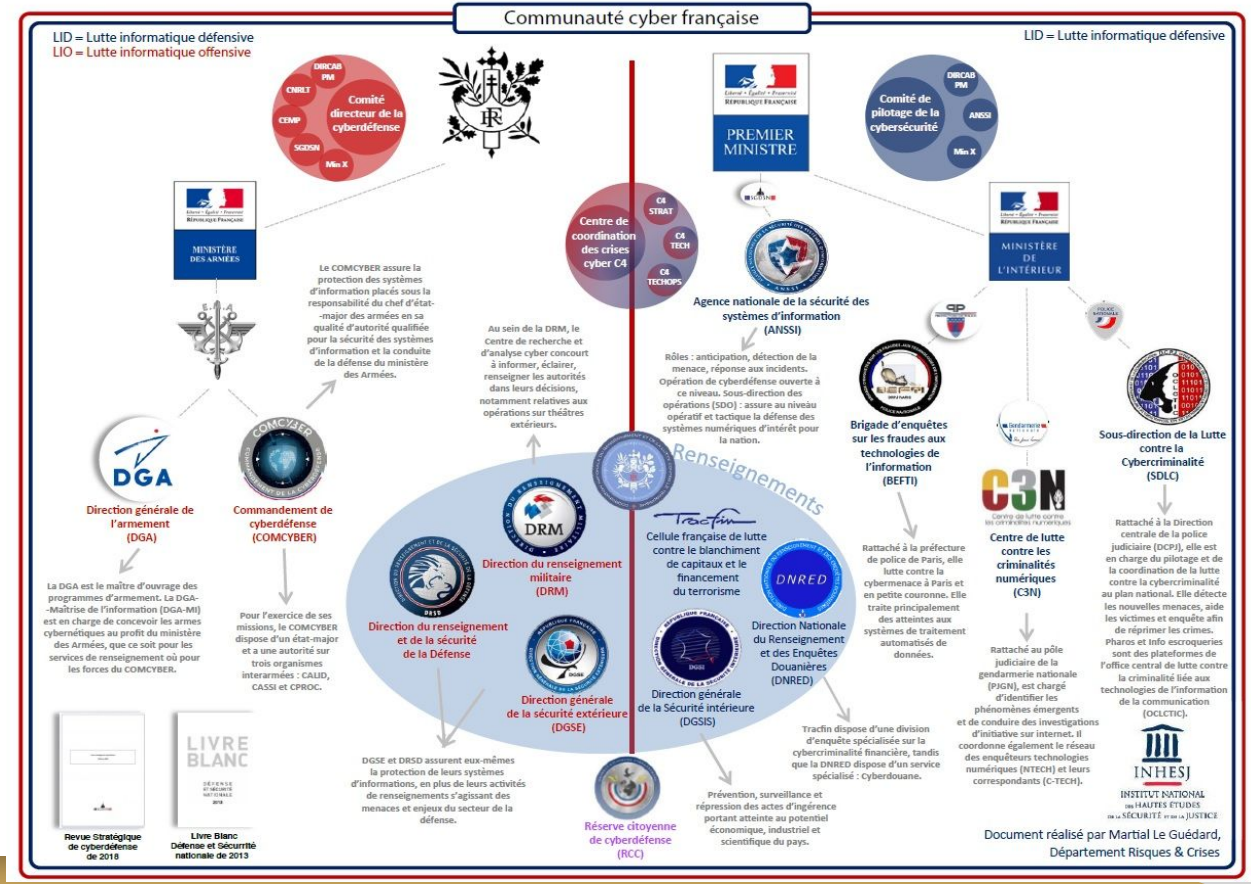
Quelles sont les motivations des acteurs de la cybercriminalité ?

Les motivations des Cybercriminel peuvent être pour l'argent, l'appât du gain motive une grosse partie des attaquants.

Ceux-ci peuvent être aussi d'un point de vue politique, pour savoir comment prendre l'avantage sur la concurrence adverse.

L'égo, la sensation d'avoir du pouvoir et de se sentir supérieur aux yeux du monde pour profiter des personnes faibles dans leurs connaissances informatiques.

Les acteurs français de la cybersécurité



Les acteurs français de la cybersécurité (dispensables)

- Le rôle de l'**ANSSI** (Agence nationale de la sécurité des systèmes d'information) est l'anticipation, la détection de la menace et la réponse aux incidents. A ce niveau, il s'agit d'Opération de cyberdéfense. L'ANSSI pilote aussi l'équipe **CERT** FR (**Computer Emergency Response Team**). Il est chargé d'assister les organismes de l'administration à mettre en place les moyens de protection nécessaires et à répondre aux incidents ou aux attaques informatiques dont ils sont victimes.

- **Sous-direction de la Lutte contre la Cybercriminalité** (SDLC) est rattaché à la Direction centrale de la **police judiciaire** (DCPJ). Elle est en charge du pilotage et de la coordination de la lutte contre la cybercriminalité au plan national. Elle détecte les nouvelles menaces, aide les victimes et enquête afin de réprimer les crimes

- Rattachée à la préfecture de police de Paris, la **Brigade d'enquêtes sur les fraudes aux technologies de l'information** (BEFTI) lutte contre la cybermenace à Paris et en petite couronne. Elle traite principalement des atteintes aux systèmes de traitement automatisés de données.

Les acteurs français de la cybersécurité (dispensables)

- La **DGA**, la **Direction Générale de l'Armée**, est le maître d'ouvrage des programmes d'armement. La **DGA-Maîtrise de l'information** (**DGA-MI**) est, quant à elle, en charge de concevoir les armes cybernétiques au profit du ministère des Armées, que ce soit pour les services de renseignement où pour les forces du **COMCYBER**, le **Commandement de la Cyberdéfense**.

- Le **COMCYBER**, **Commandement de la Cyberdéfense**, assure la protection des systèmes d'information placés sous la responsabilité du chef d'état-major des armées en sa qualité d'autorité qualifiée pour la sécurité des systèmes d'information et la conduite de la défense du ministère des Armées.

Tous ces acteurs peuvent être consultés **ICIIIII**

Les acteurs français de la cybersécurité

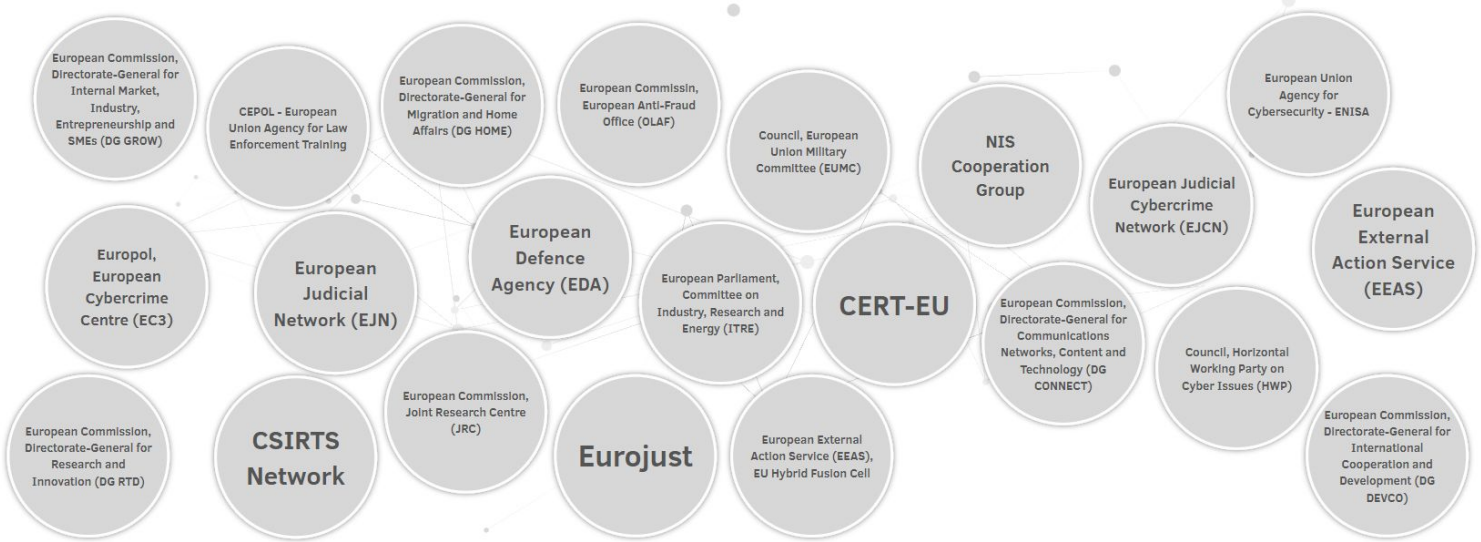
- La **Commission nationale de l'informatique et des libertés** (**CNIL**) de France est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle est surtout connue pour faire appliquer le RGPD.

  Elle est l'équivalent de l'**APD** en Belgique.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

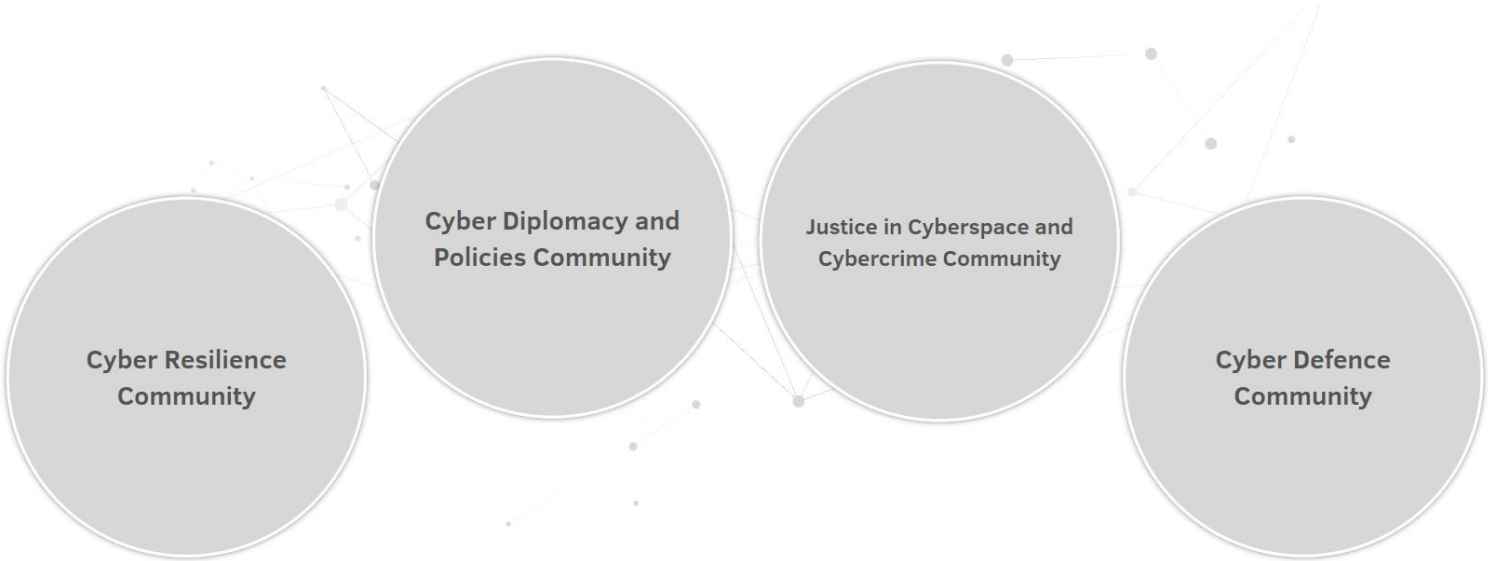
Les acteurs européens de la cybersécurité

- **22 acteurs** constituent les communautés en lien avec la cybersécurité sur le territoire européen !



Les acteurs européens de la cybersécurité

- Le site de l'**ENISA (European Union Agency for Cybersecurity)** permet de les classer par fonctions, communautés, acteurs,... VISITEZ-LE !
- Voici les environnements dans lesquels l'UE agit en cybersécurité



Les acteurs privilégiés dans l’entreprise

- Afin de gagner du temps lors de cette présentation, je vous renvoie à la veille : “*Travailler dans la Cybersécurité*” pour les différents métiers possibles dans le secteur.

A part ces différents métiers, nous avons les rôles importants suivants dans une entreprise :

- **DPO** (**Délégué à la Protection des Données**) : est chargé de **mettre en œuvre la conformité au RGPD** au sein de l’organisme qui l’a désigné s’agissant de l’ensemble des traitements mis en œuvre par cet organisme. Et de mener, entre autre, une analyse d’impact sur la protection des données personnelles, le **DPIA** (**Data Protection Impact Assessment**)

- **RSSI** : le **Responsable de la Sécurité des Systèmes d’Information** définit et **développe la politique de sécurité des systèmes d'information** (**PSSI**) de son entreprise. Il est garant de sa mise en œuvre et en assure le suivi. Il protège l’entreprise des risques potentiels liés aux cyberattaques. Il assure aussi des projets comme les politiques de sécurité interne au niveau des employés (changement de mot de passe tous les 6 mois etc…) par exemple. Le **RSSI** doit également informer le personnel sur les questions et les normes de sécurité par la mise en œuvre d'outils (chartes numériques, guidelines de sécurité) ou d'activités de communication, etc.

Les acteurs de la cybersécurité (bonus)

- Réponse aux questions de l'examen blanc TOSA :

1. A quoi correspond l'acronyme CERT ? Computer Emergency Response Team
2. Quelle est l'organisme de référence en matière de protection des données ? La CNIL

Les différents types d’attaques

DDOS et Dos (Attaque par déni de service)

Surcharge les ressources d’un système, afin qu’il ne puisse répondre et fonctionner correctement, depuis des machines infectées par un logiciel malveillant.

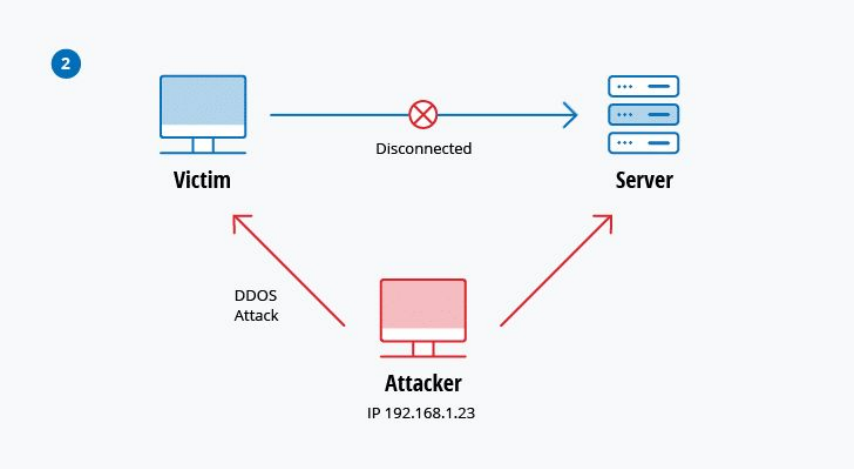
Empêche les systèmes de fonctionner, car plantage dû aux demandes de connexion trop nombreuses.

Peut servir de base à d’autres attaques informatiques.

Homme du milieu (MitM) et écoute illicite

Un pirate s'installe entre un serveur et un client, pour récupérer et écouter tout ce qui passe, après avoir analysé le réseau, et effectuer une attaque Ddos au préalable.

Une machine innocente ne peut plus accéder au serveur, et donc travailler, son adresse ip étant utilisée par le pirate qui se fait passer pour elle.



Phishing et Spear Phishing

Phishing (ou Hameçonnage) Envoie des e-mails de sources fiables et sûres (ou l'usage de faux sites web), pour récupérer des données personnelles ou pour inciter à faire quelque chose aux utilisateurs.

Le Spear Phishing (ou Harponnage) est ciblé, recherches très précises sur la cible, en volant une adresse e-mail prise auprès de proches de la personne.

Drive by Download

l’injection d’un logiciel, ou d’un script via le code d’un site web qui n’est pas sécurisé

Lorsque que l’on arrive sur ce site, le navigateur télécharge automatiquement le logiciel ou script malveillant

Attaque par Injection SQL

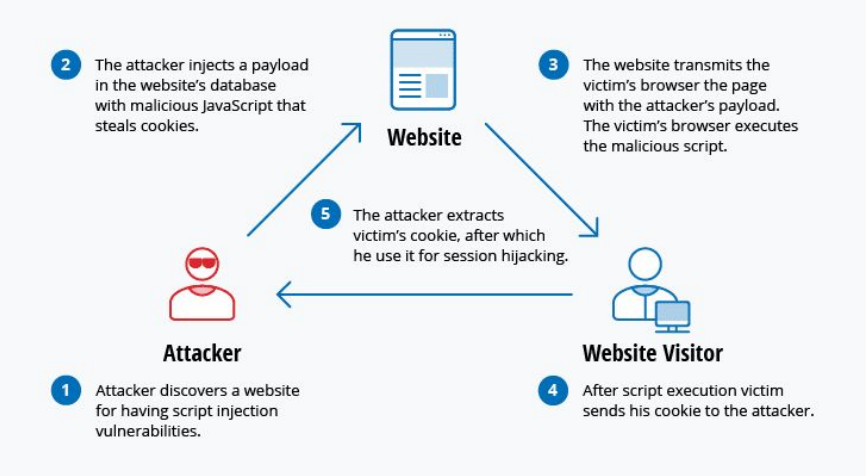
Introduire des données non sécurisées (on dit “données non sanétisées”) , dans une base de donnée, permettant des manipulations de données

Attaque par mot de passe

Récupérer le mot de passe d’un utilisateur, en cherchant sur son bureau, sa connexion, la connexion au réseau, la manipulation sociale, en accédant à une base de donnée, ou en le devinant.

Attaque XSS (Cross-site-scripting)

Injection de scripts malveillants dans des sites web non sécurisés, via des applications web ou des ressources, pouvant aller jusqu'à voler les cookies d’un utilisateur, contrôler son ordinateur, prendre des captures d’ écrans, les frappes clavier, ou collecter des informations réseau, ou des données



Attaque d’anniversaire

Attaque contre les algorithmes chargés de vérifier l’intégrité des données, logiciels, messages, signatures numériques.

Attaque par logiciels malveillants

- **Macro-virus** – Se lance lors de l'exécution d'une macro sur office, ou logiciel les prenant en charge
- **Infecteurs de fichiers** – s'attachent à des codes exécutables, comme les fichiers .exe le virus se lance dés que l'on clique sur le .exe
- **Infecteurs de système ou de secteur d'amorçage** – se lance au démarrage de l'OS ou de l'ordinateur
- **Virus divers** – se cachent dans divers chiffrement et de déchiffrement. il infecte ensuite une zone de code et prend le contrôle de certaines fonctions du système pour se dissimuler. ils masquent les modifications des fichiers
- **Chevaux de Troie** – se cachent dans un programme utile et qui ont généralement une fonction malveillante. ne se répliquent pas, et établit une porte dérobée qui peut être exploitée par des attaquants.
- **Vers** – programmes autonomes qui se propagent sur les réseaux et les ordinateurs, généralement via pièces jointes aux e-mails : l'ouverture de la pièce jointe active le ver, il envoie une copie de lui-même à chaque contact e-mail de l'ordinateur infecté, il se propage sur Internet et surchargent les serveurs de messagerie peut entraîner des attaques par déni de service contre des nœuds du réseau.
- **Rançongiciels (ransomware)** – bloque l'accès aux données et menace de les publier ou de les supprimer à moins qu'une rançon ne soit versée.une version plus avancé peut chiffrer les fichiers de la victime de manière à les rendre presque impossible à récupérer sans la clé de déchiffrement.
- **Logiciels publicitaires (adware)** : Diffuse des publicités partout
- **Logiciels espions (spyware)** : espionne ce que vous faites sur l'ordinateur

Les Failles courantes (répertoriées par L’OWASP)

1. Contrôles d’accès défaillants

Le contrôle d'accès applique une stratégie telle que les utilisateurs ne peuvent pas agir en dehors de leurs autorisations prévues. Les défaillances entraînent généralement la divulgation, la modification ou la destruction d'informations non autorisées de toutes les données ou l'exécution d'une fonctionnalité métier en dehors des limites de l'utilisateur.

Exemple : Augmentation de privilèges, modification de l’url, forcer l’accès à certaines pages web.

2. Défaillances cryptographiques

L'accent est mis sur les défaillances liées à la cryptographie (ou son absence). Cela entraîne souvent l'exposition de données sensibles.

Exemple : Utilisation d’algorithmes faibles ou désuets, force des clés de chiffrement, renouvellement des clés de chiffrement, ..

3. Injection

SQL injection, XSS. Données d’utilisateur non sanitizées.

4. Conception non-sécurisée

Nouvelle catégorie. Nécessite de rajouter des contrôles en amont du développement. La conception sécurisée est une culture et une méthodologie qui évalue en permanence les menaces et garantit que le code est conçu et testé de manière robuste pour empêcher les méthodes d'attaques connues.

5. Mauvaise configuration de sécurité

Plus il y a de possibilités de configuration d’un logiciel, plus il y a des risques d’avoir une mauvaise configuration entraînant une faille.

Exemple : autorisations mal configurées sur un service cloud, fonctionnalités inutiles sont activées ou installées, la version du logiciel est obsolète ou vulnérable, les comptes par défaut et leurs mots de passe sont toujours activés et inchangés.

6. Composants vulnérables et obsolètes

Cela concerne le système d'exploitation, le serveur web/application, le système de gestion de base de données (SGBD), les applications, API et autres composants, les environnements d'exécution et les bibliothèques. Ne récupérer des composants qu'auprès de sources officielles via des liens sécurisés.

7. Identification et authentification de mauvaise qualité

Utilisation de mots de passe faible, autorisation d’un nombre de requêtes élevées dans un laps de temps court, Autoriser les mots de passe par défaut, utiliser des processus de récupération des informations d'identification faibles ou inefficaces, exposition des identifiants de session dans l'URL.

8. Manque d’intégrité des données et du logiciel

Les défaillances de l'intégrité des logiciels et des données sont liées au code et à l'infrastructure qui ne sont pas protégés contre les violations de l'intégrité. C'est le cas, par exemple, lorsqu'une application s'appuie sur des plugins, des bibliothèques ou des modules provenant de sources, de dépôts et de réseaux de diffusion de contenu (CDN) non fiables. Enfin, de nombreuses applications intègrent désormais une fonctionnalité de mise à jour automatique, où les mises à jour sont téléchargées sans vérification d'intégrité suffisante et appliquées à l'application précédemment fiable.

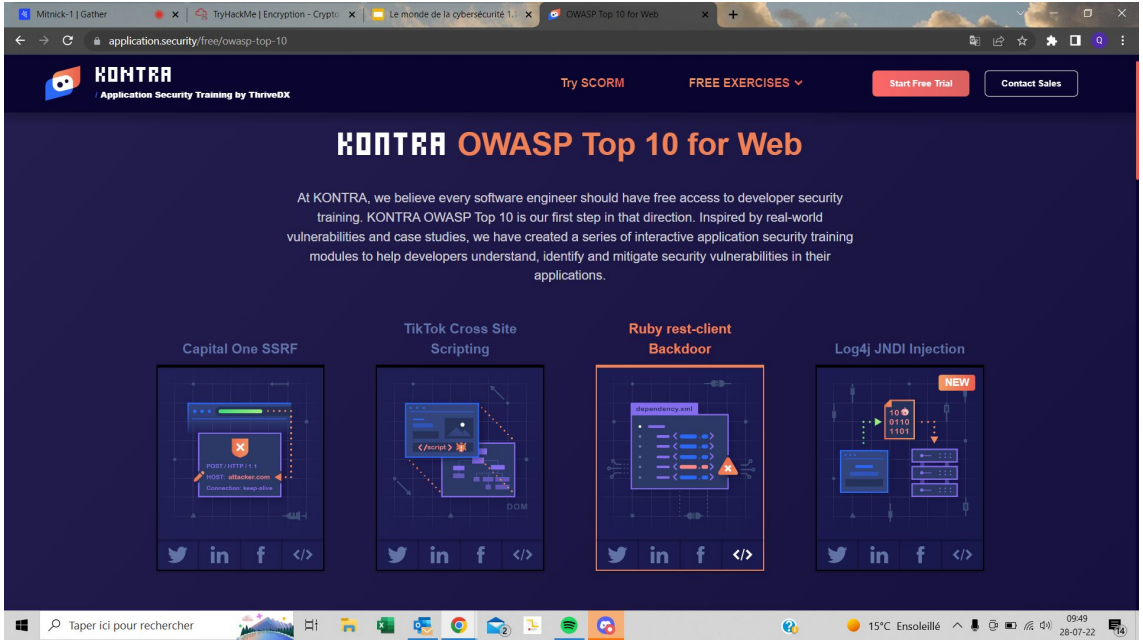
9. Carence des systèmes de contrôle et de journalisation

Cette catégorie a pour but d'aider à la détection, à l'escalade et à la réponse aux brèches actives. Sans journalisation et surveillance, les brèches ne peuvent être détectées. Une journalisation, une détection, une surveillance et une réponse active insuffisantes peuvent survenir à tout moment. Ou vous êtes vulnérable à une fuite d’information en rendant les enregistrements de journalisation et d’alertes accessibles à vos utilisateurs ou attaquants .

10. Falsification de requêtes côté serveur (SSRF)

Une faille SSRF se produit lorsqu'une application web récupère une ressource distante sans valider l'URL fournie par l'utilisateur. Elle permet à un attaquant de contraindre l'application à envoyer une requête élaborée à une destination inattendue, même si elle est protégée par un pare-feu, un VPN ou un autre type de liste de contrôle d'accès au réseau (ACL).

Lien intéressant:



https://application.security/free/owasp-top-10