COMPTE RENDU DES RECHERCHES **:**

1. LES ATTAQUES LES PLUS FREQUENTES :
2. D’une application web :

* L’injection de code :

L'**injection de code** est une technique qui consiste à injecter des données dans une application pour en modifier le comportement. Dans le cadre d'une [application web](https://fr.wikipedia.org/wiki/Application_web), on peut distinguer deux familles, les injections du côté [client web](https://fr.wikipedia.org/wiki/Client_web) et les injections du côté [serveur](https://fr.wikipedia.org/wiki/Serveur_informatique) de base de données. Ces injections sont souvent effectuées en injectant le code malicieux via les [formulaires](https://fr.wikipedia.org/wiki/Formulaire#En_informatique) disponibles dans ces applications. Nous avons entre autre :

* L’injection SQL :

L’injection SQL peut être une conséquence directe d’un mauvais contrôle des

données entrées par l’utilisateur. En effet, les caractères « ‘ » et « ; » peuvent être

utilisés pour enchaîner plusieurs requêtes SQL à la suite l’une de l’autre. Considérons par exemple une page HTML comprenant un formulaire d’authentification avec un champ Login et un champ Password. La requête SQL tournant sur le serveur est la

suivante :

SELECT user FROM table\_users WHERE champ\_login=’login’ AND

champ\_password=’password’

Si maintenant un attaquant saisit la chaîne suivante dans le champ Login :

Administrateur’; --

La requête exécutée finalement sera la suivante:

SELECT user FROM table\_users WHERE champ\_login=’Administrateur’; --’ AND champ\_password=’password’.

Le résultat est un contournement de l’authentification : on se retrouve logué en

tant qu’Administrateur.

Le cas le plus simple d’injection SQL consiste à s’authentifier dans une application

Web en saisissant un login existant et n’importe quel mot de passe suivi de «

OR 1=1». L’authentification étant vérifiée par comparaison, le résultat booléen de la

Vérification du mot de passe est toujours vrai, ce qui permet d’obtenir l’accès à l’application.

* Cross-site scripting (XSS) :

Une attaque XSS est une attaque visant les sites internet ou les applications Web. Elle consiste à injecter des scripts dans la réponse d'une application, généralement du HTML, qui sera interprétée par le navigateur. Le but de ces deux attaques est de récupérer les données sensibles de l'application et de les envoyer vers un serveur sous le contrôle de l'attaquant.

Il y a deux types d'attaque XSS, la reflected XSS (aussi communément appelée type 1 ou first-order XSS) et la persistent XSS (aussi communément appelée type 2, stored XSS ou second-order XSS).

La **reflected XSS** consiste à injecter des scripts dans une application pour qu'ils soient exécutés sur le navigateur du côté client. Cette attaque n'est pas stockée dans l'application, aucune trace ne sera visible sur le serveur. Elle intervient généralement par la propagation d'un lien et utilise le [social engineering](https://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_(s%C3%A9curit%C3%A9_de_l%27information)). Lorsque l'utilisateur clique sur ce type de lien, une requête contenant du code malicieux est envoyée vers le serveur, celui-ci va alors retourner une réponse contenant ce code à l'utilisateur (page, erreur). Le code injecté sera alors exécuté par le navigateur dans le même contexte que les scripts de l'application, permettant ainsi à l'attaquant de récupérer le cookie associé à l'utilisateur et d'envoyer ces informations vers un serveur sous son contrôle.

La **persistent XSS** est une attaque qui consiste à stocker du code malicieux à l'intérieur du système de stockage de l'application. Pour qu'elle soit effective, l'application devra utiliser ces données dans la génération de ses réponses. L'exemple courant est un message posté sur un forum. Le message sera nécessairement stocké en base de données. Si celui-ci contient du code malicieux, il sera exécuté à chaque fois qu'un utilisateur ouvrira la page le contenant. Cette attaque a donc beaucoup plus de cibles potentielles que la précédente.

* Cross-Site Request Forgery (CSRF) :

Cross-Site Request Forgery (CSRF) est une attaque qui force un utilisateur final à exécuter des actions indésirables sur une application Web dans laquelle il est actuellement authentifié. Les attaques CSRF ciblent spécifiquement les demandes de changement d'état, pas le vol de données, car l'attaquant n'a aucun moyen de voir la réponse à la demande falsifiée. Avec un peu d'aide de l'ingénierie sociale (comme l'envoi d'un lien par email ou par chat), un attaquant peut tromper les utilisateurs d'une application web dans l'exécution de ses actions. Si la victime est un utilisateur normal, une attaque CSRF réussie peut forcer l'utilisateur à effectuer des demandes de changement d'état telles que le transfert de fonds, la modification de son adresse e-mail, etc. Si la victime est un compte administratif, CSRF peut compromettre l'ensemble de l'application Web.

* Attaque par déni de services (DDOS attack) :

L’attaque par déni de service est causée en inondant un serveur ou un site web de requêtes dans le but de le rendre indisponible. Cette attaque peut être perpétrée par un petit nombre de ressources. Un pirate peut utiliser son seul ordinateur pour contrôler des zombies, c’est-à-dire d’autres ordinateurs infectés qui obéiront à ses commandes. Ces ordinateurs peuvent avoir précédemment été infectés par des virus ou des vers.

# Attaque du type Hijacking :

Il s’agit de la possibilité pour un pirate d**’utiliser l’identité d’autres personnes sur votre application.**

**Une application peut etre vulnérable à ce type d’attaque dans plusieurs cas :**

* Tout d’abord, si les éléments permettant d’authentifier un utilisateur (login / mot de passe) sont **mal protégés dans l’application web**. Dans le cas où un pirate accède à la base de données de l’application, par quelque moyen que ce soit, il peut accéder à la liste des login et des mots de passe. Les bonnes pratiques veulent que les mots de passe soient correctement “hashés” ou “cryptés » dans la base, pour être inexploitables par un pirate.
* La deuxième possibilité est de pouvoir **deviner ou modifier les éléments d’authentification** facilement. Une politique de mots de passe forte doit être mise en place afin que les utilisateurs n’utilisent pas des mots de passe trop simples à deviner. Par ailleurs, les mécanismes permettant à un utilisateur de changer de mot de passe ou de récupérer un mot de passe, s’ils sont mal pensés, permettront à un attaquant de changer ou récupérer le mot de passe à la place de l’utilisateur!
* **Références Directes à un Objet non Sécurisées**

Par exemple, si l’application est sensée gérer des photos privées, tel que sur certains réseaux sociaux, ou dans un site internet gérant des albums photos, l’aspect non sécurisé peut donner accès aux photos à n’importe qui, simplement en tapant l’URL dans un navigateur web. Un utilisateur lambda pourra ainsi changer l’URL dans son navigateur et essayer d’accéder à http://www.example.com/photos/......, affichant ainsi des photos qui peut-être ne lui appartiennent pas.

* Attaque de pishing :

Scenario de l’attaque en considérant le lien suivant comme url de redirection ttp://www.ppp.com/***login.php?goto=evil.com/login***:

* L’utilisateur visé par l’attaque reçoit un email contenant le lien ci-dessus.
* La victime clique sur le lien, ce dernier lui semblant inoffensif (site ppp.com que nous allons supposer connu)
* Une fois connectée via la page de login, ppp.com va rediriger la victime vers le site evil.com
* Le site evil.com peut par exemple demander à la victime de renseigner à nouveau son mot de passe, en prétextant un problème technique ou une erreur de saisie. Mais cette fois l’utilisateur est sur un site pirate, qui lui volera ses identifiants.
* Cookies poisonning (empoisonnement des cookies) :

Sur le Web, l'empoisonnement de cookie est la modification d'un cookie (informations personnelles dans l'ordinateur d'un utilisateur Web) par un attaquant pour obtenir des informations non autorisées sur l'utilisateur à des fins telles que le vol d'identité. L'attaquant peut utiliser ces informations pour ouvrir de nouveaux comptes ou accéder aux comptes existants de l'utilisateur.

1. D’une application mobile:

* Revêtement de l’interface de l’application ou **Clickjacking** :

Cette attaque fonctionne d’une façon très simple. Les malwares font un suivi des applications quand l’utilisateur les ouvre et dès qu’il ouvre une application que le malware connaît, il remplace la fenêtre de l’application par une fenêtre similaire ou même identique. Ce processus est instantané ; l’utilisateur n’a donc pas l’opportunité de voir quelque chose de suspect.

Ensuite, quand l’utilisateur insère des informations dans la fausse fenêtre en pensant qu’il interagit avec une application de confiance, le malware vole les identifiants de connexion, les mots de passe, les numéros de carte bancaire et toutes autres informations d’intérêt pour les hackers.

Le truc du remplacement de l’interface de l’application est compris dans l’arsenal des chevaux de Troie des banques en ligne. Mais ils ne se limitent pas à la banque : les créateurs de ces chevaux de Troie ne collectent plus uniquement que des données pour les applications de banque en ligne. En effet, ils créent maintenant de fausses fenêtres pour un grand nombre d’applications où l’utilisateur insère des numéros de carte bancaire ou d’autres informations intéressantes.

* **Injection SQL :**

Pareil que dans les applications web vue ci-dessus.

* Rupture du canal secret :

Une application malicieuse espionne une application normale en la forçant à soumettre ses données sensibles à un faux serveur. L'interception des données échangées permet de les utiliser à des fins malveillantes.

* Fuite de données :

Une application mal codée peut entraîner la fuite et le vol d'informations sensibles non chiffrées stockées dans les logs, le cache.

Les attaques que nous venons d’énumérer sont toutes dangereuses mais certaines sont plus dangereuses que d’autres .Parmi les plus dangereuses, nous avons :

Pour les applications web :

* L’injection de code
* L’attaque CSRF
* L’attaque par déni de services

Pour une application mobile :

* L’injection SQL
* La rupture du canal secret
* Le clickjacking

1. LES PLUS GRANDES ATTAQUES INFORMATIQUES DU MONDE :
2. L’attaque d’Instagram de 2017 :

La rentrée 2017 a été marquée par le piratage du réseau social Instagram. Les numéros de téléphone et les adresses e-mail de **6 millions d’utilisateurs** ont été rendus publics et sont disponibles à l’achat sur le darknet. Même si aucun mot de passe n’a été récupéré, certaines informations ont de la valeur puisqu’elles appartiennent aux chanteurs Selena Gomez, Justin Bieber et Taylor Swift par exemple. Les dirigeants d’Instagram pensent que le pirate “Doxagram” a exploité la faille d’une API qu’ils assurent avoir corrigée aujourd’hui. Mais pour certains experts, le pirate est passé par ailleurs.

1. L’attaque du site de rencontre Ashley Madison :

En août 2015, le site de rencontres extraconjugales Ashley Madison a été piraté et les données personnelles (noms, adresses e-mail, téléphones, préférences sexuelles…) de plus de 30millions d’utilisateurs à travers plus d’une quarantaine de pays ont été récupérées. Le groupe de pirates «The Impact Team» menaçait de rendre public toutes les données si le site ne fermait pas. Chose promise, chose due, le groupe a publié 30 gigaoctets de données d’utilisateurs. Et ces révélations ont viré au tragique en entraînant notamment de nombreuses démissions et 3 suicides d’inscrits.

De son côté, la société a survécu malgré tout. Elle a payé l’équivalent de 13 millions d’euros de dédommagements depuis l’affaire, qui a elle-même fait l’objet d’un documentaire en 2016 intitulé “[Ashley Madison : Sex, lies and cyber attacks](https://www.youtube.com/watch?v=X8ZY2W5NCdA)”. C’était encore une fois grâce à une faille de sécurité provenant du site que l’attaque avait pu avoir lieu. Le site disposait de système de sécurité très insuffisant et violait même plusieurs dispositions concernant la protection de la vie privée.

1. L’attaque d’Adobe :

Adobe annonce en octobre 2013 le piratage massif de son infrastructure informatique. Les informations personnelles de **2,9 millions de comptes** ont été dérobées (identifiants, mots de passe, noms, numéros de cartes bancaires et dates d’expiration). Un autre fichier découvert sur internet plus tard a porté le nombre de comptes concernés par l’attaque à 150 millions (38 millions de comptes actifs). Pour obtenir ces informations les hackers ont profité des failles de sécurité de l’éditeur. En effet, il ne respectait pas certaines pratiques de sécurité des mots de passe. Les mots de passe dérobés avaient été chiffrés au lieu d’être hachés comme il est recommandé. Si les données bancaires ont été volées, elles étaient cependant inexploitables du fait du chiffrement de haute qualité d’Adobe.

La société n’a pas été seulement attaquée pour ses informations clients mais également pour ses données produits. En effet, le problème le plus préoccupant pour Adobe a été le vol de plus de 40Go de codes source. L’intégralité du code source du produit ColdFusion a notamment été dérobée ainsi qu’une partie des sources de Reader et Photoshop. Si d’autres attaques étaient à craindre, elles n’ont finalement pas eu lieu.

1. L’attaque de Yahoo :

Yahoo annonçait avoir subi en 2014 une [cyberattaque ayant affectée 500 millions de comptes utilisateurs.](https://secludit.com/blog/consommateurs-hacking-confiance/) Cela constituait le plus gros piratage massif de données individuelles dirigé contre une seule société. Noms, dates de naissance, numéros de téléphone et mots de passe ont été volés. Si l’entreprise avait assuré que les données bancaires n’avaient pas été touchées, elle recommandait à ses utilisateurs la prudence.

Avant cela, en 2012, c’était le hacker “Peace” qui vendait pour 1900$ **200 millions de noms d’utilisateurs et de mots de passe**.

#### Jamais 2 sans 3…

En mars Yahoo! a avoué s’être une nouvelle fois piraté. Cette fois-ci, “seulement ” **32 millions de comptes** avaient été touchés. Cette cyberattaque a relancé l’enquête sur celle de 2014 puisque les attaquants se sont servis d’outil dérobé cette année-là. De la sorte, ils ont créé des cookies malveillants leur permettant de se connecter sans les mots de passe. Conséquence pour Yahoo!, la firme a été rachetée par Verizon en 2017 pour 4,5 millions de dollars au lieu des 4,8 millions annoncés en 2016.

Mise à jour : Finalement, Yahoo vient d’avouer que l’ensemble des **3 milliards de comptes utilisateurs** avaient bien été piratés en 2013. Cette cyberattaque constitue donc la plus importante de l’histoire d’internet.

1. Les attaques chez SONY :

En avril 2011, le PlayStation Network, le service de jeux multi-joueurs, d’achats de jeux en ligne et de diffusion de contenus en live de la marque japonaise a été attaqué. **Les données personnelles de 77 millions d’utilisateurs ont fuités**. Les coordonnées bancaires de quelques dizaines de milliers de joueurs ont également été compromises. Après la découverte de l’intrusion, le PSN ainsi que Sony Online Entertainment et Qriocity avaient été fermés pendant un mois. Pour calmer la colère des utilisateurs, Sony a débourser 15 millions de dollars de compensation auxquels s’ajoutent quelques millions de frais de justice et de remboursements des personnes dont les comptes bancaires ont été utilisés de façon frauduleuse. Une cyberattaque qui aurait pu être largement évité. En effet, les hackers ont utilisé une vulnérabilité réseau bien connue à laquelle Sony n’a pas prêté attention. Les données n’étaient pas chiffrées et ont pu être facilement récupérées grâce à une injection SQL très simple.

#### En novembre 2014, c’est au tour de la filiale Sony Pictures Entertainment d’être attaquée par un malware, et plus précisément par un vers informatique. Les hackers (les Guardians of Peace) avaient dérobé **100 téraoctets de données** comprenant de nombreuses informations confidentielles. Avaient été volés par exemple le scénario du James Bond en préparation, les données personnelles de 47 000 employés (noms, adresses, e-mails, numéros de sécurité sociale, salaires…), ou encore des mails compromettants. A cause du contenu choquant de ses mails, (et notamment jugé insultant envers le président de l’époque Barack Obama) la directrice du studio, Amy Pascal avait été éjectée de son poste. De plus, l’entreprise avait annulé la diffusion de plusieurs films et avait versé l’équivalent de 8 millions de dollars de dédommagement à ses salariés et ex-salariés concernés. Une cyberattaque qui aurait pu une nouvelle fois être évitée car  SonyPictures avait fait réalisé un audit de son système de sécurité quelques mois avant l’incident. Celui-ci avait alors révélé de lourdes défaillances dans la gestion de l’infrastructure notamment sur un pare-feu et plusieurs centaines de terminaux (routeurs et serveurs) qui n’étaient pas gérés par les équipes compétentes.

1. LES PLUS GRANDS BRACAGES DE L’HISTOIRE :
2. **Banque Centrale d'Irak (2003)** : 1 milliard de dollars :

Le rôle du braqueur en chef est tenu par Saddam Hussein. A la veille du début des bombardements par la coalition en 2003, Hussein se dit qu'il aurait bien besoin de liquidités, du coup il envoie son fils Qusay retirer tout ce qu'il peu de la Banque Centrale d'Irak : le fiston repart avec des caisses pleines de bons de 100$ et en 5h il grappille 1 milliard de dollars US. On retrouva 650 millions dans les murs de son palais, mais jamais les 350 restants.

1. **Vol des Bons du trésor de la ville de Londres (1990)** : 292 millions de livres

En 1990, à Londres, John Goddard travaille pour un courtier nommé Sheppard. Son travail consiste à livrer des bons du Trésor à la Banque d’Angleterre ou à des sociétés de crédit immobilier ou d’épargne. Lors d’une livraison, il est agressé dans une petite rue par un individu armé d’un couteau, qui s’empare de sa serviette contenant 292 millions de livres (348 millions d’euros) d’emprunts d’Etat. La police soupçonne Patrick Thomas, un petit escroc du sud de Londres. Il est retrouvé mort d’une balle dans la tête en décembre 1991 avant d’avoir pu être interrogé. Un homme, Keith Cheeseman, écopera cependant de six ans et demi de prison.

1. **Braquage du Musée Gardner de Boston (1990)** : 300 millions de dollars

Là on commence à tomber sur du braquage de qualité qui fait un peu rêver. Imaginez plutôt : 2 mecs habillés en policiers qui parviennent à convaincre 2 jeunes gardiens du Musée Gardner de les laisser rentrer avant de les menotter et de les emmener au sous-sol, tout cela sans utiliser d'armes. Ensuite les gaziers ont fait leur petit marché pendant plus d'une heure, sélectionnant tout un tas d’œuvres d'art dont des Rembrandt et un Vermeer pour un montant total de 300 millions de dollars (et c'était il y a 20 ans, imaginez la valeur du pactole aujourd'hui). Personne n'a encore réussi à remettre la main sur les 13 toiles volatilisées.

1. **Banque de Baghdad (2007)** : 282 millions de dollars

On continue avec l'Irak, mais cette fois ce n'est pas Saddam le responsable. Autre braquage de grande taille, celui de la banque de Bagdad en 2007, pendant l’occupation américaine. Le casse est perpétré par les propres gardes de banque, aidés par des milices qui permettent aux malfaiteurs de s'enfuir. Les hommes s’emparent de 280 millions de dollars, qui n'ont jamais été retrouvés.

1. **Chambre des coffres-fort de Knightsbridge (1987)** : 60 millions de livres

Revenons maintenant à Londres, où là encore nous avons à faire à un duo de gaziers pas frileux qui demandèrent à louer un coffre sécurisé au Centre de Knightsbridge. Une fois dans la salle des coffres, ils sortirent des calibres et maitrisèrent les employés et les gardes. Après avoir fait entrer leurs complices, ils prirent le temps de mettre un panneau "Fermé" sur la porte pour ne pas être dérangés. Normal. Leur butin s'élèverait aujourd'hui (avec l'inflation) à pratiquement 114 millions de dollars. Valerio Viccei fut arrêté un mois plus tard, il avait laissé une empreinte digitale dans la salle des coffres.

1. LES PLUS GRANDES MAFIAS DU MONDE :
2. Yamaguchi Gumi, la mafia japonaise : 80 milliards de dollars

Issus d'une principale famille, les Yamaguchi-gumi sont installés à Kobe et se développent par une stratégie bien huilée de rachats d’entreprises. Ils font partie des Yakusa, ces mafias japonaises puissantes dont les membres sont estimés à plus de 110 000. Contrairement à beaucoup de mafias, la mafia japonaise est hyper centralisée et n'opère pas dans l'ombre, mais possède des bureaux. Les membres de la Yakuza sont connus pour être tatoués de la tête aux pieds. Ils opèrent surtout dans l'industrie pornographique, la prostitution et l'immigration illégale.

1. Solntsevskaya Bratva, la mafia russe : 8.5 milliards de dollars

A l'inverse de la mafia japonaise, la mafia russe possède une structure hyper décentralisée. C'est la chute du mur de Berlin en 1989 qui lui a ouvert les portes de l'Europe occidentale. Désormais influente dans le monde entier, la mafia russe compte environ 500 000 membres. Mais le groupe de la  Solntsevskaya Bratva compte à lui seul 9000 personnes. Il opère notamment dans le trafic d'héroïne, cultivée en Afghanistan.

A noter que les "vory v zakone", implantés un peu partout en Europe, dont la France, font partie des mafias russes les plus actives et dangereuses. De véritables fortunes sont notamment constituées par ces dernières en France. En 2013, près de 215 de ses membres étaient incarcérés dans l'Hexagone contre 80 en septembre 2010.

1. Camorra,  mafia italienne : 4.9 milliards de dollars

La mafia Camorra est l'une des quatre mafias italiennes les plus puissantes. Basée à Naples, l'origine de la mafia remonte au 19e siècle, d'abord constituée par un gang en prison.

Aujourd'hui, le groupe tire un profit de 4,9 milliards de dollars grâce au trafic d'armes, de la drogue, la prostitution, la contrefaçon, le jeu et l'extorsion de fonds.

1. Ndrangheta, mafia italienne : 4.5 milliards de dollars

La 'Ndrangheta est la deuxième mafia la plus influente d'Italie. Elle est parvenue à étendre son réseau à l'international grâce à ses vendeurs de cocaïne en Amérique du Sud et aux Etats-Unis. Elle contrôle une grande partie du marché de la drogue transatlantique qui sévit surtout en Europe.

1. LES PLUS GRANDES FRAUDES AU MONDE :

##### L’affaire Ponzie :

Ponzi achetait des coupons-réponses, les échangeait contre des timbres et les revendait réalisant 50% de bénéfice en 45 jours. Il proposa ces rendements à 20000 personnes qui investirent $15M. Mais, pour distribuer ces bénéfices, il aurait fallu 160M de coupons et seulement 27000 étaient en circulation.

##### Le scandale du Panama :

Lesseps organisa des levées de fonds pour financer les travaux du canal de panama. Suite au retard et au surcoût du chantier, il lança une nouvelle souscription publique, mais une partie de cet argent fut utilisée pour soudoyer journalistes et parlementaires, ce qui entraîna la ruine de cent mille souscripteurs.

##### Stavisky :

Le fondateur du Crédit municipal de Bayonne, Serge Alexandre Stavisky fut arrêté pour fraude et mise en circulation de faux bons au porteur pour un montant de 25 millions de francs, organisant cette fraude sur le schéma Ponzi.

##### La Garantie Foncière :

La Garantie Foncière proposait aux particuliers d’investir leurs économies dans l’immobilier avec des rendements très attractifs. Cependant, Frenkel et ses complices en ont profité pour se faire racheter des immeubles qu’ils avaient acquis à des prix très bas, empochant une plus-value sur le dos des souscripteurs

1. L’un des plus grand « piratage » de l’histoire :

En volant les données de quelque 100 millions de clients, trois complices ont bâti une entreprise criminelle à grande échelle. Des millions de dollars de bénéfices frauduleux ont été déposés dans des banques helvétiques, affirme la justice américaine

C’est la plus grosse affaire de piratage informatique de l’histoire du système financier. Lors de la présentation de l’acte d’accusation, à Manhattan, le procureur new yorkais Preet Bharara s’est dit impressionné, évoquant un vol de données «dont la portée et les montants sont stupéfiants».

Grâce aux informations dérobées aux quelques 100 millions de clients de banques et d’institutions financières, dont 83 millions auprès de JP Morgan, les trois criminels ont bâti une véritable entreprise internationale d’activités illégales. En s’appuyant sur une équipe de «centaines d’employés et de complices», Gery Shalon, Joshua Samuel Aaron et Ziv Orenstein se sont livrés à la manipulation de titres boursiers, à des paris illégaux en ligne et à des fraudes à la carte de crédit notamment. Ils ont aussi, entre autres, substitué des données confidentielles de sociétés dont ils pirataient le réseau.

Le piratage des réseaux informatiques de JPMorgan a affecté les données de 76 millions de ménages et 7 millions d’entreprises. La société de nouvelles financières Dow Jones, par ailleurs éditrice du Wall Street Journal, ainsi que deux autres courtiers, ont confirmé mardi faire partie des victimes de cette attaque.