

Sécurité des applications, attaques et logiciels malveillants

Écrire du code exempt d'erreur est difficile, et les erreurs peuvent conduire à des vulnérabilités qui permettent d'attaquer le programme.

L'attaque peut permettre d'obtenir des droits non accordés au départ, faire planter l'application, introduire des données incorrectes, etc.

Attaques courantes

- **Remote Code Execution** (RCE), exécution de code à distance en soumettant une donnée précise à l'application
 - Un exemple qui a fait beaucoup de bruit est celui de la vulnérabilité [log4shell](#) dans le système de log Java "log4j" qui faisait qu'il était possible d'exécuter du code sur toute application utilisant la librairie. Cette vulnérabilité était si dangereuse qu'elle fut considérée par certains gouvernements comme l'un des problèmes de sécurité informatique la plus sérieuse des 20 dernières années.
- **SQL Injection**, injection de code SQL dans la base de donnée en soumettant des données précises.
- **Format String vulnerabilities** qui consiste à soumettre du code qui est compris comme une commande par l'application. Pour en savoir plus, des exemples de code en C sont donnés [dans cet article](#).
- **Cross-Site Scripting** (XSS), qui est encore dû à une non-vérification des soumissions de l'utilisateur-ice qui peut mener à intégrer du code HTML dans une page. Ce qui signifie que l'on peut aussi injecter du code JavaScript dans la page qui seront exécutés par tous les visiteurs de celle-ci.
- **Username enumeration**, si le système mentionne que le nom d'utilisateur est introuvable, il est possible de tester plusieurs noms d'utilisateurs pour savoir lesquels sont présents sur le système. Il est parfois aussi possible de faire cela via l'API du site (genre en regardant `/api/user/01` et les énumérer comme ça).
- **Stack/buffer overflow**, l'attaquant soumet une chaîne de caractère spécifique qui provoque un débordement de la pile. Grâce à ce débordement, le code exécuté devient celui de l'attaquant, cela peut donc lui faire prendre le contrôle du code de l'application, et si l'application s'exécute dans le domaine administrateur, lui faire devenir

administrateur (**privilege escalation**).



- **Déni de service** (DoS), le fait de rendre inaccessible un système en le bombardant de requêtes. Le système devient ainsi inaccessible durant le temps de l'attaque, bien qu'aucun dommage ne soit opéré, cela cause un problème en terme d'image pour l'entreprise et peut lui faire perdre de l'argent à cause de l'inaccessibilité du site.
 - Si une attaque DoS est fait depuis plein d'ordinateurs différents (ce qui fait qu'elle est plus compliquée à arrêter), on parle d'attaque de **déni de service distribuée** (DDoS). Chaque ordinateur est appelé un **zombie** et l'ensemble des ordinateurs infectés utilisé est appelé un **botnet**.

Programmes malveillants

Maintenant, on va parler de types de programmes malicieux,

- **Cheval de troie** (ou **trojan**), est un programme qui se fait passer pour ce qu'il n'est pas pour déclencher une action hostile. Cela peut par exemple être un faux anti-virus.
- **Backdoor** (porte dérobée), le programme installe une porte d'accès à l'utilisateur, il est ainsi possible de faire exécuter des commandes à la machine à distance.
 - C'est une méthode assez utilisée pour constituer des attaques DDoS, car la machine devient un zombie qui fait partie d'un botnet auquel l'attaquant demande de faire des requêtes à répétition sur un site.
 - Cette méthode peut aussi être utilisée pour installer un cryptomineur qui va miner des cryptomonnaies pour l'attaquant sur toutes les machines victimes

- Les **vers informatiques** (ou **WORMS**) sont des programmes qui se propagent par les réseaux informatiques. Les vers utilisent des vulnérabilités d'autres systèmes pour se propager, ainsi chaque machine infectée infecte les autres machines du réseau à son tour.
 - Un exemple très connu de WORM est celui de [WannaCry](#), un ransomware qui a infecté plus de 300000 ordinateurs sur plus de 150 pays différents et qui aurait causé des pertes de l'ordre de plusieurs centaines de millions de dollars. Ce WORM se propageait via une vulnérabilité dans un port de communication du système Windows.
- Les **virus informatiques** sont des ensembles d'instructions qui utilisent un programme pour se reproduire. Ainsi, comme un virus biologique, un virus informatique a pour principal but de se reproduire en infectant un programme hôte. Certains virus ont également une charge active qui attaque le programme à un moment déterminé. Certains virus utilisent des techniques avancées pour se cacher des systèmes de protection.
 - Les **virus script** sont des virus écrits dans un langage interprété (par exemple le VBA, langage de programmation de Microsoft Office), le virus utilise un environnement tiers pour s'exécuter et se reproduire. Cela peut par exemple être sous la forme d'une macro d'un document Microsoft Office.

