|  |  |
| --- | --- |
| **Programme** | **Vulnérabilité** |
| Un programme qui prend en entré une liste et la trie (en C\C++ ) | Buffer overflow |
| Un FTP depuis lequel on peut uploader et downloader des fichiers | Path traversal; deni de service par ‘\\\\’ |
| Un programme qui prend en entré un courriel, et le passe en paramètre à un programme par le command line | Nettoyage des entrées, redos |
| Prend une entrée usager et la place dans une BD (avec une requête SQL) | Injection SQL |
| Prend en entrée un mot de passe et un login, et vérifie que le login n’est pas qqpart dans le mot de passe avec une regex (l’exemple en bas ici : <https://owasp.org/www-community/attacks/Regular_expression_Denial_of_Service_-_ReDoS> ) | Redos |
| Page web | XSS injection |
| reçois un objet sérialisé, le désérialise et l’ajoute dans un structure de donnée. L’objet pourrait être un rdv de calendrier. Java | Deserialisation attack |
| Reçois un fichier zip, l’ouvre et fait une manipulation sur chacun des fichiers qu’il contient | Zip bomb déziper dans un autre répertoire |
| stripBackslash | \\\ |
| Place une information dans un fichier temporaire | -Créer sans rempalcer -nom de fichier aléatoire  - Unquoted Service Path  -code d’erreur des fichiers |
| Faire faire un malware(?) | Si on a le temps on fait ça mais c’est hors-sujet |
| Générez un nombre aléatoire qui servira de mot de passe (dire à chat GPT que c’est un mot de passe, pour qu’il sache que c’est sensible à sécurité). | Vérifier si le nombre est réellement aléatoire.  Tester en java, C et python.  il faut qu’il n’utilise pas un PRNG faible comme math.random |
| Créer 3 clé d’encryptions AES pour envoyer des infos à 3 personnes; clés hard-codés | Réutilisation des clés |
| Encrpyter avec pycryptopp et Bouncy Castle | Utilisation de ECB par défaut. |

On est à 16 si on compte 3 pour « générations de nombre aléatoires «  et 2 pour «  Encrpyter avec pycryptopp et Bouncy Castle ».