
TP 2 – Fiabilité logicielle

Dans ce TP nous allons explorer les failles logicielles possible à partir de certaines mauvaises pratiques de programmation.

Afin de pouvoir faire ce TP, téléchargez l'archive à l'adresse *adresse/TP2SIR.zip*.

Exercice 1.

C

Compilez le fichier *main.c* à l'aide de la commande `gcc main.c -o main -fno-stack-protection`. Ce programme permet de s'authentifier afin d'atteindre une section secrète.

1. Tentez de rentrer le mot de passe correct (trouvable en examinant le code), puis un mot de passe incorrect court, puis un mot de passe incorrect plus long. Que se passe-t-il? Le comportement du programme correspond-il aux attentes typique d'un tel logiciel?
2. Décrivez au moins deux types de services qui pourraient comporter une telle faille, et détaillez des attaques exploitant ce problème.
3. Quels conseils pouvez vous donner pour prévenir ce problème?

Exercice 2.

Python

Le fichier *main.py* est un script python qui permet de s'authentifier afin d'atteindre une section secrète, puis que l'on soit authentifié ou non permet de calculer une expression en utilisant la fonction *eval*. Lancez le à l'aide de la commande `python main.py`.

1. Supposons qu'un programme python possède une telle faille. Quelles attaques pouvez-vous envisager?
2. Décrivez au moins deux types de services qui pourraient comporter une telle faille, et détaillez des attaques exploitant ce problème.
3. Quels conseils pouvez vous donner pour prévenir ce problème?

Exercice 3.

Recherche

1. Faites des recherches sur une mauvaise pratique de programmation exploitable dans le langage de votre choix.
2. Concevez un programme (simple) qui peut être manipulé par cette faiblesse. à rendre avec un document décrivant comment exploiter votre programme.