Ruckstuhl Michael, Sauge Ryan

CWE-20

Improper Input Validation

Table des matières

1 Solution

Grâce à la fonction input() il est possible d'appeler Win() lorsque l'utilisateur doit donner son choix dans la console. En effet, il suffit d'écrire Win() dans cette dernière. Ceci donne lieu, comme dans le cas d'une victoire, à l'incrémentation de la variable score.

Cette erreur provient du traitement de l'input avec Python2. Celui interprète input comme une expression et non comme une string.

Les erreurs causées par input() en python2 sont très fréquentes et sont souvent représentée, comme dans ce cas, par la CWE-20 "Improper Input Validation" qui est en troisième position.

```
Entrez votre valeur : Win()
Entrez votre valeur : Win()
Entrez votre valeur : Win()
Entrez votre valeur : Win()
Entrez votre valeur : Win()
Entrez votre valeur : Win()
Entrez votre valeur : Win()
Entrez votre valeur : Win()
Entrez votre valeur : Win()
Entrez votre valeur : Win()
Bravo, tu as gagné 10 fois de suite
```

Figure 1 : Illustration de l'exploit

Sources :

- Documentation de la fonction : https://docs.python.org/2.7/library/functions.html#input
- https://medium.com/swlh/hacking-python-applications-5d4cd541b3f1
- https://www.geeksforgeeks.org/vulnerability-input-function-python-2-x/
- https://cysecguide.blogspot.com/2017/10/vulnerability-of-input-in-python-2x.html

2 Correction

Dans python2, il faut changer la fonction input() par raw_input() qui corrige ce problème. Alors que input() prends la valeur et le type de l'input, raw_input() converti le type en string.

L'autre solution serait de passer à python3 où a fonction input() se comporte comme raw_input de base.

3 CWE

La CWE illustré ici est la CWE-20: Improper Input Validation(3ème du top 25). L'input utilisateur n'est pas correctement vérifiée et implémentée ce qui permet à l'utilisateur de gagner.

La saisie utilisateur étant souvent utiliser pour l'authentification(login/mot de passe), on aurait aussi pu adapter notre exemple pour illustrer la CWE-863: Incorrect Authorization, qui n'est pas dans le top 25.

Lien CWE : https://cwe.mitre.org/data/definitions/20.html

4 Intérêt

La faille présente dans le code permet d'illustrer 3 points importants lors du développement d'une application :

- L'importance des mises à jour du langage de programmation, ici une mise à jour de python2 à python3 aurait permis d'éviter la faille.
- De lire la documentation liée à la fonction et de comprendre son fonctionnement. Ainsi un développeur qui copie/colle du code python sur internet sans essayer de le comprendre ne remarquera pas les problèmes liés à la fonction.
- Elle montre également que même des langages ayant la réputation d'être "plus sûr" que par exemple du C peuvent également présenter des faiblesses/dangers (même si ici la version python3 corrige ici le problème).