S7 L4

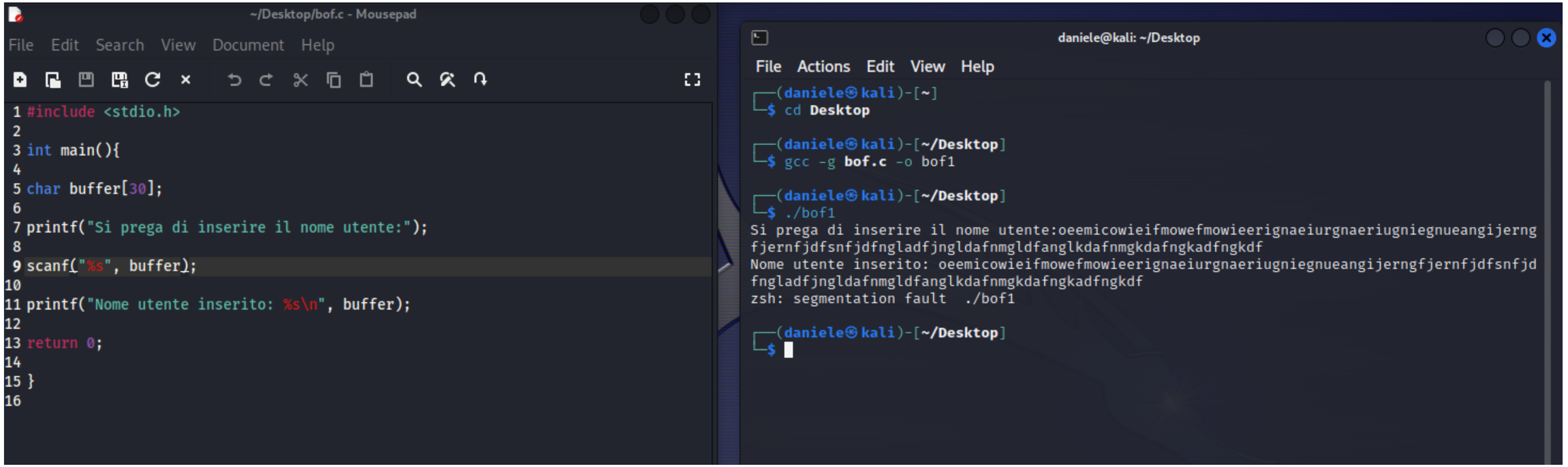
Buffer Overflow

Daniele Zizzi

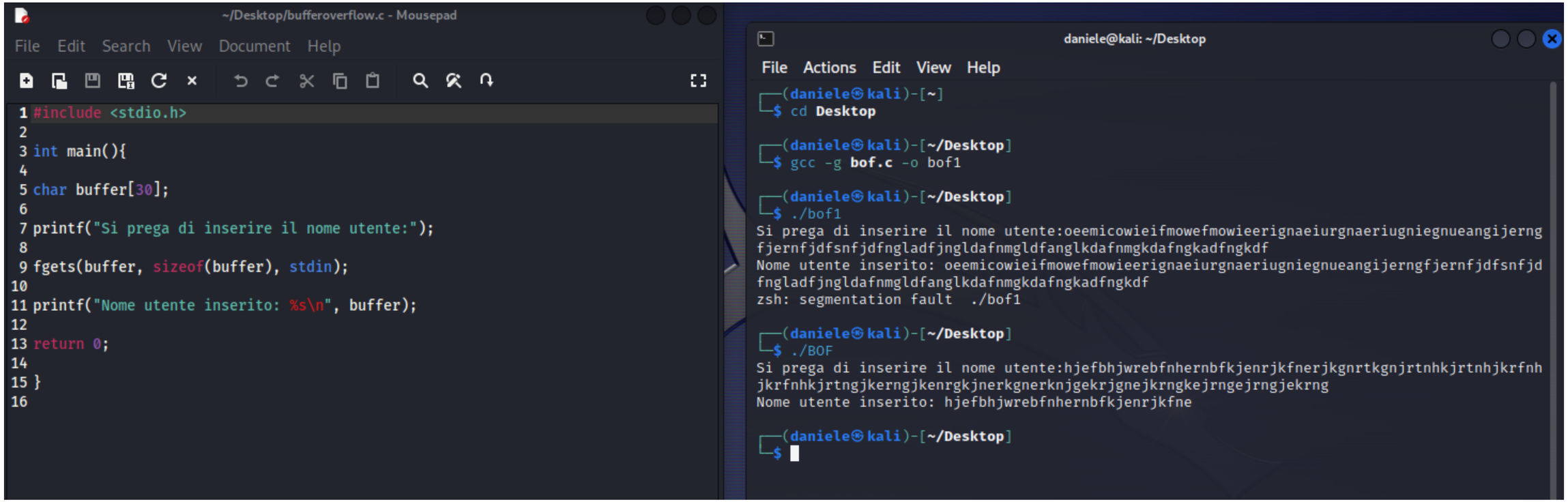
Buffer Overflow

Il buffer overflow, è un tipo di vulnerabilità che si verifica quando i dati inviati al buffer, ne superano la grandezza. Quindi comporta la sovrascrittura di altre porzioni di memoria e il danneggiamento dei dati contenuti in esso.
Le altre porzioni di memoria, posso essere sovrascritte con del codice malevolo, quindi, ogni qualvolta il sistema accederà a tale indirizzo, eseguirà il codice, compromettendo il sistema.

Codice affetto da problemi di buffer overflow, poichè, non ci sono controlli sulla lunghezza dell'input dell'utente. Possiamo notare l'errore quando nell'output riceviamo "segmentation fault"



Con l’utilizzo di fgets, al posto di scanf, posso restringere l’input in base alla grandezza dell’array “buffer”. Qualsiasi input dell’utente, viene ristretto a 31 caratteri, in questo caso. Quindi evito il buffer overflow.



Per poter verificare un buffer overflow e quindi stamparne il risultato. Dovremmo conoscere gli indirizzi di memoria, dove le informazioni vengono memorizzate, quindi assegnare al secondo array, un indirizzo di memoria adiacente al primo, in modo che i dati sovrascritti siano quelli del secondo array. Poi stamparne il risultato.