In **Zeile 9** wird im Stackframe der main() Funktion ein Charakter Array definiert und deklariert, was sich intern als Pointer auf erste Element der Stringzeichenkette verhält.

In **Zeile 12** wird die Funktion sub() aufgerufen, welches erst zur Laufzeit implizit deklariert wird, da sich werde ein Funktionsprototyp von sub() noch eine vollständigte definition und deklaration oberhalb von main() befindet.

Die sub() Funktion erwartet als Input Param ein Datentyp von Typ S, welches aber vorher in Main nicht erstellt wurde. Da Typ S intern ein Pointer auf ein Wrapper mit einem Array der Größe 64 ist, versucht der Compiler den Input parameter zu “erraten” und gibt als Parameter einen Pointer zum vermeintlichen Wrapper S, der den text[] Array aus der Main() umwickelt.

In **Zeile 29** entsteht das Problem.
strcpy() erwartet als destination param einen Pointer an das Ziel String Array (call by reference), dabei wird nicht geprüft ob das Ziel Array überhaupt Platz für den zu kopierenden String hat.
Als Pointer bekommt die strcpy() in Zeile 29 den Pointer an das vermeintliche char[64] Array vom Datentyp S und kopiert den Ziel String dort rein. Hierbei wird der ursprüngliche Inhalt von text[] überschrieben, da sich text[] innerhalb von c[64] befindet.

Nachdem in **Zeile 12** die Funktion sub() ausgeführt wurde, wird der Stack für die vermeintliche Datenstruktur S freigegeben und da S nicht per Referenz referenziert wurde und somit der c[64] Array weg ist, wird erwartet, dass die variable text[] welches noch im Scope der Main Funktion existiert weiterhin den Wert „HALLO WELT!\0“ hat.

Dies ist allerdings nicht der Fall, da über die gegebene Referenz von c[64] wo sich der Pointer zu text[] befand ebenfalls per Referenz via strcpy() überschrieben wurde.

In **Zeile 13** wird dann der Inhalt der text[] variable geprinted und als Output wird “dolor sit amet, consetetur sadipscing elitr, sed di” gedruckt. Da die Größe von text[] erst zur Laufzeit festeht, wird die größe vom ursprüngliche Wert von text[] durch strcpy() erweitert. „Lorem ipsum “ ist nicht teil von text[], da der Scope des Char Arrays in main() bei 0x7ffee4e1110c anfängt. Da der Stack von sub() Frame freigegeben wurde, ist nicht zu erwarten, dass die Zeiger vor 0x7ffee4e1110 noch die Werte „Lorem ipsum “ enthalten.