

Blatt 4

Aufgabe 1

(1) `returnValue fctName(arg1,... ,argN)`
 `returnValue` : Datentyp der Rückgabe
 `fctName` : Funktionsname zum aufrufen
 `arg1 - argN` : Argumente mit festen Datentypen welche beim
 Aufruf der Funktion mit übergeben werden müssen

```
int funk(int x, char y)
    returnValue : int
    fctName     : funk
    arg1 - argN : (int , char) in genau dieser Reihenfolge
```

Source: <http://www.lab4inf.fh-muenster.de/lab4inf/docs/Prog-in-C/04-Funktionen.pdf> Folie 5

```
(2) int main(){
    int (*fptr) (int, char);
    fptr = &funk;
    printf("Adr von func: %p\n", fptr); return 0;
}
```

(3)

(4)

Aufgabe 2

`gets()` schreibt ALLES was sie bekommt in den übergebenen Buffer, auch darüber hinaus, wenn die Eingabe größer ist als der Buffer.

Hier liegt der Buffer im Speicher vor den drei Funktionen. Heißt man kann diese überschreiben, indem man den `buf[32]` voll spammt, wobei der erste Buchstabe ein "J" sein muss, damit die Funktion auch ausgeführt wird!

"Jdhhdhdhdhdhdhdhdhdhdhdhdhdhdhd" Füllt `buf[32]` komplet

Nun muss man noch die ersten beiden Funktionen so überschreiben, dass sie nicht ausgeführt werden.

Da man selber entscheidet welche Funktion ausgeführt wird ist es man einfachsten die erste zu nehmen und dort die Adresse der Funktion 3 hinein zu schreiben. Oder `0x0000 0000 FF10` bis `0x0000 0000 FF20` mit "0" zu überschreiben. (?)