Уязвимости форматных строк

Форматные строки

printf(“Hello %s\n”, world);

Код	Формат
%d	Десятичное целое число со знаком
%u	Десятичное целое число без знака
%x	Шестнадцатеричное число без знака (строчные буквы)
%s	Строка символов
%n	**Указатель на целочисленную переменную. Спецификатор вызывает присвоение этой целочисленной переменной количества символов, выведенных перед ним**

Right way

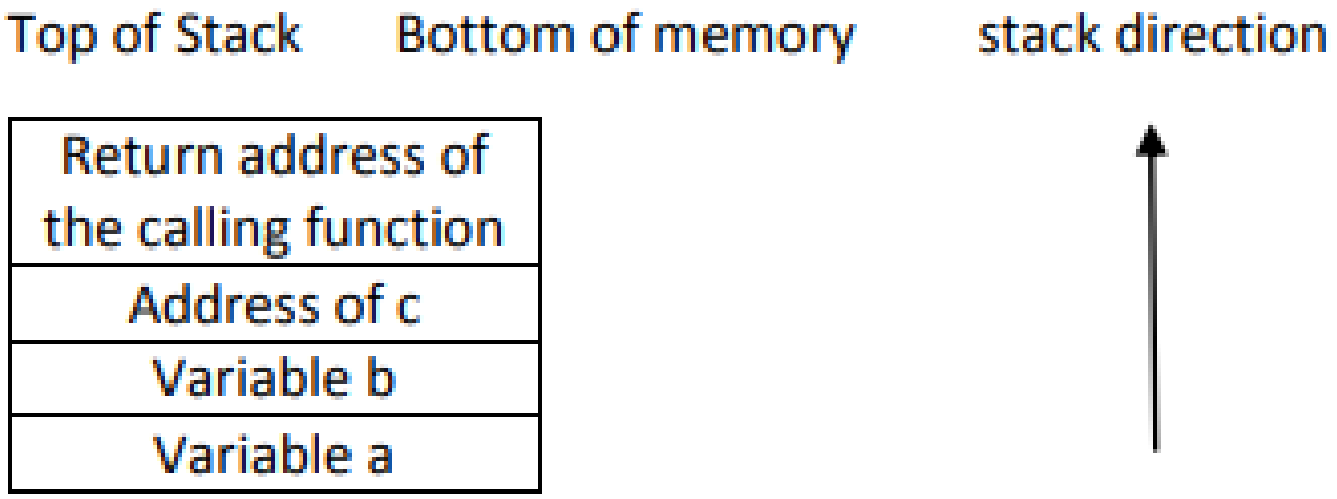
```
#include <stdio.h>
int main(int argc, char *argv[])
{
	char* i = argv[1];
	printf("You wrote: %s\n", i);
	return 0;
}
```

Wrong way

```
#include <stdio.h>
#include <string.h>
int main(int argc, char *argv[])
{
        char test[1024];
        strcpy(test,argv[1]);
        printf("You wrote:");
        printf(test);
        printf("\n");
        return 0;
}
```

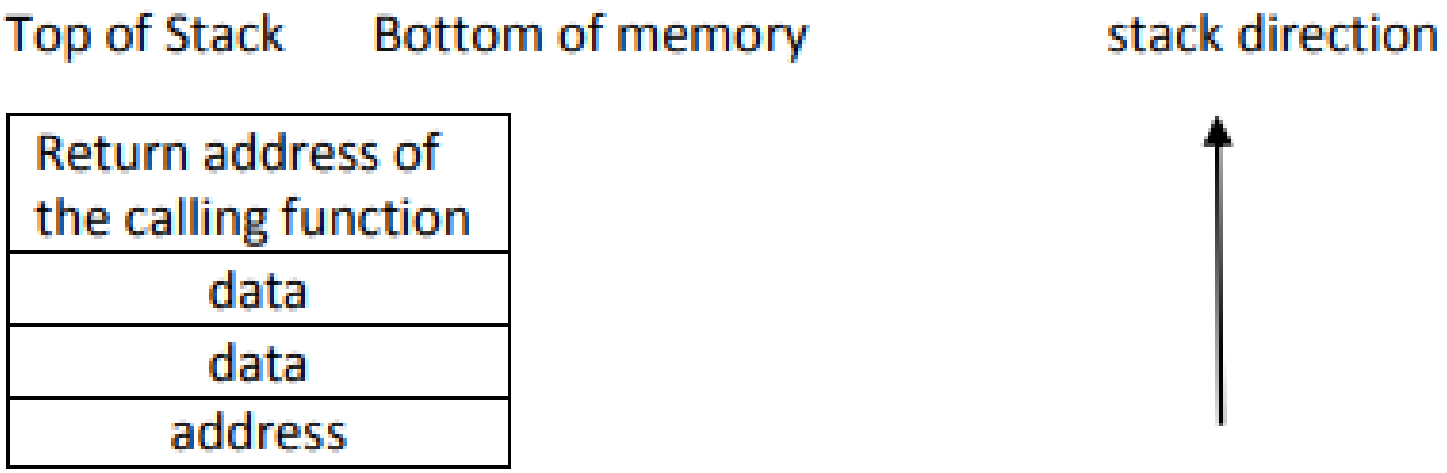
Что пошло не так?

printf("this is a %s, with a number %d, and address %08x",a,b,&c);



Что пошло не так?

printf("this is a %s, with a number %d, and address %08x",a,b,&c);



Уязвимые функции

- Printf
- sprintf
- Fprintf
- vsnprintf
- Sprint
- vfprintf
- Snprintf
- vprint
- syslog
- …….

Старый и неактуальный баг?

Date ▾	D	A	V	Title	Platform	Author
2018-02-05	⬇	-	⏱	Claymore Dual GPU Miner 10.5 - Format String	Multiple	res1n
2017-12-14	⬇	-	⏱	Multiple OEM - 'nsd' Remote Stack Format String (PoC)	Multiple	bashis
2016-07-19	⬇	-	⏱	Axis Communications MPQT/PACS 5.20.x - Server-Side Include Daemon Remote Format String	Multiple	bashis
2016-04-01	⬇	-	⏱	PHP 5.5.33/7.0.4 - SNMP Format String	Multiple	Andrew Kramer
2015-12-23	⬇	-	⏱	PHP 7.0.0 - Format String	Multiple	Andrew Kramer
2015-05-28	⬇	-	⏱	Peercast < 0.1211 - Format String	Windows	GulfTech...