University of BRISTOL

Format String Vulnerability

Sanjay Rawat

bristol.ac.uk

Format String function

- Formatted output functions consist of a format string and a variable number of arguments (corresponding to each specifier).
- Format strings are character sequences consisting of *ordinary characters* (excluding %) and *conversion specifications (%)*.
- Conversion specifications convert arguments according to a corresponding conversion specifier, and write the results to the output stream.
- Conversion specifications begin with a percent sign (%) and are interpreted from left to right.

Example functions

- `vfprintf()`
- `vprintf()`
- `vsprintf()`
- `vsnprintf()`

- `fprintf()`
- `printf()`
- `sprintf()`
- `snprintf()`

Format strings bug

Format strings bug

- So, format string is one of the arguments, followed by other optional arguments.

Format strings bug

- So, format string is one of the arguments, followed by other optional arguments.
- If there are more arguments than conversion specifications, the extra arguments are ignored.

Format strings bug

- So, format string is one of the arguments, followed by other optional arguments.
- If there are more arguments than conversion specifications, the extra arguments are ignored.

- If there are not enough arguments for all the conversion specifications, the results are undefined.

Example code

```
#include <stdio.h>
int main(int argc, char **argv)
{
    int i=0xAABBCCDD;
    if(argc>1)
        printf(argv[1]);
    return 0;
}
```

Example code

```
#include <stdio.h>
int main(int argc, char **argv)
{
    int i=0xAABBCCDD;
    if(argc>1)
        printf(argv[1]);
    return 0;
}
```

Run it as:
./ex %x%x%x%x%x%x%p%p

Another Example to try at home

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

int pin=12345;

int check(int upin, int spin)
{
    if (2*upin == spin)
        return 1;
    else return -1;
}
int main(int argc, char *argv[])
{
    char welcome[50];
    char name[40];
    int upin,auth;
    printf("Enter you name followed by your pin:\n");
    scanf("%39s%d",name, &upin);
    sprintf(welcome,"Hello %s",name);

    auth=check(upin,pin);
    printf(welcome);
    if(auth==-1)
    {
        printf("Sorry, try again...\n");
        exit(0);
    }
    return 0;
}
```