Homework Software Security 2023
Name:

This homework is due by Wednesday, December 23rd, 2023 23:59:59.

Please send your solutions by email to:
alessandra.gorla@imdea.org

The email should include a PDF file with the responses, including screenshots for the buffer overflow question. No collaboration is permitted on this assignment. Any cheating (e.g., submitting another person's work as your own, or permitting your work to be copied) will automatically result in a failing grade.

Buffer Overflow __ / 5 points

You will need access to a machine with the gcc compiler installed. This could be your own Linux machine, a Cygwin installation on Windows or a Virtual machine. If you want to install a linux virtual machine, consider installing virtualbox https://www.virtualbox.org/ or vmware https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html and get a ready-to-use linux image from here: https://www.osboxes.org/ubuntu/

(1) Examine the code below.
How can the code print the “Welcome admin” string? (1 point)

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

int main(int argc, char** argv)
{
    volatile int authenticated;
    char buffer[64];

    authenticated = 0;
    gets(buffer);

    if (authenticated != 0) {
        printf("Welcome admin\n");
    }
    else {
        printf("Permission denied...\n");
    }
}
```

(2) Save the below code into a file called overflow.c

Compile the modified code using:

gcc overflow.c -o overflow

Run the modified compiled code (i.e. **./overflow** in the terminal) and provide the output. (0.5 points)

Can the compiled code print the “Welcome admin” string? Explain why (0.5 point)

(4) Re-compile your modified code using

gcc overflow.c -o overflow -fno-stack-protector

Can the compiled code print the “Welcome admin” string? Explain why (0.5 points)
What is the minimum input length that produces an overflow? Explain why (0.5 points)
Provide an input string that prints “Welcome admin” as a result. (1 point)

Provide screenshots of each step of the exercise

(5) Name and briefly explain at least two techniques that help prevent this kind of attack to work (1 point)

Taint analysis __ / 3 points

Given the following code, would taint analysis raise a warning? Motivate your answer discussing the difference between *static and dynamic taint analysis.* Consider only **explicit** information flows.

```
x = Source();
y = x + 1;
z = 0;
while(y > 1)      {
    y = y-1;
    z = x+1;
}
Sink(z);
```

Answer:

Web vulnerabilities __ / 2 points

```
<?php
    $ip_address = $_GET[ 'ip' ];
    $cmd = exec( "ping $ip_address" );
    ….
?>
```

Given the above PHP code snippet describe the vulnerability and show how an attacker can exploit it.

Answer: