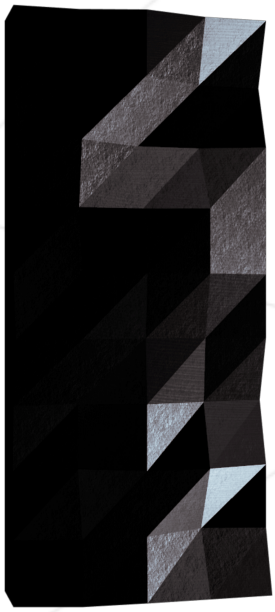

Discovery Piscine

Cell 2 - 2 - Gecko

Summary: Encodings can be reverted. This makes it not quite secure to send sensitive data, or even store it, and here is where hashes come to help. On this cell you will have to find why do they work and how to break them

Version: 1.0

Contents

Chapter I

A word about this Discovery Pool

Welcome !

You will begin the first cell of this discovery pool of computer programming. We want to both show you what the code is that makes up the software you use every day, and at the same time experience peer-learning, an educational model of 42.

Programming involves logic (not math). It provides you with elementary bricks, which you assemble as you wish. There is never THE solution to a problem. There will be your solution, there will be those of each of your neighbors. Slow or fast, ugly or beautiful, if that gets the job done, that's all it takes! This assembly of bricks will constitute a series of orders (calculation, display, ...) that the computer will perform, in the order you have chosen.

Rather than giving you a course with only one solution for each problem, and which will probably be outdated in a few years, we have chosen to put you in a peer-learning situation. You are going to look for the elements that could serve you for your challenge, sort out those that are actually interesting by testing and manipulating them, and create your own program. To do this, discuss with others, exchange your points of view, find new ideas together, and finally test for yourself even to convince you that it works.

Peer-evaluation is a key moment to discover other ways of doing things, as well as special cases that you have not thought of and that could undermine your program (think about your degree of nervousness with software which crashes). Like different clients who don't pay attention to the same things, each reviewer will be different from the last. And who knows, you might have made new acquaintances for later collaborations.

At the end of this pool, you will not have done the same things as the other participants, you will not have validated the same projects, you will have chosen to do one challenge rather than another ... .and that's normal! It's both a collective and a personal experience. Everyone will benefit from what he or she experiences during this time.

Good luck to all, we hope you will like this discovery.

Chapter II

Introduction

What this cell will make you see :

- Learn to understand and detect a well-known cipher.

Chapter III

General instructions

Unless explicitely specified, the following rules will apply every day of this Piscine.

- This subject is the one and only trustable source. Don't trust any rumor.
- This subject can be updated up to one hour before the turn-in deadline.
- The assignments in a subject must be done in the given order. Later assignments won't be rated unless all the previous ones are perfectly executed.
- Be careful about the access rights of your files and folders.
- Your assignments will be evaluated by your Piscine peers.
- All shell assignments must run using `/bin/bash`.
- You must not leave in your turn-in your workspace any file other than the ones explicitly requested By the assignments.
- You have a question? Ask your left neighbor. Otherwise, try your luck with your right neighbor.
- Every technical answer you might need is available in the `man` or on the Internet.
- Remember to use the Slack workspace dedicated to your piscine!
- You must read the examples thoroughly. They can reveal requirements that are not obvious in the assignment's description.
- By Thor, by Odin! Use your brain!!!

Chapter IV

Common Instructions

- The use of automated tools is forbidden unless specified on the exercise subject
- If no other format is specified, the flag format will be 42BCN{this_is_a_test_flag}
- Peer evaluations will evaluate your understanding on how to solve each challenge, so you must be able to clearly explain all of what you did, and your peer must be able to understand your explanation.
- Exercises within this project have a strict order and you will not be able to do further exercises if you did not complete the previous ones (e.g: You can't do exercise 3 without having exercise 2 done)

Chapter V

Exercise 2: Basic

	Exercise : 02
Exercise 2: Basic	
Turn-in directory : $ex02/$	
Files to turn in : `flag.txt`	
Forbidden functions : `None`	

On this cell, you are not dealing with encodings but with hashes.

Unlike encodings, hashes can not be reverted.

The only way to know the text hashed is to actually find a text that hashes to the same. You might want to investigate that to solve this challenge.

You must hand in the text hashed. Be aware that you will have to put it in the flag format. For example, if the hashed text was "barcelona" you will have to hand in 42BCN{barcelona}

Hash:

```
629cf0d815ccb448a2c7a4d3d9cc3989
```

`hashcat`

Your task is to crack the content of this string. When you have succeeded, you must write it into a flag.txt file.

You will need to submit the `flag.txt` on the correct folder and go through your peers.

Chapter VI

Submission and peer-evaluation

- Create a `cybersec_discovery` folder at the root of your home, and move around in it.
- Create a new `cell02` folder and navigate to it.
- From now on, all exercises should be in the correct folder rendering. Exercise 00 in the `ex00` folder, Exercise 01 in the `ex01` folder, etc ... you get the logic.

`Please note, during your defense anything that is not present in the folder for the day will not be checked.`