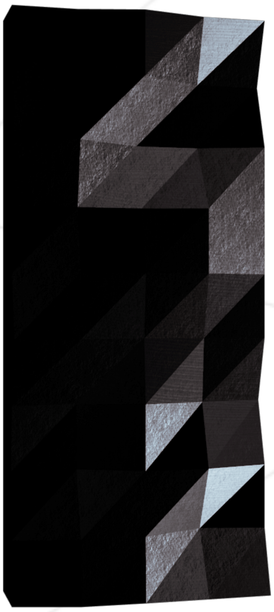

Cybersecurity Discovery Piscine

Gecko 02

by @alrodri2

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: 2.00

Contents

Chapter I

About this Cybersecurity Discovery Piscine

Welcome!

Welcome to this Discovery Piscine in cybersecurity, a challenge where you will dive into the basics of offensive cybersecurity while experiencing the unique educational model of 42. Here, you won't find traditional classes or a single correct solution; learning is collaborative, hands-on, and focused on you.

We invite you to explore the code that powers the software you use every day, while developing skills that go beyond the technical: logical thinking, problem-solving, and self-directed learning. Programming isn't about memorizing rules; it's about creatively assembling blocks to solve problems in your own unique way.

During this experience, you'll tackle key topics in cybersecurity:

- Terminal navigation: Learn to operate and navigate a system using basic commands.
- OSINT (Open Source Intelligence): Discover how to gather public information to identify potential threats.
- Web security: Understand common vulnerabilities in websites and how they are exploited.
- Cryptography: Familiarize yourself with the fundamentals of data and communication protection.

Peer learning and evaluation will play a central role in your journey. You'll exchange ideas, discuss solutions, and gain new perspectives by collaborating with your peers. This will not only enrich your learning experience but also help you build connections and develop critical skills for tackling future challenges.

Remember, this experience is as unique as you are: each participant will follow their own path, validate different projects, and face unique challenges. What truly matters is what you learn, from both your successes and your mistakes.

Good luck! We hope you enjoy this journey into the world of cybersecurity and collaborative learning.

Chapter II

Introduction

Cryptography lies at the core of data protection and communication in the digital world. While often perceived as a field reserved for mathematicians and security experts, many of the techniques it encompasses are tools we use (and depend on) every day—whether to protect our passwords, send encrypted messages, or verify the integrity of a file.

Understanding the basic principles of cryptography will not only help you better protect your information but also recognize the weaknesses of poorly implemented systems. From hashes and encodings to more complex encryptions, this module will teach you how these techniques are used in the real world and how, if not properly applied, they can be exploited.

Hashes are another common concept in cryptography. Once something is hashed, its original content cannot be determined, as hash functions are non-reversible. The only way to verify a hash is to hash the same input and compare the results. Hashes are primarily used to store passwords securely, verify data integrity, and more. In this exercise, you'll use brute force and a list of common passwords to crack a hash.

What you'll learn in this exercise:

- How hashing works and its primary use cases.
- Brute force techniques for cracking hashes.
- The importance of strong password policies to resist brute force attacks.

Chapter III

General instructions

Unless explicitely specified, the following rules will apply on every cell of this Discovery Piscine.

- This subject is the one and only trustable source. Don't trust any rumor.
- 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 read the examples thoroughly. They can reveal requirements that are not obvious in the assignment's description.
- You have a question? Ask your neighbor on the left. Otherwise, try your luck with your neighbor on the right.
- Every technical answer you might need is available in the `man` or on the Internet.
- Remember to read the documentation and to use Slack!
- By Thor, by Odin! Use your brain!!!

Chapter IV

Exercise 02

	Exercise : 02
Basic	
Turn-in directory : *ex*02/	
Files to turn in : `flag.txt`	
Forbidden functions : `None`	

On this excercise, you are not dealing with encodings but with hashes. Do you know already the difference?
Once again, we are giving you a text and you will have to find out the flag, which is the text that serve as a base to create the following:

```
629cf0d815ccb448a2c7a4d3d9cc3989
```

Got it? You have to unhash this text, except that I have just invented the verb and the notion of "unhashing" hehehe ;)

`hashcat`

Chapter V

Submission and peer-evaluation

- Have you found the flag? When you have succeeded, you must write it into a `flag.txt` file.
- The `flag.txt` file should be located at `/gecko/ex02`.

`Please note that during the evaluation, what we want to verify is that you have understood the excercise. You should be able to explain it and justify the decisions you made.`