



Cybersecurity Discovery Piscine

Gecko 03

by @alrodri2

Summary: You will see that not all passwords can be found that easy on a pre-build wordlist. On this cell you will learn how to create your own wordlists based on a base wordlist.

Version: 2.00

Contents

I	About this Cybersecurity Discovery Piscine	2
II	Introduction	3
III	General instructions	4
IV	Exercise 03	5
V	Submission and peer-evaluation	6

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.

Building on the previous exercise, you'll once again use brute force to break a hash. This time, you'll work with a provided list of potential passwords, putting your skills to the test as you analyze and crack the hash efficiently.

What you'll learn in this exercise:

- Advanced brute force techniques for hash cracking.
- How to use password lists effectively.
- Practical experience in analyzing and breaking hash-based systems.

Chapter III


General instructions

Unless explicitly 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 03

	Exercise : 03
	Hard
Turn-in directory : <i>ex03/</i>	
Files to turn in : flag.txt	
Forbidden functions : None	

Thanks to the security team of 42 once again, we found some words that could potentially be part of the hash that stores the password we are looking for. Your goal is to break that hash and get the clear-text password.

The flag is the unhashed text, but you already know that unhashing does not work. Hash:

c967d488512ab5559b446f97843de1be0d615088



You MUST use John the ripper.

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/ex03`.



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