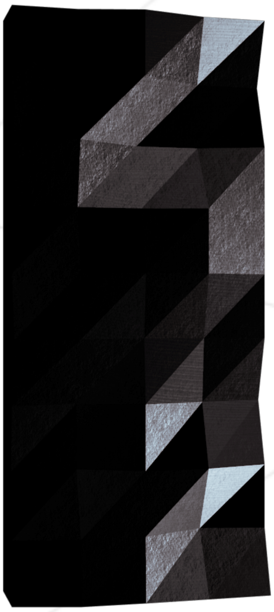

Cybersecurity Discovery Piscine

Weasel 01

by @alrodri2

Summary: This time you will learn to use a really useful tool for website security testing and information gathering. Will you be able to find the hidden directory?

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

When you visit a webpage, it's easy to assume that everything is visible at first glance, functioning securely and reliably. However, behind every button, form, and route lies a complex structure of code and configurations that, if not properly managed, can become entry points for attackers.

Web security isn't just about protecting information; it's about understanding how users interact with a page, how data is processed, and what vulnerabilities might arise. Learning to identify and exploit errors in web applications will allow you to see the digital world from a new perspective, preparing you to design safer and more resilient systems.

In many web applications, not all routes have a visible link or button exposing them. Some systems, such as content management platforms, include specific routes for administration or debugging that can only be accessed by knowing their exact address. This exercise will teach you how to perform brute force enumeration to find these routes and assess their security.

What you'll learn in this exercise:

- Techniques for enumerating routes in web applications.
- Using tools to detect undocumented routes.
- Identifying insecure configurations in content management systems.

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 01

	Exercise : 01
Fizzbuzz	
Turn-in directory : *ex*01/	
Files to turn in : `flag.txt`	
Forbidden functions : `None`	

Here is the URL of the website you are going to exploit: `http://cybersec.[campus].[tld.]:3318`.
This website has a hidden directory, are you be able to find it?

`Fuzzing.`

`The goal of the exercise is to discover the vulnerability, not the URL. If it doesn't work, ask the campus staff for the correct URL.`

Chapter V

Submission and peer-evaluation

- Have you found the flag.txt file?
- Once you have it you should place it at `/weasel/ex01`.

```
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.
```