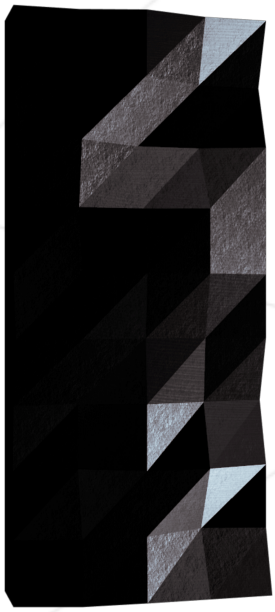

Immersion Cybersecurity (CTF)

Day 01: Weasel - Cell 04

Summary: This cell will introduce you to website misconfigurations that can lead to file exposure.

Version: 1.0

Contents

Chapter I

Introduction

What this cell will make you see :

- Learn basic web security.

Chapter II

General instructions

Unless explicitely specified, the following rules will apply every cell of this Immersion.

- This subject is the one and only trustworthy source. Don't trust any rumors.
- Be careful about the access rights of your files and folders.
- Your assignments will be evaluated by your Immersion peers.
- All shell assignments must run using /bin/bash.
- You must not leave in your turn-in your remote repository any files other than the ones explicitly requested by the exercise.
- 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 pages or on the Internet.
- Remember to use the Discord server dedicated to your Immersion.
- You must read the examples thoroughly. They can reveal requirements that are not obvious in the assignment's description.

Chapter III

Common Instructions

- The use of automated tools is forbidden unless specified in the subject.
- If no other format is specified, the flag format will be 42SP{this_is_a_test_flag}.
- Peer evaluations will assess your understanding of how to solve each challenge, so you must be able to clearly explain everything you did, and your peers must be able to understand your explanation.
- Exercises within this project follow a strict order, and you will not be able to proceed to further exercises if you have not completed the previous ones (e.g., You can't do cell01 without completing cell00).

Chapter IV

Cell 04

	Cell: 04
Cell 04	
Turn-in directory : `weasel-cell04/`	
Files to turn in : `flag.txt`	

In the same privileged network where Marvin captured the packets being exchanged with the social media platform server, the local IP address of your target's computer was also recorded. This information wouldn't be very significant unless we had access to the network, enabling us to interact with the IP address. Thanks to Marvin, who discreetly planted a credit card-sized computer within the same infrastructure that was analyzed, we now possess remote access to the network.

With this access, we can conduct a comprehensive network analysis and attempt to infiltrate your target. Your target's IP is 10.51.1.198, and your mission is to determine if any services are running on your target's device.

You should be able to locate the flag.

`Directory listing.`

`The use of automated tools not created by you is not allowed in this exercise.`

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

Chapter V

Submission and peer-evaluation

- Create a new 'weasel-cell04' folder and navigate to it. Place your 'flag.txt' file inside the folder and then push it.

Please note that during your evaluation, anything that is not present in the folder for the cell will not be checked.