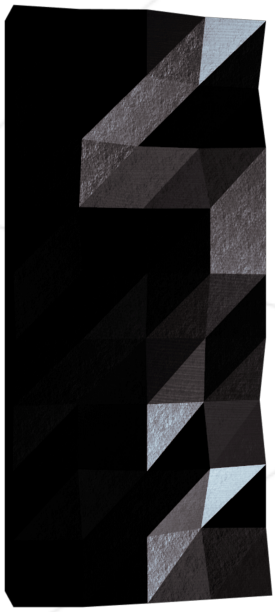

Immersion Cybersecurity (CTF)

D01: Weasel - Cell 03

Summary: This cell will introduce you to website misconfigurations that may result in data exposure.

Version: 1.0

Contents

Chapter I

Introduction

What this cell will help you understand:

- Learn the basics of 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 03

	Cell: 03
Cell 03	
Turn-in directory : `weasel-cell03/`	
Files to turn in : `flag.txt`	

One of the files that you can discover leads to an authentication page granting access to a secrets manager.

This page, even though it requires authentication to be accessed, might offer a new layer of exploration.

Your mission is to successfully authenticate with the user who can access the secrets manager and access the data within.

Here is our target address once more: 10.51.1.198.

You should be able to locate the 'flag.txt' file.

`SQL Injection.`

`man curl.`

Chapter V

Submission and peer-evaluation

- Create a new 'weasel-cell03' 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.